CYBER SECURITY OF SMART GRIDS INFRASTRUCTURE: PROTECTIVE MEASURE AGAINST ATTACKS

Balduino Estison Mugilila CAMACHI[1], Dan POPESCU[2]

This article discusses two methods, one method is intrusion and the other method is to protect the network. The purpose of this paper is to illustrate the vulnerabilities found through the studies, mainly through the Methods of preventing an attack of a Smart Grid. Understanding the impact of attacks on a smart grid communication depends on understanding the concept of cyber incident. The main goal of this article is to prevent cyber-attacks of Smart Grid using MAC Value Analysis. Other goal is to protect the network from the respective attack, the tests and simulation will be shown in the experimental results.

Keywords: Smart Grid, SCADA, Cyber Security, Attack, Network, MAC address, IP address

Abbreviations

SG	Smart Grid
SCADA	Supervisory Control and Data Acquisition
IED	Intelligent Electronic Device
NIST	National Institute of Standards and Technology
MAC	Media Access Control
IP	Internet Protocol
GOOSE	Generic Object Oriented Substation Events
ARP	Address Resolution Protocol
HAN	Home Area Network
NAN	Neighborhood Area Network
WAN	Wide Area Network
DNP3	Distributed Networking Protocol 3.0
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT	Information Technology

1. Introduction

Smart grids (SGs) are electrical grids that use digital technologies to control, monitor and automate the entire generation, transmission and distribution of electricity [1]. The deployment of SGs can be considered a technological revolution in the electric power sector, especially in the distribution segment.

[1] PhD student, Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: estison@hotmail.com

[2] Prof. Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: dan_popescu_2002@yahoo.com

There are several expectations regarding the expected benefits, worldwide the main objectives are: reduction of commercial loss rates, improvement of the quality of energy supplied, energy efficiency and reduction of operating costs [2].

In recent years, power system has faced several cyber related attacks which have raised the question regarding the security vulnerabilities and its large-scale impact on the critical power system infrastructure. Some significant issues related to cyber-attack on the power grid are discussed in the following section [1]. Since power grids are essential to the physical and economic well-being of a nation, with the deployment of SGs solutions, it is imperative that safety should be considered to protect the critical assets of the electric power system. According to the annual report of the ICS-CERT in 2014, the energy sector received 32% of cyber-attacks in urban infrastructure services in the United States [3]. Usually, the focus of cyber security is related with IT systems, aiming at protecting information and information systems, regarding to unauthorized access, use, modification or any type of action that could compromise the privacy, integrity or availability of the information. However, cyber security for SGs requires a combined focus of information security for IT systems, the communications network, and physical electrical network equipment.

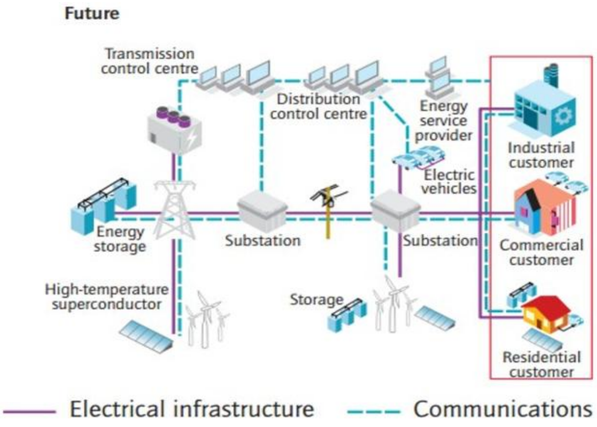


Fig. 1. Future vision of smart grid systems [1]

Fig. 1 represents a future vision of SG system, where it is possible to observe the strong dependence between the electrical system and the communication networks [1]. But these deployments can also create new vulnerabilities if appropriate security controls are not considered. Without proper care in designing the communication architecture, as well as in the choice of data communication technologies, especially wireless technologies, the system may not be secure enough and can be subjected to cyber-attacks. As the architecture of SG is based on telecommunications networks, thus advantages and disadvantages should be the object of analysis to define the architecture to be adopted [4].

2. Methods and Materials

2.1. Smart grid features

The SG concept is evolved to make the power grid more energy efficient and intelligent. It is an advanced network that manages the demand for electricity in a sustainable, reliable and economical way, based on an advanced infrastructure adapted to facilitate the integration of all its components. Electricity is the most versatile and most widely used form of energy, and its demand is growing all over the world. However, electricity production is the primary source of carbon dioxide emissions, which implies a major influence on climate change. To mitigate the consequences of climate change, the current electricity system must suffer major changes. Moreover, SG systems are expected to enable electric vehicles as replacements for conventional vehicles, reducing energy used by customers and reducing energy losses within the grid [5].

2.2. Smart grid conceptual model

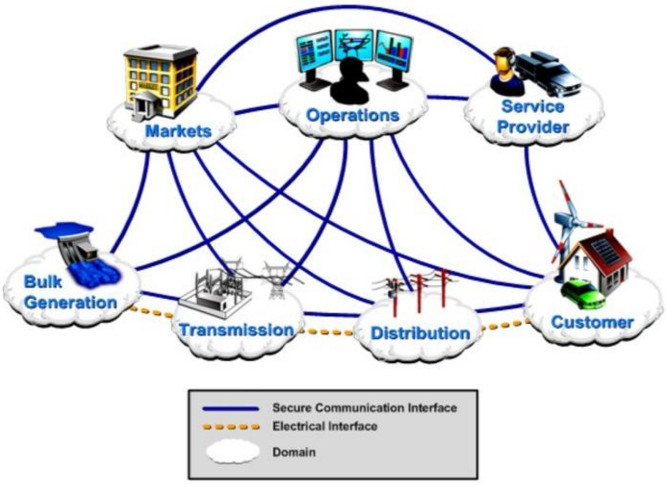


Fig.2. Smart grid conceptual model based on NIST [1][6]

The NIST defines the architecture of SGs with a model that consists of seven domains, defined as follows [6]:

- Customers - the end user of electricity, which can also generate, store and manage the use of energy. Usually, customers are categorized as residential, commercial and industrial.
- Market - operators and contributors in the market for the purchase and sale of energy;
- Service providers - are the organizations that provide electricity services to customers and concessionaires;

- Operation - energy flow managers at all levels, from generation, transmission and distribution;
- Generation - which includes traditional centralized generation and distributed generation;
- Transmission - responsible for transporting energy over long distances;
- Distribution - distributes electricity to customers.

