People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

University of Abdelhamid Mehri – Constantine 2

Faculty of New Technologies of Information and Communication (NTIC)

Department of Fundamental Computing and its Applications (IFA)

MASTER'S THESIS

to obtain the diploma of Master degree in Computer Science

Option: Sciences and Technologies of Information and Communication (STIC)

Cybersecurity of smart grid infratsructure communication

Realized by:

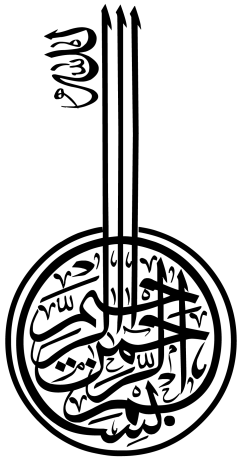
ochetati ilyes chiheb eddine

kechicheb ahmed

Under supervision of:

Salim benayoune

June 2024



Chapter 1

State of the Art

Introduction

Electricity grids, commonly referred to as "grids," play a vital role in modern energy infrastructure. They facilitate power generation, transmission, distribution, and control. Over time, grids have evolved from localized systems to interconnected networks, adapting to meet increasing demands and technological advancements. These grids contribute significantly to economic and societal progress.

Amidst dynamic changes in the energy landscape, the emergence of the "smart grid" presents transformative possibilities. Leveraging data, automation, and connectivity, smart grids enhance energy management and promote sustainability. In this chapter, we delve into the evolution of grid systems and explore the challenges and opportunities associated with smart grid technology, shaping the future of energy.

1.1 Definition smart grid

The Smart Grid is a comprehensive electrical network that employs cutting-edge communication technologies, computational intelligence, and cybersecurity protocols throughout the entire process of generating, transmitting, distributing, and consuming electricity. Its objective is to establish a system that is environmentally friendly, secure, dependable, adaptable, energy-efficient, and environmentally sustainable. While the ultimate vision of the Smart Grid is ambitious, its practical implementation demands careful evaluation of costs, rigorous testing, and validation. Introducing new functionalities can occur autonomously, with each necessitating justification and a reasonable return on investment. The compatibility of open systems facilitates smooth integration into the Smart Grid once the technologies have been validated.[1] The National Institute of Standards and Technology (NIST), operating within the U.S. Department of Commerce, has classified the smart grid into seven distinct domains, as illustrated in Figure 1.1. A concise overview of these domains and their stakeholders is provided in Table 1.2.[2]

