Analysis of Threats and Attacks Impacts on Smart Grid Networks

J. Horalek, F. Holik
University of Pardubice, Faculty of Electrical Engineering and Informatics, Pardubice, Czech Republic.
josef.horalek@upce.cz

***Abstract*—This paper introduces the results of theoretical and practical analysis of threats and attacks on Smart Grid networks. Authors introduce Smart Grid as a complex system composed from two basic subsystems. These subsystems have characteristics of pure data networks and grid networks. Due to the fact that these subsystems are interconnected into one complex Smart Grid system, it was necessary to conduct an analysis of their interrelations. A company focused on power distribution (located in the Czech Republic) was consulted about these relations and their influence on security. The paper also introduces analysis of reasons to conduct attacks on SG networks. Analysis also describes impacts of the most basic attacks on data networks, from the Smart Grid networks' point of view. The main contribution of the analysis is its practical impact on functionality of the whole Smart Grid and verification of the results within the complete Smart Grid environment.**

***Index Terms*—DDoS; IP Spoofing; MAC Address Flooding; Smart Grid Attacks; Smart Grid Networks; Smart Grid Security.**

I. INTRODUCTION

The current viewpoint on the Smart Grid (SG) topic is mostly as a system. This system contains well-known and precisely defined relationships between each component of the system. These components consist of a grid network (transferring electricity) and data network (transferring data frames or packets). Interconnecting these networks brings many security risks, even while the relationship of these networks are well defined. These risks have, in SG networks, a much larger impact, than the same risks in data networks. This is caused by higher availability required in SG networks. Current industrial networks based on TCP/IP and Ethernet are more vulnerable than similar traditional data networks. This is caused by the fact that manufacturers of industrial end devices like Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), etc. are focusing on the correct functionality of these devices, but not on integration of security protocols into these components. Some manufacturers even lack practical experiences from the field of data networks and data network security. Another reason is, that there is an assumption of physical separation of SG network from the Internet or other external networks. This assumption is often wrong, due to the necessity of data transfer into the controlling centralization systems. For threat analysis, communication realized using TCP/IP is essential. In the current state of the SG system, it is necessary to consider known attacks from the data networks and consider their applicability in the SG networks [1,2].

Control of devices in SG using communication infrastructure can be done using the following two options:

1. Using RTU – a PC with an interface with the following industrial communication standards: Modbus, Profibus, and IEC 60870-5-104 Slave for communication with master level. At the same time, RTU has an Ethernet connection with communication over TCP/IP and IEC 60870-5-104 protocol.
2. Conversion means (CONV) – it is an alternative to the "solution without an intelligent element". This means a solution without RTU in the rack for low voltage (LV) control. This solution requires creation of a transparent channel within LAN/MAN, for transferring industrial standards Modbus and Profibus. This traffic is sent to a higher control level, where data concentrator of LV is present. Instead of a RTU, converter, CONV is present. This device encapsulates the industrial traffic into TCP. This option is being used mainly for cost saving reasons [3].

Data and service networks for high voltage (HV) and LV are both based on TCP/IP. The goal is to create communication infrastructure for transfer of messages defined in IEC 60870-5-104. This network composes of router on a Distribution Substation (DTS) level, or of switch, if there is a requirement for more ports. Access from SG LAN into Smart Region MAN is always realized through a router [4]. Routers on all DTS should be connected with each other, in order to achieve redundancy in the case of transit device failure. All the routers should use a dynamic routing protocol (recommended and highly used is OSPF) and MPLS. Border routers (between LAN and MAN) should use a Virtual Router Redundancy Protocol (VRRP) for achieving high availability provided by router redundancy [5].

The paper is analyzing and testing the behavior of the SG network if an attack is realized on a data part of the SG system.

II. REASONS OF ATTACKS ON INDUSTRIAL SMART GRID NETWORKS

This part is firstly describing reasons to attack SG networks. Following, analysis of impact of these attack is conducted. Due to the very heterogeneous nature of the SG networks, the most suitable criterion for the attacks classification is their intention. The most common intentions are: data theft, denial of service, and service manipulation.