2.3. Smart grid systems

Specialized systems are fundamental components for SGs and are responsible for centralizing and integrating the information generated by sensors, actuators, customers and collaborators in the field and operations center. SG is composed of several distributed and heterogeneous applications, including AMI (advanced metering infrastructure), EMS (energy management system), DMS (distribution management system), SCADA, GIS (geographic information system), CIS (customer information system) and BS (billing system).

2.4. Smart grid network protocols

There are several models and technologies for the implementation of SGs, each energy distributor should consider in the implementation project the relevant situations, communication models and telecommunications available in the region, as well as the ease and costs to support the infrastructure. In the design of the SG deployment architecture, in addition to the items previously mentioned, it is necessary to carefully analyze which technology is best suited to the needs and objectives of the utility. For example, the required signal range may differ according to the physical characteristics of the installation region, as well as the required maximum and minimum bandwidth, which may differ according to the volume and frequency at which the data will be transmitted. However, it is important to point out that the safety issue must also be the object of study and the analysis in the architecture design must be carried out to determine which technologies must be used. Table 1 represents potential data communication technologies for the implementation of SG.

Table 1

Smart grid technologies [7]

Technology	Spectrum	Bandwidth	Range
GSM, GPRS	400-1800MHz	Up to 170kbps	1-10 km
4G	2.5 GHz	Up to 200 Mbps	1-50 km
WLAN IEEE 802.11	2.4-5.9 GHz	Up to 155 Mbps	1-300 m
WiMAX	2.5 GHz, 3.5 GHz, 5.8 GHz	Up to 75 Mbps	1-5 km, 1-5 km, 10-50 km
PLC	3-500 kHz, 1.8-30 MHz	Up to 3 Mbps	1-3 km
ZigBee	2.4 GHz,	Up to 250 kbps	30-90m

	868-915 MHz		
Bluetooth	2.4-24835 MHz	Up to 721 kbps	1-10 m

Distributed and heterogeneous applications in SG require different communication protocols. Fig. 3 illustrates the SG network architecture and the protocol used within each network. In the HAN, home appliances use ZigBee and Z-wave protocols [8]. In the NAN, devices are usually connected via IEEE 802.11, IEEE 802.15.4, or IEEE 802.16 standards [8]. In the WAN and in SCADA applications, several industrial protocols are used specially DNP3 and Modbus (Modicon Communication Bus) [9]. Within substation automation, protocol IEC 61850 is used [10].

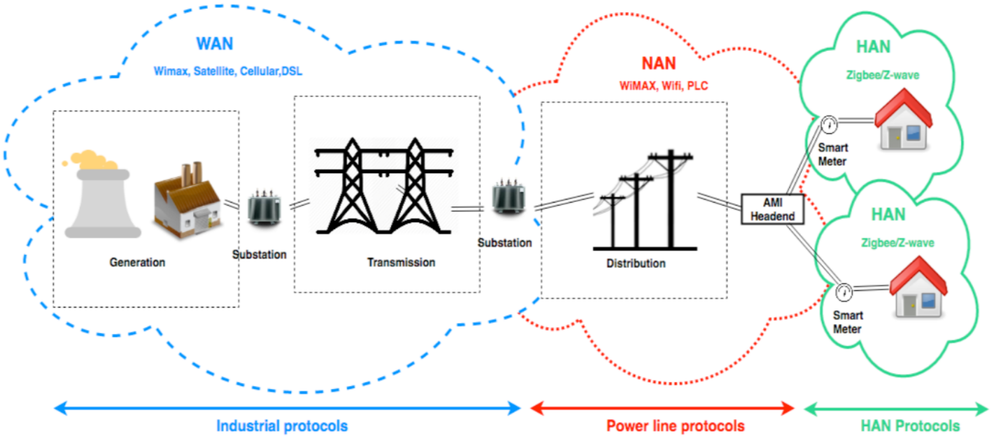


Fig. 3. Typical smart grid architecture [8]

3. Security requirements of smart grids

SGs technologies are expected to introduce new components into the power grid, many of them will be the key to interoperability and reliability, communicating bidirectionally, and being responsible for preserving confidentiality, integrity and vital availability for the operation of systems. Cyber Security for SGs should also support the reliability of the electrical network and the confidentiality (and privacy) of the information that is transmitted. Knowing that a country's national and economic security depends on the reliable functionality of critical infrastructures, it is necessary to have a structured Cybersecurity approach to help owners and operators of those infrastructures manage cybersecurity-related risks and, at the same time, protect business confidentiality, individual privacy and civil liberties [11]. Usually, cyber security for IT emphases on the protection needed to ensure the confidentiality, integrity, and availability of electronic reporting systems. When it comes to SGs, cyber security needs to be properly applied to the IT communication system, combined with the power system and domains previously mentioned to maintain SG reliability and consumer information privacy.

