Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management

Alvaro Llaria, Jessye dos Santos, Guillaume Terrasson, Zina Boussaada, Christophe Merlo, Octavian Curea

energies

MDPI

Review

Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management

Alvaro Llaria *, Jessye Dos Santos, Guillaume Terrasson, Zina Boussaada, Christophe Merlo and Octavian Curea

ESTIA Institute of Technology, University Bordeaux, F-64210 Bidart, France; j.dossantos@estia.fr (J.D.S.); g.terrasson@estia.fr (G.T.); z.boussaada@estia.fr (Z.B.); c.merlo@estia.fr (C.M.); o.curea@estia.fr (O.C.)
* Correspondence: a.llaria@estia.fr

Abstract: During the last decade, the smart grid (SG) concept has started to become a reality, mainly thanks to the technical progress achieved in telecommunications, informatics and power electronics, among other domains, leading to an evolution of the traditional electrical grid into an intelligent one. Nowadays, the SG can be seen as a system of smart systems that include cyber and physical parts from different technologies that interact with each other. In this context, intelligent buildings (IBs) constitute a paradigm in which such smart systems are able to guarantee the comfort of residents while ensuring an appropriate tradeoff of energy production and consumption by means of an energy management system (EMS). These interconnected EMSs remain the objective of potential cyber-attacks, which is a major concern. Therefore, this paper conducts a survey, from a multidisciplinary point of view, of some of the main security and privacy issues related to IBs as part of the SG, including an overview of EMS, smart meters, and the main communication networks employed to connect IBs to the overall SG. Future research directions towards a security enhancement from both technical and human perspectives are also provided.

Keywords: intelligent building; cyber-security; smart grid; system of systems; cyber-physical system; energy management; communication technologies

Citation: Llaria, A.; Dos Santos, J.; Terrasson, G.; Boussaada, Z.; Merlo, C.; Curea, O. Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management. *Energies* **2021**, *14*, 2733. https://doi.org/10.3390/en14092733

Academic Editor: Jesús Lázaro

Received: 31 March 2021
Accepted: 6 May 2021
Published: 10 May 2021

1. Introduction

The theoretical concept of the smart grid (SG), proposed several years ago [1,2], has become a reality during the last decade [3], and nowadays is evolving towards new paradigms like the Internet of Energy (IoE) [4,5]. Many research works are currently being conducted in different knowledge areas to implement smart grids, highlighting their multidisciplinary nature. The benefits of SGs are well known, and they have been described in many papers; these include an increase of the overall resilience and efficiency of the electrical grid [6], introduction of renewable power sources, application of demand response and load control mechanisms, and improvement of the energy quality [7], to cite some classic examples. The need for a more flexible, reliable and protected network became evident during the year 2020, and this is still true in 2021, as a result of the impact in energy use caused by the pandemic situation [8]. On the other hand, the recent rise of cyber-physical systems (CPSs) has conferred a novel regard of the SG [9], whose structure and key elements constitute a remarkable paradigm of CPS [10]. Furthermore, SG can be seen as a cyber-physical system of systems (CPSoS), due to the diversity and complexity of its components, whose interoperability must be ensured [11]. The varied interactions among the elements inside the SG must be managed through interdisciplinary and integrated systems engineering approaches [12].

From this perspective, intelligent buildings (IBs) can be viewed as one of the key systems which compose the whole CPSoS that is the smart grid [13]. There are several essential characteristics of an IB that can be cited [14]: integration of a monitoring system

to notice its own environment, communication with occupants and with the grid, energy management capability by means of an energy management system (EMS), and self-learning ability to enhance its performance. Some of these abilities are shared with the SG, namely energy management and optimization or operation enhancement, just to name a few. This vision of IB as a subsystem of the SG can additionally be supported, since there are different technologies inherent to the SG that can be also integrated into IBs, enabling the mutual interaction between them [15]:

- Electrical microgrids (MGs) at building level or for groupings of several buildings, allowing flexibility and distributed energy generation [16];
- Virtual power plants, as a part of the SG, which employ smart metering and communication technologies [17].

Special attention must be paid to bidirectional communications, which take advantage of the cyber (software) and physical (hardware) features of the Internet of Things (IoT) [18,19]. In this context, smart meters (SMs), together with wired and wireless communication technologies are the most usual widely adopted solutions [20,21]. In addition, IBs are able to participate in the power grid energy balance, becoming grid-responsive buildings, and taking advantage of the communication network of the SG to ensure an optimal coordination [22]. This interaction of IBs with SGs as a part of them can be extended, reaching a group of buildings and even the overall city, which will become smart, too [23,24]. Since the early stages of smart grid development, it has been clear that reliability would be also a crucial requirement to be guaranteed [25]. Indeed, the application of worldwide communication technologies related to the IoT is one of the main reasons for the security problems that concern the SG. Many different incidents have been reported in the power system in the last several years, with the Stuxnet attack marking a turning point because of its virulence and the severe failures that it caused in different countries [26]. Since then, it has been clear that cyber-security must be guaranteed in intelligent power grids as a tool for increasing their resilience face to cyber-attacks [27], including all the different subsystems of the SG, such as MGs and IBs [28,29].

Taking all these elements into consideration, this paper conducts a survey, from a multidisciplinary point of view, of some of the main security and privacy issues related to IBs as part of the SG, including an overview of building energy management systems (BEMS) and the main communication networks employed to connect IBs to the overall SG. To carry out this survey, the main guideline was to adopt a global and systemic attitude in order to ensure exhaustivity and coherency when studying the different types and levels of security issues. As a consequence, we needed to first study the whole ecosystem in which physical and cyber elements of an IB and an SG can be represented as systems, by exploring the systems engineering domain. Thereafter, we were able to study the identified elements and their interactions by prospecting more detailed topics from different knowledge domains: telecommunications, informatics, electronics, and energy management. The methodology followed in order to carry out this survey then started with a literature review on the previously cited domains. The main criteria applied to this literature review were database, year of publication, and type of publication, prioritizing survey papers published in journals with Impact Factor. The main keywords to select the bibliography were cyber-physical systems, intelligent buildings, building energy management systems, communications, smart metering systems, and cyber-security, always mixed with the term smart grid. Regarding each one of the different sections of the paper, the final validation of the selected references was conducted using a top-down approach, starting from the most general concepts to the most accurate ones: SG and IBs viewed as two systems of systems (SoS) interacting together; presentation of the inherent characteristics of an IB to finally focus on the technical aspects of energy management and communication technologies; and lastly, the cyber-security concerns of communications employed in IBs that contribute to the energy management are detailed according to the OSI model, to better delimitate the proposed solutions.

As a result, the principal contributions of this work are cited as follows:

- Proposition of a perspective of IBs as an SoS, composed of cyber and physical parts, which is also a part of the SG, another SoS. This global concept is then applied to BEMS and communications to analyze the close relationship and bidirectional connection between IBs and the SG;
- Overview of the most relevant security objectives and requirements from a CPS perspective, along with a study of attacks and privacy issues concerning the communication protocols and metering infrastructure of IBs;
- Identification of different open issues, including both technical and human factors, with respect to reinforced security of the SG.

The structure of this paper is as follows. Section 2 describes the proposed vision of SG and IBs as SoS, including their respective cyber and physical infrastructures. In Section 3, two of the main inherent characteristics that make a building intelligent are studied: energy management systems and communication networks. A synthesis of several characteristics of control techniques and communications technologies is also included, to point out the main concerns affecting IB and SG security. Consequently, Section 4 carries out an exhaustive analysis of security and privacy problems and proposes several solutions for mitigating them. Perspectives for future research and security recommendations are described in Section 5, while Section 6 concludes this document.

2. From the Smart Grid to Intelligent Buildings

2.1. The Smart Grid, a System of Systems

As previously mentioned, an SG is an example of a system of systems. The work presented in [30] considers the modern energy SG as an SoS that requires interdisciplinary knowledge to be shared, considering the seven SG domains identified by [31]: bulk generation, transmission, distribution, markets (selling), operations, service provider, and customer. For [32], an SG is composed of independent systems that share goals and act jointly. According to [33], "a system of systems is an assemblage of components which individually may be regarded as systems and which possesses two additional properties: operational independence of the components and managerial independence of the components". This introduces a very interesting perspective of the SG as an SoS, composed of a set of technological subsystems, a control and set of management subsystems, and a set of communication subsystems [34]. Moreover, this definition is enhanced by [35], which defines an SG as a cyber-physical system, including a description of the "cyber infrastructure" (communications, control, measurement, i.e., control/management and communication set) and the "physical infrastructure" (i.e., the power network infrastructure [10]: power plant, transmission system, and distribution system, i.e., technological set + end users/customer premises), as shown in Figure 1.

From this perspective, the impact of different kinds of attacks on the SG can be evaluated from both cyber and physical points of view, making it possible to select the most appropriate security solution to reduce the impact in each of the two parts [36]. Several authors have applied the CPS concept to production systems (cyber-physical production system—CPPS [37]) to improve their performance and their efficiency by introducing new types of sensors [38], collecting data, and supporting decision making through big data technologies, which can be associated with the implementation of Industry 4.0 technologies [39]. In addition, cyber-physical human systems (CPHS) are able to consider human actors as resources participating in the "production" of the technological subsystems of a CPS, but also as users or decision makers in the cyber subsystems of the CPS [40,41]. Furthermore, an SG can be seen as a specific CPS, called a cyber-physical power system, composed of a physical system (power network infrastructure) and cyber systems, proposing the integration of the real and virtual worlds, dynamic communication, information processing such as big data streams, and autonomous capabilities [42].

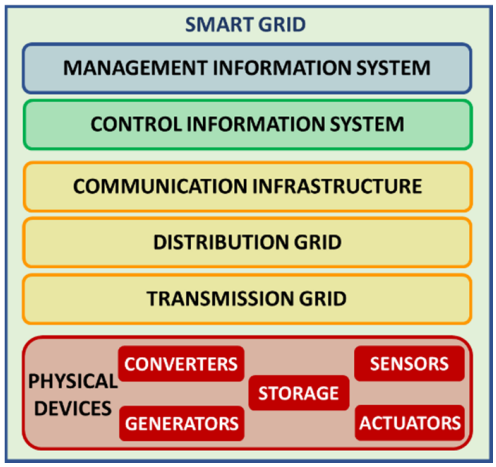

Figure 1. Global perspective of the SG as an SoS, with the physical and cyber infrastructures.

The SG can be seen as a cyber-physical system of systems (CPSoS), which also belongs to another, higher-level, multidisciplinary SoS, the smart city, contributing to its development and deployment thanks to the opportunities made possible by SGs for delivering sustainable energy [43]. In this frame, the SG constitutes an SoS that includes different elements:

- Traditional electrical system, composed of power plants, transmission grid and distribution grid;
- Customer-side system, including several elements located at the end of the distribution network, like electrical microgrids (MGs), intelligent buildings (IBs) and smart homes (SHs), and electrical vehicles (EVs);
- Communication system, which gives the SG its intelligent nature, mainly composed of communication networks and data storage and processing centers.

2.2. The Intelligent Building, a System of Systems

The first time the concept of the intelligent building appeared was in the United States during the 1980s [44]. From this starting point, IBs have evolved as another example of CPS, which is a system of the overall SG, while, at the same time, the IB constitutes an SoS in itself, composed of different types of subsystems, namely technological, economical, and human. Nowadays, IBs are in a position to be considered cyber-physical ecosystems interacting with their environment, both external (SG and other IBs) and internal (aimed towards the upgrade of their occupants' comfort) [45]. Some of the main features of IBs that can be cited include automation, multifunctionality, adaptability, interactivity, and energy efficiency, and IBs include several technologies such as control systems, renewable energy, energy storage systems, sensors and actuators, and SM [46].

We consider an SG to be both an SoS and a CPS. A CPS is a set of systems that integrates cyber components and physical components [47]. Cyber components have communication capabilities and collaborate to control and coordinate physical processes. An IB is composed of physical components that produce, store and consume energy, and cyber components that control, communicate and coordinate the physical components. We therefore consider an IB as a CPS. Incidentally, due to this conception of the CPS, an IB is also an SoS, composed of cyber and physical systems as well as, of course, physical power networks.

Other authors have proposed the concept of the "cyber power internetwork" to define the current structure of intelligent power networks [48]. Here again, on one hand, the power network is composed of a physical part, namely the power system, while, on the other hand, the cyber part includes information and communications technologies (ICT) with different components: acquisition, processing, implementation, and communication. The interdependencies between the different elements of the cyber-power system also

influence the reliability and the security of the system as a whole. Figure 2 depicts the proposed vision of SGs as a CPSoS, integrating an IB as a CPS.

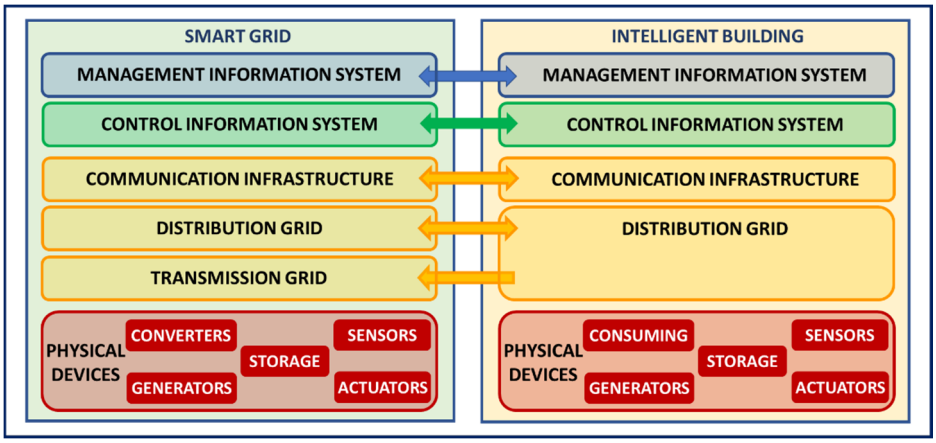

Figure 2. Global perspective of the integration of IBs and SG as SoS.

3. Main Features of Intelligent Buildings as Part of Smart Grids

The proposed perspective, which overlaps two complex systems in the form of IBs and SGs, although presented and justified from a theoretical approach, must also be supported from a technical point of view. At the beginning of this paper, some technologies inherent to SGs that can be applied to IBs are raised. However, conversely, there are several capabilities of IBs that require interaction with SGs in order to operate in a proper manner [49]:

- Smart metering, a part of the whole advanced metering infrastructure (AMI) of the SG;
- Management and control methods to guarantee the energy efficiency in the building and the power balance in the electrical grid.

This perspective of IBs as active systems of the SG, including the existing electrical and communication interactions, is schematized in Figure 3 [45,49].

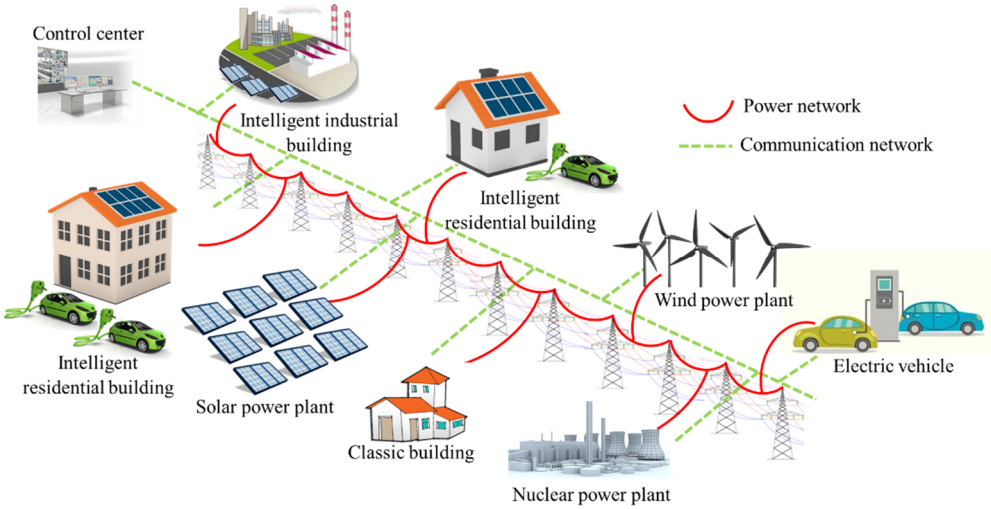

Figure 3. Intelligent buildings as systems within the whole smart grid.

Bidirectional communications, wired and wireless, allowing data transfer inside a building, but also between individual buildings and the power grid, are needed. This feature, together with energy management capabilities, constitute two inherent particularities that define the nature of IBs compared to conventional buildings, while at the same time reflecting the integration of IBs in the SG [50]. Thus, in the following subsections, the

focus will be placed on energy management systems as the core of IBs, along with the most relevant communication technologies.

3.1. Energy Management in Intelligent Buildings

Recent studies have highlighted that buildings are responsible for around 40% of total energy use [51], and the lockdowns imposed to address the COVID-19 pandemic during 2020 also had a non-negligible impact, increasing the residential energy demand by between 11% and 32% [52]. Consequently, IBs are regarded as being the main actors in the context of aiming for more responsible use of energy, while at the same time ensuring a tradeoff between energy efficiency and indoor environmental quality in order to guarantee the comfort of building occupants [53]. The application of appropriate energy management in buildings is interesting both from an ecological and a pecuniary perspective, thanks to the energy savings that it provides, which can reach a yearly augmentation varying between 11.39% and 16.22%, according to the study conducted in [54]. Considering the relevance of these results, the essential aspects of energy management systems are presented next.