A. Data Theft

Systems of control and its other parts used in SG networks contain large numbers of sensitive information. This includes personal data of costumers like their name, address, billing information, etc. and information about network functionality like power consumption of individual consumers. If this data

is stolen, provided information can be used by competing companies or misused by the attacker. Especially interesting for the attacker can be data about power consumption of a household. Even while this data is typically summarized for the whole household, the attacker can use some form of extraction algorithm to get the un-summarized data [6]. It is then possible to recognize some electronic devices used in the household, or to learn a typical lifestyle and habits of the family. Fortunately, there are existing methods for secure data collection, using encryption [7].

B. Denial of Service

One of the most common attacks on any network is Denial of Service (DoS). This attack can be very easily done in SG networks, which typically does not have such a large link capacity as data networks. A typical DoS requires a large number of cooperating systems in order to bring a network down. These systems are usually ordinary devices, infected by a malicious software and used in the attack without an owners' knowledge. SG networks are very suitable to DoS due to their limited throughput and lack of security in industrial protocols and systems. The SG network in a DoS attack can be flooded by large traffic data, packets with duplicated IP address, or demanding network scanning. Even not a fully successful DoS can disrupt the correct behavior of the SG network. If the network load became higher than normal, strict latency requirements in specific parts of SG network cannot be meet. In some cases, these requirements can be as low as 3ms for GOOSE messages within a substation network [8]. Even other industrial protocols like Modbus, IEC 60870, or IEC 61850 all require real time communication.

C. Service Manipulation

Service manipulation affects control of services in order to influence the flow of electrical power, or to provide incorrect tariff information. It is very hard to prevent this type of attack, due to the real time operations of the SG network. The example of this type of attack is following: an attacker falsifies GPS timing information in order to receive electrical power in a different tariff group. Another example would be to improperly use energy resources, which are normally used only to equalize grid peak demands. Table 1 summarizes selected targets of SG attacks, their influence and impacts.

Table 1
Targets of attacks and their impacts in SG networks

Attack targets	Possible influence	Impacts
Transformers	Voltage/frequency changes	Lifetime of transformers, security of the substation, security of grid network, control of stress situations
System for energy management	Network load, historical statistics	Errors in system for energy management and automatic meter management, wrong tariffication of electrical power
Smart meters	Consumption of electrical power, gas, water	Data from smart meters, billing system, information for costumer, system of electricity demands
Events and notifications in SG network	Wrong events, notifications and other system messages	All information, events and notifications

III. Comparison of Attacks, Threats and Security in Data and SG Networks

Data and SG networks have many common features in the field of communication. The following section describes the most important attacks and their impacts on SG networks. Only the most specific and common attacks in the SG area are described. Comparing to the data networks, impacts of attacks on SG networks can have more serious consequences. There are also a lot of motives for attacking SG networks, comparing to data networks. On the TCP/IP level, conducting attacks is very easy similar to both SG and data networks. Different are the attack targets, methods of network penetration and aimed services. This is often caused by the physical separation of SG networks from the Internet. If data has to be sent from a device to the control center via the Internet, a secure tunnel connection using encryption is typically used. Table 2 summarizes the most notable differences between SG and data network security, in a typical industrial environment.

Table 2
Comparison of security in SG and data networks

The security component	SG network	Data network in a corporate environment
Antivirus	Unusual / Problems of implementation	Commonly available / easy implementation
Lifetime of components	About 20 years	Most often, 3-5 years
Outsourcing	Very limited usability	Common and easy to use
Components updates	Specific according to specific needs	Regular / planned
Real-time operation	Absolutely essential for security	A small delay is acceptable
Security testing	Rarely (rules for operating network)	Planned and standardized
Physical security	Very variable according to the situation and equipment	High
Knowledge of safety	Increasing	High
Confidentiality of data	Low - Medium	High
Data integrity	High	High
Data availability	24/7/365	In some cases, acceptable downtime
The requirement for lossless data	High	Medium

A. MAC Address Flooding Attack

MAC address flooding is a well-known attack in data networks and is therefore relevant even for SG networks. The basic protocol used in SG networks; for protection, management, data and service networks; is Ethernet [9] as shown in Figure 1. All the switches using Ethernet are vulnerable to the same type of attacks like in data networks.