Thus, cyber security in SGs should include a balance between cybernetic system and IT processes and operations and governance of the electrical system. In addition, safety and reliability are paramount in power systems; however, all cyber security measures in those systems should not impede the operations of the power system [12]. The NIST has defined three criteria required to maintain security of information in the SG and keep it protected, specifically confidentiality, integrity, and availability [5].

4. Experimental Results

The present work intends to present two experimental results: SG attack and SG countermeasure of this attack.

4.1. Case study 1 – Smart Grid attack

To perform the simulation, was used the Arena Simulation software. Arena is a discrete event simulation and automation software developed by Systems Modeling and acquired by Rockwell Automation in 2000. In Arena, the user builds an experiment model by placing modules (boxes of different shapes) that represent processes or logic. The proposed testbed consists of two Control Centers, two Substations as illustrated in Fig. 4. All subsystems are connected through LAN, using industrial communication protocols. The details about this testbed are in the next subsection.

Control Center: In this test bed, there are two different protocols for the Control Centers, as we can see in Fig. 4: ICCP (Inter-control center communication protocol) over TCP/IP and IEC 60870-5-101 Serial. IEC 60870-5-101 protocol is a serial based communications protocol. This protocol is designed to be used on systems where there are permanent direct connections between Control Centers and Substations. And the ICCP protocol is usually used for communication between Control Centers. DTS (Dispatcher training simulator) also known as an OTS (operator training simulator) is used for training of operators and simulation of system operation, control and restoration scenarios.

Power System and Substations: The test bed contain three parts: power system simulator, user interface and IEDs. The so-called GOOSE communication service provides the user with a high-speed control messaging capability. This service allows transmitting messages with states, controls and analog measurements through the network for use by other devices in horizontal communications - peer-to-peer [13]. The power system simulator and user interface communicate through OPC (allows clients and servers communicate with each other).

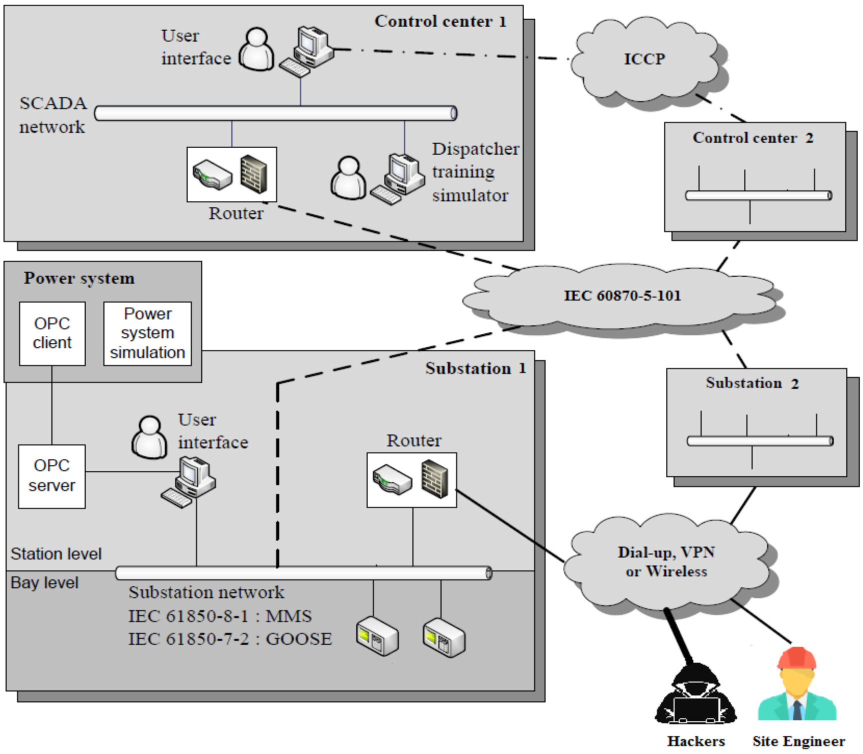


Fig. 4. Simulation for cyber security

Hacker: In this simulation it’s supposed that the substation has remote access point: dial-up and VPN for the site engineers that are not in the substation. The hacker can access a substation network through dial-up and VPN and perform malicious activities such as ping sweep, port scan, eavesdrop, modify packet and access user interface or an IED. In this case are presented only results associated to access controls. The tool used to perform a network scan is ZMap. ZMap is a network scanner designed to perform full scans over a range of IPv4 addresses, or in large portions. Developers say ZMap is a tool for researchers and should be kept in mind that when running ZMap, we are potentially scanning entire ranges of IPv4 addresses at a rate of 1.4 million packets per second. They advise when performing even small scans, we should contact the network administrator [14]. For a better performance of results, it is better to use Linux over Windows, the command must be used as root. The results were a big csv file, in the following table were filtered the vulnerable ones. Table 2 represents the result of the IPv4 addresses that are unprotected. With this IP address’s list is possible to perform the DoS attack, to make the machine unavailable temporarily.