3.1.1. Building Energy Management System Architecture

At present, modern buildings, as they are SoS, include a great variety of heterogeneous systems and devices, ranging from classical appliances like lighting, hot water or heating ventilation and air conditioning (HVAC) to more recent ones such as renewable energy generation, electrical vehicles and intelligent storage systems. Therefore, in order to achieve a coordinated and tuned operation of all these elements inside a building in an interactive and automatic way, integrated complex algorithms called building energy management systems (BEMS) need to be applied [55]. BEMS are heavily based on building automation systems (BAS), the CPS nature of which is accentuated, since they are composed of HW and SW parts, as explained in [56]. The conceptual architecture of a BEMS is presented in Figure 4 from a twofold point of view: control layers, and cyber and physical parts, including the interaction with the SG.

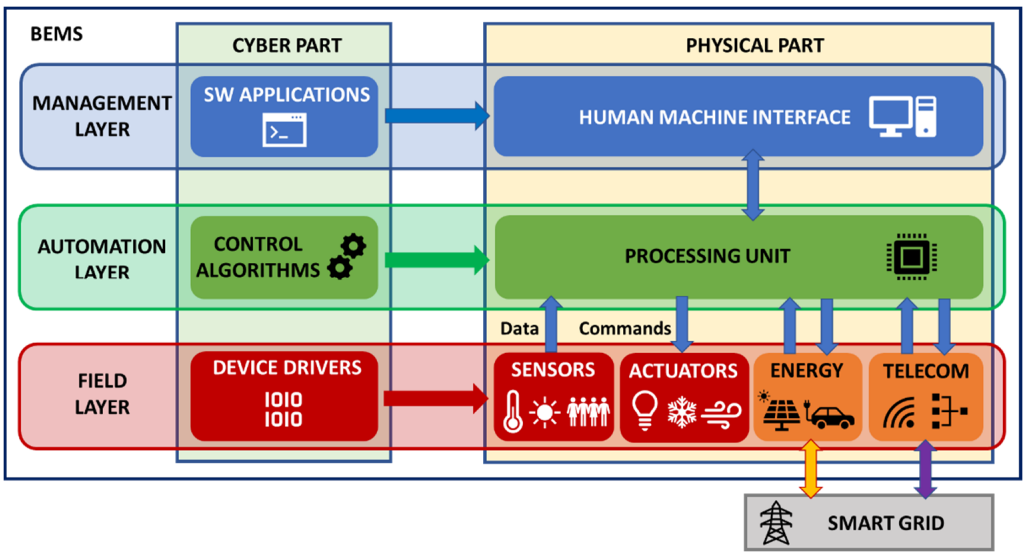

Figure 4. BEMS conceptual architecture.

Several types of sensing technologies are employed to gather the data needed for the optimal energy management of the building [57], alongside the functionality of interaction both with the SG and with other BEMS by means of wired and wireless communication technologies. When the BEMS includes bidirectional transmission of data and power between the IB and the SG, it can be considered to be an integrant part of the IoE. An exhaustive review is performed in [58], analyzing the opportunities provided by the key technologies of the IoE for the maximization of the energy efficiency in buildings. As will

be presented later, this twofold exchange is based on the IoT and a number of different control mechanisms, and it is mandatory for ensuring the power balance of buildings when integrating local distributed generation. Accordingly, the concepts of the zero energy building (ZEB) and the net-zero energy building (NZEB) have emerged over the last few years [59]. A ZEB adds renewable energy generation to the "green building" principle, resulting in a building capable of balancing its own energy generation and consumption. Two kinds of ZEB can be defined, depending on their connection to the grid [60]: autonomous/standalone ZEB, which is not connected to the grid, and NZEB, which is in turn connected to the electrical grid. Thus, the NZEB is able to balance the energy interacting with the SG in a bidirectional transfer of power. A review of recent advancements in the NZEB field was performed in [61]. A future approach is represented by positive energy buildings (PEB), which will produce more energy than they require for their operation, making it possible for them to supply other buildings connected in the surrounding area [62].

In the same way, many efforts have been carried out in recent years concerning the development of home energy management systems (HEMS) [63], which can be considered a particular case of BEMS. The final purpose of HEMS is the same—the reduction of energy consumption—but the requirements for achieving this objective are slightly different from BEMS. Certainly, ensuring the development of low-cost IoT-based solutions compatible with existing gadgets that are affordable for the general public is one of the main goals of HEMS, in contrast to BEMS, which focuses on industrial or office buildings, where the most important goal is to assure a high level of reliability. The basic architecture of an energy management system of a NZEB is shown in Figure 5.

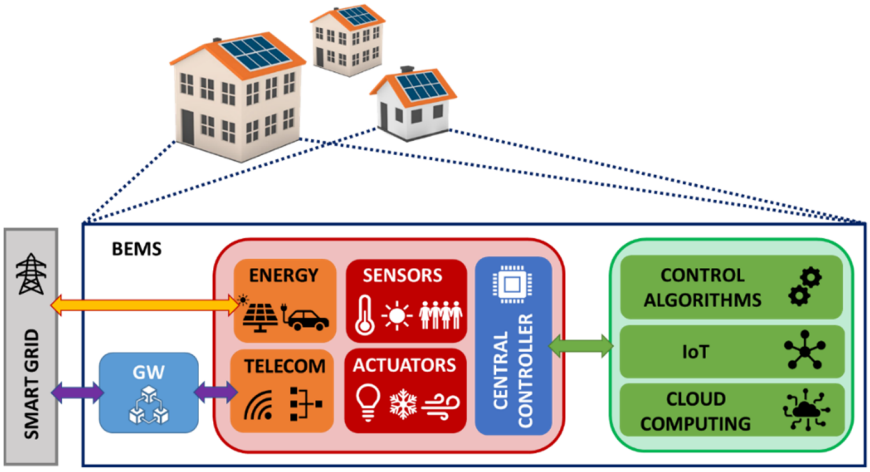

Figure 5. General architecture of a BEMS of a NZEB.

As can be seen, on one hand, the global system consists of a physical part, including sensing and measuring devices, smart appliances and actuators, local renewable energy generation, energy storage devices, communication facilities, a gateway (GW) to allow the interconnection with other IBs and the SG, and a central processing unit [64]. On the other hand, there is also a cyber part, comprising the different computing solutions, which are based on the IoT, edge computing (EC), and cloud computing [65]. Last but not the least, the energy management system must adequately cope with occupant behavior in order to be really accepted by building users [66,67].

A crucial requirement for the correct operation of the whole power grid is to ensure the balance between energy demand and supply. Traditionally, this task was only carried out by power plants, that is, on the generation side. The emergence of new actors in the SG such as distributed energy resources, electrical vehicles, and energy storage systems, often as part of a greater whole such as an IB, is changing this typical top-down operation, since generation is now placed at the distribution and demand level, close to the final

consumers. In this context, the emergence of BEMS and HEMS and their associated intelligence, combined with their ability to communicate with the grid, has boosted the materialization of demand-side management (DSM) programs [68], which constitute a typical example of bidirectional interaction between IBs and the SG. DSM tries to achieve energy efficiency in households and buildings by means of consumption shifting, the goal of which is to push the energy use towards valley periods. This approach is more popular in residential buildings, since users are able to choose the manner in which they use their energy, and when to use it [69].

Among the different already-existing DSM solutions, demand response (DR) is considered one of the most suitable options for providing electricity flexibility to IBs interacting with the grid, because of the possibility of load shifting, including renewable energies, at an affordable price, as was described in the comprehensive survey conducted in [70]. The main DR strategies can be classified into two categories [71]: price-based, which is centered on changes in the grid price, and incentive-based, which encourages customers to shift their consumption to outside peak hours by providing discounts in the billed amount, or even allowing the grid operator to turn off/on several customer loads to match energy consumption and generation. The nature of the load (uncontrollable, curtailable, uninterruptible, interruptible, regulating and energy storage) is also considered by the BEMS to decide how to proceed, from simple scheduling to complete load disconnection [72]. Moreover, the DR program can also be combined with smart energy storage devices to use the stored energy during peak hours instead of using energy from the grid, leading to a price reduction of up to 18% [73].

Load-side energy management strategies can be also applied for groups of buildings at the distribution grid level. In this case, the main risk is the lack of coordination between the set of buildings and the SG when applying this management strategy, leading to a reduction in efficiency and, worse, to a stress situation for the distribution system. To ameliorate these sorts of problems, [74] proposed an operation framework for load aggregation and disaggregation involving three types of intelligent entities: the system operator at the transmission level, the distribution system operator, and, finally, the BEMS for load scheduling. Another approach was implemented in [75] to manage the energy of a cluster of buildings, including photovoltaic generation. This solution was based on load scheduling (hybrid heat and power), and two types of DR were applied: increase of power consumption and reduction of heat generation, and vice versa, depending on the PV generation level.

3.1.2. Making the Energy Management Systems More Intelligent

- General management methods

Data gathered using sensing devices are processed by the central platform, which can employ different control schemes in order to find the right decision. These control schemes, which can be defined as general purpose management strategies, can be classified as either conventional or intelligent [76]. Conventional controllers, a category that includes basic types such as on/off switching, PID controllers and predictive and adaptive methods, are mainly oriented towards guaranteeing energy savings, without taking into account the comfort of the occupants of the building. To override this limitation, intelligent control schemes have been developed. As presented in [76], these control schemes mostly include model-based predictive control (MPC) and artificial intelligence (AI)-based techniques like multiagent systems (MAS) and fuzzy logic. However, the role of the MPC in energy management is often that of a DSM [77,78]. To efficiently integrate distributed generation, AI techniques must take into account both the consumer and producer sides of energy management, which has recently resulted in more promising solutions for the design of BEMS.

A BEMS was proposed in [79] for the management of heating ventilation and air conditioning in a commercial building using fuzzy logic algorithms (FLA). In [80], the authors proposed a fuzzy logic controller (FLC) for the energy management of a university

building. The BEMS was developed using Matlab/Simulink software (MathWorks, Inc., Natick, MA, USA) and aimed to make a selection or a combination from among three energy sources: the main grid, local solar PV, and a local battery. It was also able to control the charging of the battery while keeping in view the demand of loads, in addition to providing energy to the main grid in the case of excess power. Also using Matlab/Simulink, a FLC for a residential building was designed in [81]. A recent work using FLA proposed a solution for processing the environmental data to advise building users with the aim of achieving minimum energy consumption [82].

Considering the distributed nature of an MAS, this technique is prevalent in the management of complex systems in general, and in the energy management of SGs in particular [83,84]. The work conducted in [85] studied several MAS dedicated to power engineering applications, as did that presented in [86], whereas [87] proposed two solutions for the supervision and analysis of a large quantity of data from a multisource electric network. An MAS for controlling production units, storage equipment and charges, based on Matlab/Simulink, was developed in [88]. Other works have defined an MAS as a set of several agents interacting with each other or with their environment [89]. The interest in the MAS is due to its agent properties and abilities. An agent is defined as a software or hardware entity, autonomous, i.e., able to interact with its environment and to make decisions with respect to its own strategies using artificial intelligence techniques such as machine learning (ML) and deep learning (DL) [90]. Depending on the level of autonomy and intelligence of an agent, different types are possible. For example, [91] studied a MAS for managing the energy consumption of a microgrid and classified agents as follows:

- Reactive agents, with a stimulus–response behavior based on sending and receiving messages;
- Cognitive agents, with a high level of intelligence and autonomy. These agents can memorize their history and develop a learning ability by adopting ML behavior. An example of an MAS with a "learning" phase for better managing a large and complex microgrid was proposed in [92];
- Hybrid agents, offering combined behavior: reactive with respect to some properties and cognitive with respect to other properties. The main properties to consider here are autonomy, cooperation, and adaptation.

To conclude, MAS dedicated to the management of IBs strengthen BEMSs and help human people manage their warmth by supporting energy consumption optimization. Table 1 provides an overview of the energy management methods cited in this paragraph, including their most important features or weakness.

Table 1. Active energy management methods for buildings.

Energy Management Method Classification	Energy Management Method	Kind of Building	Observation
Conventional Methods	On/Off switching	Nonresidential	Based on classic rules algorithms
	PID controllers		Can be software implemented or use an external device
	Predictive and adaptive methods		
Intelligent Methods	Model predictive control	Nonresidential	Often used for DSM
	Fuzzy logic	Nonresidential & residential	Supports cloud or edge computing
	Multi Agent System	Nonresidential & residential	Distributed nature Supports cloud or edge computing Supports learning ability

- Contribution of computing tools in intelligent energy management

Several intelligent energy management methods, in particular AI techniques, are benefiting from the development of other AI techniques such as ML and DL, as well as other new technologies such as big data, IoT, and cloud computing.

In this way, the FLC proposed in [93] aimed to design a BEMS using cloud computing. The FLC was integrated into a cloud service, providing the BEMS with the following features: automation, and intelligent monitoring services, through both the web and through smartphones. Cloud computing accelerates and facilitates the deployment of BEMS, since it allows data processing in the cloud. A more recent concept than cloud computing, edge computing (EC), which consists of data processing performed close to the IoT sensor or device instead in the cloud, has begun to be promoted as a suitable option for SG management. EC provides several benefits for the SG [94] that are also useful for energy management in buildings: reduction of processing latency for time-sensitive applications (load control, DR) and support for the application of cognitive solutions (data fusion, reinforcement learning), while at the same time fostering interoperability among the different elements and systems of the SG and the interactions between the SG and these systems (users, buildings, energy sources).

Deep learning techniques are a solution that is becoming more and more popular in recent years for BEMS. One interesting application is the forecasting of the energy consumption in buildings in order to implement adapted mechanisms to optimize the energy management [95]. The BEMS based on MAS have also combined some DL techniques, for making agents more adaptative and intelligent. A sailboat microgrid managed by MAS, where an agent has used a recurrent neural network (RNN) to forecast the available daily solar energy which can be converted by the photovoltaic panel installed in the boat, has been developed in [96]. Always related to the energy consumption forecasting, a solution based on convolutional neural networks (CNN) along with a long short-term memory autoencoder is implemented in [97], resulting in smaller prediction errors than other concurrent solutions for periods of 1 h and 1 day. In fact, the artificial neural networks (ANN) are among the tools used by DL to perform the artificial learning, and the two relevant types of ANNs used in DL are CNNs and RNNs.

- The Internet of Things and related computing solutions

The recent emergence of the IoT has made this paradigm one of the key components of modern BEMS and HEMS [98]. Indeed, the benefits offered by the application of the IoT in BEMS are large: a set of low-power distributed intelligent sensors for monitoring different parameters of the building (temperature, lighting, humidity, air quality), processing capability allowing the application of the aforesaid control methods, different sorts of bidirectional communication technologies, and a wide range of actuators for optimizing energy consumption following the control system instructions. A recent study concerning the use of the IoT to improve building energy management was conducted in [99], highlighting the suitability of IoT technologies for five main applications: energy consumption control, predictive control for temperature regulation, sensing of residents' comfort, integration of controllable devices, and smart home applications. In [100], an energy management system for homes, based on the IoT, was proposed. This solution incorporates an Electronic Device Sleep Scheduling Algorithm to handle the energy consumption of sensors, which is a major concern in these systems. Similarly, the IoT for a BEMS was recently applied in a commercial building, the main aim of which was to implement a DSM strategy [101]. The proposed solution included smart compact energy meters to monitor the power quality (sag, swell, transients) and the energy use, as well as communicating with the building users. For its part, the system proposed in [102] goes further, and takes advantage of the IoT and the existing BEMS of an academic building to monitor environmental conditions and their influence on the learning experience.

3.2. Communication Networks and Intelligent Buildings

To provide the previously mentioned services, including DSM and customer participation, the implementation of a bidirectional communication infrastructure constitutes a key feature of the SG. This infrastructure is essential for offering the ability to exchange data between the different entities of this SoS, including generation, distribution, substations and end user entities [103]. Therefore, IBs, to be a part of the overall AMI, need to

possess this two-way communication capability in order to provide reliable and real-time information for optimal power delivery, avoiding disturbances and outages as much as possible from the generating units to the end users.

3.2.1. Communication Technologies for Interconnecting IBs to the SG

Regarding the need for a two-way communication infrastructure, the scientific literature reveals that a large number of communication technologies are already available for interconnecting IBs to the overall SG. In [104,105], these technologies are categorized in consideration of their main communication medium: wired or wireless. From an IB point of view, this communication infrastructure needs to support two main information flows [106,107]. The first flow is dedicated, inside the IB, to gathering data from sensors and electrical appliances that are stored in data concentrators, like SM, and used to provide information to end users and to control, using actuators, their appliances. The second information flow is used to exchange data between the back-haul of the SG and the IB through SM or GW. Thus, in the context of IBs, communication network technologies, as illustrated in Figure 6, can be classified into Inward-IB and Outward-IB communication networks.