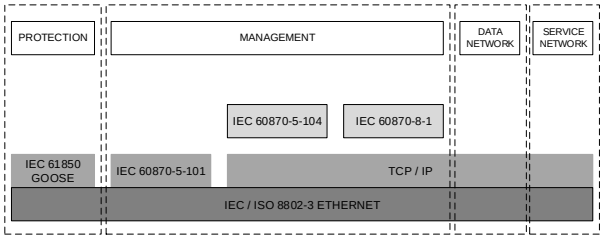

Figure 1: Protocols used in SG networks

In MAC address flooding, the attacker is generating a large amount of frames with random MAC addresses in order to fill the switch MAC table. This table contains mapping between ports and MAC addresses available on each of these ports. If the table gets full, the switch will transit into a fail open state and start to behave like a hub. In this mode, all received frames are forwarded on all the ports (except the receiving one). This means that the attacker, connected to a one port, can capture all the traffic coming through the switch. This action requires a packet capturing tool, able to gather frames in promiscuous mode. Captured frames can be used in the Man-in-the-middle attacks.

In data networks, a MAC address flooding attack, is used to collect all the traffic otherwise unavailable to the attacker. If this traffic is not encrypted, the attacker can read all the communication data, including user names and passwords. The attacker can also just observe and analyze the type of communication present on the network. This attack also negatively affects the network performance, due to the amount of otherwise unnecessary traffic.

Impacts of this attack in SG environment are very similar, but it is important to consider the nature of transferred data. This data contains sensitive information about costumers including their power consumption and state of devices located in grid network, power plants or cogeneration units.

Risk of misuse of these data by a third party or competing companies is high. Defense against a MAC address flooding attack, is the same in both SG and data networks, and is based on securing switch ports. In Cisco switches, commonly deployed in a SG network, the function *switchport port-security* allows the limitation of number of MAC addresses learned on the port, and even to specify these addresses. MAC addresses can be learned *statically, dynamically* or as *sticky* (learned dynamically, but saved into the configuration like in *static* mode). The *switchport* feature also allows a specification of action on security violation. These actions are *protect* (drop traffic only), *restrict* (drop traffic and notify), and *shutdown* (shutdown the port and notify – port must be manually enabled in order to work again) [10].

B. DoS Attack

A DoS attack causes service unavailability by overloading a server or network infrastructure. The principle of this attack is to exhaust target system resources like bandwidth, CPU performance, or disk storage. The second option is to disrupt network forwarding functionality via routing information modification, or to reset the TCP connection. The most common targets of DoS attack are servers hosting many critical services which are essential for the correct functionality of the company.

One example of a DoS attack in TCP is SYN flood. An attacker is sending SYN packets for establishing a TCP connection with a non-existent source IP address. The server is then waiting for the acknowledgment packet in the half-open state. This state consumes server resources and is typically maintained for 60 seconds. If there is a sufficient number of half-opened connections, services like emails, data transfer, and web pages, became unavailable.

Nowadays, a distribution variant of DoS called DDoS (Distributed DoS) is often being used. In DDoS, many computers are participating in the attack, so it is easier to overwhelm even the most powerful servers and links with high throughput. For an effective attack, so called zombie networks, controlled by the attacker, are often used.

In the recent times, attackers begun to target application logic, more than networking infrastructure. This is based on the fact that service response, use much more computational performance than clients request. This principle ensures that even average, or below-average devices like a laptop or tablet can, under certain circumstances, overload a much more powerful server hosting the service. This type of attack is very dangerous in data networks, because it can be conducted very easily. On the other hand, typical services in data networks are usually not critical, and temporal unavailability is not such a problem. In the SG networks, these services can be represented by the Supervisory Control and Data Acquisition (SCADA) systems. These systems are used for grid control and their unavailability therefore presents a high danger. Other devices particularly vulnerable to DoS, are devices used for smart metering. These devices have very limited computational capabilities and to overload them is therefore very easy. A similar situation is with IEDs. Some of these devices even do not support certain types of traffic and receipt of this kind of traffic can cause them to fail. Therefore, even the simple ping can overwhelm them, and bring them down. If the smart meters are offline, it is impossible to gather current consumption, and the distributor has to find another way to bill the customer. If the DoS is successfully launched at a Remote Terminal Unit (RTU) for switching low or high voltage, the dispatching center must send a team for physical examination of the unit. The device in offline state cannot be controlled by the attacker, but also cannot maintain its functionality. This makes DoS especially serious if the attack is combined with an attack on physical infrastructure.

