Cyber Security in Smart Grid Communications

The *Smart Grid* refers to the project of making a new electric grid for power distribution that will be integrating advanced computing and communications technologies. This Smart Grid will use a digital communication that allows a two-ways communication between the customer and the distributers. This grid will be similar to the Internet, the customers will give their usage information to the utilities and those will deliver the electricity in a *smart* way. The security of this network is really crucial, because there will be millions of electrical devices connected through it. The consequences of cyber-attacks can go from a global slowdown of the network to a total electricity blackout. We are going to discuss about these critical issues.

The Smart Grid

Our current electricity grid was built in the 1890, and was made to satisfy the electrical needs of the past century. But nowadays, it is not optimized anymore, our consumption of electricity has increased exponentially, the production means have changed and the technology has advanced. The new Smart Grid will consist in new technologies, automations and computers in order to answer to the quickly changing electricity demand. In addition of allowing a more efficient transmission of electricity, it is a perfect occasion to move to a greener world, as the grid can include renewable energy production, as wind and solar energy, and can manage it easily. It can support the charge of electrical vehicles as well.

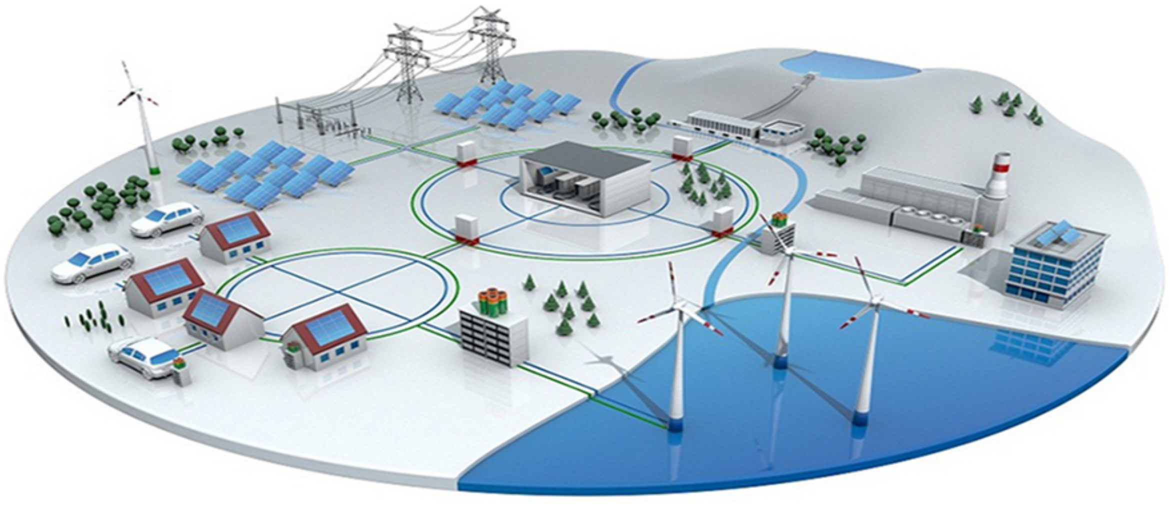

Figure 1 - The Smart Grid

The houses will progressively turn into smart houses. The owners of the smart houses will be able to control precisely their electricity usage, for example to avoid using a lot of electricity during the peak hours, when the price is high. They could for example, program from their smartphone the washer machine to run during the night, to enjoy the low-cost energy. And it will have a huge impact on the electricity distribution, because the customers can inform the distributers about the time they would need energy. All the electricity that is produced have to be instantly and totally use, because we cannot store it efficiently, so this two-ways communication grid will help the utilities to produce the exact amount of energy needed.

Furthermore, now at the peak hours, the utilities have to turn on additional power plants to satisfy the electricity demand. The smart houses will help reducing the amount of energy needed at peak hours, the electricity demand will become more constant, and the electricity rates will lower. Consequently, the utilities would not need the additional power plants, and less energy will be lost because unused. And the system will even allow the consumers to produce and sell electricity from their house, if for example they possess a solar panel.