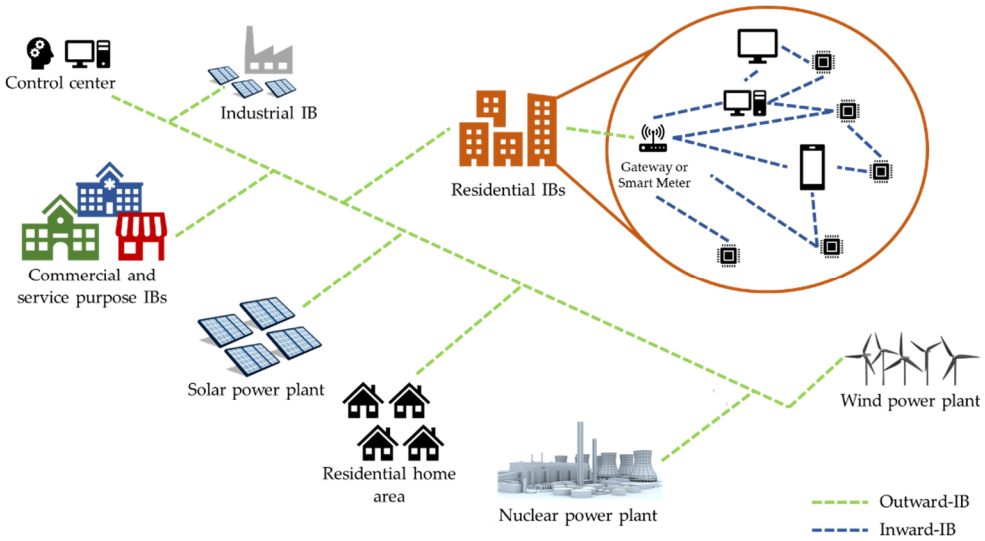

Figure 6. Inward-IB and Outward-IB communication infrastructure for the SG.

The proposed classification can be correlated with another classical one, proposed in [16,108], where SG communication technologies are categorized into home area network (HAN), neighborhood area network (NAN), and wide area network (WAN). Considering this classification, HAN and NAN could cover Inward-IB communication networks, since a building can also be considered to be an association of several neighbors, as in residential buildings, for example. To cover this perspective, the building area network (BAN) level was also defined in [109]. Furthermore, NAN and WAN technologies could be used for Outward-IB communication networks, because an IB can be interconnected with other neighboring IBs or with the utility's back-haul system of the SG. Table 2 compiles the main technologies that can be used for IB communications purposes, including their proposed classification and the main classifications employed in the literature.

Table 2. Main communication technologies for Inward-IB and Outward-IB networks.

Communication Technologies	Inward-IB Network	Outward-IB Network	Media	HAN	NAN	WAN
PLC	✓	✓	Wired	✓	✓	✓
Optical fibers		✓	Wired			✓
Digital Subscriber Lines		✓	Wired		✓	✓
Wi-Fi	✓		Wireless	✓		
Bluetooth	✓		Wireless	✓		
EnOcean	✓		Wireless	✓		
ZigBee	✓		Wireless	✓	✓	
Z-Wave	✓		Wireless	✓	✓	
LPWAN		✓	Wireless		✓	✓
DASH7		✓	Wireless		✓	✓
Cellular technologies		✓	Wireless		✓	✓
WiMax		✓	Wireless		✓	✓
Cognitive radio		✓	Wireless			✓
Satellite communication		✓	Wireless			✓

3.2.2. Communication Infrastructure Requirements for IBs as a Part of the SG

As mentioned previously, a two-way communication infrastructure is essential for enhancing the efficiency of the electrical grid with respect to power generation and distribution to customers. As for the whole SG, this communication infrastructure, deployed at the IB level, needs to be secure, available and scalable. In parallel, its reliability, as well as the interoperability between different devices used to collect data or control appliances, must be also ensured [106].

Firstly, to guarantee the availability of SG services, an IB should provide a communication infrastructure that allows data exchange within itself and among the entities of the overall electrical grid. Furthermore, the adopted communication infrastructure must consider that an IB could be dedicated to different purposes: industrial, residential, or commercial, or to services, such as hospitals [56]. As a result, this infrastructure will differ from one building to another. For example, in some of them, the SM can act directly as a GW within the overall SG [110], whereas in residential buildings, several smart meters, one per customer, will be interconnected with a concentrator, which plays the role of GW with the Outward-IB world and enables, at the same time, different BEMS services. In addition, to transfer information into and out of the IB, its communication infrastructure needs to guarantee the interconnection of heterogeneous devices and communication technologies [107]. As one example, sensors and actuators from different manufacturers could be interconnected, using a mesh network based on ZigBee technology, with a BEMS, which also offers end users a way of controlling their smart appliances through more common network technologies such as Wi-Fi or Bluetooth [111].

Secondly, latency and bandwidth also constitute a major issue for providing a reliable and scalable communication infrastructure at the IB level. Latency and bandwidth requirements, particularly, depend on the nature of SG services [105,112]. In AMI, low-latency performance for real-time monitoring (12–20 ms) is needed in order to better regulate and adapt the energy demand. On the other hand, higher latency is generally allowed for remotely connecting or disconnecting the IB, as an electrical load, from the overall SG. With respect to bandwidth requirements, transferring low-payload data from sensors to smart meters typically requires low bandwidth, whereas the exchange of information between the SG back-haul and IBs through gateways needs a larger bandwidth.

Furthermore, the coexistence of several heterogeneous devices or networks that must be interconnected causes a major issue in terms of interoperability. Nowadays, as suggested above, GW or SM already plays, at the IB level, an important role in connecting devices that use two or more different communication protocols. Nevertheless, interoperability remains a key issue in SG development, and requires efforts towards the standardization of activities [106,113]. In this way, as stated in [65,114], open protocols used for building automation, such as BACnet, KNX or LonWorks, appear to be a major solution, allowing several products provided by different manufacturers to be compatible with one another. Moreover, the need to converge towards a scalable and interoperable communication infrastructure makes TCP/IP-based networks an interesting solution [112]. Exploiting emerging IoT technologies built on IP architecture offers many advantages over other solutions, such as the ability to support data flow over multiple link layers or to connect many devices [115,116]. Thus, using IoT protocols such as 6LoWPAN or RPL [117,118], sensors, actuators and SM connected through an Inward-IB communication network based on ZigBee or Z-Wave technologies could be more easily interfaced with Outward-IB networks, which generally also use IP-based solutions.

Finally, as shown previously, a set of distributed and interconnected devices is necessary at the IB level to provide a reliable BEMS while serving, at the same time, the global functions of the SG. This characteristic makes security and privacy a complex issue in IBs, as entities of the SG SoS [105,119]. Therefore, ensuring secure data storage and transportation from IBs to SG while also protecting information provided by the IB stakeholders is a fundamental requirement for guaranteeing the stability and reliability of power delivery. In this context, the use of heterogeneous devices and network technologies to communicate inward and outward in IBs is a major source of vulnerabilities that could severely disturb the operation of BEMS and SG services [120]. Indeed, sensors and actuators deployed in a distributed manner inside IBs to collect data and control electrical appliances are, in general, resource-constrained and low-powered devices that communicate at low data rates and through mesh networks like ZigBee. Thus, these devices are more vulnerable to attacks. This explains why GW or SM that embed robust security layers are mainly used as communication bridges between IBs and external SG entities [118]. In addition, IBs seem to be easier to attack since they are more accessible than, for example, SG control centers or power plants. By exploiting the weaknesses in their communication infrastructure, such as low-security-level devices or vulnerabilities related to end users, unauthorized users could compromise, through the IB, the performance of the whole electrical grid by manipulating control applications, changing control parameters or interfering with exchanged data [121].

4. Security Protocols and Privacy Issues

As it has been presented in the previous sections, IBs and their related energy management systems employ communication networks and technologies, very often based on the IoT, which increase the vulnerability of the overall SG. In addition, according to the proposed vision, which considers the SG as a CPSoS, the interconnection between the cyber and physical parts creates additional vulnerabilities that need to be considered [122]. Consequently, attacks can be performed against the cyber, the physical, or the cyber-physical parts of an SG [123].

Physical attacks concern hardware deployment, which requires physical access. Deterioration, relocation, masking, or theft lead to resources being unavailable and can also cause mechanical destruction, premature aging, or even direct damage of the SG. Attackers can clone the SM or compromise it. Moreover, cryptographic secrets can be extracted through side-channel attacks such as electromagnetic waves or laser injections. Few papers consider physical attacks due to the necessary of physical access [124]. However, the SG includes IBs, which are open to external people, so a first possible solution is to protect physical access. The use of crypto processors and secure elements or firmware can prevent the lack of tamper protection.

From a cyber-side point of view, attacks usually target databases and applications. Attackers exploit software flaws and misconfigurations in order to disrupt data management applications. Illegal access to employees' computers by means of social engineering attacks can lead to the introduction of malware programs that can help intruders access the database. In this context, attacks against databases can be launched in order to tamper with or steal data with the aim of manipulating the energy market. Stock ciphering data can prevent such leakage and tampering [125], whereas random access to the database can solve privacy problems.

Finally, in SG metering networks, data are generally exchanged in a single or multihop path. Some structures and devices of an SG that are usually targeted by cyber-attacks include SCADA network devices, phasor measurement units (PMUs), and AMI. Smart meters are basic components of the AMI, and represent a significant back door for eventual attacks to IBs and SHs, in which they are most frequently installed [126]. Attacks on SMs, which are caused by the lack of security and privacy in SM wireless communications, can disrupt energy provision, destroy hardware, and cause loss of customer data. Hence, security and privacy in the cyber-physical area of AMI are of utmost significance.

4.1. Cyber-Physical Security Objectives and Requirements

In AMI, a huge amount of heterogeneous private technologies and standards must coexist in a closed space, increasing security and privacy risks [127]. Security and privacy solutions must be compatible with hardware and existing standards, while at the same time preserving the correct performance of communication networks. It is necessary to find a trade-off between efficient pseudo real-time data collection and secure and private communications [128]. It is widely established that, also for the SG environment, the main security objectives that need to be ensured are confidentiality, integrity, and availability [129], together with authentication, freshness and nonrepudiation. Additionally, mechanisms of trust, authorization and access control for users must be deployed. With respect to confidentiality, data must be disclosed only to legitimate users, also avoiding privacy leaks. In the case of the SG, confidentiality can be ensured by allowing only the energy company to access customers' energy consumption data. For its part, integrity ensures that received data are correct, enabling the detection of communications that have been intentionally tampered with. Integrity also allows consumers to be certain of receiving the correct bill, correlated with their energy consumption, sensed by their own SM. Network and data availability ensures that users can access applications and services even in the case of attacks. Authentication and nonrepudiation solutions are used to verify the identity of the sources of the messages, so senders cannot disclaim their ownership. In the case of the SG, each SM can be authenticated by the energy provider in order to deliver legitimate bills. Freshness is the countermeasure employed against replay attacks. Finally, trust between the heterogeneous devices present in the SG is challenging [107]. Access control prevents unauthorized users from accessing resources, while authorization verifies the legitimacy of devices and allows them to join the network.

Communication networks collect a huge amount of data, which can lead to privacy leaks for users. Attackers can, for example, try to infer information regarding consumers' habits (wake up hour, lunch time) by analyzing their energy consumption data [123]. Therefore, ensuring the confidentiality of data and metadata is paramount. To deploy more efficient countermeasures, a model of attackers based on their capabilities and their intentions is necessary, since their capabilities can be important to a greater or lesser degree [130]. An internal attacker is an employee or a corrupted legitimate device that knows security material and appears to be legitimate, and is capable of accessing the available resources. In the case of external attackers, like cyber criminals, terrorists, or state-sponsored groups, network secrets are not usually known by them [131]. A strong attacker, who can use a PC and does not follow transmission power restrictions, has greater capabilities than legitimate devices. In the case of ordinary attackers, their capabilities are the same as those of network devices. It must be also pointed out that it is easy

to deploy a hardware platform with which to conduct attacks, which can be used by nonexperts to damage communication networks. Finally, it is crucial to correctly identify the intentions or aims of attackers in order to choose the optimal solution. Four intentions can be defined [132]:

- Interruptions of communications, avoiding delivery of data to their destinations. The QoS is disrupted and, at the same time, attackers try to tamper with data during the interruptions;
- Exhaustion, where attackers try to drain the constrained resources of SM such as computing units;
- Identification, employed by attackers that want to appear to be legitimate in order to join the network;
- Authorization, the objective of which is to counter the access control mechanisms in order to access data or security secrets.

In conclusion, different criteria for a model of attackers were proposed on the basis of their capabilities and intentions. This model is useful for studying the attacks and countermeasures proposed in the scientific literature, where different security requirements have been defined in order to ensure security and privacy. In the SG environment, security requirements have different priorities, depending on the part of the SG. Regarding the AMI, because of the data sensitivity, confidentiality has the highest priority, followed by integrity and, finally, availability, as shown in Figure 7.

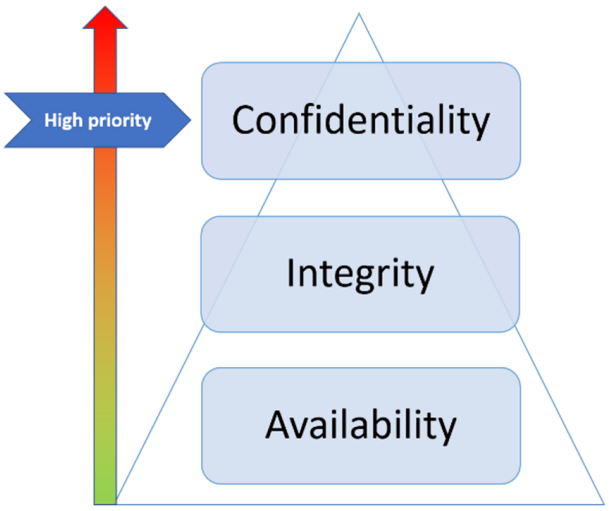

Figure 7. Priority of security requirements for AMI.

4.2. Overview of Attacks Against the Smart Grid Security

The communication standards employed in SGs were deployed without proper consideration of security [124]. Indeed, electric utilities do not generally foresee the cohabitation of different communication technologies, and mainly base their security on the physical isolation of their systems. To apply the best adapted countermeasures, possible attacks must be identified. However, the complexity of the SG and the variety of communication protocols make the enumeration of all possible attacks difficult [129]. One first solution for overcoming this problem is to classify the attacks on the basis of OSI layers [133], even if attacks are very often applied to several layers in order to cause more harm. Next, cyber-physical menaces will be analyzed layer by layer, which makes it possible to simultaneously deploy security mechanisms in a more efficiently manner.

4.2.1. Multilayer Attacks

One of the most typical threats for the SG, which affects all OSI layers, is denial of service (DoS), because it harms grid availability through attacks targeting the constrained

devices present in the AMI. By means of a DoS, an external hacker has the capacity to degrade the SG performance, blocking or destroying a part or all of the grid [134].

4.2.2. Physical Layer Attacks

A simple way to realize a DoS at the physical layer is by means of a jamming procedure, which can be performed from outside the network. The physical layer IEEE 802.15.4 is particularly sensitive to this attack [127]. The goal of the adversary is to interfere with the radio frequencies employed in order to damage communications [135]. Jamming can be performed in three different manners: spot jamming, where only one frequency is affected, sweep jamming, where several precisely targeted frequencies are under attack, and barrage jamming, where a frequency range is targeted [136]. The QoS and the availability of the grid are especially touched by jamming attacks. Another possible attack is the time synchronization attack (TSA) [137], which targets the timing information transmitted by the SM to detect failures in PMU applications or to localize incidents in the electrical grid. This attack forges false GPS data for the PMU, causing false alerts and incorrect localization. In the same way, integrity is also compromised.

4.2.3. MAC Layer Attacks

In order to execute a DoS attack at the MAC layer, the attacker (who can be a common external user) tries, by means of certain types of messages such as acknowledgement messages, to create collisions that interfere with legitimate communications [138]. Media access protocols such as slot allocation are particularly vulnerable to these attacks [139], the main aim of which is to interrupt any communication, which in turn impacts network availability. Exhaustion attacks are oriented toward the MAC layer too, taking advantage of the limited resources (energy, memory, processing) of the equipment. One way to conduct such an attack is based on request to send (RTS) frames, which are used for SMs to request channel access [140]. Thereby, legitimate SMs will ask continuously for channel access, without obtaining any answer, until their batteries have been completely discharged. External assailants can carry out this attack, compromising network availability. By implementing a duty-cycle-based MAC protocol, limited-resource devices can achieve a maximum lifetime exceeding 99% of their time in a sleep state [141]. However, unauthenticated frames can be broadcast through the network to conduct a denial of sleep attack, with the aim of keeping the devices awake [142]. Masquerading attacks are used to either spoof MAC identifiers, illegally modify the address resolution protocol (ARP), or carry out cache poisoning [143]. The broadcasting of false ARP packets allows an attacker to interrupt the communications temporally or definitively between power substations and the AMI. Confidentiality, integrity and availability are impacted by masquerading attacks, together with authentication and access control, especially in the ethernet protocol [144]. Finally, man-in-the-middle (MITM) attacks represent an important security breach for the AMI [145], since the attacker intercepts, without corrupting them, messages exchanged by the data concentrator and the AMI, with the result that such attacks are almost undetectable. Similarly, the DNP3 SCADA protocol is also vulnerable to MITM threats [146]. Once again, confidentiality, integrity and availability are compromised.