The defense against DoS is never simple or one hundred percent reliable, but there are ways and practices to minimize the risks from these attacks. On the TCP/IP level, the defense is the same as in data networks, and it is recommended to integrate it into SG infrastructure. A particular solution depends on the networking equipment manufacturer, but it can be Cisco Guard Top Layer or Juniper solution. It is also appropriate to optimize traffic flows in the SG network and to use links with sufficient bandwidth capacity. Moreover, there are techniques to protect SCADA systems with Intrusion Detection Systems (IDS) [11]. The following techniques can be also used to minimize the risks from DoS attacks against SG networks:

- *Blocking of ICMP and UDP* – both of these protocols are often used for DoS attacks and are not typically essential in the working SG network.
- *Filtering of incoming traffic* – some traffic can be denied on the SG network boundary. Example are packets with a private source IP address coming from the Internet, or packets with an unknown source IP address, if it is possible to specify all connecting devices.
- *Disabling broadcast traffic* – this traffic can be otherwise used to increase the attack strength via Smurf or Fraggle attacks. Broadcast traffic can also negatively influence the network performance.
- *Authentication of routing table modifications* – ensures, that routing tables cannot be modified by an attacker. Unauthorized modification could result in packet forwarding to the destinations, which the attacker chooses. This can result in Man-in-the-middle type of attack, data theft, or service unavailability.
- *Use of a "trash" router* – which can collect all redundant traffic for later analysis.

- *Use of SDN* – which can increase the security in many ways, depending on the logic programmed in the SDN Controller. A typical application for DoS defense could detect increased suspicious traffic and subsequently insert a flow rule to temporally block this traffic type. All the subsequent packet can therefore be blocked in hardware of the switch with-out Controller participation. Another option is to insert a different flow rule, which redirects suspicious traffic into separate virtualized network made specifically for traffic analysis. This can be realized by an end device with a packet capturing tool and analyzer. Analyzed data can be later used to increase the network's security.

In the case of an attack, security of SG networks can be restored by the option to switch, all electricity distribution and control devices, into manual mode. In this mode, the network has no intelligence, but it is fully functional. Each device can be controlled only physically, for example in a distribution substation. This option provides enough time to solve the ongoing attack and to return to partially or fully automated control without the electricity supply failure.

C. IP Spoofing

IP spoofing is not a dedicated attack, but it is rather a technique used in many other attacks. It can also be used in DoS attacks, or attacks on Access Control Lists (ACLs) by breaking through IP address security.

IP spoofing falsifies an attacker's IP address in order to hide his real address or to overcome any security based on source IP addresses. The most vulnerable services to IP spoofing are Network File System and Server Message Block. If the attacker is successful, he can continue with the Man-in-the-middle attack. In this type of attack, the attacker pretends to be one of the two entities in the communication. The second side is unaware of ongoing attack and the fact, that com-munication goes to the attacker. The attacker can therefore easily steal sensitive information like passwords. If TCP protocol is used, the situation is for an attacker more complicated. TCP for every connection uses sequence and acknowledgment numbers, which have to correspond. If the attacker is in the same network as the victim, he can easily capture these numbers from the regular communication. If he is not in the same network, he cannot capture these packets and the process becomes much more difficult. This is caused by functionality of modern operating systems, which generate these numbers randomly.

By IP spoofing, the attacker can also get access to the networking devices. These devices often allow administrative access only to verified source IP addresses, which attacker can spoof. He can then change settings of the entire network. This can also result in Smurf and Fraggle attacks, or DoS attacks with hidden identity.

Impact of the attack in SG networks can be critical when compared to data networks. In data networks, impacts as change of configuration, non-functional web browser or email client are inconvenient and can cause financial loss. Nonetheless, the same attack in SG networks is much more dangerous. If the attack is combined with other attacks, an attacker can present himself as a control device for the entire SG network. He can then use RTU to shutdown electricity from the selected part of the grid. If the attacker continues with DoS attack on RTU, this device will become unavailable, so the legitimate control center is unable to remotely access it and restore the correct behavior. The only other option is then to send a team of technicians to correct the problem physically.