Smart Grid Communication Network

The electricity distribution grid is a very complex physical network, as it contains a huge number of energy generators, distribution substations and customers. According to NIST's conceptual reference model, this network contains seven different logical domains. The *Customers* are the end users of electricity, they can use, store, generate and manage their use of energy. The *Markets* are the operator and participants in electricity market. The *Service Providers* are the organizations providing services to the consumers and utilities. The *Operations* manage the movements of electricity. The *Bulk Generation* generates electricity in large quantities, and may also store it in order to distribute it later. The *Transmission* carries the electricity over long distance, and can generate and store it. And finally, the *Distribution* distribute to and from the customers, it can also generate and store it. The *Bulk Generation*, the *Transmission*, the *Distribution* and the *Customers* feature two-way power and information flow, and the *Markets*, *Operations* and *Service Provider* feature information collection and power management.

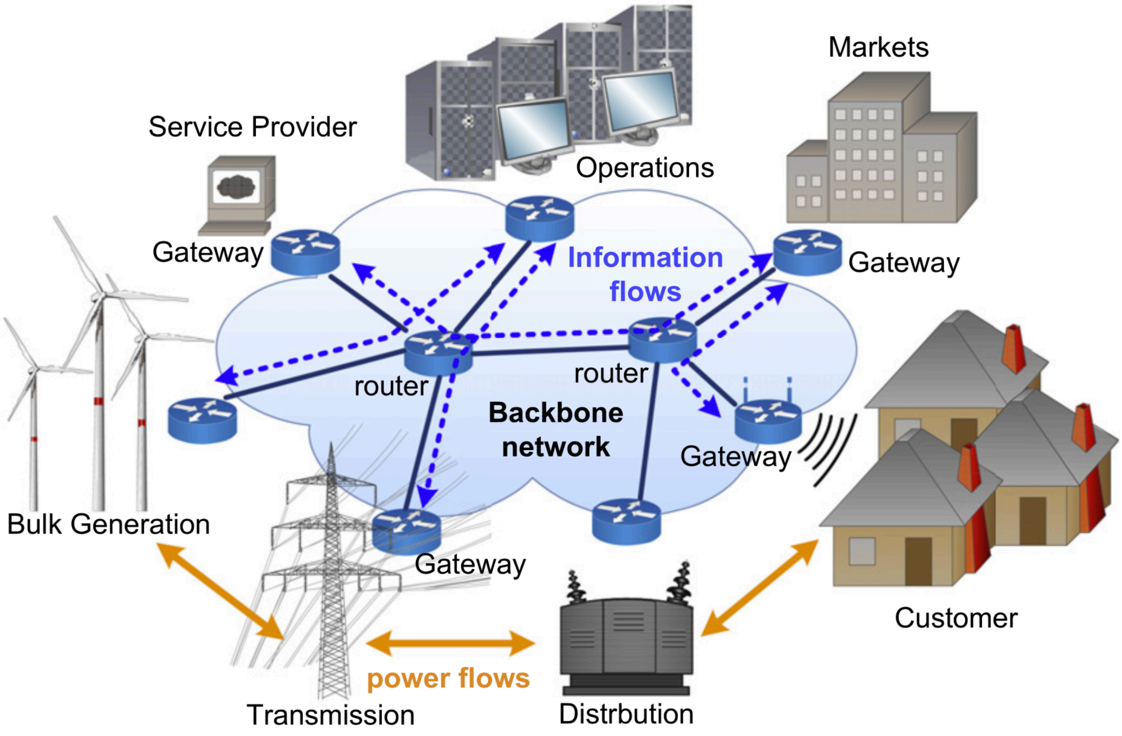

Figure 2 - The Smart Grid communication network

As shown in Figure 2, the backbone network is established for inter-domain communication. This network consists in routers and gateways linked by wireline communication technologies, as optical fiber, to allow high speed data between the different domains. For the intra-domain communication, a local area network composed of ad hoc nodes will be used. The ad hoc nodes can be sensors, meters or intelligent electronic devices installed on the power infrastructure. Many of these ad hoc nodes are supposed to use wireless technologies, such as Wi-Fi, but they can use the wireline technologies as well.