4.2.4. Network Layer Attacks

Selected messages transmitted by one device or a set of devices (AMI, utility center) can be routed or discarded by an attacker by means of the "selective forwarding" attack [147]. Electricity prices can thus be impacted by varying the offer and demand balance, but not only this: the intruder can assign a higher priority to their messages, and chaos can be caused in the network by adding intentional delays in the routing procedure. Such an attack poses a threat to confidentiality, integrity and availability. The blackhole attack is a paradigmatic example of selective forwarding, where the assailant will conduct a DoS, avoiding the routing of all packets to the network [148]. A "sinkhole attack" is realized by hackers in order to direct most of the network traffic to them. For this purpose, one

possibility for the attacker is to declare to an SM that they have the best path towards the data concentrator [149], which is also known as a "hello flood attack". The BACnet protocol can also fall victim to this kind of threat because of I-am-router-to-network messages [150]. If the hello flood attack is made prior to a selective forwarding, the latter is easier and more harmful [151]. If the communication topology is not optimal, confidentiality and QoS, along with integrity, can be threatened by sinkhole attacks. Another possibility for attackers is to go into the network, either spoofing the identities of legitimate users or generating false identities, performing a "sybil attack" [152]. In this way, an SM whose identity has been spoofed will lose access to the data sent to it and, at the same time, it will not be able to transmit energy consumption information. The QoS is affected by such an attack, which can be conducted by an attacker without any special skills. Router advertisement flooding can be used by attackers in order to exhaust the resources of a device by means of the routing maintenance protocol [153], resulting in a DoS. In BACnet, this methodology can be applied using who-is-router-to-network messages and the source addresses SADR and SNET. It is important to point out that attacks can be performed by more than one assailant, which is the case in the "wormhole", where an out-of-band communication tunnel is created between two distant attackers, one of them near the data concentrator and the other far away in the network [154]. Since communications are faster through the tunnel, this latter is employed by the nodes of the network. The integrity of data employed to detect problems within the SG is impacted by such attacks. Finally, the DoS in the AMI can also be accomplished by employing a "puppet attack" [155]. In this case, the attacker tries to exhaust the bandwidth, as well as the device's batteries, implementing a flooding mechanism from a puppet node in the network. The packet delivery rate is also affected, falling as low as 10%, impacting the smooth operation of SG applications.

4.2.5. Application Layer Attacks

Attacks conducted at the application level try not only to drain batteries and bandwidth, but also the memory and even the CPU of the network devices [156]. In this context, the purpose of a desynchronization attack is to persuade two entities (AMI and utility company data center) to believe that they are unsynchronized [157], discharging the SM batteries, and reducing the QoS. For its part, a flooding attack allows a hacker to exhaust the resources of the devices by starting application layer protocols, while at the same time avoiding their completion. The attacker can, for instance, take advantage of the TCP handshake protocol [156] to flood the devices' memory and avoid the connection of legitimate entities, which is also known as a smashing attack [158]. In addition to threats concerning network availability, the application layer is prone to privacy and integrity attacks involving manipulation or access to data, as well [129]. An attacker can inject false control commands into the network to harm the SM and the overall AMI availability [152], resulting in a global dysfunction of the SG. Additionally, fake control commands have the capacity to disconnect the SM. This injection of fraudulent data can be made using the MODBUS protocol, as explained in [159]. Hackers can additionally inject new data into the network, causing incorrect quantifications of the consumed and generated power, leading to financial losses [107]. This false injected information could also damage the AMI and the data aggregation mechanisms, without forgetting that every actor in the SG, including the SCADA system, makes use of this information for operation and security, which are ultimately compromised. In conclusion, Table 3 summarizes the presented attacks and their impact on confidentiality (C), integrity (I) and availability (A).

Table 3. Attacks by OSI layers.

Layers	Attacks	Confidentiality (C), Integrity (I), Availability (A)	Countermeasures
Physical	Jamming	A	[160,161]
	TSA	A, I	[162]
MAC	Collision	A	[163]
	Exhaustion	A	[164]
	Denial of sleep	A	[142]
	Masquerading	C, I, A	[165]
Network	Selective forwarding/blackhole	C, I, A	[166,167]
	Sinkhole/hello flood	C, I, A	[168,169]
	Sybil	C, I	[170]
	Router advertisement flooding	A	[171]
	Wormhole	A, I	[172,173]
	Puppet	A	[155]
Application	Desynchronization/flooding/stack smashing	A	[174]
	Control command/alert message injection	C, I, A	
	Data tampering	C, I	[175]

4.3. Privacy Issues

During the communication process, the payload (data measured by the SM, for instance) is encapsulated within different headers added successively by each crossed OSI layer. These headers contain metadata, which allow the receiver to process the frame and to identify its format. Hence, a malicious user can conduct privacy attacks against the payload and the metadata. In the case of metadata, attacks take place in the acknowledgment and scanning stages of the SG attack strategy [176]. To adequately ensure privacy, it is mandatory to deploy solutions to avoid massive data collection, but also to prevent the use of metadata by an attacker. These solutions must allow the sharing of the collected data while protecting sensitive information. It also necessary that the application of privacy protection mechanisms not undermine the existing security methods. Three attacker models can be considered [177]:

- External, where the attacker does not belong to the network. This attacker does not participate in communications or routing, and does not interact with legitimate participants, realizing passive attacks;
- Internal, where the attacker is able to take control of network equipment or resources. Since such attackers are perceived as legitimate users, they can participate in even secured communications, gaining access to all the traffic passing across them. Such attackers, qualified as active, have, however, a limited view of the network;
- Global, where the attacker is internal and possesses an entire view of the network. Consequently, they are able to control and observe all the communications, and, therefore, to gather any available information regarding the whole network. Frequently, this attacker is also the network administrator.

Privacy attacks are grouped following two categories: eavesdropping and traffic analysis (Figure 8).

The first privacy attack is eavesdropping, which is also an MITM attack [178]. In this case, the attacker will listen, for a long time, to the communications that take place in the network, while simultaneously collecting packets on one or more specific targets. The eavesdropping is carried out via a sniffer that retrieves and saves in a file all the frames exchanged in the AMI at the MAC level (raw frames) or at the network layer. This attack is carried out by an external hacker, and it is difficult to detect it because the network continues to operate without disturbance. The saved file is then processed by a network analyzer such as "Wireshark", which makes it possible to dissect the different fields of the received frames. In this manner, the attacker can, on one hand, attempt to exploit the data periodically reported by the SM to determine location information or, on the other hand,

to collect users' consumption patterns in order to infer daily living habits. This kind of attack is known as nonintrusive load monitoring (NILM) [179]. In addition to supposing a significant privacy information leak that could damage users' trust with respect to the SG, the stolen data could help burglars to identify when a home may be empty, or even allow them to interfere with the electricity tariffs and reuse consumers' identities for the purpose of fraud. Metadata can in turn be extracted in order to discover the identities of participants (MAC addresses, IP addresses, UDP ports) and their roles, but also the characteristics of the network, allowing attackers to identify the communication protocols employed and thus to exploit their weaknesses. This is the case of ZigBee, which offers many vulnerabilities as regards eavesdropping [180].

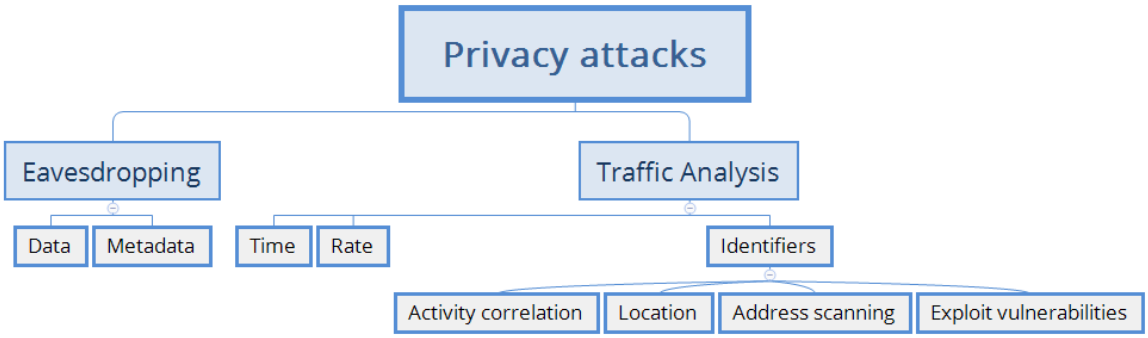

Figure 8. Taxonomy of privacy attacks.

The second kind of attack is traffic analysis. By means of this method, the external attacker seeks to determine, from the communication patterns collected via eavesdropping, information regarding the location or the identification of a special device (for example, the data concentrator). There are three types of traffic analysis [181]. One of the first types of information available through traffic analysis is temporal data. In such an attack, the relevant data are the frame routing time, or the required time for data to travel from the source (an SM, for example) to the destination (such as a data concentrator). From this information, an attacker that knows the network and its operation will be able to deduce the transmission time of privacy packets to the data concentrator, and also to determine the source location when a frame is sent. In the scientific literature, this situation is known as the "panda hunter game" [182]. During such an attack, the malicious user is external, and their goal is to localize the sources of the collected data. Once the location has been determined, the SM carrying the information can be identified, and a subsequent DoS attack can be launched against these strategic targets to damage the QoS. However, the attacker needs an overview of the overall network and communications to find the source. To do this, depending on the size and nature of the network, the attacker can either deploy only one sniffer that offers a large range (moderate size network), or install multiple sniffers that cover the entire area (for vast networks). In the second form of traffic analysis, the relevant data are statistical data, especially the rate of incoming vs. outgoing packets [183]. In this schema, the attacker considers that SMs located close to the data concentrator route more frames than those located far away from it. In this way, the data concentrator can be located on the basis of the positions of those devices having the highest traffic, following a learning phase for understanding the usual values related to the application and the protocol. The main aim of this attack is to perform a DoS to block communications. Finally, the third way traffic analysis can be conducted is based on the use of identifiers, which are placed in the headers of the different OSI layers. To facilitate network management, these identifiers are often static, resulting in attacks conducted in constrained networks, which are being increasingly studied [184]. Four sorts of attacks can be performed on the basis of static identifiers:

- Activity correlation. As long as an address stays valid, even if a device changes its network, an attacker can associate communications, and thus the activity, of this address;
- Location. An attacker can try to probe a network to look for a previously observed address, recovering the topology and observing movements, mainly in wireless scenarios. By leading an eavesdropping attack on a network implementing the KNX protocol, an attacker can list the devices present in the network [185]. Later, by analyzing the traffic on these identifiers, the hacker can track the people in the building. Tracking of network users can also be done in a simple way by means of the WiFi protocol [186];
- Address scan. Once the protocol used to generate the addresses in the network has been identified, an attacker can reduce the potential addresses in order to carry out attacks;
- Exploitation of specific equipment vulnerabilities. A MAC address, referred to a an organizationally unique identifier (OUI), is composed of 24 bits assigned by the IEEE. The OUI not only identifies the equipment manufacturer, but also allows a hacker to know the hardware's weakness in order to conduct a targeted attack, such as against the AMI infrastructure.

In conclusion, the objective of privacy attacks is to infer information about the network, its behavior, and its participants in order to give an advantage to the attacker, who can then employ the identified vulnerabilities in order to carry out more effective and powerful strikes. In the same manner, information regarding the security systems deployed can be obtained in order to better counter them. The protection of privacy is therefore an important criterion in the deployment of SGs.

4.4. Solutions for Improving Security and Privacy

Three kinds of solution can be used to ensure security and privacy: prevention mechanisms defined in standards, detection solutions such as intrusion detection systems (IDS), and dedicated solutions for countering one or a group of attacks.

4.4.1. Prevention Mechanisms Defined in Standards

The deployment of encryption of communications is the first solution for ensuring confidentiality in SGs, since it prevents eavesdropping by an external attacker [187]. For this purpose, three ciphering schemes exist [188]. In symmetric schemes, fast algorithms are used with a common key to encrypt and decrypt communications [189]. The Advanced Encryption Standard (AES), proposed by the NIST, is the most popular algorithm [190]. In asymmetric encryption, the message, which is encrypted by a public key, can only be decrypted by a private key [191]. Key management solutions such as Public Key Infrastructure (PKI) are used to distribute the key over the network. Rivest, Shamir and Adleman (RSA) [192], and more recently, solutions based on elliptic curve cryptography (ECC) [193] are some examples of asymmetric schemes. Finally, homomorphic solutions enable complex mathematical operations to be performed on ciphered data without decryption, which improve confidentiality, especially in database applications [194]. Symmetric encryption is faster than asymmetric encryption, which reduces energy consumption. However, lightweight cryptography mechanisms, such as tiny AES, have been designed to fit with constrained networks [195]. To ensure the authentication and integrity of messages, a message integrity code (MIC) is generated thanks to a hash function and a secret key. In this context, HMAC-SHA-1 and HMAC-MD5 are examples of hash protocols [196].

Still, MIC and ciphering use keys whose creation, distribution and maintenance represent a challenge in constrained environments, including in SGs [197]. First, a common key shared by all the participants of network communications, called a global key, is the easiest solution and saves memory. However, it offers poor authentication, and it is a poor solution against corrupted devices. Secondly, through the use of a key group, the number of devices sharing the same key is limited, restricting internal attackers to one group. Several groups can be formed in the same network based on common characteristics (location, role or application), using different keys: one for communications between members of the

group and another one for communications between groups. In the latter solution, a key can be used for each hop-by-hop communication, improving security against intruders, but impacting memory, especially in huge networks. The creation and distribution of a key (global, group or hop-by-hop) can be made in a centralized manner by a trusted third party, but maintaining good performance is complicated in the SG. In a distributed way, devices perform the management of keys by using a preshared key stored in memory before deployment, or by deploying the key during the join phase through the intervention of the network owner. The last solution is to use common metrics such as link radio to generate the key autonomously without the intervention of the network owner [198].

Encryption mechanisms, authentication and integrity solutions, and key generation must be defined in the employed protocol or standard. Table 4 shows the solutions for some communications standards of SG.

Table 4. Security mechanisms in SG standards.

Standard	Ciphering Suite	Authentication/Integrity Suite	Key Management Protocol
IEEE 802.15.4 [199]	AES-CTR 128 bits	AES-CBC-MAC 128 bits	Upper layers
Z-Wave [200]	AES 128 bits	AES 128 bits	Elliptic Curve Diffie-Hellman (ECDH)
En-Ocean [201]	AES-CBC 128 bits or VAES (recommended)	AES-CMAC	Preshared Key (PSK)
ZigBee [180]	AES 128 bits	AES 128 bits	Master, Network (default) or link Key
IPsec [202]	Several	Several	IKEv2
DTLS [203,204]	Several	Several	Handshake
WiFi [205]	AES-CCMP 128 bits (WPA2) AES-GCMP-256 (WPA3)	EAP (WPA2) HMAC-SHA-384 (WPA3)	PSK (personal)/RADIUS server (Entreprise) ECDH (WP3)
Bluetooth [206]	E0 (Bluetooth) AES-CCM (LE)	HMAC-SHA-256 (Bluetooth) AES-CCM (LE)	PIN pairing or ECDH (Bluetooth) Long-Term-Key (LE)
DLMS/COSEM [127]	AES-GCM-128 bits	MD5/SHA1/GMAC/SHA256/ECDSA	Preshared
KNX [207]	No (old) AES-CCM 128 bits (new)	No (old) AES-CCM 128 bits (new)	No (old) Factory Device Set up Key
BACnet [208]	No	No	No
ModBus [209]	No	No	No

IEEE 802.15.4 defines encryption and authentication solutions, but it lets upper layers manage the keys. Z-Wave, En-Ocean, ZigBee, WiFi, Bluetooth and DLMS/COSEM propose solutions for managing keys based on preshared keys or heavy handshake protocols. IPsec and DTLS deployed in a GW allow interoperability and end-to-end security if the encryption and integrity mechanisms deployed are identical on each side. KNX in its old version did not provide security features such as BACnet and ModBus [159]. Even when SG protocols define security mechanisms, they are often deployed without, and some popular standards have no solutions. Moreover, even when cryptography is used, security and privacy attacks can be performed. Therefore, additional dedicated solutions must be deployed.

4.4.2. Detection Systems

The first step in deploying the best countermeasure is to detect and identify the type of attack using an intrusion detection system (IDS). IDS can detect signatures, anomalies, or can be based on specifications [210]. In signature-based IDS, attack detection is performed on the basis of known patterns, which is the method employed by antivirus software. A database of misuse is created by the network administrator to be compared with the run time network activity in order to detect any abnormal behavior. In SGs, IDS using the deep packet inspection method can be deployed to secure SCADA [211], while an IDS based on 50 signatures has been used in ModBus communications [212]. However, this kind of IDS,

very popular in classic networks, is not suitable for AMI, where the storage of signatures overflows the memories of constrained SMs, and the comparison algorithms cannot be run using a limited CPU. Moreover, misuse-based IDS are useless against zero-day attacks or unknown patterns, and require frequent additional updates to integrate new attacks. In anomaly-based IDS, the network is first analyzed to understand the "normal" behavior, without attackers, to be used as a reference for the detection of anomalies [213]. Based on statistical data (transmission time, number of packets, number of devices, topologies) anomaly-based IDS can detect new attacks, but results in a high false positive rate. DoS attacks on SG can be detected using anomaly-based IDS with an accuracy of 95% [214]. IDS can be deployed in the data collector of the AMI to detect DoS attacks, fuzzing or worms based on entropy [215]. Finally, a specification-based IDS is similar to an anomaly-based one, with the exception of the learning phase, which is replaced by a manual definition of normal behaviors to limit false positives while maintaining the detection ratio of new attacks. IDS can be deployed in HAN to detect attacks on IEEE 802.15.4 [216]. A petri colored network can be implemented in IDS to model communications between SM [217]. However, specification-based IDS requires the creation of a database by the administrator, as well as additional computational power.

