

Communication architectures in Smart Grids - SR04 project

Group 6

January 2, 2015

Contents

1	Abbreviations	3
2	Introduction	5
2.1	Smart grid history and ecological issues	5
2.2	Smart grid solution	6
2.3	What smart grids are going to change?	6
2.3.1	How can smart grids answer these needs?	7
2.3.2	What are the obtacles?	7
3	Smart Grid architectures	8
3.1	Conceptual model	8
3.2	Information networks for the smart grids	10
3.3	Communication network architecture	11
3.3.1	Access tier	11
3.3.2	Distribution tier	12
3.3.3	Core tier	12
3.4	Interoperability - a new challenge	13
4	Smart Grid components	14
4.1	Active Network Management (ANM)	14
4.2	Automatic Voltage Control (AVC)	14
4.3	Dynamic Line Rating (DLR)	14
4.4	Intelligence Electronic Device (IED)	15
4.5	Phasor Measurement Unit (PMU)	15
4.6	Smart meters	15
5	Security	17
5.1	Requirements	18
5.1.1	Attack detection and resilience operations	18
5.1.2	Identification, authentication and access control	18
5.1.3	Secure and efficient communication protocols	18
5.2	Network security threats in the Smart Grid	19
5.3	Attack targeting availability	19
5.3.1	Denial-of-service attacks	19
5.3.1.1	Physical layer	20
5.3.1.2	MAC layer	20
5.3.1.3	Network and transport layers	20
5.3.1.4	Application layer	21

5.3.2	Network countermeasures of DoS attacks for the Smart Grids	21
5.3.2.1	Signal-based detection	21
5.3.2.2	Packet-based detection	22
5.3.2.3	Proactive method	22
5.3.2.4	Hybrid method	22
5.3.2.4.1	Network-layer mitigation	22
5.3.2.4.1.1	Rate-limiting	22
5.3.2.4.1.2	Filtering	22
5.3.2.4.1.3	Reconfiguration	22
5.3.2.4.2	Physical-layer mitigation	22
5.3.2.4.2.1	Coordinated protocols	23
5.3.2.4.2.2	Uncoordinated protocols	23
5.4	Attacks targeting integrity and confidentiality	23
5.4.1	Sneaky attacks	23
5.4.2	Cryptographic countermeasures for the Smart Grid	23
5.4.2.1	Encryption	24
5.4.2.1.1	Public-key or asymmetric key cryptography	24
5.4.2.1.2	Symmetric key cryptography	24
5.4.2.2	Authentication	25
5.4.2.2.1	Basic requirements in the Smart Grid	25
5.4.2.2.1.1	High efficiency	25
5.4.2.2.1.2	Tolerance to faults and attacks	25
5.4.2.2.1.3	Support of multicast	25
5.4.2.2.2	Overview of authentication schemes for power systems	26
5.4.2.2.2.1	Secret-information asymmetry	26
5.4.2.2.2.2	Time asymmetry	26
5.4.2.2.2.3	Hybrid asymmetry	26
5.4.2.2.3	Emerging physical-layer authentication	27
5.4.3	System key management	27
5.4.3.1	Key	27
5.4.3.1.1	Public key	27
5.4.3.1.2	Private key	27
5.4.3.2	Key management	28
5.4.3.2.1	Public key infrastructure (PKI)	28
5.4.3.2.1.1	PKI elements	28
5.4.3.2.2	Symmetric key management	29
6	Conclusion	30

Chapter 1

Abbreviations

AMI : Advanced Metering Infrastructure

AMR : Adaptative Multi Rate

ANM : Active Network Management

API : Application Programming interface

AVC : Automatic Voltage Control

ATCP : Ad-hoc Transmission Control Process

CA : Certificate Authority

DoS : Denial of Service

DMS : distribution management system

DLR : Dynamic Line Rating

ECN : Early Congestion Notification

EMU : Energy Management Units

FFD : Full Function Device

HDFS : Hadoop Distributed File System

ICMP : Internet Control Message Protocol

ICT : Information and Communication Technologies

IDC : Internet Data Centers

IEC : International Electrotechnical Commission

IED : Intelligence Electronic Device

McWiLL : Multicarrier Wireless information Local Loop

Net-AMI : Netbook advance metering infrastructure

NIST : National Institute of Standards and Technology

PKI : Public Key Infrastructure

PLC : Power Line Communication

PMU : Phasor Measurement Unit

RA : Registration Authority

RFD : Reduced Function Device

RSSI : Received Signal Strength Information

SCADA : Supervisory Control and Data Acquisition

TOU : Time-Of-Use

WLAN : Wireless Local Area Networks

WMN : Wireless Mesh Networks

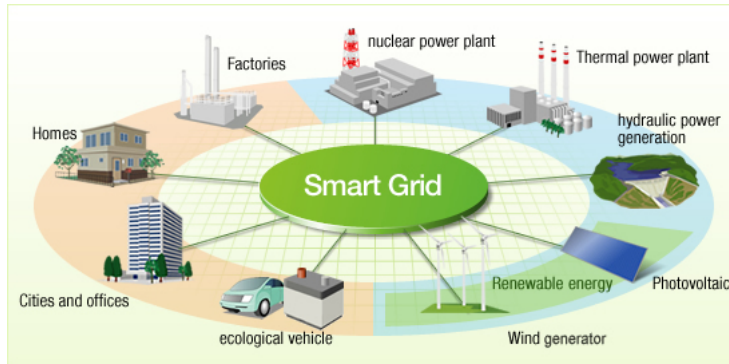
WPAN : Wireless Personal Area Networking

WSN : Wireless Sensor Networks

Chapter 2

Introduction

2.1 Smart grid history and ecological issues



A smart grid is an electricity distribution network that is changing our way to distribute electricity from power stations to houses.

Most electricity today is produced from carbon-rich energy sources, like coal and gas. New low carbon generation systems appeared, such as nuclear and renewable energies, but they are less flexible and predictable in term of increasing or decreasing output in a short time, compared to a gas-fired plant. The challenge is to find a sustainable generation that can cover consumer demands.