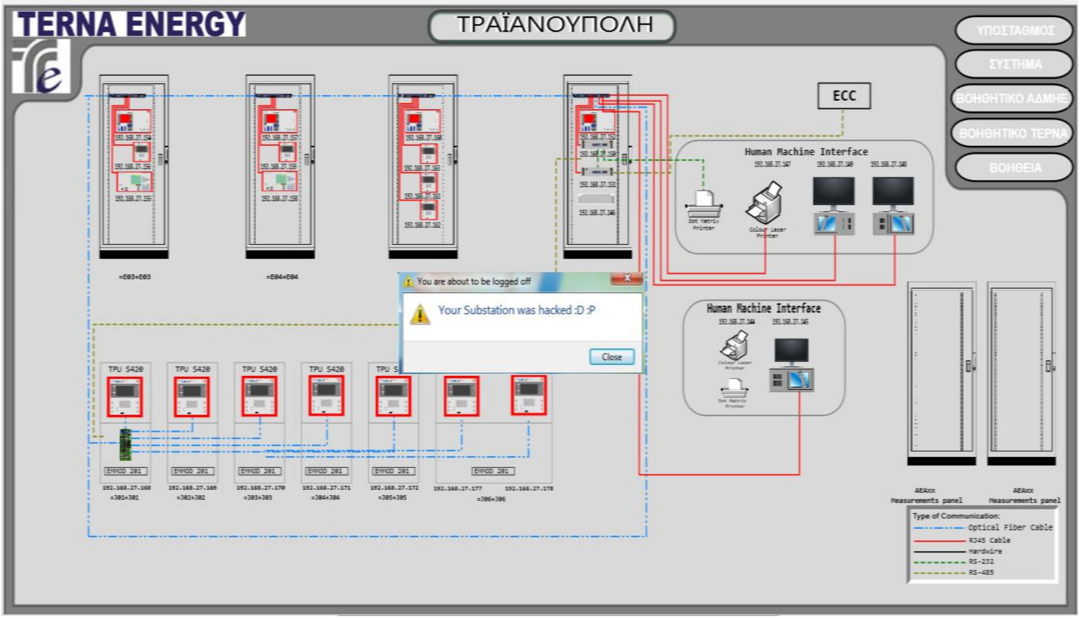
This kind of attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Table 2

Zmap ping results

IPv4 Addresses	Latency	MAC Address	Host
192.168.27.1	1ms	00:1E:32:AB:52:ED	Host is up
192.168.43.1	31ms	D8:D3:85:EB:12:E3	Host is up
192.168.34.112	80ms	00:0C:29:07:CB:15	Host is up
192.168.27.150	1ms	00:80:C8:E3:4C:BD	Host is up
192.168.43.229	3ms	D0:BD:9C:26:A5:31	Host is up
192.168.0.23	5ms	00:80:C8:E3:4C:BD	Host is up

But the main goal was to shut down the target machine through “cmd”. The main target as it is possible to be seen in Fig. 5 is “Terna Energy”, the Substation name is Traianoupolis, from Greece.



You are about to be logged off

Your Substation was hacked :D :P

Fig. 5. SCADA substation being shutting down

To shut down the machine was used a simple command from “cmd” as administrator “shutdown -i” (windows cmd) and then is opened another window with the option to add the computer that has to be shut downed, was chosen the IPv4: 192.168.27.150, and there is an option to write a comment before performing the shut down as can be seen in the Fig. 5.

A real example is a solar panel substation made by Efacec in 2013 in Targu Mures - Romania, which was connected via remote access but with harmless/basic protection, was invaded by intruders and they had access to the database using known methods of intrusion into a network. Luckily the substation was not connected into a SG, and the problems were minor, but if it had been connected into a SG, it would be a serious problem and difficult to solve.

4.1.1. Case study 1: Conclusion

From the studies made it is possible to observe that the remote access will increase the level of power system digital safety risk of the SG, once opened certain ports the SG is compromised. Actually with this new technologies, it is inevitable to have access to a SG only from the communication network that covers the SG, but we must think about the risks that everyone knows, as explained above, the methods are known, and in order to avoid it, is even necessary to consider a more rigid protection. The conclusion is that substations or SGs connected over the internet is not safe. It's proposed to be avoided at the moment the use of internet thought SGs or substations, one of the best solutions is to be connected through an isolated network, in other words the use of fiber optic between substation and Control Centers as used in Transelectrica – Romania.

4.2. Case study 2 – Smart Grid protection

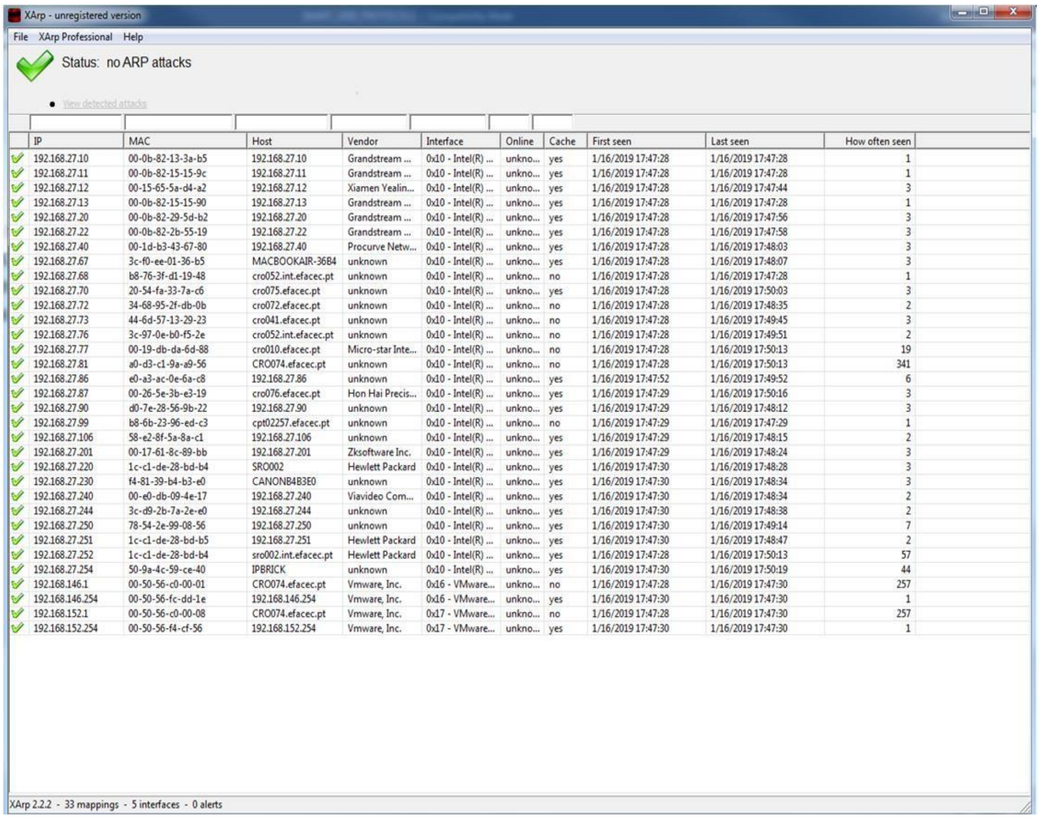
In this case study the testbed is the same as the one presented in the first case study, the tests were made in a different way, the test made was to protect the grid from an ARP cache poisoning. Most of the time we cannot predict the attacks, but we can prevent some attacks that are well known. Although not the focus of the case, there is another way to perform attacks, with smart meters, but in this case, we didn't test this possibility. Smart meters are possibly the weakest link in SG security, smart meters are far away the heart of the system, but there is a point that we have to take in consideration, usually the companies send a person to connect/disconnect the meter, but it can be performed as well remotely, and it shows the danger if someone has access of many smart meters, a blackout may occur. Right now, we must putour efforts to prevent such attacks in future.