Anomaly-based IDS is therefore the more widely adopted solution for SG, but it again represents a challenge with respect to its deployment and realization [218]. Indeed, classic IDS are too heavy and energy consuming to be deployed in constrained devices as SM. Some solutions are starting to be published, but it is important to identify the right place to implement them [219]. First, centralized IDS employed in powerful trusted third parties such as GW can detect several types of attack. However, centralized IDS requires a global vision of communications, which is complicated in large networks and presents a single point of failure. In decentralized solutions, IDS is deployed in constrained devices, which can exhaust their memory and energy, limiting the number of signatures in the database [220,221]. Therefore, IDS uses a rule of uniqueness, which is effective, while the behavior of the attacker (modification of number of packets, no optimum path) fits this rule. Consequently, in order to detect all the attacks described in the scientific literature, a great number of IDS is necessary. The last solution is a hybrid IDS, where detection is performed by an SM while decisions are taken by more powerful devices, at the cost of additional communications for IDS applications. In conclusion, in SGs, IDS will be able to help detect attacks when some remaining issues have been resolved, such as the space available for system implementation. As soon as attacks are identified, dedicated countermeasures can be deployed.

4.4.3. Dedicated Solutions

In this section, the previously identified solutions dedicated to security and privacy attacks will be presented, such as spread spectrum techniques [160] and code-division multiple access [161], which are used to counter jamming at the physical layer. TSA can be mitigated with a reliable temporal system [162].

Error-correcting code [163] and encryption are solutions against DoS at the MAC layer. When an exhaustion attack is performed, one possible solution consists of limiting the rate of control packets sent by one device (quota), or of using a temporal division MAC access [164]. An authentication scheme is used for denial of sleep [142], in combination with quota, as in exhaustion attacks. Masquerading can be mitigated by encryption and authentication at the MAC layer. Whitelists can be used to save authenticated identities [165]. In this way, GW can play an important role by comparing the numbers of ARP requests/responses.

At the network layer, selective forwarding/blackhole attacks are countered with dynamic multipath routing protocols [166]. Detection based on routing patterns can be performed by network participants or a watchdog, enabling devices to route frames in the case of attacks [167]. Encryption routing metrics or the implementation of two-way metrics, linked to media such as received signal strength indication (RSSI), can be used

to combat sinkhole attacks. Routing protocols verifying the bidirectional reliability of the path on the basis of latency and QoS are also possible solutions [168]. IDS using a blacklist was proposed for sinkhole attacks in [169]. As sybil attacks use identifiers, authentication can be used to prevent them. A distributed hash table (DHT) [170] makes it possible to save several instances of each identity or device location with the aim of detecting spoofing addresses. Encryption at the network layer is a solution for router advertisement flooding. Secured protocols can also verify the authenticity of routers [171]. A router advertisement guard can drop requests from incorrect sources. Ciphering is useless for limiting wormhole attacks and, at the same time, its detection is complicated. The use of directional antennas reduces the possibility of launching this attack [172]. To detect a wormhole, the neighbor relationship can be used as a rule [173]. Lastly, puppet attacks can be detected by means of routing protocols [155]. When identified, the attacker is blocked in a blacklist, and communications are stopped with him.

Finally, at the application layer, DoS attacks such as desynchronization, flooding or stack smashing can be mitigated using integrity and authentication mechanisms, or by introducing a quota to limit the number of exchanged packets. The client puzzle solution has been used to prevent protocol exploitation [174]. When frames are ciphered and authenticated, attackers cannot perform data or control packet injection without security knowledge. Blockchain, deployed in smart contracts, can be used to securely stock and share data without recourse to a third party [175]. However, blockchain is based on heavy cryptographic process that are impossible to implement in constrained environments such as SM.

In addition to dedicated security countermeasures, privacy mechanisms make it possible to prevent eavesdropping and traffic analysis attacks. With limited transmission power, communications can be obfuscated at the physical layer to prevent eavesdropping [222]. Traffic analysis based on temporal information can be mitigated by employing mixing solutions that modify the frame format [223], introduce a random or probabilistic delay [224], or reorder packets. False traffic generated randomly or based on real traffic prevents data rate traffic analysis [225]. The combination of random routing protocols with false packet injection can mitigate traffic analysis [226]. Even if the use of static identifiers eases network deployment and management, they can be analyzed in order to launch more powerful targeted security attacks.

Anonymity solutions use obfuscation techniques to prevent identity being correlated with network activities [227]. Mixing solutions as the onion routing (TOR) [228], based on encryption and padding methods, are the most popular anonymity solutions, limiting header analysis and MITM attacks. However, this solution harms network performance and requires a header overhead of 500 bytes or 48 bytes [229], which is impossible for constrained protocols. The IPsec tunnel mode, similar to a virtual private network, provides anonymity, but again at the cost of 40 bytes in additional headers. Encryption at the MAC layer combined with a bloom filter can hide MAC addresses in the star topology and unidirectional communications of limited networks [230].

Because anonymity complicates access control features and IDS deployment, the implementation of pseudonyms is recommended. Pseudonyms replace addresses in headers, preventing the correlation of activities or locations, and the retrieval of real identities. Access control and authentication can always be performed, but it is impossible for an attacker to link several pseudonyms between them. Moreover, updating pseudonyms in run time is necessary in order to limit any eventual impact of traffic analysis. Devices can choose a pseudonym from a list distributed by a trusted third party that can either be reused [231] or removed after use [232]. In the former solution, an attacker can take advantage of the reuse of pseudonyms to infer information. The use of a trusted party is complicated when using a remote SM due to the unreliability of communications. To enable devices to generate their own list, RFC 4941 proposed the use of the MD5 hash function [233]. However, only source addresses can be computed and so, destination addresses are still in clear. To allow

faster and more flexible autoconfiguration, devices must be able to generate their own pseudonyms, but also those of their neighbors, in order to prevent device tracking [234].

With dynamically generated pseudonyms, devices do not stock or share a list, but rather generate, when necessary, a new pseudonym. IPv6 source addresses can be replaced by pseudonyms generated using the SHA-1 hash function in broadcast [235] or in unicast communications [236]. To overcome the drawbacks of the heavy process of generation and verification of pseudonyms, ECC can be used in combination with a trusted third party [237]. Two-way physical metrics such as RSSI and round trip–time of flight were used in [238] to generate identities. Moving target IPv6 defense (MT6D) provides pseudonyms for IPv6 and MAC addresses obtained through the use of a symmetric algorithm [239]. Even if MT6D prevents intruders and enables authentication, synchronization methods are still necessary, a requirement which is difficult to meet on constrained networks. Finally, Ephemeral leans on AES in counter mode to enable each device to compute pseudonyms for MAC addresses, combined with MAC layer encryption to hide other identifiers [240]. The synchronization process is useless, because generation features are shared in communications at the cost of MAC header overhead (2 bytes). Pseudonyms can be updated on either an event-driven or time-driven basis.

Table 5 presents the advantages and drawbacks of the countermeasures proposed for the SG. The "Suitable" column indicates whether each solution is adaptable/adapted (✓) or not (✗) to embedded systems. Next, the network performances and main drawbacks are studied: the symbol "-" indicates a loss of performance (data rate, QoS, etc.). The greater the number of "-", the worse the performance compared to a network without security and privacy solutions. In conclusion, even if some SG standards define cryptography mechanisms, they are often deployed without security. IDS for constrained environments are beginning to be published, but these are still in need of evaluation in real systems. These IDS can help to detect attacks and apply the right dedicated countermeasures. However, some open issues remain to be addressed before achieving a secure AMI.

Table 5. Comparison of the proposed countermeasures.

Countermeasures	Suitable	Nwk Perfs.	Main Drawbacks
Spread spectrum [160]	✗	-	Heavy protocols
Error-correcting code [163]	✓	–	Latency
Whitelist [165]	✗	-	Table management
Dynamic multi path routing [166]	✗	–	Energy consumption
DHT [170]	✓	-	Not suitable for large network
Authenticity [171]	✗	–	Heavy protocols
Puppet detection [155]	✓	-	Long time to detect
Blockchain [175]	✗	—	Heavy cryptographic process
Physical obfuscation [222]	✓	–	Dedicated hardware necessary
Mixing [223,224,228,229]	✗	—	Header overhead
False traffic injection [225]	✗	–	Energy consumption
Bloom filter [230]	✓	-	Star topology and unidirectional communications
Lists [231,232]	✓	-	Memory exhaustion
RFC 4941 [233]	✗	-	Only source addresses hidden
CGA [235,236]	✗	–	Heavy
SSAS [237]	✓	-	Trust parti
MT6D [239]	✓	-	Synchronization algorithm

5. Perspectives

Studying security and privacy issues in order to identify and develop solutions requires a global perspective and multidisciplinary skills. The aim of this paper from the beginning has been to characterize IBs within their environment, i.e., the global SG into which they are integrated. Both IBs and the SG can be considered as SoS, as well as CPS. This point of view led us to propose architectural models based on several layers: physical layers, transmission/distribution layers, communication layers, and automation/management layers. Based on this architecture, we were able to identify the protocols and tools used at each layer to integrate IBs into the SG and to manage energy production, storage and consumption within IBs. Security and privacy failures can then be associated with their respective levels, and specific solutions can be proposed to avoid such failures, with both a layer focus as well as a multilayer focus. In order to do so, we proposed not only considering the technical aspects of security and privacy, but also the human factor, as potential risks. Analyzing security and privacy failures should start with a human-centered approach, by defining use cases and personas. For example, [241] pointed out that, for industrial CPS, the completely different forms of interaction between machines and humans have still not been adequately explored. For them, designing CPS for users is a real challenge. A use case allows us to characterize situations in which security and/or privacy is concerned. Personas make it possible to define different types of "users" of IBs. Their combinations may highlight the different behaviors of users in each situation. We were then able to analyze the resulting scenarios to propose relevant solutions and their level of performance, thus improving the user experience [242]. When designing a new IB, questions of security and privacy can then be integrated into the global design process of the building through a user-centered methodology, involving multidisciplinary teams. Such a methodology is an important issue for our future work. Last but not least, it is necessary to emphasize that, in order to manage the energy of IBs in an efficient manner, all of the solutions mentioned in the previous sections must consider other nontechnological aspects, which are very often forgotten, including the human dimension [243,244] as well as environmental challenges, such as climate change [245,246].

As mentioned previously, the SG is an SoS even in communication networks. ICT is used to exchange information among the various systems of the SG (outward), but also information coming into this system (inward). Various heterogeneous devices and communication standards (wired or wireless) coexist in the same network. This heterogeneity causes threats to security and privacy. Some standards define security features, but most of them are configured to send data in clear text by default. Others exist in old versions without security and new versions with cryptography functions but with no backward compatibility, with the latter implementing no security. Given the lack of standardization, vendors can choose on the basis of the level of security offered. One unresolved issue is the standardization of SG to ensure interoperability with respect to security. Data provided by the SM can be used to infer information about the habits of consumers, which can be used for marketing or for burglaries. Metadata can also be exploited by attackers to launch more powerful attacks on the SG. Lightweight ciphering at the MAC layer must be deployed to prevent privacy leaks. However, ciphers at the MAC layer lead to interoperability problems. There is also a lack of solutions for hiding MAC header metadata in order to prevent traffic analysis in AMI.

Authentication, access control and trust are important features for allowing SG deployment. Authentication can prevent integrity attacks, but the needs are different depending on the level of the SG. For example, energy providers need reliable authentication schemes to link SM with its consumers in order to provide energy cost estimations. In the database, authentication is required for access to the data. New SM or devices can be deployed in run time in the SG. These devices are managed by different companies. Establishing trust between two devices managed by the same company is easy, but it is more complicated when there are two entities. Cryptography helps to enable security and privacy. These protocols lean on symmetric keys, which is appropriate the constrained nature of the devices

(with respect to, e.g., memory and CPU). However, the distribution and management of secret keys remains an open issue in large distributed networks and is dependent on the SG level.

IDS are very prevalent in traditional networks. Even if they represent a good tool for preventing attacks, efficient deployment in uncertain networks such as SG remains an open issue. Decentralized solutions seem to be the best option, but challenges remain with respect to embedding them into SM. The use of new techniques for detection and classification, such as ML, neural networks or data mining, have to be studied and network performances compared. AMI deploys constrained devices that are vulnerable to DoS attacks. Efficient solutions against DoS, especially at the physical and MAC layers, are challenging. Blockchain, as a solution for the prevention of data tampering, has to be developed in order to enable its deployment in constrained devices. The cost of this kind of solution needs to be evaluated. Ensuring end-to-end security and privacy from physical devices for the control and management of information systems is also challenging. Gateways are deployed to ensure interoperability between communication protocols (e.g., BACnet to KNX or Modbus or IEEE 802.15.4 to IEEE 802.11). However, as we explained previously, the compatibility of implementations is difficult with different manufacturers, even when employing the same protocol, and certifications are needed. From a security point of view, too, several open issues remain. The GW must decrypt and encrypt frames between the two worlds, so the keys of the two sides have to be negotiated and stocked. The same level of security is needed in the two parts. The GW must be a trusted element, since each GW brings a point of failure with respect to end-to-end security. One solution for security interoperability is to use TCP/IP layers in each part and deploy identical security protocols. However, certain heavy protocols cannot be deployed in constrained devices like SM. New protocols must be designed to be deployed in each network with their specifications. The lack of security and privacy policies adapted to the SG paradigm is mainly a result of the difficulty of achieving experimental testbeds, the deployment of which is too expensive for many researchers. On the other hand, using real systems to test classical techniques (fuzzing, penetration test) can damage the infrastructure, breaking down the SG and disrupting energy distribution.

Finally, vulnerabilities and defenses from a social and human point of view are in need of more attention. On one hand, vendors and operators have a lack of awareness of security solutions and policies, and tend to focus on QoS and performances. On the other hand, customers are not careful with respect to security and privacy, and workers and customers can be formed and informed. In this context, social attacks were studied and several problems were highlighted. Attacks based on phishing procedures are important in the context of SG companies. To avoid these, solutions to isolate the ICT from the outside must be adopted, and firewalls can identify and remove phishing emails sent to professional mailboxes. Therefore, limiting access to personal mailboxes from professional networks could help to reduce social attacks.

6. Conclusions

In this paper, we considered the SG as an SoS and modeled its architecture considering it is a CPS, consisting of physical layers, transmission/distribution layers, communication layers, then control/management layers. We showed that an IB, as a system integrated into an SG, was also an SoS, and it was also modeled as a CPS in its own right. By doing so, we were able to study security and privacy issues as a generic topic, but also to address these issues for each layer of the architecture and to propose specific solutions. With respect to energy management methods, these can be divided into conventional and intelligent methods. Conventional methods aim to manage energy without considering the comfort of the building occupants, whereas intelligent energy management methods take this into consideration. This family consists mostly of MPC and AI-based methods. MPC are preferentially used for DSM, which controls the energy consumer side but not the producer side. For this reason, AI-based methods are more promising, especially since they benefit

from new technologies such as cloud and edge computing, big data, IoT, and from some other AI techniques such as ML and DL.

We also studied security attacks in AMI, classified by OSI communication layers. Privacy leaks based on data and metadata were also identified, and we presented some examples of exploitation of this information by an attacker, e.g., the launch of more powerful targeted attacks. As a result of such security and privacy problems, users as consumers can be distrustful of the benefits of SG and its deployment, potentially slowing its adoption. In addition, we identified countermeasures appropriate for constrained networks. First, some standards define prevention solutions as either encryption or authentication on the basis of their cryptographic mechanisms, but these are often deployed in the SG without efficient implementation. Secondly, the detection of attacks with IDS can make it possible to be alert to attackers, but classical IDS are too heavy to be employed in AMI, while lightweight IDS retains some unsolved issues. Finally, dedicated countermeasures were presented according to the security and privacy attacks identified. This study allows us to highlight unresolved issues in order to improve the security, privacy and trust in the SG. Future research directions from both technical and human perspectives aiming towards the enhancement of security were also provided in order to help researchers further advance this field, which is vital for the optimal operation of the SG as a power system of the future, which has become a reality.

Author Contributions: Conceptualization, A.L., J.D.S. and C.M.; methodology, A.L. and C.M.; formal analysis, A.L., J.D.S., G.T. and Z.B.; investigation, A.L., J.D.S., G.T., Z.B., C.M. and O.C.; data curation, A.L., J.D.S., G.T. and C.M.; writing—original draft preparation, A.L., J.D.S., G.T., Z.B. and C.M.; writing—review and editing, A.L., J.D.S., G.T., Z.B., C.M. and O.C. All authors have read and agreed to the published version of the manuscript.