Traditionally, conventional distribution grids are using “build and connect” principle. Produced by a small number of large power stations, power is transported through high voltages to a distribution network that adjusts its flow to supply an end customer. When a new house is built, it is connected to the actual electricity distribution system. Then, the power distribution is sized for the likely maximum anticipated load needed by its customers, based on implemented and tested principles.

However, a new problematic appeared these past years concerning global warming consciousness. Humans are trying to reduce energy wasting and useless consumption. It called into question the traditional “build and connect” principle. We are now moving to a “connect and manage” culture. It means

that devices are not only providing electricity, they are now able to adjust the network flow based on real-time customers demands. The challenge is not only electricity is provided to make sure it covers the demand, but also adapts providing with each customer needs, to remove electricity waste. Smart grids are provoking a re-think about how we generate, deliver and use electricity.

2.2 Smart grid solution

To implement a smart grid, an existing grid can be used, but Information and Communication Technologies (ICT) need to be added. Actually smart grids can manage both power demand and power generation connected to the network, which offers a better of electricity distribution. Power is delivered in a “smarter” way than before in term of efficiency and reliability. Here are some new features smart grids can allow :

- automatically re-routing power and shifting loads : when there is more power than needed in a network, the smart grid can route it to another network that needs it;
- in case of outages on the network, the smart grid can control embedded generation;
- reducing maintenance cost, as the smart grid system is better monitoring network devices (it is possible to predict potential failures);
- distributing power according demands to avoid electricity loss, because the distribution is now managed.

Saying it with a short and complete definition would be the one published by the European Commission Task Force for Smart Grids : "A Smart grid is an electricity network that can intelligently integrate the behaviors and actions of all users connected to it - generators, consumers and those that do both - in order to efficiently ensure sustainable, economic and secure electricity supply."

2.3 What smart grids are going to change?

A lot of people think that smart grids are a simple layer of information and communication technology added to the existing network equipment. Adding technologies is only a small part of what makes a smart grid. A massive cultural change is also required, it modifies commercial relationships between distribution, supply, generation and transmission companies. Moreover, customers also have a new electricity consumption experience. They are going to be more engaged in electricity distribution than before, as sustainable generation needs consumers to be aware of their power consumption.

However, managing a grid with ICT means handling a lot of data, more automation and more dependence to IT technologies : that is why smart grids have to be well secured against cyber attacks. Security aspects are developed in chapter 4.

We can also highlight the fact that another challenge is managing growth in electricity generation and consumption, because humanity is consuming more and more power. As we are trying to reduce carbon, electricity is needed to electrify transportation for example.

2.3.1 How can smart grids answer these needs?

First of all, smart grids offer good visibility of the network, as distributors can locate and resolve outages more quickly. There is also less interference with communication systems and other electronics. Being able to see power flows on the network help to see where there are power losses and to react quickly. It is not a passive network anymore.

2.3.2 What are the obstacles?

Implementing smart grids in electrical architecture means changing some regulations about each players involved on it. In countries where they are only one dominant electricity operator, responsibilities don't really change with smart grids implementation. However, in deregulated markets where there are several actors, responsibilities are split and it is harder to ensure a coherent smart grid strategy. As we are living in a money-driven society, finding investment for smart grids is difficult, because there is no credible business case that encourages distribution network operators to invest on it. Nevertheless, powerful governments from European Union and the USA support smart grid program. It is more than 56 billion euros by 2020 that will be invested on it, according Pike Research in 2011.

Moreover, consumers are also main actors in smart grid project : if they are not onboard and don't accept to have smart meters to measure they real energy consumption, then smart grids programme hasn't a chance to be viable. Indeed, some consumer are opponents of smart grids and they denounce a violation of the consumer's privacy, and so a violation of the European Convention of Human rights. Instead of let the consumers think this, they need to be aware of the consequences their engagement can have on saving power. In fact, if consumers can manage their consumption by knowing their energy use and its associated costs, they can use in a more efficient way power.

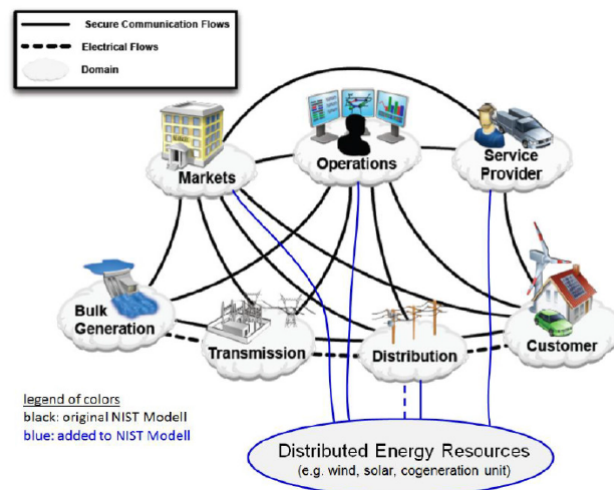
Chapter 3

Smart Grid architectures

3.1 Conceptual model

As we saw with the introduction, smart grids can be described as an upgraded electricity network enabling two-way information and power exchange between suppliers and consumers. This is possible thanks to an “intelligent” network based on communication monitoring and systems management.

The United States National Institute of Standards and Technology (NIST) has proposed a conceptual model to represent a smart grid complete system, from generation to customers and from customers to generation. It is now the smart grid reference architecture, even used by the European Commission. This model is used for the analysis of standardization gaps, cyber-security threats and option for future market models.



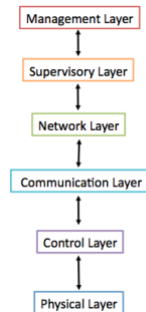
Above is the original NIST Smart grid model adapted for the European Commission context, including Distributed Energy Resources domain, like wind or solar power. The NIST Smart grid model shows all the communications and interrelations between these players and how they exchange energy/electricity

flows. This model is not a designed diagram that defines a solution implementation, its function is to describe how it works, just like the OSI model in IT network that doesn't precise which protocols are implemented.