After scanning the network, was used a tool named Scapy. To launch the attack to gain access, from Windows/Linux's terminal the command "arp-a" is executed to check the associated ARP cache to check the MAC addresses associated to the scanned IP's, was collected the MAC addresses of the targeted machine randomly, with the Scapy tool is possible by convincing the target machine that the attacker is the gateway, and then convincing the gateway machine as well that all traffic should pass thought the attacker machine. Before starting "Scapy" is installed on a Linux platform ($ pip install scapy) and then the tests done using the ARP poisoning script, the script does the following steps [15]: Define constant values, set our interface card, and turn off output. Resolve the gateway and target MAC address. The function "**get_mac**" use the "**srp**" method to emit an ARP request to an IP address to resolve the MAC address. Start the poison thread to perform the ARP poisoning attack. This will start the sniffer that captures the packets. The function "**poison_target"** builds ARP requests for poisoning both the target IP and the gateway (in a loop). Write out the captured packets and restore the network. The function "**restore_target**" sends out the ARP packets to the network broadcast address to reset the ARP caches of the gateway and target machines. After these steps it’s possible to forward the packets along both gateways (including attacker gateway). To convince the target machine we used the following command from Linux terminal:

“~# echo 1 /proc/sys/net/ipv4/ip_forward”

The simulation tools used in this case are the following: ZMap, XArp and Scapy. XArp is a security application that uses advanced techniques to detect ARP based attacks. Using active and passive modules XArp detects hackers inside your network. ARP spoofing attacks are not detected by firewalls and operating systems [16]. Scapy: is a powerful program for handling interactive packets. It is capable of forging or decoding packets of a wide number of protocols, sending them on the wire, capturing them, making matches requests and replies, and much more [16].

Unlike the previous case, on this case were used XArp that helped to identify threats on the system as IP/MAC modifications. This tool is very useful because sends notification of modification in the network. With the help of XArp, it’s possible to create an ARP table with the all devices connected on the network: Fig. 6 represents the network before the attack, and Fig. 7 represents the network after the attack.