The Smart Grid communication is very similar to the Internet but has a few differences. The goal of the Internet is to have a high throughput to provide data services. But the Smart Grid network needs to provide reliability, security and real-time message delivery. So, the latency will be favorited over the throughput. The traffic is also different than Internet's one. The traffic of the Internet is irregular, as the World Wide Web (WWW) traffic, whereas in the Smart Grid network, a large amount of data flows periodically. The timing requirement for the Smart Grid is time-critical (3 ms) to best effort, while it is only delay-sensitive (100 ms) to best effort for the Internet. The communication model is not exactly the same, Internet uses end-to-end communication allowing global peer-to-peer, whereas the Smart Grid network uses a two-way communication model and would allow peer-to-peer only in local-area network for security purpose. The protocol stacks are slightly different, Internet is built upon the IP protocol, while Smart Grid also uses IP protocol, but is not limited to it, it can use heterogeneous protocol stacks as well.

The two most used communication protocols are DNP3 and IEC 61850. DNP3 is a protocol that was made public by General Electric in 1993. It was designed with four layers: physical, data link, transport and application layer. Now it has been ported over to TCP/IP layer to support end-to-end communication. IEC 61850 is a more recent protocol, and the main difference with the DNP3 is that it can support a variety of services including TCP/IP, UDP/IP and application-directly-to-MAC. DNP3 is intended to be replace by IEC 61850 in the power substations. But both initial design of DNP3 and IEC 61850 don't include any security system. So, it means that the packets can be intercepted or falsified in the network, which can lead to information leakage or incorrect operation in power device.

Attacks in the Smart Grid

The Smart Grid network needs to ensure at any moment *availability*, *confidentiality* and *integrity*. The system needs to be always available, otherwise the people using the network cannot use it properly, they cannot get or send any information. It requires confidentiality to protect privacy and proprietary information. And integrity needs to be guaranteed, because the destruction or modification of information can lead to incorrect decisions in the power management. Availability and integrity are more important than confidentiality for system reliability. So, the attacks will particularly be target these aspects, and try to compromise them. The main attack possible on the Smart Grid is the Denial of Service.

Denial of Service (DoS)

The Denial of Service attack targets the availability of the network. The DoS attacks usually degrade the communication performance and slow down the traffic and sometimes even make the network totally unreachable. There are many DoS attacks types at different layers:

- Physical layer. The channel jamming targets especially wireless communications. It is very easy for the intruders to launch a DoS attack at physical layer, as intruder doesn't need to connect to authenticated network, but only to the communication channel. Jamming attacks can go from slowing down the delivery of time-critical messages to a total Denial of Service.

- MAC Layer. The attacker can choose to change its MAC address in order to impersonate another device in the network, and send wrong information to the other nodes. Spoofing is really dangerous for the Smart Grid network as it compromises the integrity and the availability. For example, in a power substation network, an attacker could broadcast a wrong address resolution protocol (ARP) in order to prevent the other nodes to reach the gateway.
- Network and Transport Layer. In the Network and Transport Layer, the same attacks as the ones that are done on the Internet are possible. The attacker can flood the network with a huge number of request, and it will cause a slowdown on the network, this method is called traffic flooding. Or the attacker can also perform an attack called buffer flooding. This attack consists in filling the buffers of the host will data, that will cause a packet loss for most of the other requests as the buffers have a limited capacity.

Vulnerability attack

The vulnerability attack is induced by a malfunction in a device or in the network. The information circulating into the network may be deteriorated by inaccurate data or unreliable channel condition, which cause an incorrect control process at the control center. This vulnerability is more due to the unreliability of the channel than to a malicious attack.