The NIST model defines seven important domains :

1. Bulk Generation : it involves all power generation ways, such as renewable energies generation (biomass, geothermal, wind etc...) and non-renewable ones (nuclear, coal, gas) .
2. Transmission : it transfers electrical power from generation sources to distribution domains. Its main responsibility is to maintain stability on the electric grid by balancing generation (supply) with load (demand) across the transmission network.
3. Distribution : this domain distributes the electricity to the end customers in the smart grid. The distribution network allows us to connect smart meters and intelligent devices. These devices are managed and controlled through a wireless communication network.
4. Customers : it includes all end customers, such as homes, buildings or industrials. Each customer is connected to the electricity network through smart meters. A customer can potentially generate and store energy too.
5. Operations : the operation domain is responsible for managing and controlling the electricity flow over the network. It is using the communication network to provide reporting and supervision status. Thanks to these data, a smart grid can make decisions by processing gathered data from the customer and from the network.
6. Markets : the markets domain coordinates all the players in electricity markets within the smart grid and handles information exchange.
7. Service Providers : it handles all services such as portals that provide energy management to customers.

We can divide a smart grid into multiple foundational layers that we are going to describe below, which looks more like the OSI model (similar to a network approach).



1. Physical layer : it is the lowest level where there are physical processes we need to control or to monitor power. The control layer includes control

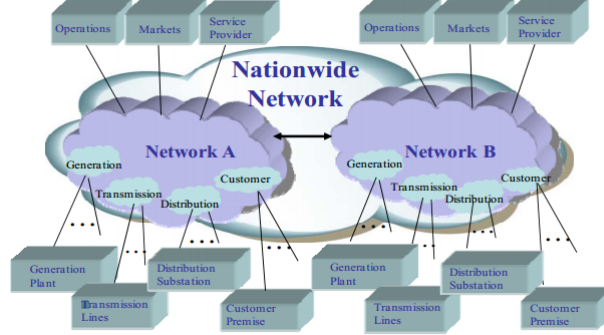
devices that are encoded with control algorithms that have robust, reliable, secure and fault-tolerant features.

2. Control layer : this layer consists of multiple control components, including observers/sensors, intrusion-detection systems (IDSs), actuators and other intelligent control components. Observers can collect data from the physical layer and may estimate the physical state of the current system.
3. Communication layer : it creates a communication channel (wireless, physical cable, bluetooth, ...) between control layer components or network-layer routers. This layer handles the data communication between devices or layers.
4. Network layer : it concerns the topology of the architecture. It is comprised of two major components : one is network formation and the other one is routing.
5. Supervisory layer : it coordinates all layers by designing and sending appropriate commands. It can be viewed as the brain of the system. Its main function is to perform critical data analysis or fusion to provide immediate and precise assessment of the situation.
6. Management layer : it is the high-level decision-making engine, where we deal with problems such as how can we budget resources to different systems in order to accomplish a goal and how to manage patches for control systems.

3.2 Information networks for the smart grids

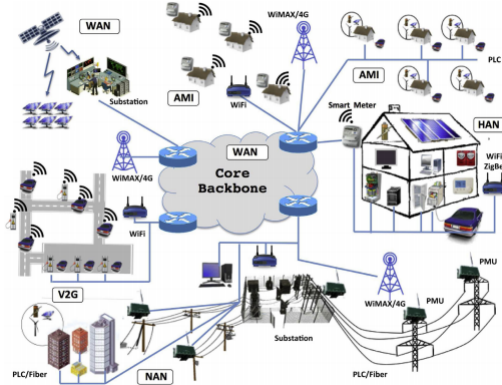
A smart grid is a network of many systems and subsystems as we saw with the conceptual model. We can compare it to a network of networks, where systems are interconnected to each other to provide end-to-end services between grid actors and intelligent devices. Each network can have its own sub-network and can be handled by various ownership. The information network may have multiple interconnected networks. For example, we can have a smart grid regional network A communicating with another network B, and both networks belong to the national network. A smart grid network can never be limited to a single area, and different devices can communicate with another ones over the information network; like telecommunications, intelligent devices etc... The information network has to support smart grid control and information exchange. This is possible thanks to a proper management to control to who and where applications can be connected. To make this information transfer reliable, security is required to ensure confidentiality, integrity and availability of smart grid information. We will see more in details this problematic in Security chapter. The network also requires routing capability to all network end points. It has to ensure that communication is possible between different applications with different bandwidths and different latency. Communication also includes ability to uniquely identify and address elements in the network. To conclude, it has to handle all an IT network does.

The following figure illustrates the communication between two smart grids network.



3.3 Communication network architecture

This section is illustrating a possible smart grid communication network. Smart grid communication network can be seen as a hierarchical network, with a three-tier architecture : an access tier, a distribution tier, and a core tier. The following figure shows an example of an end-to-end communication into a smart grids.



3.3.1 Access tier

The communication networks in access tier are responsible for enabling real-time information flows between end-customers and energy manager systems. Home Area Network (HAN) are very important for the access tier. Indeed, HAN are deployed at customers' buildings because they can provide low-cost solutions to control electric devices. HAN is made to monitor and control the electricity consumption in houses. This concept can be applied to larger networks, like Building Area Networks (BANs) and Industrial Area Networks (IANs). These networks will be used in the access tier to monitor and control the electricity consumption in buildings and industrial facilities.

This network can be built with low-range wired and wireless technologies. WIFI is generally excluded, because it is expensive for HAN devices and it

consumes too much power. The most popular solution is ZigBee, which can provide a low-power wireless communication to various devices. We are going to detail ZigBee on this paper later.

3.3.2 Distribution tier

The communication networks in the distribution tier of the smart grid communication infrastructure are responsible for real-time control of the distribution among the grid and for providing interconnection of local area networks (i.e., HANs, BANs and IANs) with the smart grid communication backbone. The distribution tier also helps the communication support, which is crucial. Indeed, the data management services, that handle the large amount of data collected, need strong communication networks.