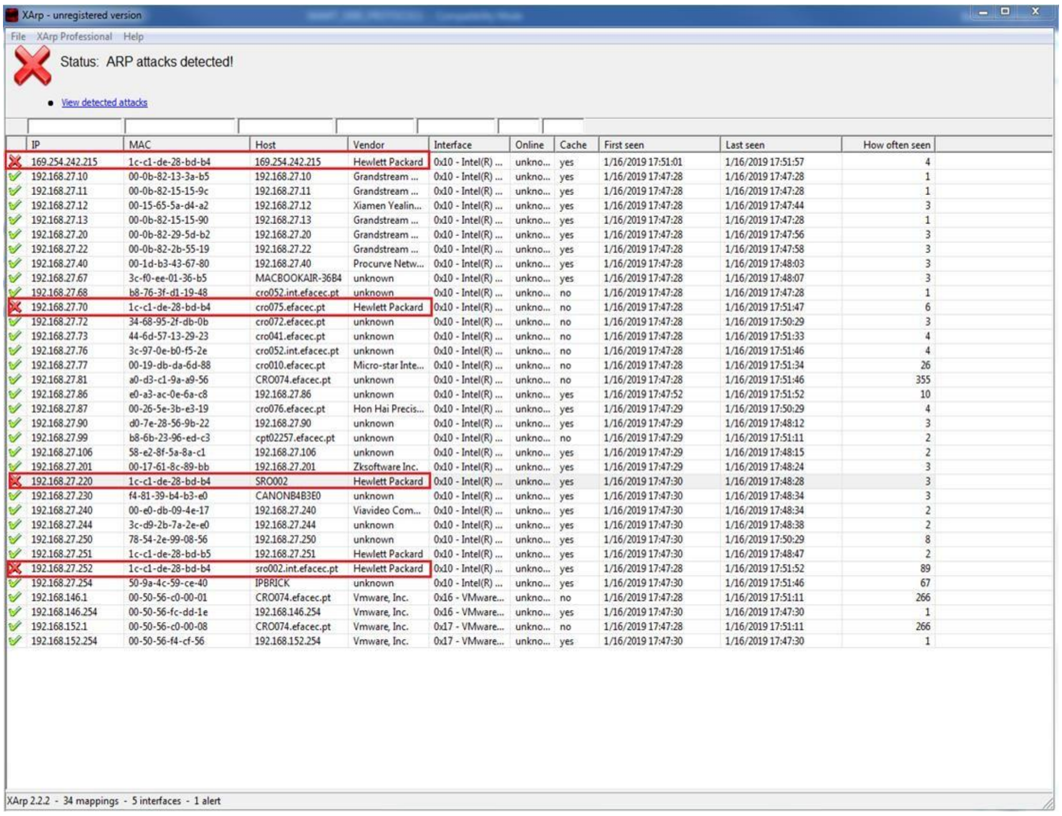


Status: no ARP attacks

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
✓	192.168.27.10	00-0b-82-13-3a-b5	192.168.27.10	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.11	00-0b-82-15-15-9c	192.168.27.11	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.12	00-15-65-5a-d4-a2	192.168.27.12	Xiamen Yealin...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:44	3
✓	192.168.27.13	00-0b-82-15-15-90	192.168.27.13	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.20	00-0b-82-29-5d-b2	192.168.27.20	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:56	3
✓	192.168.27.22	00-0b-82-2b-55-19	192.168.27.22	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:58	3
✓	192.168.27.40	00-1d-b3-43-67-80	192.168.27.40	Procurve Netw...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:48:03	3
✓	192.168.27.67	3c-f0-ee-01-36-b5	MACBOOKAIR-36B4	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:48:07	3
✓	192.168.27.68	b8-76-3f-d1-19-48	cro052.int.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.70	20-54-fa-33-7a-c6	cro075.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:50:03	3
✓	192.168.27.72	34-68-95-2f-db-0b	cro072.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:48:35	2
✓	192.168.27.73	44-6d-57-13-29-23	cro041.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:49:45	3
✓	192.168.27.76	3c-97-0e-b0-f5-2e	cro052.int.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:49:51	2
✓	192.168.27.77	00-19-db-da-6d-88	cro010.efacec.pt	Micro-star Inte...	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:50:13	19
✓	192.168.27.81	a0-d3-c1-9a-a9-56	CRO074.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:50:13	341
✓	192.168.27.86	e0-a3-ac-0e-6a-c8	192.168.27.86	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:52	1/16/2019 17:49:52	6
✓	192.168.27.87	00-26-5e-3b-e3-19	cro076.efacec.pt	Hon Hai Precis...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:50:16	3
✓	192.168.27.90	d0-7e-28-56-9b-22	192.168.27.90	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:12	3
✓	192.168.27.99	b8-6b-23-96-ed-c3	cpt02257.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:29	1/16/2019 17:47:29	1
✓	192.168.27.106	58-e2-8f-5a-8a-c1	192.168.27.106	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:15	2
✓	192.168.27.201	00-17-61-8c-89-bb	192.168.27.201	Zksoftware Inc.	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:24	3
✓	192.168.27.220	1c-c1-de-28-bd-b4	SRO002	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:28	3
✓	192.168.27.230	f4-81-39-b4-b3-e0	CANONB4B3E0	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:34	3
✓	192.168.27.240	00-e0-db-09-4e-17	192.168.27.240	Viavideo Com...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:34	2
✓	192.168.27.244	3c-d9-2b-7a-2e-e0	192.168.27.244	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:38	2
✓	192.168.27.250	78-54-2e-99-08-56	192.168.27.250	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:49:14	7
✓	192.168.27.251	1c-c1-de-28-bd-b5	192.168.27.251	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:47	2
✓	192.168.27.252	1c-c1-de-28-bd-b4	sro002.int.efacec.pt	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:50:13	57
✓	192.168.27.254	50-9a-4c-59-ce-40	IPBRICK	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:50:19	44
✓	192.168.146.1	00-50-56-c0-00-01	CRO074.efacec.pt	Vmware, Inc.	0x16 - VMware...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:47:30	257
✓	192.168.146.254	00-50-56-fc-dd-1e	192.168.146.254	Vmware, Inc.	0x16 - VMware...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:47:30	1
✓	192.168.152.1	00-50-56-c0-00-08	CRO074.efacec.pt	Vmware, Inc.	0x17 - VMware...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:47:30	257
✓	192.168.152.254	00-50-56-f4-cf-56	192.168.152.254	Vmware, Inc.	0x17 - VMware...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:47:30	1

XArp 2.2.2 - 33 mappings - 5 interfaces - 0 alerts

Fig. 6. Network before the attack.



Status: ARP attacks detected!