Data injection attack

The goal of the data injection attack is to alter the measurement or the messages in order to manipulate the operations of the Smart Grid. This attack against integrity, is mostly used to make some little profits for the attackers in a local network.

Intentional attack

An intentional attack happens when the attacker is able to get a full understanding of the network topology and can use this knowledge to paralyze some fraction of nodes, with highest degree, in the network. If the attack is successful, then the result is the same as if the node has been removed from the network, from a graph-theoretic point of view. This kind of attack can be really harmful, because it is very effective in disintegrating the network and difficult to be detected as not all the nodes are attacked.

Eavesdropping

The eavesdropping is an attack on the confidentiality. The devices in the same network or the routers can record the messages that are not destined to them, and so violate the privacy of the message. It can result in the leakage of massive customer information.

Countermeasures

As the security of the Smart Grid is really primordial, because of the impact that attacks could have on the grid, it is crucial to find some countermeasures to these attacks. The primary security objective is the availability because if the network is down nothing is possible, so the most important attack to counter is the DoS.

DoS countermeasures

To counter an attack, the attack needs first to be detected. A DoS attack can be spotted if many packets larger than the threshold coming from the same MAC address are detected. It is the signal-based method. The Packet-based detection method consists in watching if there is a significant increase of packet transmission failures. The proactive method uses algorithms that try to identify DoS attacks at early stage, by sending packets to test the status of potential attackers. A hybrid method combining both proactive and passive methods can be used for more efficiency.

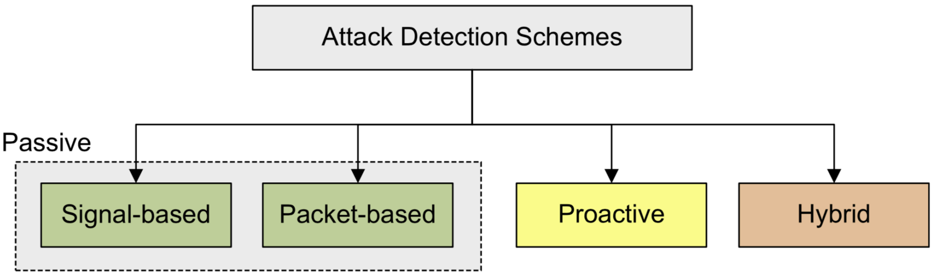

Figure 3 - DoS Attack Detection Schemes

Once we have detected the attack, the three most widely used approaches are *Rate-Limiting*, *Filtering* and *Reconfiguration*. The first strategy consists in setting a limit on a set of packets that have been characterized as malicious by the detector. It is mainly used when the attack stream cannot be precisely characterized. The idea about *filtering*, is to have a blacklist with all malicious sources addresses, and for every packet, we look up in the list to see if the sender is blacklisted. If it is the case, then the packets will not be forwarded or routed to the victims. To mitigate the impact of DoS attack, we can use the *reconfiguration*, which reconfigure the network architecture by changing the topology of the victim or intermediate network in order to isolate the victim from the attacker.

Cryptography

Cryptography is the best way to deal with attacks targeting integrity and confidentiality. Encryption is an elementary method to ensure secure communication and information protection. There are two main types of encryption methods, the Symmetric Key Cryptography and the Asymmetric Key Cryptography. The first one consists in using the same key for encryption and decryption. And the second one uses respectively private and public keys to encrypt and decrypt the data. Symmetric key cryptography requires less computational resource than asymmetric key cryptography, but needs to update the secret keys among network nodes complicating the process of key management. If the security keys are not compromised it is almost impossible to crack the messages encrypted with symmetric or asymmetric key cryptography.