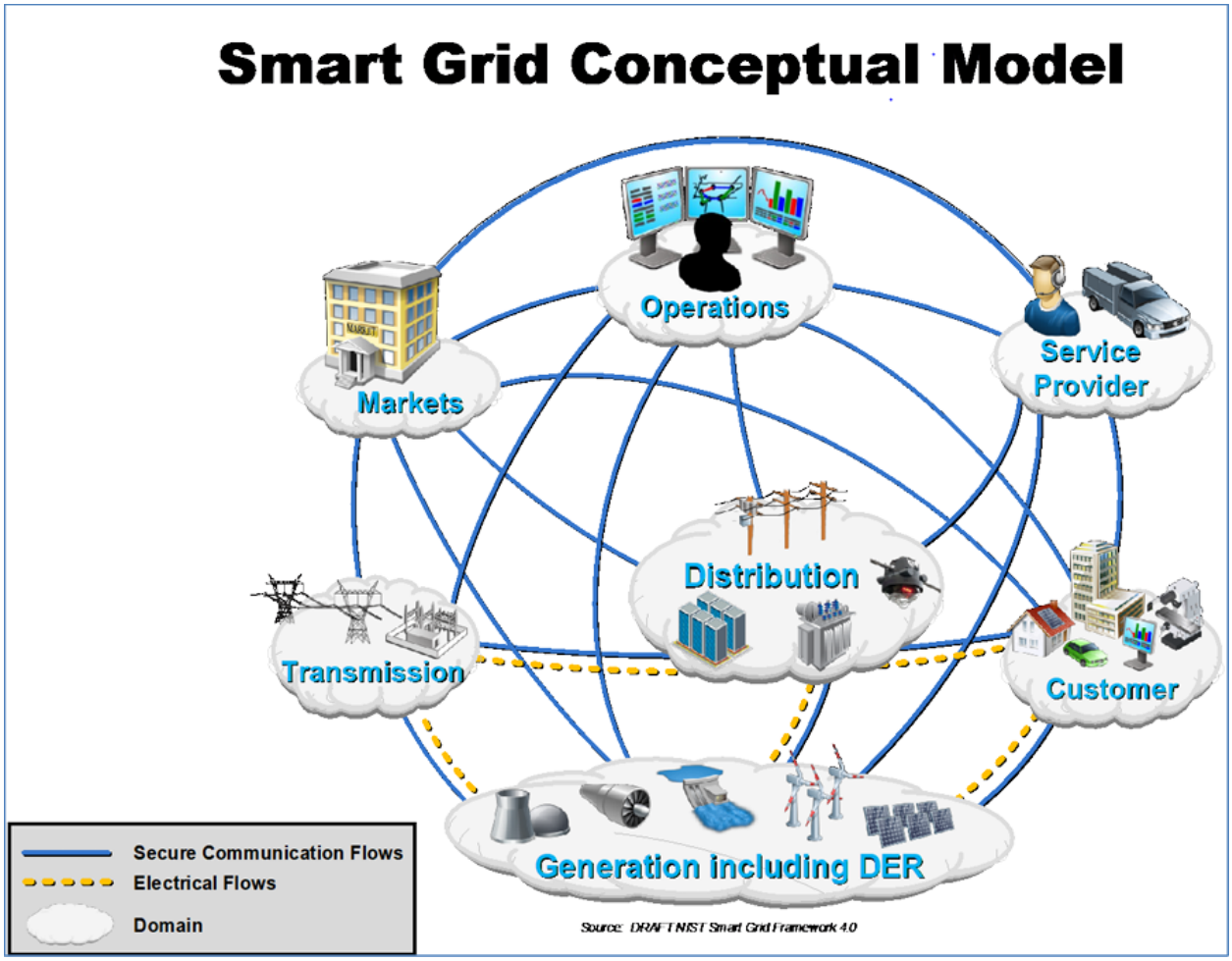


Figure 1.1: The NIST Conceptual Model for SG [2]

Domain	Roles/Services in the Domain
1 Customer	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own sub-domain: residential, commercial, and industrial.
2 Markets	The facilitators and participants in electricity markets and other economic mechanisms used to drive action and optimize system outcomes.
3 Service Provider	The organizations providing services to electrical customers and to utilities.
4 Operations	The managers of the movement of electricity.
5 Generation Including DER	The producers of electricity. May also store energy for later distribution. This domain includes traditional generation sources and distributed energy resources (DER).
6 Transmission	The carriers of high voltage electricity over long distances. May also store and generate electricity.
7 Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

Table 1.1: Domains and their associated roles/services [2]

1.2 Smart grid attributes

Many smart grid advocates cite some or all of its following attributes as representative of its promise:

- **Efficiency:** Capable of meeting growing consumer demand without the need for additional infrastructure.
- **Flexibility:** Able to accept energy from various sources, including solar and wind, with the same ease as traditional fuels like coal and natural gas. It can integrate new technologies, such as energy storage, as they become commercially viable.
- **Empowering:** Facilitating real-time communication between consumers and utility providers, allowing consumers to adjust their energy usage based on factors like price and environmental concerns.
- **Opportunistic:** Creating new markets and opportunities by leveraging plug-and-play innovations whenever suitable.
- **Focus on Quality:** Able to deliver reliable power without disruptions, ensuring the smooth operation of digital technologies crucial to our economy.
- **Resilience:** Increasingly resistant to cyber attacks and natural disasters through decentralization and the implementation of smart grid security measures.
- **Environmental Sustainability:** Contributing to the mitigation of climate change

and offering a viable path towards reducing the environmental impact of electricity generation. [3]