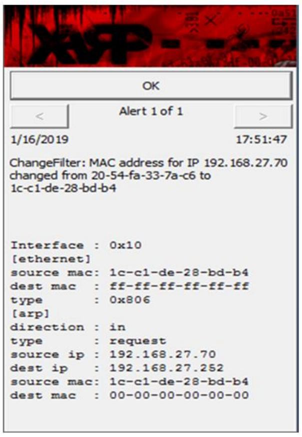
- View detected attacks

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
✗	169.254.242.215	1c-c1-de-28-bd-b4	169.254.242.215	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:51:01	1/16/2019 17:51:57	4
✓	192.168.27.10	00-0b-82-13-3a-b5	192.168.27.10	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.11	00-0b-82-15-15-9c	192.168.27.11	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.12	00-15-65-5a-d4-a2	192.168.27.12	Xiamen Yealin...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:44	3
✓	192.168.27.13	00-0b-82-15-15-90	192.168.27.13	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✓	192.168.27.20	00-0b-82-29-5d-b2	192.168.27.20	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:56	3
✓	192.168.27.22	00-0b-82-2b-55-19	192.168.27.22	Grandstream ...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:47:58	3
✓	192.168.27.40	00-1d-b3-43-67-80	192.168.27.40	Procurve Netw...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:48:03	3
✓	192.168.27.67	3c-f0-ee-01-36-b5	MACBOOKAIR-36B4	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:48:07	3
✓	192.168.27.68	b8-76-3f-d1-19-48	cro052.int.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:47:28	1
✗	192.168.27.70	1c-c1-de-28-bd-b4	cro075.efacec.pt	Hewlett Packard	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:47	6
✓	192.168.27.72	34-68-95-2f-db-0b	cro072.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:50:29	3
✓	192.168.27.73	44-6d-57-13-29-23	cro041.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:33	4
✓	192.168.27.76	3c-97-0e-b0-f5-2e	cro052.int.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:46	4
✓	192.168.27.77	00-19-db-da-6d-88	cro010.efacec.pt	Micro-star Inte...	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:34	26
✓	192.168.27.81	a0-d3-c1-9a-a9-56	CRO074.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:46	355
✓	192.168.27.86	e0-a3-ac-0e-6a-c8	192.168.27.86	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:52	1/16/2019 17:51:52	10
✓	192.168.27.87	00-26-5e-3b-e3-19	cro076.efacec.pt	Hon Hai Precis...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:50:29	4
✓	192.168.27.90	d0-7e-28-56-9b-22	192.168.27.90	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:12	3
✓	192.168.27.99	b8-6b-23-96-ed-c3	cpt02257.efacec.pt	unknown	0x10 - Intel(R) ...	unkno...	no	1/16/2019 17:47:29	1/16/2019 17:51:11	2
✓	192.168.27.106	58-e2-8f-5a-8a-c1	192.168.27.106	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:15	2
✓	192.168.27.201	00-17-61-8c-89-bb	192.168.27.201	Zksoftware Inc.	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:29	1/16/2019 17:48:24	3
✗	192.168.27.220	1c-c1-de-28-bd-b4	SRO002	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:28	3
✓	192.168.27.230	f4-81-39-b4-b3-e0	CANONB4B3E0	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:34	3
✓	192.168.27.240	00-e0-db-09-4e-17	192.168.27.240	Viavideo Com...	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:34	2
✓	192.168.27.244	3c-d9-2b-7a-2e-e0	192.168.27.244	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:38	2
✓	192.168.27.250	78-54-2e-99-08-56	192.168.27.250	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:50:29	8
✓	192.168.27.251	1c-c1-de-28-bd-b5	192.168.27.251	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:48:47	2
✗	192.168.27.252	1c-c1-de-28-bd-b4	sro002.int.efacec.pt	Hewlett Packard	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:28	1/16/2019 17:51:52	89
✓	192.168.27.254	50-9a-4c-59-ce-40	IPBRICK	unknown	0x10 - Intel(R) ...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:51:46	67
✓	192.168.146.1	00-50-56-c0-00-01	CRO074.efacec.pt	Vmware, Inc.	0x16 - VMware...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:11	266
✓	192.168.146.254	00-50-56-fc-dd-1e	192.168.146.254	Vmware, Inc.	0x16 - VMware...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:47:30	1
✓	192.168.152.1	00-50-56-c0-00-08	CRO074.efacec.pt	Vmware, Inc.	0x17 - VMware...	unkno...	no	1/16/2019 17:47:28	1/16/2019 17:51:11	266
✓	192.168.152.254	00-50-56-f4-cf-56	192.168.152.254	Vmware, Inc.	0x17 - VMware...	unkno...	yes	1/16/2019 17:47:30	1/16/2019 17:47:30	1

XArp 2.2.2 - 34 mappings - 5 interfaces - 1 alert

Fig. 7. Network after the attack.

One of biggest advantages is that the software sends immediately a report on screen when attack took place as shown in Fig. 8 and XArp alerts that is a new IP/MAC entry on the network. In fact, XArp detects the same MAC but a different IP address than the one that the system is registered.



1/16/2019 17:51:47

ChangeFilter: MAC address for IP 192.168.27.70 changed from 20-54-fa-33-7a-c6 to 1c-c1-de-28-bd-b4

```
Interface : 0x10
[ethernet]
source mac: 1c-c1-de-28-bd-b4
dest mac  : ff-ff-ff-ff-ff-ff
type      : 0x806
[arp]
direction : in
type      : request
source ip : 192.168.27.70
dest ip   : 192.168.27.252
source mac: 1c-c1-de-28-bd-b4
dest mac  : 00-00-00-00-00-00
```

Fig. 8. Alert after the attack.

With the help of XArp tool it was possible to the detect threats on the system. The best defense against ARP- Poisoning is to enable MAC binding on the switch. This is a setting that can be found in CISCO, Moxa switches and some other industrial switches, that do not allow the MAC addresses associated with a port to change after they are configured. Legitimate MAC changes can be made by the network administrator and is considered a good defense.

In addition to this method, the only other defense method available is detection. And, there are several tools for detection ARP attack like XArp already mentioned in this case, Arpwatch, ArpON (ARP handler inspection), AntiARP, anti'arpspoof, etc. Those tools use a user-level packet-capture method for detecting ARP attacks, keep the administrator informed when a new machine acquires a network address, and alert if a MAC address has changed from IP. Fig. 9 represents a flow chart of the proposed work:

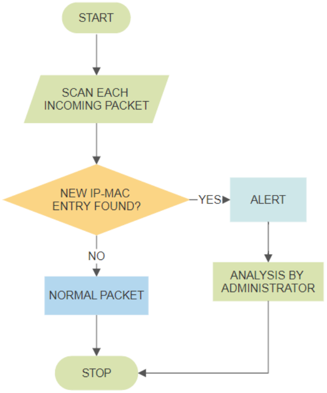


Fig. 9. Flow chart of the proposed test

It means that every equipment that is connected in the network has to be scanned, and if appears an equipment that is not registered on the network, it is going to alert, and if it is registered proceeds to next packet, this method helps the system to identify intruders. This proposed flow chart technique also detects the correct MAC to IP address mapping of the systems.