We are introducing one of the most important components of this communication infrastructure : the advanced metering infrastructure (AMI). First of all, electric utilities can use AMI as data acquisition networks. Collecting data about power consumption, electricity production helps utilities to monitor power quality and electricity needs. This large amount of metering data can be exploited to proactively identify failure conditions to take countermeasures. The key component of the distribution tier is AMI networks because they are able to interconnect smart meters with data aggregators and control systems deployed in the distribution grid. However, there is not a single technology that can meet all requirements of all AMI deployment scenarios. That's why there are multiple options which include for example point-to-point communications using cellular or medium-range wireless (e.g., WiMax or WiFi) technologies.

In addition to AMI networks, the distribution tier includes specialized networks to provide reliable communications to a large number of heterogeneous sensors and actuators that will be deployed in smart grids. These devices allow monitoring and controlling power system equipment, such as sustainers transformers or circuit breakers. These networks are commonly named Field Area Networks (FANs), or Neighborhood Area Networks (NANs). The communication technologies used in FANs might not be the same as in AMI, as elements in FANs are physically distant.

Indeed, FANs can also be considered an evolution of existing SCADA-based networks that are used for power grid protection, and they have more real-time requirements than AMI networks.

3.3.3 Core tier

The core tier of the smart grid communication system is a Wide Area Network (WAN). The backbone needs a high-capacity communication in order to deliver the large amounts of data collected by the highly dispersed AMI systems and FANs. Core tier communication networks also have to be able to remote control centers over long distances. Various options have been considered for the deployment of a WAN in smart grids, such as all-IP core networks or MPLS-based networks. However, the need of high reliability, security and low latency are the most important facts taking in consideration, that's why most utilities are

choosing to deploy a private hybrid fiber/wireless network as the backbone for their electric grid. So far we have presented a general reference model of the network.

3.4 Interoperability - a new challenge

As we saw in the previous sections, various devices are communicating together from different network areas. The interoperability is one of the requirements of the Smart Grids. The Smart Grid is a system of interoperable systems where different networks, systems, devices, applications, and components are able to exchange information. Those exchanges have to be secure, effective and with little or no inconvenience to the user.

Different vendors, users and utility companies may adopt different communication technologies. Communication of a large number of distributed energy distribution networks, power sources and energy consumers under many different administrative domains is challenging. Therefore interoperability becomes a large challenge to make a Smart Grid work so that multiple heterogeneous communication technologies and standards could coexist in different parts of the Smart Grid. For example, in a home area, both ZigBee and Wifi could be used.

Chapter 4

Smart Grid components

This is an overview of the main technological objects used to implement a smart grid.

4.1 Active Network Management (ANM)

It is a technology category for objects that allow network monitoring and intelligence into the network : voltage control, fault levels and network restoration. In power system, a fault is an abnormal electric current; a fault level is the difference between the current standard value, and the current value in the power grid (it needs to be minimize). It offers the ability to connect distributed generation, meaning adding a new source of power to reinforce an existing network. ANM is fast and reliable communication infrastructures between substations on the network and the central Distribution Management System (DMS). A DMS is an application software that supports the electric systems operations.

4.2 Automatic Voltage Control (AVC)

An AVC is a component used to avoid unnecessary energy losses when high voltage levels are not required. It also deals with a form of intelligence, as it monitors voltages levels to maintain preset limits.

4.3 Dynamic Line Rating (DLR)

DLR is using line parameter measurements and weather conditions to determine the capacity of a section of a network. It means DLR provides the operator with the actual line ability to carry power at any moment. By exploiting this information, DLR helps the network when it is functioning at peak performance, by reliably optimizing and managing the power transfer capacity of the grid in real time.

4.4 Intelligence Electronic Device (IED)

IED is a smart tool that combines control, power quality recording and measurement capability. It is basically controllers composed with a microprocessors, and these are controllers of power system equipment, such as circuit breakers or transformers. IEDs receive data from sensors and power equipments, and can operate control commands, like tripping circuit breakers (meaning when circuit breakers are switched on, they cut power) if they sense voltage anomalies for example. IEDs include protective relaying device, circuit breaker controllers, voltage regulators...

4.5 Phasor Measurement Unit (PMU)

PMU takes voltage samples and gives the distributor a real-time view of the power system's behavior. It is a device which measures the electrical waves of an electricity grid. PMU is using a time synchronization to synchronize real-time measurements of multiple remote measurement devices on the grid.

Like IEDs, PMU is also participating in power-system automation implemented in smart grids. The main goal is to control automatically the power system via control devices. By using all collected data from IEDs and PMU, some control and automation capabilities allow a substation to be automated. A substation is a part of an electrical generation, transmission, and distribution system.

4.6 Smart meters



Smart meters are advanced meters that offer to the users a remote access to consumption data, so that they can save energy. They can also receive data from a power generation about real-time energy usage.

Smart grid implementation is not as easy as we can think, because all this devices are not under the distributor's control. For example, smart meter might

be under the suppliers' control. Smart grids were created to give network management to distributors, but the consumer flexible demand information will go to suppliers. It can cause a potential commercial and regulatory revolution besides the technological one.

Chapter 5

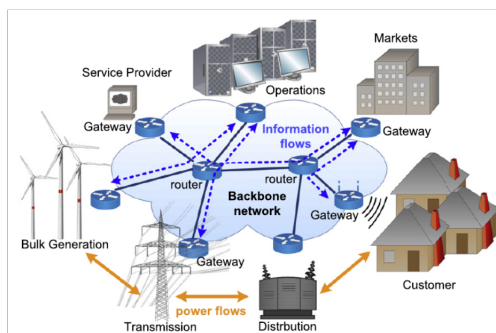
Security

The Smart Grids integrate information networks into the current power grid system. The privacy and the security are Smart Grids issues due to the vulnerabilities introduced by IT networks. For example, hackers can steal customers' power data without any trace being left.

That's why the NIST has written a guideline about cyber security and privacy issues in the Smart Grid. The major priority is making Smart Grids robust and secured because metering data can leak sensitive and private information.

New capabilities for smart grid systems and networks, such as distributed intelligence and broadband capabilities can enhance efficiency and reliability, but they may also create many new vulnerabilities if not deployed with the appropriate security controls.