Similarly, like for many other attacks, there is no ultimate defense against IP spoofing. Risk can only be minimized by the correct security setting. The first step is to filter packets from the private address range. This ACL has to be placed on a border router and set on Internet interface in the incoming direction. On the same interface, but in the opposite direction (to the Internet), a second ACL should be placed, blocking all packets with source IP address range, which is different from the one used inside an internal network. This measure prevents IP spoofing. Another precaution is to use authentication and encrypted data transfer whenever possible. This includes routing protocols and protocols for network control and management.

An example of a security measure against IP spoofing, is technology Reverse Path Forwarding (RPF), which is widely available on Cisco devices [12] (typically used in SG networks). RPF checks the source IP address of packets and compares it with the routing table. Packets with IP address from a different subnet than the interface's IP address are dropped.

IV. Conclusions

The goal of this paper was to analyze security threats and their impacts on a data network part of the SG system. Firstly, the concept of the SG as a system with a large number of different components with distinct features was introduced. Reasons of attacks to SG networks were listed and their impacts were evaluated based on technical knowledge.

The main part of the paper introduced individual types of attacks. For each attack type, analysis of impacts, and threat level to both coherent subsystems of SG system was conducted. Emphasis was put on comparison of chosen behavior of data networks and SG networks. Security risks and functionalities of these networks were also described. This research was based on practical experiences of authors and testing in the isolated environment of a power distribution company. Presented analysis is nowadays used as a basis for testing of SG networks, which are implemented in the electrical environment of the Czech Republic.

Acknowledgment

This work and contribution is supported by the project of the student grant competition of the University of Pardubice, Faculty of Electrical Engineering and Informatics, Intelligent Smart Grid networks protection system, using software-defined networks, no. SGS_2016_016.

References

[1] Begovic, M.M.: Electrical transmission systems and smart grids: selected entries from the Encyclopedia of sustainability science and technology. Issue 1, pp. 326. Springer, New York (2013). ISBN 14-614-5829-3.

[2] Xiao Y.: Communication and networking in smart grids. First edition, pp. 309. CRC Press, Boca Raton (2012). ISBN 14-398-7873-0.

[3] Borlase, S.: Smart grids: infrastructure, technology, and solutions. First edition, pp. 577. Taylor, Boca Raton, FL (2012). ISBN 978-143-9829-059.

[4] Stephens J., Wilson E., Peterson T.: Smart grid (r)evolution: electric power struggles. First edition, pp. 218. Cambridge University Press, New York (2015). ISBN 978-110-7635-296.

[5] Knapp E., Samani R.: Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. First edition, pp. 202. Elsevier, Amsterdam (2013). ISBN 978-159-7499-989.

[6] Hewett R., Rudrapattana S., Kijsanayothin P.: Smart Grid Security: Deriving Informed Decisions from Cyber Attack Game Analysis. In: Smart Grid Communications, pp. 946-951. IEEE, Venice (2014). DOI: 10.1109/SmartGridComm.2014.7007770

[7] Yang L., Xue, H., Li F.: Privacy-preserving data sharing in Smart Grid systems. In: Smart Grid Communications, pp. 878-883, Venice (2014). DOI: 10.1109/SmartGridComm.2014.7007759

[8] Lopes Y., Fernandes N., Bastos C., Muchaluat-Saade D.: SMARTFlow: a solution for autonomic management and control of communication networks for smart grids. In: ACM Symposium on Applied Computing, pp. 2212-2217. ACM, New York (2015). DOI: 10.1145/2695664.2695733

[9] Horalek, J., Sobeslav V.: Data networking aspects of power substation automation. In: Communication and Management in Technological Innovation and Academic Globalization - Proceedings, pp. 147-153 (2010). ISBN: 978-960-474-254-7.

[10] Cisco: Configuring Port Security (2013). Available: http://goo.gl/iQwp5M

[11] Gao W., Morris T., Reaves B., Richey D.: On SCADA Control System Command and Response Injection and Intrusion Detection. In: eCrime Researchers Summit, pp. 1-9, TX, Dallas (2010). DOI: 10.1109/ecrime.2010.5706699

[12] Cisco: Configuring Unicast Reverse Path Forwarding (2014). Available: http://goo.gl/KxgaEp.