Funding: The work presented in this paper has not received external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Acronyms

AI	Artificial Intelligence
AMI	Advanced metering infrastructure
ANN	Artificial neural network
BAS	Building Automation System
BEMS	Building Energy Management System
CNN	Convolutional neural network
CPS	Cyber-Physical System
CPSoS	Cyber-Physical System of Systems
DL	Deep learning
DoS	Denial of Service
DR	Demand response
DSM	Demand Side Management
EC	Edge computing
EV	Electrical vehicle
FLA	Fuzzy logic algorithm
FLC	Fuzzy logic controller
GW	Gateway
HAN	Home Area Network
HEMS	Home Energy Management System
HMI	Human-Machine Interface
IB	Intelligent building

ICT	Information and communications technology
IDPS	Intrusion detection and prevention system
IDS	Intrusion Detection System
IoE	Internet of energy
MAC	Medium access control
MAS	Multiagent system
MG	Electrical microgrid
MITM	Man-in-the-Middle
ML	Machine learning
MPC	Model-based predictive control
NAN	Neighborhood Area Network
NZEB	Net-Zero Energy Building
OUI	Organizationally Unique Identifier
PEB	Positive Energy Building
PMU	Phasor measurement unit
PV	Photovoltaic
QoS	Quality of service
RNN	Recurrent neural network
RTS	Request to Send
SCADA	Supervisory control and data acquisition
SG	Smart Grid
SH	Smart home
SM	Smart meter
SoS	System of Systems
WAN	Wide Area Network
ZEB	Zero Energy Building

References

1. Ipakchi, A.; Albuyeh, F. Grid of the future. *IEEE Power Energy Mag.* **2009**, *7*, 52–62. [CrossRef]
2. Gharavi, H.; Ghafurian, R. Smart Grid: The electric energy system of the future [Scanning the issue]. *Proc. IEEE* **2011**, *99*, 917–921. [CrossRef]
3. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* **2020**, *146*, 2589–2625. [CrossRef]
4. Joseph, A.; Balachandra, P. Smart grid to energy internet: A systematic review of transitioning electricity systems. *IEEE Access* **2020**, *8*, 215787–215805. [CrossRef]
5. Mahmud, K.; Khan, B.; Ravishankar, J.; Ahmadi, A.; Siano, P. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. *Renew. Sustain. Energy Rev.* **2020**, *127*, 109840. [CrossRef]
6. Bie, Z.; Lin, Y.; Li, G.; Li, F. Battling the extreme: A study on the power system resilience. *Proc. IEEE* **2017**, *105*, 1253–1266. [CrossRef]
7. Gellings, C.W.; Samotyj, M. Smart Grid as advanced technology enabler of demand response. *Energy Effic.* **2013**, *6*, 685–694. [CrossRef]
8. Wormuth, B.; Wang, S.; Dehghanian, P.; Barati, M.; Estebsari, A.; Filomena, T.P.; Kapourchali, M.H.; Lejeune, M.A. Electric power grids under high-absenteeism pandemics: History, context, response, and opportunities. *IEEE Access* **2020**, *8*, 215727–215747. [CrossRef]
9. de C Henshaw, M.J. Systems of systems, cyber-physical systems, the internet-of-things . . . whatever next? *Insight* **2016**, *19*, 51–54. [CrossRef]
10. Yu, X.; Xue, Y. Smart grids: A cyber–physical systems perspective. *Proc. IEEE* **2016**, *104*, 1058–1070. [CrossRef]
11. Chapurlat, V.; Daclin, N. System interoperability: Definition and proposition of interface model in MBSE Context. *IFAC Proc. Vol.* **2012**, *45–46*, 1523–1528. [CrossRef]
12. Masior, J.; Schneider, B.; Kürümlüoglu, M.; Riedel, O. Beyond Model-Based Systems Engineering towards Managing Complexity. *Procedia CIRP* **2020**, *91*, 325–329. [CrossRef]
13. Penya, Y.K.; Borges, C.E.; Haase, J.; Bruckner, D. Smart Buildings and the Smart Grid. In Proceedings of the 39th Annual Conference of the IEEE Industrial Electronics Society (IECON), Vienna, Austria, 10–13 November 2013. [CrossRef]
14. Mofidi, F.; Akbari, H. Intelligent buildings: An overview. *Energy Build.* **2020**, *223*, 110192. [CrossRef]
15. Tang, H.; Wang, S.; Li, H. Flexibility categorization, sources, capabilities and technologies for energy-flexible and grid-responsive buildings: State-of-the-art and future perspective. *Energy* **2021**, *219*, 119598. [CrossRef]
16. Llaria, A.; Terrasson, G.; Curea, O.; Jiménez, J. Application of wireless sensor and actuator networks to achieve intelligent microgrids: A promising approach towards a global smart grid deployment. *Appl. Sci.* **2016**, *6*, 61. [CrossRef]
17. Adu-Kankam, K.O.; Camarinha-Matos, L.M. Towards collaborative Virtual Power Plants: Trends and convergence. *Sustain. Energy Grids Netw.* **2018**, *16*, 217–230. [CrossRef]

18. Jia, M.; Komeily, A.; Wang, Y.; Srinivasan, R.S. Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. *Autom. Constr.* **2019**, *101*, 111–126. [CrossRef]
19. Ahmad, T.; Zhang, D. Using the internet of things in smart energy systems and networks. *Sustain. Cities Soc.* **2021**, *68*, 102783. [CrossRef]
20. Llaria, A.; Jiménez, J.; Curea, O. Study on communication technologies for the optimal operation of smart grids. *Trans. Emerg. Tel. Tech.* **2014**, *25*, 1009–1019. [CrossRef]
21. Kabalci, Y. A survey on smart metering and smart grid communication. *Renew. Sustain. Energy Rev.* **2016**, *57*, 302–318. [CrossRef]
22. Wang, S. Making buildings smarter, grid-friendly, and responsive to smart grids. *Sci. Technol. Built Environ.* **2016**, *22*, 629–632. [CrossRef]
23. Taveres-Cachat, E.; Grynning, S.; Thomsen, J.; Selkowitz, S. Responsive building envelope concepts in zero emission neighborhoods and smart cities—A roadmap to implementation. *Build. Environ.* **2019**, *149*, 446–457. [CrossRef]
24. Kim, H.; Choi, H.; An, J.; Yeom, S.; Hong, T. A systematic review of the smart energy conservation system: From smart homes to sustainable smart cities. *Renew. Sustain. Energy Rev.* **2021**, *140*, 110755. [CrossRef]
25. Moslehi, K.; Kumar, R. A reliability perspective of the smart grid. *IEEE Trans. Smart Grid* **2010**, *1*, 57–64. [CrossRef]
26. Chen, T.M.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer* **2011**, *44*, 91–93. [CrossRef]
27. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
28. Tan, S.; Wu, Y.; Xie, P.; Guerrero, J.M.; Vasquez, J.C.; Abusorrah, A. New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience. *IEEE Electrif. Mag.* **2020**, *8*, 98–106. [CrossRef]
29. Mylrea, M.; Gourisetti, S.N.G.; Nicholls, A. An Introduction to Buildings Cybersecurity Framework. In Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, USA, 27 November–1 December 2017. [CrossRef]
30. Lopes, A.J.; Lezama, R.; Pineda, R. Model Based Systems Engineering for Smart Grids as Systems of Systems. *Procedia Comput. Sci.* **2011**, *6*, 441–450. [CrossRef]
31. NIST—National Institute of Standard and Technology. NIST—National Institute of Standard and Technology. NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0. In *Special Publication (NIST SP)–1108*; Locke, G., Gallagher, P.D., Eds.; Office of the National Coordinator for Smart Grid Interoperability: Gaithersburg, MD, USA, 2010. [CrossRef]
32. Nielsen, C.B.; Larsen, P.G.; Fitzgerald, J.; Woodcock, J.; Peleska, J. Systems of Systems Engineering: Basic concepts, model-based techniques, and research directions. *ACM Comput. Surv.* **2015**, *48*, 18. [CrossRef]
33. Maier, M.W. Architecting principles for systems-of-systems. *Syst. Eng.* **1998**, *1*, 267–284. [CrossRef]
34. Merlo, C.; Girard, P. Information system modelling for engineering design co-ordination. *Comput. Ind.* **2004**, *55*, 317–334. [CrossRef]
35. Marashi, K.; Sarvestani, S.S.; Hurson, A.R. Consideration of cyber-physical interdependencies in reliability modeling of smart grids. *IEEE Trans. Sustain. Comput.* **2018**, *3*, 73–83. [CrossRef]
36. Hossain, M.M.; Peng, C. Cyber–physical security for on-going smart grid initiatives: A survey. *IET Cyber Phys. Syst. Theor. Appl.* **2020**, *5*, 233–244. [CrossRef]
37. Monostori, L. Cyber-physical production systems: Roots, Expectations and R&D challenges. *Procedia CIRP* **2014**, *17*, 9–13. [CrossRef]
38. Rudtsch, V.; Gausemeier, J.; Gesing, J.; Mittag, T.; Peter, S. Pattern-based business model development for cyber-physical production systems. *Procedia CIRP* **2014**, *25*, 313–319. [CrossRef]
39. Al-Mhiqani, M.N.; Ahmad, R.; Abdulkareem, K.H.; Ali, N.S. Investigation study of cyber-physical systems: Characteristics, application domains, and security challenges. *ARPN J. Eng. Appl. Sci.* **2017**, *12*, 6557–6567.
40. Nunes, D.S.; Zhang, P.; Sá Silva, J. A survey on Human-in-the-Loop applications towards an Internet of All. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 944–965. [CrossRef]
41. Cimini, C.; Pirola, F.; Pinto, R.; Cavalieri, S. A human-in-the-loop manufacturing control architecture for the next generation of production systems. *J. Manuf. Syst.* **2020**, *54*, 258–271. [CrossRef]
42. Zhao, J.; Wen, F.; Xue, Y.; Li, X.; Dong, Z. Cyber-physical power systems Architecture, implementation techniques and challenges. *Autom. Electr. Power Syst.* **2010**, *34*, 1–7.
43. Masera, M.; Bompard, E.F.; Profumo, F.; Hadjsaid, N. Smart (electricity) grids for smart cities: Assessing roles and societal impacts. *Proc. IEEE* **2018**, *106*, 613–625. [CrossRef]
44. Wong, J.K.W.; Li, H.; Wang, S.W. Intelligent building research: A review. *Autom. Constr.* **2005**, *14*, 143–159. [CrossRef]
45. Manic, M.; Amarasinghe, K.; Rodriguez-Andina, J.J.; Rieger, C. Intelligent buildings of the future: Cyberaware, deep learning powered, and human interacting. *IEEE Ind. Electron. Mag.* **2016**, *10*, 32–49. [CrossRef]
46. Dakheel, J.A.; Del Pero, C.; Aste, N.; Leonforte, F. Smart buildings features and key performance indicators: A review. *Sustain. Cities Soc.* **2020**, *61*, 102328. [CrossRef]
47. Lee, E.A. Cyber-Physical Systems—Are Computing Foundations Adequate? In Proceedings of the Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, TX, USA, 16–17 October 2006.
48. Jimada-Ojuolape, B.; Teh, J. Impact of the integration of information and communication technology on power system reliability: A review. *IEEE Access* **2020**, *8*, 24600–24615. [CrossRef]
49. Kolokotsa, D. The role of smart grids in the building sector. *Energy Build.* **2016**, *116*, 703–708. [CrossRef]

50. Lawrence, T.M.; Boudreau, M.C.; Helsen, L.; Henze, G.; Mohammadpour, J.; Noonan, D.; Patteeuw, D.; Pless, S.; Watson, R.T. Ten questions concerning integrating smart buildings into the smart grid. *Build. Environ.* **2016**, *108*, 273–283. [CrossRef]
51. Li, C.Z.; Lai, X.; Xiao, B.; Tam, V.W.Y.; Guo, S.; Zhao, Y. A holistic review on life cycle energy of buildings: An analysis from 2009 to 2019. *Renew. Sustain. Energy Rev.* **2020**, *134*, 110372. [CrossRef]
52. Krarti, M.; Aldubyan, M. Review analysis of COVID-19 impact on electricity demand for residential buildings. *Renew. Sustain. Energy Rev.* **2021**, 110888. [CrossRef]
53. Takigawa, T.; Wang, B.L.; Sakano, N.; Wang, D.H.; Ogino, K.; Kishi, R. A longitudinal study of environmental risk factors for subjective symptoms associated with sick building syndrome in new dwellings. *Sci. Total Environ.* **2009**, *407*, 5223–5228. [CrossRef] [PubMed]
54. Lee, D.; Cheng, C.C. Energy savings by energy management systems: A review. *Renew. Sustain. Energy Rev.* **2016**, *56*, 760–777. [CrossRef]
55. Yang, T.; Clements-Croome, D.; Marson, M. Building energy management systems. In *Encyclopedia of Sustainable Technologies*; Abraham, M.A., Ed.; Elsevier: Amsterdam, The Netherlands, 2017; pp. 291–309. [CrossRef]
56. Domingues, P.; Carreira, P.; Vieira, R.; Kastner, W. Building automation systems: Concepts and technology review. *Comp. Stand. Inter.* **2016**, *45*, 1–12. [CrossRef]
57. Kumar, A.; Singh, A.; Kumar, M.; Singh, M.K.; Mahanta, P.; Mukhopadhyay, S.C. Sensing technologies for monitoring intelligent buildings: A review. *IEEE Sens. J.* **2018**, *18*, 4847–4860. [CrossRef]
58. Hannan, M.A.; Faisal, M.; Ker, P.J.; Mun, L.H.; Parvin, K.; Mahlia, T.M.I.; Blaabjerg, F. A review of internet of energy based building energy management systems: Issues and recommendations. *IEEE Access* **2018**, *6*, 38997–39014. [CrossRef]
59. Sartori, I.; Napolitano, A.; Voss, K. Net zero energy buildings: A consistent definition framework. *Energy Build.* **2012**, *48*, 220–232. [CrossRef]
60. Cao, X.; Dai, X.; Liu, J. Building energy-consumption status worldwide and the state-of-the-art technologies for zero-energy buildings during the past decade. *Energy Build.* **2016**, *128*, 198–213. [CrossRef]
61. Wei, W.; Skye, H.M. Residential net-zero energy buildings: Review and perspective. *Renew. Sustain. Energy Rev.* **2021**, *142*, 110859. [CrossRef]
62. Magrini, A.; Lentini, G.; Cuman, S.; Bodrato, A.; Marenco, L. From nearly zero energy buildings (NZEB) to positive energy buildings (PEB): The next challenge—The most recent European trends with some notes on the energy analysis of a forerunner PEB example. *Dev. Built Environ.* **2020**, *3*, 100019. [CrossRef]
63. Zhou, B.; Li, W.; Chan, K.W.; Cao, Y.; Kuang, Y.; Liu, X.; Wang, X. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renew. Sustain. Energy Rev.* **2016**, *61*, 30–40. [CrossRef]
64. Leitão, J.; Gil, P.; Ribeiro, B.; Cardoso, A. A survey on home energy management. *IEEE Access* **2020**, *8*, 5699–5722. [CrossRef]
65. Zafar, U.; Bayhan, S.; Sanfilippo, A. Home energy management system concepts, configurations, and technologies for the smart grid. *IEEE Access* **2020**, *8*, 119271–119286. [CrossRef]
66. Hong, T.; Yan, D.; D'Oca, S.; Chen, C. Ten questions concerning occupant behavior in buildings: The big picture. *Build. Environ.* **2017**, *114*, 518–530. [CrossRef]
67. Nguyen, T.A.; Aiello, M. Energy intelligent buildings based on user activity: A survey. *Energy Build.* **2013**, *56*, 244–257. [CrossRef]
68. Palensky, P.; Dietrich, D. Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Trans. Ind. Inf.* **2011**, *7*, 381–388. [CrossRef]
69. Mariano-Hernández, D.; Hernández-Callejo, L.; Zorita-Lamadrid, A.; Duque-Pérez, O.; Santos García, F. A review of strategies for building energy management system: Model predictive control, demand side management, optimization, and fault detect & diagnosis. *J. Build. Eng.* **2021**, *33*, 101692. [CrossRef]
70. Chen, Y.; Xu, P.; Gu, J.; Schmidt, F.; Li, W. Measures to improve energy demand flexibility in buildings for demand response (DR): A review. *Energy Build.* **2018**, *177*, 125–139. [CrossRef]
71. Shareef, H.; Ahmed, M.S.; Mohamed, A.; Al Hassan, E. Review on home energy management system considering demand responses, smart technologies, and intelligent controllers. *IEEE Access* **2018**, *6*, 24498–24509. [CrossRef]
72. Beaudin, M.; Zareipour, H. Home energy management systems: A review of modelling and complexity. *Renew. Sustain. Energy Rev.* **2015**, *45*, 318–335. [CrossRef]
73. Shakeri, M.; Pasupuleti, J.; Amin, N.; Rokonuzzaman, M.; Low, F.W.; Yaw, C.T.; Asim, N.; Samsudin, N.A.; Tiong, S.K.; Hen, C.K.; et al. An overview of the building energy management system considering the demand response programs, smart strategies and smart grid. *Energies* **2020**, *13*, 3299. [CrossRef]
74. Liu, Y.; Yu, N.; Wang, W.; Guan, X.; Xu, Z.; Dong, B.; Liu, T. Coordinating the operations of smart buildings in smart grids. *Appl. Energy* **2018**, *228*, 2510–2525. [CrossRef]
75. Liu, N.; Wang, J.; Yu, X.; Ma, L. Hybrid energy sharing for smart building cluster with CHP system and PV prosumers: A coalitional game approach. *IEEE Access* **2018**, *6*, 34098–34108. [CrossRef]
76. Shaikh, P.H.; Nor, N.B.M.; Nallagownden, P.; Elamvazuthi, I.; Ibrahim, T. A review on optimized control systems for building energy and comfort management of smart sustainable buildings. *Renew. Sustain. Energy Rev.* **2014**, *34*, 409–429. [CrossRef]
77. Freire, V.A.; Arruda, L.V.R.; Bordons, C.; Teno, G. Home Energy Management for a AC/DC Microgrid Using Model Predictive Control. In Proceedings of the International Conference on Smart Energy Systems and Technologies (SEST), Porto, Portugal, 9–11 September 2019. [CrossRef]