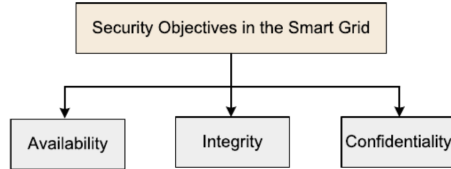
Increased interconnection and integration also introduce cyber vulnerabilities into the grid. Failure to address these problems will slow the modernization of the existing power system.



As we saw in the above figure, in the grid, all the main actors are exchanging data through the backbone network. These new data flows require new security systems to ensure the following requirements.

5.1 Requirements

Availability, integrity, and confidentiality are three high-level cyber security objectives for the Smart Grid.



The NIST also recommends specific security requirements for the Smart Grid, including both cyber security and physical security.

In particular, the cyber security part specifies detailed security issues and requirements related to Smart Grid information and use of the network systems.

The physical security part specifies requirements pertaining to physical equipment and environment protection as well as employee and staff security policies.

5.1.1 Attack detection and resilience operations

The Smart Grid is an open communication network over large geographical areas, contrary to legacy power system which is a large closed network. So, it is almost impossible to ensure every part or node in the Smart Grid to be invulnerable to network attacks. Without being invincible, Smart Grid can try to avoid problems by monitoring the network traffic to be aware of attacks or network's failures. Moreover, the network must also have the self-healing ability to continue network operations in the presence of attacks. Due to the major importance of power infrastructures, resilience operation in communication networks is essential to ensure a constant network availability in the Smart Grid.

5.1.2 Identification, authentication and access control

The Smart Grid network infrastructure incorporates millions of electronic devices and users. Identification and authentication is the key process of verifying the identity of a device or user for granting him access to resources in the Smart Grid information system. The focus of access control is to ensure that resources are accessed only by the appropriate personnel which are correctly identified. Strict access control must be created to prevent unauthorized users from accessing sensitive information and accessing to critical infrastructures. To meet these requirements, every node in the Smart Grid must have at least basic cryptographic functions to perform data encryption and authentication.

5.1.3 Secure and efficient communication protocols

Differing from conventional networks, message delivery in the Smart Grid requires both time-criticality and security. The two objectives that usually contradict with each other. As networks (especially sub-networks) in the Smart

Grid cannot always use secure, physically-protected and high-bandwidth communication channels, optimal tradeoffs are required to balance communication efficiency and information security in the design of communications protocols and architectures for the Smart Grid.

5.2 Network security threats in the Smart Grid

As security challenges mainly come from malicious cyber attacks via communication networks, it is essential to know the potential vulnerabilities in the Smart Grid under network attacks. We first classify network attacks into general classes, then analyze their potential threats in the Smart Grid and summarize research challenges.

In communication networks, security attacks can be classified into two types: selfish misbehaving and malicious. Selfish misbehaving are from users attempting to obtain advantage over other users by violating communication protocols. In contrast, malicious users have no will to benefit for their own; however, they aim to illegally acquire, modify or disrupt information in the network. Both pose challenging security problems to communication networks.

In the Smart Grid, however, malicious behavior is a more concerned issue than selfish misbehavior, as there are millions of access point to the Smart Grid information system spread all over the infrastructure which can be concern by an attack. Thus, malicious attacks may induce catastrophic damage to power supplies and widespread power outage. As any attack is possible, we are going to consider malicious attacks as three types based on the Smart Grid security objectives:

1. Attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt the communication in the Smart Grid. Recently, research efforts have been focused on studying this kind of attack.
2. Attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange in the Smart Grid.
3. Attacks targeting confidentiality intend to acquire unauthorized information from network resources in the Smart Grid.

5.3 Attack targeting availability

In what follows, we present a review of these attacks and also the most common attacks against communication networks in the Smart Grid.

5.3.1 Denial-of-service attacks

As a primary security goal of Smart Grid is availability, we are going to look the attacks targeting it and the most known : the Denial of Service attack, which

can severely degrade the communication performance and impair the operation of electronic devices.

5.3.1.1 Physical layer

Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications. Since intruders only need to connect to communication channels rather than authenticated networks, it is very easy for them to launch DoS attacks at the physical layer. With the use of wireless technologies in local-area systems, wireless jamming becomes the primary physical-layer attack in such networks. Jamming attacks can lead to different types of damages, from an impact on the network performance of power substation systems, to delayed delivery of time's messages and in the worst case a complete denial-of-service.

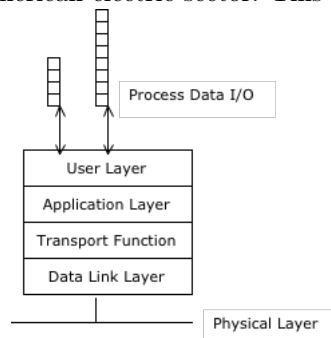
5.3.1.2 MAC layer

In the Smart Grid, spoofing is a strong threat at the MAC layer because it targets both availability and integrity. A spoofing attacker can disguise itself as another device to send fake information to other devices. For example, in a power substation network, a malicious node can broadcast forged ARP packets to shut down connections of all IEDs to the sub station gateway node.

5.3.1.3 Network and transport layers

DoS attacks at both layers can severely degrade the end-to-end communication performance as they are responsible of the reliability control. For example, a buffer-flooding attack on the DNP3-based SCADA network with real SCADA system hardware and software, is quite efficient.

DNP3 (Distributed Network Protocol) is a protocol which works with a system of client (called master) and server (called outstation) used on the North American electric sector. This is the protocol stack of DNP3 :



That represents the communication stack which places the DNP3 Data Link Layer Frame directly on the physical layer. When DNP3 is sent over an IP network the DNP3 Data Link Frame is encapsulated in either a TCP or UDP packet. DNP3 can also supports unsolicited response which occurs when an object value at an outstation exceeds a set threshold, and the outstation sends a response to the master station without receiving a request (unsolicited). When the costs are high or there is a large number of points and it is not feasible to

poll them often enough, unsolicited response become very important.

DNCP3 are secured. In 2007, the DNP3 User Group released the Secure DNP3 specification in which five new security functions have been added. These functions offers data and source authentication. A secure protocol DNCP3 can be used on serial DNP3 or DNP3 encapsulated in TCP because the security takes place at the application layer. This security is not perfect. A key management standard is missing so the top-level, pre-shared key is manually loaded and changed. This is likely to be an administrative burden for all but the smallest networks.