1.3 Differences between Traditional grid and Smart grid

Table 1.1 offers a thorough comparison of the conventional power grid with the smart grid. In contrast to the traditional grid where customers play a passive role, the smart grid actively engages them through bi-directional communication technologies. For instance, rooftop photovoltaic solar panels produce electricity during the day, enabling customers to sell surplus energy back to the grid. At night, these panels continue to power home appliances as usual. Moreover, the smart grid incorporates innovative technologies like distributed generation, electric vehicle charging and discharging, and Flexible Alternating Current Transmission Systems (FACTS) to improve energy distribution and management.[4]

Table 1.2: Comparison between conventional grid and smart grid [5]

Aspects	Conventional Grid	Smart Grid
Interaction between Grid and Customers	Customers passively accept service from grid	Customers participation on the grid action
Renewable Energy Integration	Having trouble with renewable penetration	Integration with renewable resources enhancement
Options for Customers	No choice for customer, monopoly market	With digital market trading, PHEV, introduce bids and competition, more choice for customer
Options on Power Quality (PQ)	No choice on power quality, no price plan options for consumers	Power quality levels for different consumers
System Operation	Ageing power assets, no efficient operation	Assets operating optimization, less power loss
Protection	Only rely on protection devices, fault detect manually	Have capability of self-healing, less damage affected by fault
Reliability and Security	Susceptible to physical and cyber attack	More reliable for national security and human safety

1.4 Components of the Smart Grid

1.4.1 Smart Meters

The interplay between smart meters and smart grids is depicted in Figure 1.1. From the perspective of the smart grid, the applications primarily revolve around leveraging smart meters to facilitate the coordination of various electrical devices, thereby achieving a dependable power system. Simultaneously, these applications strive to enhance the performance and efficiency of smart metering. These objectives align with the defining characteristics of smart grids, which drive the advancement of smart meter technologies.[6]

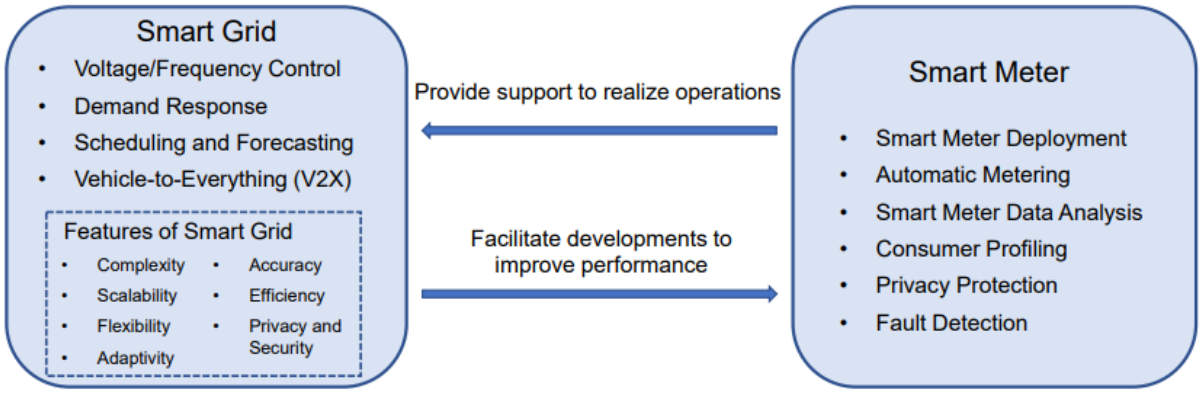


Figure 1.2: Applications from smart grid and smart meter perspectives. [6]

1.4.2 Advanced Distribution Management Systems

An ADMS is a software platform designed to support the comprehensive suite of tasks related to managing and optimizing the distribution of electricity. It encompasses functions that automate outage recovery and enhance the effectiveness of the distribution grid. These functions being developed for electric utilities include fault location, isolation, and restoration; optimization of voltage and reactive power; energy conservation through voltage reduction; management of peak demand; as well as support for microgrids and electric vehicles [7].