78. Novickij, I.; Joós, G. Model Predictive Control-Based Approach for Microgrid Energy Management. In Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019. [CrossRef]
79. Hamidi, M.; Bouattane, O. Commercial Building Energy Management Design for HVAC System Based on Fuzzy Logic. In Proceedings of the 7th International Renewable and Sustainable Energy Conference (IRSEC), Agadir, Morocco, 27–30 November 2019. [CrossRef]
80. Ghaffar, M.; Naseer, N.; Sheikh, S.R.; Naved, M.; Aziz, U.; Koreshi, Z.U. Electrical Energy Management of Building Using Fuzzy Control. In Proceedings of the International Conference on Robotics and Automation in Industry (ICRAI), Rawalpindi, Pakistan, 21–22 October 2019. [CrossRef]
81. Tingting, H.; Abhisek, U. Design of Fuzzy Logic Based Controller for Energy Efficient Operation in Building. In Proceedings of the 42nd Annual Conference of the IEEE Industrial Electronics Society IECON, Florence, Italy, 23–26 October 2016. [CrossRef]
82. Kontogiannis, D.; Bargiotas, D.; Daskalopulu, A. Fuzzy control system for smart energy management in residential buildings based on environmental data. *Energies* **2021**, *14*, 752. [CrossRef]
83. Aung, H.N.; Khambadkone, A.M.; Srinivasan, D.; Logenthiran, T. Agent-based intelligent control for real-time operation of a microgrid. In Proceedings of the 2010 Joint International Conference on Power Electronics, Drives and Energy Systems & 2010 Power India, New Delhi, India, 20–23 December 2010. [CrossRef]
84. Oliveira, P.; Gomes, L.; Pinto, T.; Faria, P.; Vale, Z.; Morais, H. Load Control Timescales Simulation in a Multi-Agent Smart Grid Platform. In Proceedings of the IEEE PES ISGT Europe, Lyngby, Denmark, 6–9 October 2013. [CrossRef]
85. McArthur, S.D.J.; Davidson, E.M.; Catterson, V.M.; Dimeas, A.L.; Hatziargyriou, N.D.; Ponci, F.; Funabashi, T. Multi-agent systems for power engineering applications—Part I: Concepts, approaches, and technical challenges. *IEEE Trans. Power Syst.* **2007**, *22*, 1743–1752. [CrossRef]
86. Khamphanchai, W.; Pipattanasomporn, M.; Rahman, S. A Multi-Agent System for Restoration of an Electric Power Distribution Network with Local Generation. In Proceedings of the Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012. [CrossRef]
87. Chen, M.; McArthur, S.D.J.; Kockar, I.; Pitt, J. Evaluating a MAS Architecture for Flexible Distribution Power Flow Management. In Proceedings of the 18th International Conference on Intelligent System Application to Power Systems, Porto, Portugal, 11–16 September 2015. [CrossRef]
88. Lagorse, J.; Paire, D.; Miraoui, A. A multi-agent system for energy management of distributed power sources. *Renew. Energy* **2010**, *35*, 174–182. [CrossRef]
89. Ferber, J. *Multi-Agent Systems. An Introduction to Distributed Artificial Intelligence*; Addison Wesley: London, UK, 1999.
90. Cirrincione, M.; Cossentino, M.; Gaglio, S.; Hilaire, V.; Koukam, A.; Pucci, M.; Sabatucci, L.; Vitale, G. Intelligent Energy Management System. In Proceedings of the 7th IEEE International Conference on Industrial Informatics, Cardiff, UK, 23–26 June 2009. [CrossRef]
91. Boussaada, Z.; Curea, O.; Camblong, H.; Mrabet, N.B.; Hacala, A. Multi-agent systems for the dependability and safety of microgrids. *Int. J. Interact. Des. Manuf.* **2016**, *10*, 1–13. [CrossRef]
92. Dimeas, A.L.; Hatziargyriou, N.D. A MAS Architecture for Microgrids Control. In Proceedings of the 13th International Conference on Intelligent Systems Application to Power Systems, Arlington, VA, USA, 6–10 November 2005. [CrossRef]
93. Iksan, N.; Udayanti, E.D.; Arfriandi, A.; Widodo, D.A. Automatic Control Using Fuzzy Techniques for Energy Management on Smart Building. In Proceedings of the International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), Surabaya, Indonesia, 26–27 November 2018. [CrossRef]
94. Feng, C.; Wang, Y.; Chen, Q.; Ding, Y.; Strbac, G.; Kang, C. Smart grid encounters edge computing: Opportunities and applications. *Adv. Appl. Energy* **2021**, *1*, 100006. [CrossRef]
95. Runge, J.; Zmeureanu, R. A review of deep learning techniques for forecasting energy use in buildings. *Energies* **2021**, *14*, 608. [CrossRef]
96. Boussaada, Z.; Curea, O.; Camblong, H.; Mrabet, N.B. Energy management for embedded microgrid using multi agent system. In Proceedings of the 7th International Conference on Automation, Control Engineering & Computer Science (ACECS), Sousse, Tunisia, 12–13 October 2020; pp. 26–31. Available online: http://ipco-co.com/PET_Journal/ACECS%20Proceedings/A-3.pdf (accessed on 25 March 2021).
97. Khan, Z.A.; Hussain, T.; Ullah, A.; Rho, S.; Lee, M.; Baik, S.W. Towards efficient electricity forecasting in residential and commercial buildings: A novel hybrid CNN with a LSTM-AE based framework. *Sensors* **2020**, *20*, 1399. [CrossRef] [PubMed]
98. Verma, A.; Prakash, S.; Srivastava, V.; Kumar, A.; Mukhopadhyay, S.C. Sensing, controlling, and IoT infrastructure in smart building: A review. *IEEE Sens. J.* **2019**, *19*, 9036–9046. [CrossRef]
99. Yaïci, W.; Krishnamurthy, K.; Entchev, E.; Longo, M. Recent advances in Internet of Things (IoT) infrastructures for building energy systems: A review. *Sensors* **2021**, *21*, 2152. [CrossRef]
100. Iqbal, J.; Khan, M.; Talha, M.; Farman, H.; Jan, B.; Muhammad, A.; Khattak, H.A. A generic internet of things architecture for controlling electrical energy consumption in smart homes. *Sustain. Cities Soc.* **2018**, *43*, 443–450. [CrossRef]
101. Karthick, T.; Charles Raja, S.; Jeslin Drusila Nesamalar, J.; Chandrasekaran, K. Design of IoT based smart compact energy meter for monitoring and controlling the usage of energy and power quality issues with demand side management for a commercial building. *Sustain. Energy Grids Netw.* **2021**, *26*, 100454. [CrossRef]

102. Hossain, M.; Weng, Z.; Schiano-Phan, R.; Scott, D.; Lau, B. Application of IoT and BEMS to visualise the environmental performance of an educational building. *Energies* **2020**, *13*, 4009. [CrossRef]
103. Usman, A.; Haider Shami, S. Evolution of Communication Technologies for Smart Grid applications. *Renew. Sustain. Energy Rev.* **2013**, *19*, 191–199. [CrossRef]
104. Ancillotti, E.; Bruno, R.; Conti, M. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun.* **2013**, *36*, 1665–1697. [CrossRef]
105. Shaukat, N.; Ali, S.M.; Mehmood, C.A.; Khan, B.; Jawad, M.; Farid, U.; Ullah, Z.; Anwar, S.M.; Majid, M. A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid. *Renew. Sustain. Energy Rev.* **2018**, *81*, 1453–1475. [CrossRef]
106. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergüt, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
107. Saleem, Y.; Crespi, N.; Rehmani, M.H.; Copeland, R. Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions. *IEEE Access* **2019**, *7*, 62962–63003. [CrossRef]
108. Zhu, Z.; Lambotharan, S.; Chin, W.H.; Fan, Z. Overview of demand management in smart grid and enabling wireless communication technologies. *IEEE Wirel. Commun.* **2012**, *19*, 48–56. [CrossRef]
109. Ahmed, S.; Gondal, T.M.; Adil, M.; Malik, S.A.; Qureshi, R. A Survey on Communication Technologies in Smart Grid. In Proceedings of the IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), Bangkok, Thailand, 19–23 March 2019. [CrossRef]
110. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Review of communication technologies for smart homes/building applications. In Proceedings of the IEEE Innovative Smart Grid Technologies—Asia (ISGT ASIA), Bangkok, Thailand, 3–6 November 2015. [CrossRef]
111. Vega, A.M.; Santamaria, F.; Rivas, E. Modeling for home electric energy management: A review. *Renew. Sustain. Energy Rev.* **2015**, *52*, 948–959. [CrossRef]
112. Emmanuel, M.; Rayudu, R. Communication technologies for smart grid applications: A survey. *J. Netw. Comput. Appl.* **2016**, *74*, 133–148. [CrossRef]
113. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38. [CrossRef]
114. Lohia, K.; Jain, Y.; Patel, C.; Doshi, N. Open Communication Protocols for Building Automation Systems. *Procedia Comput. Sci.* **2019**, *160*, 723–727. [CrossRef]
115. Gungor, V.; Hancke, G. Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Trans. Ind. Electron.* **2009**, *56*, 4258–4265. [CrossRef]
116. Risteska Stojkoska, B.L.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
117. Lobaccaro, G.; Carlucci, S.; Löfström, E. A review of systems and technologies for smart homes and smart grids. *Energies* **2016**, *9*, 348. [CrossRef]
118. Mocrii, D.; Chen, Y.; Musilek, P. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet Things* **2018**, *1–2*, 81–98. [CrossRef]
119. De Almeida, L.F.F.; Dos Santos, J.R.; Melo Pereira, L.A.; Cerqueira Sodré, A., Jr.; Leonel Mendes, L.; Rodrigues, J.J.P.C.; Rabelo, R.A.L.; Alberti, A.M. Control networks and smart grid teleprotection: Key aspects, technologies, protocols, and case-studies. *IEEE Access* **2020**, *8*, 174049–174079. [CrossRef]
120. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
121. Granzer, W.; Praus, F.; Kastner, W. Security in Building Automation Systems. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3622–3630. [CrossRef]
122. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
123. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
124. Ciholas, P.; Lennie, A.; Sadigova, P.; Such, J.M. The security of smart buildings: A systematic literature review. *arXiv* **2019**, arXiv:1901.05837, under review.
125. Deshmukh, A.P.A.G.; Qureshi, D. Transparent data encryption-Solution for security of database contents. *IJACSA* **2011**, *2*, 25–28. [CrossRef]
126. Lombardi, F.; Aniello, L.; De Angelis, S.; Margheri, A.; Sassone, V. A Blockchain-Based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids. In Proceedings of the Living in the Internet of Things Conference: Cybersecurity of the IoT, London, UK, 28–29 March 2018. [CrossRef]
127. Butun, I.; Lekidis, A.; Dos Santos, D. Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities. In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP), Valletta, Malta, 25–27 February 2020. [CrossRef]

128. Pöhls, H.C.; Angelakis, V.; Suppan, S.; Fischer, K.; Oikonomou, G.; Tragos, E.Z.; Mouroutis, T. RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects. In Proceedings of the IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Istanbul, Turkey, 6–9 April 2014. [CrossRef]
129. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
130. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. In Proceedings of the 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018. [CrossRef]
131. Osisiogu, U. A review on Cyber-Physical Security of Smart Buildings and Infrastructure. In Proceedings of the 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 10–12 December 2019. [CrossRef]
132. Znaidi, W. Quelques Propositions de Solutions Pour la Sécurité des Réseaux de Capteurs Sans Fil. Ph.D. Thesis, Institut National des Sciences Appliquées (INSA), Lyon, France, 10 October 2010.
133. Khaund, K. Cybersecurity in Smart Buildings Inaction is not Option any More. *Frost Sullivan Collab. Ind. Perspect.* **2015**, *9835-19*, 1–37.
134. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
135. Zheng, J.; Lee, M.J.; Anshel, M. Toward secure low rate wireless personal area networks. *IEEE Trans. Mob. Comput.* **2006**, *5*, 1361–1373. [CrossRef]
136. Dhunna, G.S. Low Power MAC Security Mechanisms for WSNs in a Smart Grid Environment. Ph.D. Thesis, Faculty of Graduate Studies and Research, University of Regina, Regina, SK, Canada, 4 August 2017.
137. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time synchronization attack in smart grid: Impact and analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [CrossRef]
138. Zhang, Z.; Wu, J.; Deng, J.; Qiu, M. Jamming ACK Attack to Wireless Networks and a Mitigation Approach. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), New Orleans, LA, USA, 30 November–4 December 2008. [CrossRef]
139. Sajjad, S.M.; Yousaf, M. Security analysis of IEEE 802.15. 4 MAC in the context of Internet of Things (IoT). In Proceedings of the Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 12–13 June 2014. [CrossRef]
140. Ghildiyal, S.; Mishra, A.K.; Gupta, A.; Garg, N. Analysis of denial of service (dos) attacks in wireless sensor. *IJRET* **2014**, *3*, 140–143. [CrossRef]
141. Dos Santos, J.; Terrasson, G.; Llaria, A. Improving Low Power Listening (LPL) Mechanism to Save Energy Consumption. In Proceedings of the IEEE Sensors, Rotterdam, The Netherlands, 25–28 October 2020. [CrossRef]
142. Raymond, D.R.; Marchany, R.C.; Brownfield, M.I.; Midkiff, S.F. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE Trans. Veh. Technol.* **2009**, *58*, 367–380. [CrossRef]
143. Hijazi, S.; Obaidat, M.S. Address resolution protocol spoofing attacks and security approaches: A survey. *Secur. Priv.* **2019**, *2*. [CrossRef]
144. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. *Energies* **2018**, *11*, 2360. [CrossRef]
145. Kulkarni, S.; Rahul, R.K.; Shreyas, R.; Nagasundari, S.; Honnavalli, P.B. MITM Intrusion Analysis for Advanced Metering Infrastructure Communication in a Smart Grid Environment. In Proceedings of the 3rd International Conference on Computational Intelligence, Security and Internet of Things, Agartala, India, 29–30 December 2020. [CrossRef]
146. Darwish, I.; Igbe, O.; Celebi, O.; Saadawi, T.; Soryal, J. Smart Grid DNP3 Vulnerability Analysis and Experimentation. In Proceedings of the IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015. [CrossRef]
147. Malik, R.; Sehrawat, H.; Singh, Y. Comprehensive study of selective forwarding attack in wireless sensor networks. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1–10. [CrossRef]
148. Ali, S.; Khan, M.A.; Ahmad, J.; Malik, A.W.; ur Rehman, A. Detection and Prevention of Black Hole Attacks in IOT & WSN. In Proceedings of the Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018. [CrossRef]
149. Ibhaze, A.E.; Akpabio, M.U.; John, S.N. A Review on Smart Grid Network Security Issues over 6LoWPAN. In Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC'17), Cambridge, UK, 22–23 March 2017. [CrossRef]
150. Holmberg, D.G.; Evans, D. BACnet wide area network security threat assessment. *NIST Interag. Intern. Rep. (NISTIR)* **2003**, *7009*. [CrossRef]
151. Swathi, B.H.; Gururaj, H.L. A critical analysis on network layer attacks in wireless sensor network. *IRJET* **2018**, *5*, 377–384.
152. Kumari, D.; Singh, K.; Manjul, M. Performance evaluation of sybil attack in cyber physical system. *Procedia Comput. Sci.* **2020**, *167*, 1013–1027. [CrossRef]
153. Kaur, J.; Tonejc, J.; Wendzel, S.; Meier, M. Securing BACnet's Pitfalls. In Proceedings of the IFIP International Information Security and Privacy Conference, Hamburg, Germany, 26–28 May 2015. [CrossRef]
154. Prakash, R.A.; Jeyaseelan, W.S.; Jayasankar, T. Detection, prevention and mitigation of wormhole attack in wireless adhoc network by coordinator. *Appl. Mat.* **2018**, *12*, 233–237. [CrossRef]

155. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Pan, L. Puppet attack: A denial of service attack in advanced metering infrastructure network. *J. Netw. Comput. Appl.* **2016**, *59*, 325–332. [CrossRef]
156. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* **2017**, *13*. [CrossRef]
157. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
158. Suciu, G.; Sachian, M.A.; Dobrea, M.; Istrate, C.I.; Petrache, A.L.; Vulpe, A.; Vochin, M. Securing the smart grid: A blockchain-based secure smart energy system. In Proceedings of the 54th International Universities Power Engineering Conference (UPEC), Bucharest, Romania, 3–6 September 2019. [CrossRef]
159. Rajesh, L.; Satyanarayana, P. Vulnerability analysis and enhancement of security of communication protocol in industrial control systems. *Helix* **2019**, *9*, 5122–5127. Available online: https://helixscientific.pub/index.php/home/article/view/6 (accessed on 28 March 2021).
160. Shin, I.; Cho, M. On Localized Countermeasure against reactive jamming attacks in smart grid wireless mesh networks. *Appl. Sci.* **2018**, *8*, 2340. [CrossRef]
161. Song, T.; Zhou, K.; Li, T. CDMA system design and capacity analysis under disguised jamming. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2487–2498. [CrossRef]
162. Al-Kahtani, M.S.; Karim, L. A survey on attacks and defense mechanisms in smart grids. *Int. J. Comput. Eng. Inf. Technol.* **2019**, *11*, 94–100.
163. Liu, H.; Ma, H.; El Zarki, M.; Gupta, S. Error control schemes for networks: An overview. *Mobile Netw. Appl.* **1997**, *2*, 167–182. [CrossRef]
164. Falconer, D.D.; Adachi, F.; Gudmundson, B. Time division multiple access methods for wireless personal communications. *IEEE Commun. Mag.* **1995**, *33*, 50–57. [CrossRef]
165. Meghana, J.S.; Subashri, T.; Vimal, K.R. A Survey on ARP Cache Poisoning and Techniques for Detection and Mitigation. In Proceedings of the Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 16–18 March 2017. [CrossRef]
166. Khan, W.Z.; Xiang, Y.; Aalsalem, M.Y.; Arshad, Q. The selective forwarding attack in sensor networks: Detections and countermeasures. *IJWMT* **2012**, *2*, 33. [CrossRef]
167. Xin-Sheng, W.; Yong-Zhao, Z.; Shu-ming, X.; Liang-min, W. Lightweight Defense Scheme against Selective forwarding Attacks in Wireless Sensor Networks. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Zhangjiajie, China, 10–11 October 2009. [CrossRef]
168. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad. Hoc. Netw.* **2003**, *1*, 293–315. [CrossRef]
169. Coppolino, L.; D'Antonio, S.; Romano, L.; Spagnuolo, G. An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network Technologies. In Proceedings of the 5th International Conference on Critical Infrastructure (CRIS), Beijing, China, 20–22 September 2010. [CrossRef]
170. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil Attack in Sensor Networks: Analysis & Defenses. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, 27 April 2004. [CrossRef]
171. Arjuman, N.; Manickam, S.; Karuppayah, S.; Rehman, S.U. Review of Security Issues in IPv6 Router Discovery. In Proceedings of the 4th International Conference on Mathematical Sciences and Computer Engineering (ICMSCE), Langkawi, Malaysia, 4–5 May 2017.
172. Hu, L.; Evans, D. Using Directional Antennas to Prevent Wormhole Attacks. In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 5–6 February 2004.
173. Znaidi, W.; Minier, M.; Babau, J.P. Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information. In Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes, France, 15–18 September 2008. [CrossRef]
174. Gonzalez, H.; Gosselin-Lavigne, M.A.; Stakhanova, N.; Ghorbani, A.A. Chapter 13—The Impact of Application-Layer Denial-of-Service Attacks. In *Case Studies in Secure Computing: Achievements and Trends*; Issac, B., Israr, N., Eds.; CRC Press: Boca Raton, FL, USA, 2014. [CrossRef]
175. Hasankhani, A.; Hakimi, S.M.; Shafie-khah, M.; Asadolahi, H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106811. [CrossRef]
176. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
177. Hollick, M.; Nita-Rotaru, C.; Papadimitratos, P.; Perrig, A.; Schmid, S. Toward a taxonomy and attacker model for secure routing protocols. *ACM Sigcomm. Comp. Com.* **2017**, *47*, 43–48. [CrossRef]
178. Gunduz, M.Z.; Das, R. Analysis of Cyber-Attacks on Smart Grid Applications. In Proceedings of the International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018. [CrossRef]
179. Lisovich, M.A.; Mulligan, D.K.; Wicker, S.B. Inferring personal information from demand-response systems. *IEEE Secur. Priv.* **2010**, *8*, 11–20. [CrossRef]
180. Dos Santos, J.; Hennebert, C.; Lauradoux, C. Preserving privacy in secured ZigBee wireless sensor networks. In Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015. [CrossRef]

181. Luo, X.; Ji, X.; Park, M.S. Location privacy against traffic analysis attacks in wireless sensor networks. In Proceedings of the International Conference on Information Science and Applications, Seoul, Korea, 21–23 April 2010. [CrossRef]
182. Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C. Enhancing source-location privacy in sensor network routing. In Proceedings of the 25th IEEE international conference on distributed computing systems (ICDCS'05), Columbus, OH, USA, 6–10 June 2005. [CrossRef]
183. Deng, J.; Han, R.; Mishra, S. Countermeasures against traffic analysis attacks in wireless sensor networks. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 5–9 September 2005. [CrossRef]
184. Cooper, A.; Gont, F.; Thaler, D. Security and privacy considerations for ipv6 address generation mechanisms. *Netw. Work. Group RFC* **2016**, *7721*, 1–18. Available online: https://tools.ietf.org/html/rfc7721 (accessed on 28 March 2021).
185. Mundt, T.; Wickboldt, P. Security in building automation systems-a first analysis. In Proceedings of the International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), London, UK, 13–14 June 2016. [CrossRef]
186. Bonné, B.; Barzan, A.; Quax, P.; Lamotte, W. WiFiPi: Involuntary tracking of visitors at mass events. In Proceedings of the IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Madrid, Spain, 4–7 June 2013. [CrossRef]
187. Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based internet of things. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 794326. [CrossRef]
188. Sharma, V.; You, I.; Andersson, K.; Palmieri, F.; Rehmani, M.H.; Lim, J. Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. *IEEE Access* **2020**, *8*, 167123–167163. [CrossRef]
189. Kong, J.H.; Ang, L.M.; Seng, K.P. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. *J. Netw. Comput. Appl.* **2015**, *49*, 15–50. [CrossRef]
190. Daemen, J.; Rijmen, V. *AES Proposal: Rijndael*; NIST—National Institute of Standard and Technology: Gaithersburg, MD, USA, 1999.
191. Saho, N.J.G.; Ezin, E.C. Survey on Asymmetric Cryptographic Algorithms in Embedded Systems. *IJISRT* **2020**, *5*, 544–554.
192. Milanov, E. The RSA algorithm. *RSA Lab.* **2009**, 1–11. Available online: https://sites.math.washington.edu/~{}morrow/336_09/papers/Yevgeny.pdf (accessed on 28 March 2021).
193. Lara-Nino, C.A.; Diaz-Perez, A.; Morales-Sandoval, M. Elliptic curve lightweight cryptography: A survey. *IEEE Access* **2018**, *6*, 72514–72550. [CrossRef]
194. Fontaine, C.; Galand, F. A survey of homomorphic encryption for nonspecialists. *EURASIP J. Inf. Secur.* **2007**, *013801*, 1–10. [CrossRef]
195. Dutta, I.K.; Ghosh, B.; Bayoumi, M. Lightweight cryptography for internet of insecure things: A survey. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019. [CrossRef]
196. Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-hashing for message authentication. *Netw. Work. Group RFC* **1997**, *2104*, 1–11.
197. Ghosal, A.; Conti, M. Key management systems for smart grid advanced metering infrastructure: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2831–2848. [CrossRef]
198. Delaveau, F.; Mueller, A.; Ngassa, C.K.; Guillaume, R.; Molière, R.; Wunder, G. Perspectives of physical layer security (physec) for the improvement of the subscriber privacy and communication confidentiality at the air interface. *Perspectives* **2016**, *27*, 1–33.
199. Hennebert, C.; Dos Santos, J. Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet Things J.* **2014**, *1*, 384–398. [CrossRef]
200. Unwala, I.; Taqvi, Z.; Lu, J. IoT Security: Z-Wave and Thread. In Proceedings of the IEEE Green Technologies Conference (GreenTech), Austin, TX, USA, 4–6 April 2018. [CrossRef]
201. Kambourakis, G.; Kolias, C.; Geneiatakis, D.; Karopoulos, G.; Makrakis, G.M.; Kounelis, I. A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks. *Symmetry* **2020**, *12*, 579. [CrossRef]
202. Azzouz, L.B.; Aouini, I. A lightweight IPsec-based energy home area networks. *Trans. Emerg. Tel. Tech.* **2019**, *30*, e3715. [CrossRef]
203. Restuccia, G.; Tschofenig, H.; Baccelli, E. Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3. In Proceedings of the 2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN), Berlin, Germany, 1–3 December 2020. [CrossRef]
204. Raza, S.; Shafagh, H.; Hewage, K.; Hummen, R.; Voigt, T. Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sens. J.* **2013**, *13*, 3711–3720. [CrossRef]
205. Kohlios, C.P.; Hayajneh, T. A Comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics* **2018**, *7*, 284. [CrossRef]
206. Padgette, J.; Scarfone, K.; Chen, L. Guide to bluetooth security. *NIST Spec. Publ.* **2012**, *800*, 25.
207. Marksteiner, S.; Jiménez, V.J.E.; Valiant, H.; Zeiner, H. An overview of wireless IoT protocol security in the smart home domain. In Proceedings of the Internet of Things Business Models, Users, and Networks, Copenhagen, Denmark, 23–24 November 2017. [CrossRef]
208. Liaisons, S.; Hall, R.; Modera, M.; Neilson, C.; Isler, B.; Osborne, M.; Lenart, J. BACnet-A Data communication protocol for building automation and control networks. *ANSI/ASHRAE Standard* **2012**, *135*, 404–636.

209. Huitsing, P.; Chandia, R.; Papa, M.; Shenoi, S. Attack taxonomies for the Modbus protocols. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 37–44. [CrossRef]
210. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
211. Yang, Y.; McLaughlin, K.; Littler, T.; Sezer, S.; Pranggono, B.; Wang, H.F. Intrusion detection system for IEC 60870-5-104 based SCADA networks. In Proceedings of the IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013. [CrossRef]
212. Morris, T.H.; Jones, B.A.; Vaughn, R.B.; Dandass, Y.S. Deterministic intrusion detection rules for MODBUS protocols. In Proceedings of the 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2013. [CrossRef]
213. Jose, S.; Malathi, D.; Reddy, B.; Jayaseeli, D. A survey on anomaly based host intrusion detection system. *J. Phys. Conf. Ser.* **2018**, *1000*, 012049. [CrossRef]
214. Al Baalbaki, B.; Pacheco, J.; Tunc, C.; Hariri, S.; Al-Nashif, Y. Anomaly behavior analysis system for ZigBee in smart buildings. In Proceedings of the IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November 2015. [CrossRef]
215. Vijayanand, R.; Devaraj, D.; Kannapiran, B. Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid. In Proceedings of the 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017. [CrossRef]
216. Jokar, P.; Nicanfar, H.; Leung, V.C.M. Specification-based Intrusion Detection for home area networks in smart grids. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011. [CrossRef]
217. Liu, X.; Zhu, P.; Zhang, Y.; Chen, K. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Trans. Smart Grid* **2015**, *6*, 2435–2443. [CrossRef]
218. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
219. Abduvaliyev, A.; Pathan, A.S.K.; Zhou, J.; Roman, R.; Wong, W.C. On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1223–1237. [CrossRef]
220. Krontiris, I.; Dimitriou, T.; Giannetsos, T.; Mpasoukos, M. Intrusion detection of sinkhole attacks in wireless sensor networks. In Proceedings of the International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (ALGOSENSORS), Wroclaw, Poland, 14 July 2007. [CrossRef]
221. Krontiris, I.; Giannetsos, T.; Dimitriou, T. LIDeA: A distributed lightweight intrusion detection architecture for sensor networks. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, Istanbul, Turkey, 22–25 September 2008. [CrossRef]
222. Muntwyler, B.; Lenders, V.; Legendre, F.; Plattner, B. Obfuscating IEEE 802.15. 4 communication using secret spreading codes. In Proceedings of the 9th Annual Conference on Wireless On-Demand Network Systems and Services (WONS), Courmayeur, Italy, 9–11 January 2012. [CrossRef]
223. Diaz, C.; Preneel, B. Taxonomy of mixes and dummy traffic. In *Information Security Management, Education and Privacy*; Deswarte, Y., Cuppens, F., Jajodia, S., Wang, L., Eds.; Springer: Boston, MA, USA, 2004; pp. 217–232. [CrossRef]
224. Kamat, P.; Xu, W.; Trappe, W.; Zhang, Y. Temporal privacy in wireless sensor networks: Theory and practice. *ACM T Sens. Netw.* **2009**, *5*, 1–24. [CrossRef]
225. Shbair, W.M.; Bashandy, A.R.; Shaheen, S.I. A new security mechanism to perform traffic anonymity with dummy traffic synthesis. In Proceedings of the International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009. [CrossRef]
226. Erdene-Ochir, O.; Minier, M.; Valois, F.; Kountouris, A. Enhancing resiliency against routing layer attacks in wireless sensor networks: Gradient-based routing in focus. *Int. J. Adv. Netw. Serv.* **2011**, *4*, 38–54. Available online: http://www.iariajournals.org/networks_and_services/netser_v4_n12_2011_paged.pdf (accessed on 28 March 2021).
227. Kelly, D.J. A Taxonomy for and Analysis of Anonymous Communications Networks. Ph.D. Thesis, Air Force Institute of Technology, Dayton, OH, USA, 18 March 2009. Available online: https://scholar.afit.edu/cgi/viewcontent.cgi?article=3540&context=etd (accessed on 28 March 2021).
228. Dingledine, R.; Mathewson, N.; Syverson, P. Tor: The second-generation onion router. In Proceedings of the 13th Conference on USENIX Security Symposium, San Diego, CA, USA, 9–13 August 2004; Available online: https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf (accessed on 28 March 2021).
229. Matos, A.; Sargento, S.; Aguiar, R.L. Waypoint routing: A network layer privacy framework. In Proceedings of the IEEE Global Telecommunications Conference-GLOBECOM, Houston, TX, USA, 5–9 December 2011. [CrossRef]
230. Park, S.; Bang, J.; Ahn, M.; Lee, W.; Kwon, T. A method for hiding link layer addresses using bloom filter in wireless sensor networks. *J. Internet Serv. Inf. Secur.* **2014**, *4*, 71–81.
231. Wang, X.; Mu, Y. Addressing and privacy support for 6LoWPAN. *IEEE Sens. J.* **2015**, *15*, 5193–5201. [CrossRef]
232. Oualha, N.; Olivereau, A.; Boudguiga, A. Pseudonymous communications in secure industrial wireless sensor networks. In Proceedings of the 2013 Eleventh Annual Conference on Privacy, Security and Trust, Tarragona, Spain, 10–12 July 2013. [CrossRef]

233. Narten, T.; Draves, R.; Krishnan, S. Privacy extensions for stateless address autoconfiguration in IPv6. *Netw. Work. Group RFC* **2007**, *4941*, 1–23.
234. Sengupta, S.; Chowdhary, A.; Sabur, A.; Alshamrani, A.; Huang, D.; Kambhampati, S. A survey of moving target defenses for network security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1909–1941. [CrossRef]
235. Aura, T. Cryptographically generated addresses (CGA). In Proceedings of the International Conference on Information Security (ISC), Dallas, TX, USA, 13–15 November 2013. [CrossRef]
236. Cheneau, T.; Laurent, M. Using SEND signature algorithm agility and multiple-key CGA to secure proxy neighbor discovery and anycast addressing. In Proceedings of the Conference on Network and Information Systems Security, La Rochelle, France, 18–21 May 2011. [CrossRef]
237. Rafiee, H.; Meinel, C. SSAS: A simple secure addressing scheme for IPv6 autoconfiguration. In Proceedings of the Eleventh Annual Conference on Privacy, Security and Trust, Tarragona, Spain, 10–12 July 2013. [CrossRef]
238. Tunaru, I.; Denis, B.; Uguen, B. Location-based pseudonyms for identity reinforcement in wireless ad hoc networks. In Proceedings of the IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015. [CrossRef]
239. Dunlop, M.; Groat, S.; Urbanski, W.; Marchany, R.; Tront, J. Mt6d: A moving target ipv6 defense. In Proceedings of the Military Communications Conference (MILCOM), Baltimore, MD, USA, 7–10 November 2011. [CrossRef]
240. Dos Santos, J.; Hennebert, C.; Fonbonne, J.C.; Lauradoux, C. Ephemeral: Lightweight pseudonyms for 6LoWPAN MAC addresses. In Proceedings of the 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016. [CrossRef]
241. Leitão, P.; Colombo, A.W.; Karnouskos, S. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Comput. Ind.* **2016**, *81*, 11–25. [CrossRef]
242. Bongard-Blanchy, K.; Bouchard, C. Dimensions of user experience-from the product design perspective. *J. Interact. Pers. Syst. Assoc. Francoph. Interact. Homme Mach. (AFIHM)* **2014**, *3*, 2.
243. D'Oca, S.; Hong, T.; Langevin, J. The human dimensions of energy use in buildings: A review. *Renew. Sustain. Energy Rev.* **2018**, *81*, 731–742. [CrossRef]
244. Harputlugil, T.; de Wilde, P. The interaction between humans and buildings for energy efficiency: A critical review. *Energy Res. Soc. Sci.* **2021**, *71*, 101828. [CrossRef]
245. Ciancio, V.; Salata, F.; Falasca, S.; Curci, G.; Golasi, I.; de Wilde, P. Energy demands of buildings in the framework of climate change: An investigation across Europe. *Sustain. Cities Soc.* **2020**, *60*, 102213. [CrossRef]
246. Fonseca, J.A.; Nevat, I.; Peters, G.W. Quantifying the uncertain effects of climate change on building energy consumption across the United States. *Appl. Energy* **2020**, *277*, 115556. [CrossRef]