5.3.1.4 Application layer

Lower layer attacks focus mainly on transmission bandwidth in communication channels, computers or routers. Application-layer DoS attacks, however, intend to exhaust resources of a computer, such as CPU or I/O bandwidth.

Through the application layer an attacks can easily overwhelm a computer with limited computing resources by flooding with intensive computationally requests. As lots of computing and communication devices in the Smart Grid are equipped with limited computational abilities, they can be potential victims of application-layer DoS attacks.

Communication layer	Attacks in power systems
Application layer	CPU or I/O overwhelm
Network layer	Traffic flooding
Transport layer	Buffer flooding
Mac layer	ARP spoofing
Physical layer	Jamming in substations

In the Smart Grid, a DoS attacker does not need to completely shut down network access but instead he may launch simpler versions of attacks to intentionally delay the transmission of a time-critical message to violate its timing requirement. This can also be catastrophic for power infrastructures. For example, an attacker can cause severe damages to power equipments if it successfully delays the transmission of a protection message in the case of trip protection in substations.

5.3.2 Network countermeasures of DoS attacks for the Smart Grids

To summarize, existing DoS attack detection can be categorized into several schemes :

5.3.2.1 Signal-based detection

At the physical or MAC layer, a DoS attack detector can measure the Received Signal Strength Information (RSSI) to detect the presence of an attack (e.g. wireless jamming : if the RSSI of many packets is larger than a threshold (which means the receiver should correctly receive them) but the packet decoder outputs errors, the attack detector can raise an alarm of the presence of an attacker.

5.3.2.2 Packet-based detection

This kind of solutions can be implemented at every layer to measure the transmission result of each packet and discover potential attacks by identifying a significant increase of packet transmission failures. The packet-based detection is a general and effective detection scheme since DoS attacks can always lead to network performance degradation in terms of packet loss or delay.

5.3.2.3 Proactive method

The main idea is to design algorithms that attempt to identify DoS attacks at the early stage by proactively sending probing packets to test or measure the status of potential attackers.

5.3.2.4 Hybrid method

It is also common to design one scheme that combines different ideas to improve attack detection accuracy.

5.3.2.4.1 Network-layer mitigation The most widely used approaches for mitigating DoS attacks are designed for the network layer and many of them have been demonstrated to be effective for the Internet :

5.3.2.4.1.1 Rate-limiting The basic idea of rate-limiting mechanisms is to impose a rate limit on a set of packets that have been characterized as possibly malicious by the detection mechanism. It is usually deployed when the detection mechanism has many false positives or cannot precisely characterize the attack stream.

5.3.2.4.1.2 Filtering Corroborating with attack detection methods filtering mechanisms can compare the source addresses of packets with the black-list provided by attack detectors to filter out all suspicious flows. As such, packets from attackers will not be further forwarded or routed to victims.

5.3.2.4.1.3 Reconfiguration In order to mitigate the impact of DoS attacks, one solution is to reconfigure network architecture, such as changing the topology of the victim or the intermediate network to either add more resources to the victim or to isolate the attacked machines.

The Smart Grid features two major predictable directional information flows: bottom-up and top-down. This in fact makes it easy for gateway and router softwares to perform rate-limiting and filtering mechanisms to block undesired or suspicious traffic flows.

5.3.2.4.2 Physical-layer mitigation Recently, great progress has been made on the development of jamming-resilient schemes for wireless networks. Such schemes can be designed in either coordinated or uncoordinated manner.

5.3.2.4.2.1 Coordinated protocols They are conventional anti-jamming transmission schemes that have already been explored in the area of wireless communications. The issue associated with coordinated protocols is that the secret, is assumed confidential to others (e.g., attackers). And in the case of the open networks the secret is no more private due to its working, such as WiFi and cellular networks. So, coordinated protocols are vulnerable to intentional attacks with the knowledge of protocol information.

5.3.2.4.2.2 Uncoordinated protocols Uncoordinated protocols do not need the transmitter and the receiver to share a pre-known secret with each other. They randomly generate a secret (e.g., hopping pattern in FHSS) for each transmission and prevent attacks from acquiring sufficient knowledge to disrupt the communication.

Both coordinated and uncoordinated protocols can be used in the Smart Grid to achieve anti-jamming wireless communications.

5.4 Attacks targeting integrity and confidentiality

5.4.1 Sneaky attacks

These attacks targeting the data integrity are considered as more sophisticated than the DOS attacks. This kind of attacks need to be more stealth to stay undetected in order to let the corrupted data corrupted. The attack can target either customer information (e.g., pricing information and account balance) either data of the power systems (e.g., voltage readings and device running status). The false data injection against power grids have increasing attention as we understand the impact that can have such an attack.

For example, if we imagine that an attacker has already compromised one or several meters, then falsified data can easily be injected in the SCADA center, and at the same time pass the data integrity check. Thus, well organized this type of attack will be difficult to discover and the snowball effect can be quit strong. For instance, if false data injection attacks is extended to the electric market to deliberately manipulate the market price information. In this way, the result will be significant financial losses to the social welfare.

The load redistribution attack is another special kind of false data injection attacks, here only load bus injection measurements and line power flow measurements are attacked. Such attacks are realistic : false data injection attacks with limited access to specific meters. This is currently a priority research in Smart Grid research.

5.4.2 Cryptographic countermeasures for the Smart Grid

Network approaches are primary countermeasures to detect, mitigate and eliminate DoS attacks that actively lead to network traffic dynamics. However, they

are much less effective to deal with attacks targeting integrity and confidentiality that cause negligible effect on the network performance. Cryptographic primitive based approaches become major countermeasures against such attacks. There are three key topics of cryptographic countermeasures: encryption, authentication, and key management for power systems.