4.2.1. Case study 2: Conclusion

In a network are many devices (different IP addresses), it's very important to verify if there are devices with the same MAC addresses as well. The purpose of the attacks is not to compromise the wireless network, but to gain access or compromise the network. The objective of the tests performed is essentially to prove the existence of a given vulnerability, as well as to validate the attack techniques found. With this method is possible to prevent ARP- Poisoning. In order to prevent an attack, it's important to have control of the MAC/IP addresses of all the equipment that are connected in the network. MAC addresses should be considered important as the IP addresses. The analysis of the approach proposed confirms its efficiency and robustness. This model could differentiate the attacker by the mismatch in their MAC address.

5. Conclusion

The electricity generation and distribution systems were not designed to be connected or accessed over the Internet and making these critical infrastructures accessible certainly has advantages, but it can also make the system vulnerable. The system thus gets exposed to potential cyber security risks inherent in any Internet connected system. The collapse or compromise of critical infrastructures like smart grid could result from malicious users, inadvertent mistakes, natural calamity, and disgruntled employees. Such failures of the system can have far reaching consequences on the economy and society creating public security issues.

➢ Following are the benefits or advantages of SG:

- It reduces electricity theft;
- It reduces electricity losses (transmission, distribution, etc);
- It reduces electricity cost, meter reading cost, maintenance costs, etc;
- It reduces air emissions of CO_2.
- SG is capable of meeting increased consumer demand without adding infrastructure.

➢ Following are the drawbacks or disadvantages of SG:

- High cost due to replacement of analog meters by more sophisticated electronic meters;
- Lack of regulatory norms for standards for technologies of SG;
- Continuous communication network should be available;
- Some smart meters can be hacked, which can be used to increase or decrease the demand for power.

➢ Requirements of SG

- The installation cost, where the benefits of utilizing the smart grids can only be seen after years of installation;
- The extent of technology to be included within the smart grids during the installation, where the design of the smart energy meters can be quite tedious in some cases because of having to support additional features. These features include providing additional security, remote controlling of house appliances, etc;
- Integration of smart grids becomes harder with an increasing number of consumers, and the establishment of communication infrastructure in some areas might be difficult due to terrestrial difficulties.

In this paper, we showed many solutions (tools) of address resolution protocol. One of the biggest advantages of using these tools is that can be used simultaneously in order to get good results on the tests. Future work will be about other methods of prevention against Cyber-attacks, it is a vast subject, as prevention method are being applied, the hackers are becoming more sophisticated.

REFERENCES

[1]. IEA - International Energy Agency, "Technology Roadmap Smart Grids", April 2011.

[2]. *M. Faheem, S. Shah, R. Butt, B. Raza, M. Anwar, M. Ashraf, M. Ngadi, V. Gungor, "*Smart grid communication and information technologies in the perspective of Industry 4.0": Opportunities and challenges, November 2018.

[3]. *A. Mahmood*, "Cyber security of smart grid infrastructure", The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, 2014, pp. 449-472.

[4]. Cyber Security of the Smart Grids, European Commission, April 2011.

[5]. S. G. I. Panel, "Guidelines for smart grid cyber security: **vol. 1**, smart grid cyber security strategy, architecture, and high-level requirements, and **vol. 2**, privacy and the smart grid, National Institute of Standards and Technology (NIST)," Interagency Rep, **vol**. 7628, 2010.

[6]. National Institute of Standards and Technology - NISTr 7628 revision 1- Guidelines for smart grid cybersecurity – **vol. 1,2 and 3** – 2014.

[7]. Review of Communication Technologies for Smart Grid applications, The national conference on: New approaches in power industry: Science and Research Branch, Islamic Azad University Tehran, Iran, 2017.

[8]. *M. Faisal, Z. Aung, J. Williams, A. Sanchez*, "Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," IEEE Systems Journal, **vol. 9**, no. 1, pp. 31–44, 2015.

[9]. *R. Radvanovsky and J. Brodsky*, "Handbook of SCADA/control systems security". CRC Press, 2013.

[10]. *W. Wang and Z. Lu*, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, **vol. 57**, no. 5, pp. 1344–1371, 2013.

[11]. *N. Komninos*, "Survey in smart grid and smart home security: issues, challenges and countermeasures", IEEE Communication Surveys & Tutorials, **vol. 16**, no. 4, 2014.

[12]. *A. Metke, R. Ekl*, "Security technology for smart grid networks, 2010, IEEE Transactions on Smart Grid", **vol. 1**, 2010.

[13]. *B. Camachi, O. Chenaru, L. Ichim, D. Popescu*, "A Practical Approach to IEC 61850 Standard for Automation, Protection and Control of Substations", 9th International Conference on Electronics, Computers and Artificial Intelligence, 2017.

[14]. http://www.iicybersecurity.com/internet-port-scanner.html.

[15]. *J. Seitz*, "Black Hat Phyton" Phyton Programming for Hackers and Pentesters, 2014.

[16]. *B. Camachi, D. Popescu, L. Ichim*, "Smart Grid protection using MAC value analysis", 7th International on Workshop Safety & Security, 2019.