1.4.3 Communication Infrastructure

1.4.4 Smart Appliances and Devices

1.4.5 Renewable Energy Integration

1.5 Benefits of Smart Grid

1.5.1 Increased Efficiency

1.5.2 Improved Reliability

1.5.3 Sustainability and Environmental Benefits

1.5.4 Cost Savings

1.5.5 Consumer Empowerment

1.6 Challenges and Considerations

1.6.1 Cybersecurity

Without a shred of doubt, cybersecurity stands out as one of the foremost and intricate challenges confronting IoT devices. Sensors, devices, and networks connected to the internet are persistent targets for various online threats like probing, espionage, ransomware, theft, and potential destruction. Considering that an IoT-driven smart grid can encompass potentially millions of interconnected nodes spread across extensive geographic regions, it emerges as the most susceptible to substantial cyber assaults. Consequently, a cyber-attack on such a system would have devastating consequences, leading to significant financial losses and potentially bringing entire countries to a standstill. The diagram in Figure 1.3 illustrates the number of articles reviewed per year of publication and smart grids impacted by cyber-attacks. Hence, security stands as a major hurdle in both the deployment and operation of IoT-based smart grid networks.[8].

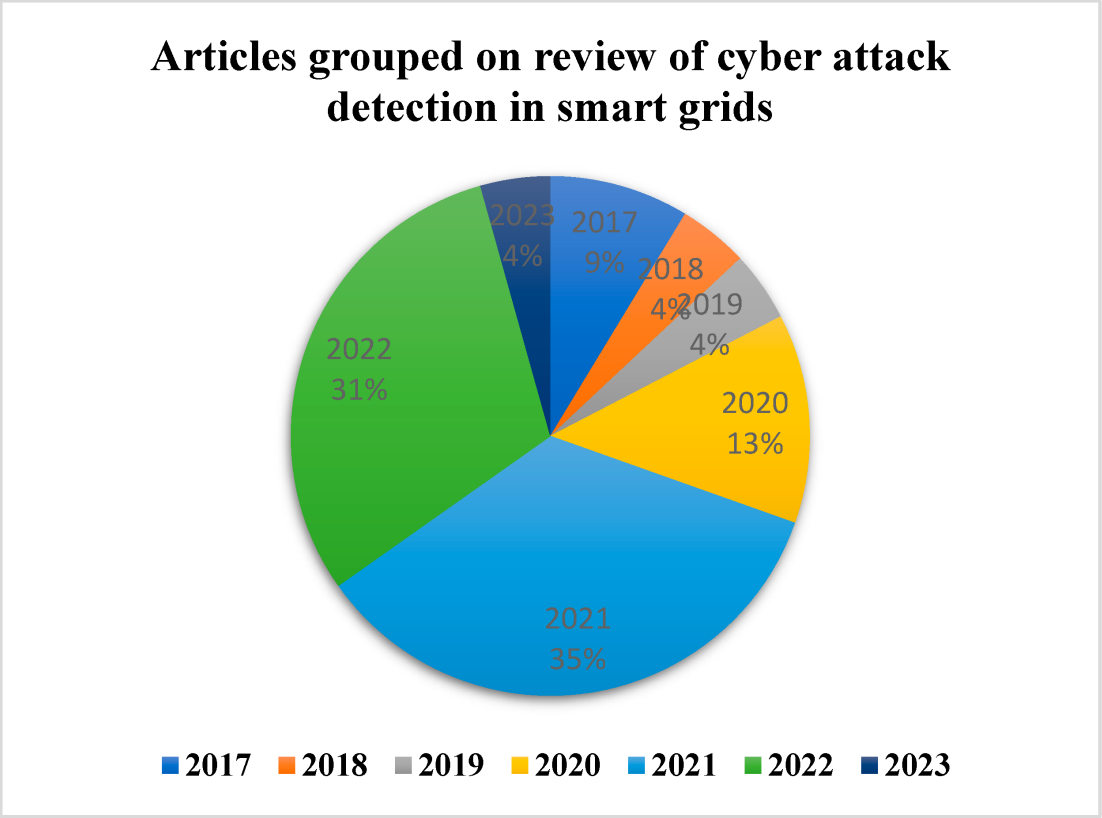


Figure 1.3: Estimate: cyber attacks will increase exponentially [9]

1.6.2 Data Privacy

1.6.3 Cost of Implementation:

1.6.4 Regulatory Frameworks

1.6.5 Public Awareness and Education

1.7 The Future of Smart Grids

1.7.1 Distributed Generation

1.7.2 Energy Storage

Conclusion

The smart grid revolution is not a destination, but a continuous journey towards a more efficient, reliable, and sustainable energy future. While challenges exist, the potential benefits of the smart grid are undeniable. By embracing innovation, fostering collaboration, and empowering consumers, we can unlock the full potential of this transformative technology.

A smarter grid paves the way for a future where clean energy sources like solar and wind power are seamlessly integrated, homes and businesses actively participate in energy management, and power outages become a rarity. It's a future where we have a more secure and sustainable energy infrastructure for generations to come.

Let's continue exploring the exciting world of smart grids and work together to build a brighter energy future for all.