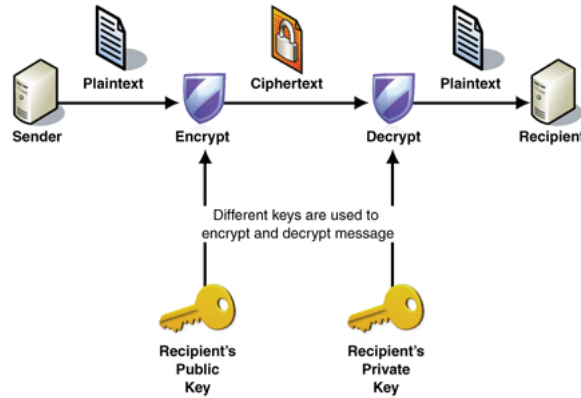
5.4.2.1 Encryption

Encryption is an elementary cryptographic method to achieve secure communication and information protection for any information system. This is the basic mechanism to protect data confidentiality and integrity in the Smart Grid.

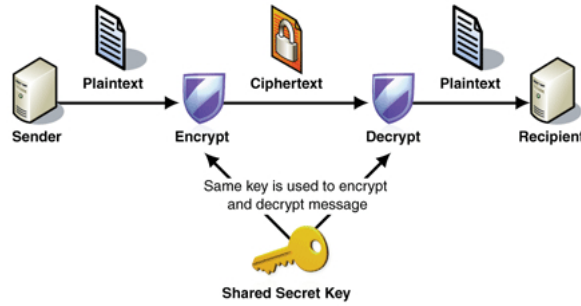
As the Smart Grid communication network consists of millions of embedded computing systems with limited computational ability (e.g., IEDs and smart meters), computational efficiency becomes an important factor for an encryption scheme to be adopted in the Smart Grid.

Encryption schemes can be based on symmetric key cryptography or asymmetric key cryptography. Symmetric key cryptography uses the same key for encryption and decryption. Asymmetric or public key cryptography uses private and public keys to encrypt and decrypt, respectively.

5.4.2.1.1 Public-key or asymmetric key cryptography It requires more computation resources than symmetric key cryptography for long key size (strong security). Thus, the use of asymmetric key encryption may be limited in embedded computing systems.



5.4.2.1.2 Symmetric key cryptography It requires approximately constant computational resources regardless of the key size. However, it requires secure exchange and update of secret keys among network nodes, thereby complicating the process of key management.



5.4.2.2 Authentication

Authentication is an identification process to eliminate attacks targeting data integrity. However, the authentication design process is prone to significant errors if adequate care is not taken for power systems.

5.4.2.2.1 Basic requirements in the Smart Grid An authentication protocol for the Smart Grid must ensure full security to protect data integrity. In addition, the authentication protocol should meet the following requirements from the network perspective.

5.4.2.2.1.1 High efficiency Efficiency is crucial to achieve the high availability requirement in real-time Smart Grid applications. The indication of high efficiency is twofold. First, the authentication schemes should not include too much redundancy for security. However, for an authentication protocol, less redundancy results in less security. Hence, it is always desirable to balance a good tradeoff between redundancy and security. Second, computation involved in authentication (e.g., digital signature and verification) must be fast enough to satisfy timing requirements of messages in the Smart Grid.

This indicates that the use of public key based authentication, which provides strong authentication at the cost of more processing overhead, will be limited in the Smart Grid, in particular in distribution and transmission systems.

5.4.2.2.1.2 Tolerance to faults and attacks Authentication schemes can offer strong protection against attacks targeting data integrity, but cannot by themselves provide all the necessary security. Hence, authentication schemes are required to detect malicious attacks, collaborate with attack detection and response systems.

5.4.2.2.1.3 Support of multicast Multicast has wide applications in the Smart Grid, including monitoring protection. For example, in a power substation, if an IED that keeps monitoring the status of a power feeder senses any anomaly (e.g., high voltage or current), it will try to activate a tripping circuit breakers to protect power equipments. In such a case, unicasting the same time-critical tripping command to each of the breakers unavoidably leads to large delay and potential damages of power equipments. Then multicast a time-critical message to all related breakers that belong to the same multicast

group is the best solution. Hence, authentication schemes in the Smart Grid must be able to efficiently support multicast.

5.4.2.2.2 Overview of authentication schemes for power systems The fundamental requirement for authentication design is to provide efficient multicast authentication schemes for the Smart Grid applications. Works on this theme are currently developed : fast multicast authentication protocols for power control systems.

The easiest multicast authentication scheme is to use public key based authentication. It is communication-efficient as only one authenticator is appended to the message. Nevertheless, it is quite computationally inefficient for embedded devices in power systems.

An intuitive alternative is to use computationally efficient symmetric key instead of public key. However, using one key through multicast is not a very secure way, because when multiple nodes share a single key, it is easy for an attacker that has obtained the key by compromising a node to masquerade as a different sender and inject fake information into the network.

In general, multicast authentication can be categorized into three categories : secret-information asymmetry, time asymmetry and hybrid asymmetry.

5.4.2.2.2.1 Secret-information asymmetry The underlying idea of secret-information asymmetry is that all receivers are associated with different secrets at the sender. The sender computes the corresponding authenticator of a message with each receiver's secret, appends all authenticators to the message and multicasts it to all receivers. When receiving the message, each receiver uses its own secret to verify the authenticity of the message. This method is the most intuitive one, but suffers from the scalability problem. Thus, existing solutions attempted to balance a good tradeoff between the scalability and security. Based on secret-information asymmetry, a multicast authentication schemes was proposed for embedded control system applications. This schemes validate truncated message authentication codes across multiple packets to achieve a good tradeoff among authentication cost, delay performance, and tolerance to attacks, thereby showing their potential use in Smart Grid applications.

5.4.2.2.2.2 Time asymmetry This approach uses different keys in different time slots (rather than in different receivers). The sender and receivers are synchronized with each other. The sender discloses a key to all receivers after they have received and buffered the message. The key is only valid in a limited time interval, thereby preventing malicious users from forging messages after obtaining the key. Time-asymmetry methods have excellent computational efficiency and low communication overhead. However, packet buffering and delayed key disclosure limit the use of time-asymmetry in time-critical applications in the Smart Grid.