Secure DNP3

The secure DNP3 is a security protocol based on DNP3. The improvement is mainly the insertion of a Security Layer between DNP3 and TCP/IP, as shown on Figure 4. This security layer helps the DNP3 protocol on basic security requirement on integrity and confidentiality. At the transmitter level, the security layer encrypts the data and send the encrypted message to the TCP/IP layer. At the receiver level, the security layer decrypts the data and send the decrypted message to the DNP3.

IEC 61850 and IEC 62351

IEC 61850 is a recent standard for substation communications, but do not have its own security mechanism. IEC 62351 comes to add security to the IEC 61850 process. IEC 62351 defines authentication and encryption mechanisms. Like for the secure DNP3, there is an encryption and authentication layer between the TCP/IP layer and the Application layer. This layer is used for time-critical messages based on TCP/IP in substation systems, and use data encryption. There is a second authentication layer between the MAC and IP layers. This layer is used for authenticating time-critical messages in IEC 61850 which do not pass through the TCP/IP layer. Compared with secure DNP3, IEC 6180 with IEC 62351 is a more modern power communication protocol that balance security and time-criticality in power systems.

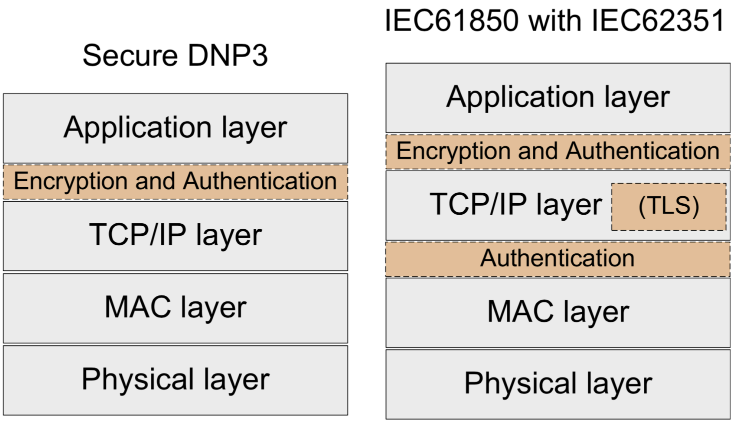

Figure 4 - Secure DNP3 and IEC61850 with IEC62351

Conclusion

Cyber security in the Smart Grid is still under development, and so it is not ready yet. There will be an attack and defense game, the attackers will pass through the security, and then the defense will develop a countermeasure and that game will enrich cyber security of the grid. So, the security is going to evolve with the time, and it will start when the Smart Grid will be ready to launch, before it is launched we cannot make real tests to be sure that the system is unbreakable for the hackers. It is harder to guarantee cyber security than on the Internet, because the security must be taken into account along with the electrical power systems. It is critical to keep discussing about it while the grid is evolving, to ensure the best security possible for the Smart Grid customers.

Sources

Wenye Wang, Zhuo Lu, “Cyber security in the Smart Grid: Survey and challenges“, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA, Available online 17 January 2013

Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi, Concordia University, “Communication Security for Smart Grid Distribution Networks”, Published in: IEEE Communications Magazine (Volume: 51, Issue: 1, January 2013), INSPEC Accession Number: 13196063

Pin-Yu Chen, University of Michigan, Shin-Ming Cheng, and Kwang-Cheng Chen, National Taiwan University, “Smart Attacks in Smart Grid Communication Networks”, Published in: IEEE Communications Magazine (Volume: 50, Issue: 8, August 2012), INSPEC Accession Number: 12895166

Xin Miao, Xi Chen, “Cyber Security Infrastructure of Smart Grid Communication System”, Published in: Electricity Distribution (CICED), 2012 China International Conference on, INSPEC Accession Number: 13500120

Patrick D. Gallagher, National Institute of Standards and Technology, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0”, January 2010

Figure 1: Retrieved from: http://solutions.3m.com/wps/portal/3M/en_EU/SmartGrid/EU-Smart-Grid/
Figure 2, 3 & 4: Retrieved from “Cyber security in the Smart Grid: Survey and challenges“ mentioned above