Chapter 2

Intrusion detection for smart grids

2.1 Introduction

An intrusion detection system is a piece of hardware or software that is responsible for detecting suspicious and malicious activity, and in a network or an information system, the anomaly can either be reported to a systems administrator or saved to a security information and even management system (SIEM), the SIEM combines the output from multiple sources, then uses some filtering techniques to decide if the reported activity is malicious. [10]Intrusion detection systems are categorized into 2 categories based on the location of the detection, which are either network or host-based (HIDS or NIDS), There are also two primary methods of intrusion detection: signature-based and anomaly-based. [11]

Bibliography

[1] Hamid Gharavi and Reza Ghafurian. *Smart grid: The electric energy system of the future*, volume 99. IEEE Piscataway, NJ, USA, 2011.

[2] Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, Nelson Hastings, David Wollman, et al. *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology . . . , 2021.

[3] Mohamed E El-Hawary. The smart grid—state-of-the-art and future trends. *Electric Power Components and Systems*, 42(3-4):239–250, 2014.

[4] Haotian Zhang. *Smart Grid Technologies and Implementations*. PhD thesis, City University London, 2014.

[5] Joe Miller. Understanding the smart grid: Features, benefits and costs. In *Illinois Smart Grid Initiative–Workshop*, 2008.

[6] Zhiyi Chen, Ali Moradi Amani, Xinghuo Yu, and Mahdi Jalili. Control and optimisation of power grids using smart meter data: A review. *Sensors*, 23(4):2118, 2023.

[7] Artur R Avazov and Liubov A Sobinova. Advanced distribution management system. In *EPJ Web of Conferences*, volume 110, page 01004. EDP Sciences, 2016.

[8] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. Cyber security challenges for iot-based smart grid networks. *International journal of critical infrastructure protection*, 25:36–49, 2019.

[9] Link to mdpi article. URL `https://www.mdpi.com/1996-1073/16/4/1651`. Accessed on April 20, 2024.

[10] Stanislav Abaimov and Maurizio Martellini. Selected issues of cyber security practices in cbrnecy critical infrastructure. page 31, 2017.

[11] John R. Vacca. Computer and information security handbook. 2009.