5.4.2.2.2.3 Hybrid asymmetry Secret-information asymmetry can verify packets as soon as they are received but needs to balance a tradeoff between

security and scalability. Time asymmetry has low overhead and is robust to attacks since a single key is used in a short time period, but has the problem of packet buffering. The main idea of hybrid asymmetry is to combine the two asymmetry mechanisms together to achieve time efficiency, scalability, and security at the same time.

5.4.2.2.3 Emerging physical-layer authentication Conventional authentication schemes have to strike a tradeoff between security and time-criticality. Recently, physical-layer authentication emerges as a promising alternative for fast and low-overhead authentication. Compared with conventional data origin authentication mechanisms that exist at the link layer and above, physical-layer authentication usually requires no additional bandwidth to transmit authentication information.

Physical-layer authentication can be mainly classified into superimposed authentication and link-signature-based authentication. In superimposed authentication, authentication is added into the physical-layer signal via a carefully designed modulation on the waveforms. Hence, authentication information and data information are transmitted at the same time to the receiver, thereby reducing the communication overhead. In link-signature-based authentication for wireless networks, the physical-layer link signature (or channel impulse response) has the reciprocal property between a transmitter–receiver pair, which provides a unique secret for the pair to authenticate with each other. Therefore, authentication can be performed in the channel estimation process at the physical layer and even requires no overhead to transmit.

Given the nice property, i.e., low-overhead and short latency, of emerging authentication mechanisms at the physical layer, they are considered as a promising approach in the Smart Grid, especially in wireless-based systems. However, dynamic, time-varying characteristics of wireless channels may result in error-prone authentication results. How to assess such a risk and design robust physical-layer authentication is quite challenging for Smart Grid applications.

5.4.3 System key management

5.4.3.1 Key

A key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

5.4.3.1.1 Public key A public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.

5.4.3.1.2 Private key A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that

if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

5.4.3.2 Key management

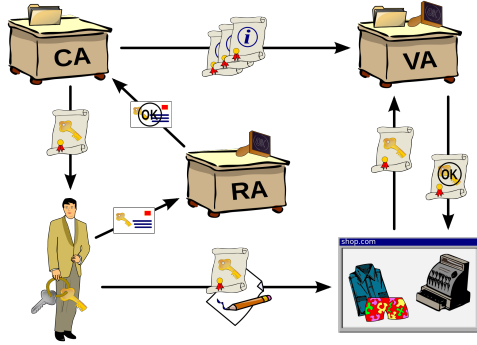
Encryption and authentication are essential cryptographic processes for the Smart Grid to protect data integrity and confidentiality. Moreover, cryptographic countermeasures for the Smart Grid entail not only such cryptographic processes, but also key management on different scales, from tens (e.g. a power substation network) to millions of credentials and keys (e.g. the AMI network).

Inadequate key management can result in possible key disclosure to attackers, and even jeopardizing the entire goal of secure communications in the Smart Grid. Therefore, key management is another critical process to ensure the secure operation of the Smart Grid. Based on cryptographic primitives, key management can be also classified into public key infrastructure and symmetric key management.

5.4.3.2.1 Public key infrastructure (PKI) A PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. It is a networked system that enables companies and users to exchange information and money safely and securely. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

5.4.3.2.1.1 PKI elements

- A Certificate Authority (CA) : is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.
- A Registration Authority (RA) : is an authority in a network that verifies user requests for a digital certificate and tells the CA to issue it. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.
- A certificate database which stores certificate requests and issues and revokes certificates;
- A certificate store which resides on a local computer as a place to store issued certificates and private keys.



The figure above illustrates the principle of PKI. Here, a user wants to communicate with a secure resource. He starts with sending a Certificate Signing Request (CSR) to the RA. It analyses the request and if it is correct, it signs the CSR and forwards it to the CA. Next it issues the certificate and sends it to the user. Later when he wishes to access a secure resource, he will send this certificate. The secure resource validates the certificate typically by requesting the certificate status from a validation authority (VA), who replies in the positive if the certificate is valid. Then, the user would be able to reach the secure resource.

PKI is a powerful tool that can be used to provide secure authentication and authorization for security association (establishment of shared security attributes between two network entities to support secure communication) and key establishment. However, PKI can be difficult to deploy and operate.

5.4.3.2.2 Symmetric key management This is the key management scheme for symmetric cryptography, which includes key generation, key distribution, key storage, and key update. For time-critical applications in the Smart Grid, symmetric key cryptography is more appropriate than public key cryptography because of its computational efficiency.

However, symmetric key management is a major issue associated with symmetric cryptography. Symmetric keys often have a shorter lifespan than asymmetric keys due to amount of data that is protected using a single key. Limiting the amount of data protected by a symmetric key helps reduce the risk of compromise of both the key and the data. This means that the key management system has to keep generating new keys and distributing them to power devices via communication networks frequently, which entails not only the critical trust problem between the key producer and key consumers, but also the risk of key disclosure during the key distribution process.

Symmetric key management still remains as an important issue in the Smart Grid. It requires more coordination and interaction between two or more entities than PKI. However, the advantage of symmetric key cryptography is the efficiency for large amounts of data.

Chapter 6

Conclusion

Smart grids are intelligent power grids, including an information layer that a basic grid doesn't have. Smart grids don't create an entire new grid system, as it is using the actual power grid. We mainly saw how a smart grid works, which components are used, and which architecture the grid has. Nevertheless, implementing a smart grids is first a business transformation that affects all power grid's users. Moving to smart grids make engineers think about people as much as the technology. Through this paper, we mainly speak about technologies, but they is also a huge human factor.

Then, we review communication protocols used in smart grids, and security features required to ensure data transmission and protection. We also evoke interoperability, to ensure communications between various devices.

Finally, we investigate why using cloud computing in smart grid is an asset. They are a lot of opportunities of cloud platforms for smart grid applications, that's why we analyzed their compatibility with smart grids needs in order to understand which challenges they faced.

There are still key research areas. For example, as data are going to explode, a lot of research are still conducted for data storage and management, along with optimizing power strategies. Also due to increased interconnection and integration, for example between electric grid and monitoring and communication network, new cyber-vulnerabilities appear, and security is a central question in smart grids.