Current and Future Threats Framework in Smart Grid Domain

A. Procopiou, N. Komninos, *Member, IEEE*

***Abstract*—Due to smart grid's complex nature and criticality as an infrastructure, it is important to understand the key actors on each domain in depth so the potential vulnerabilities that can rise are identified. Furthermore, the correct identification of threats affecting the smart grid's normal functionality must be realised, as well as what impact these threats can have so appropriate countermeasures are implemented. In this paper a list of vulnerabilities that weaken the smart grid is outlined. Also structured analysis of attacks regarding the three key security objectives across the different layers is presented along with appropriate examples applicable to the smart grid infrastructure and what impact each of them has to the smart grid on each case. Finally, a set of new attack scenarios that focus on attacks being initiated from the smart home part of the smart grid is described targeting these security objectives with the potential consequences they can cause to the smart grid.**

***Keywords*—Smart Grid; Information Security; Vulnerabilities; Threats; Confidentiality; Integrity; Availability; Attacks**

I. Introduction

Smart Grid consists one of the most pioneering concepts of today transforming the well-known established traditional electric grid into a smart and efficient system of its own. Its main objectives is to ensure a two-way communication procedure between the customer and the services, improve the global warming situation and provide fast and integrate solutions in emergency situations. The different services provided are due to the deployment of information networking and the TCP/IP protocol. In contrast, due to the services used mentioned above, smart grid is in a constant and continuous communication with the Internet for the effective operation of its services. Due to it, the complexity in the system has been increased.

Hence, the smart grid a potential target for malicious activities, as it no longer consists of a disconnected set of entities that are isolated. In all systems in order to ensure security at least the three most important security principles must be satisfied, Confidentiality, Integrity and Availability. The correct identification smart grid's vulnerabilities and the types of security threats can lead to choosing the appropriate countermeasures. As a result, our motivation is the proper investigation and correct identification of the smart grid's vulnerabilities and threats that can lead to the demonstration of new attack scenarios.

II. Smart Grid Security

A. Smart Grid Architecture

NIST established a conceptual model for the smart grid [1] consisting a total of seven conceptual domains in order to modularise its complex and heterogeneous nature, presented below. A representation of the smart grid is given in Figure 1.

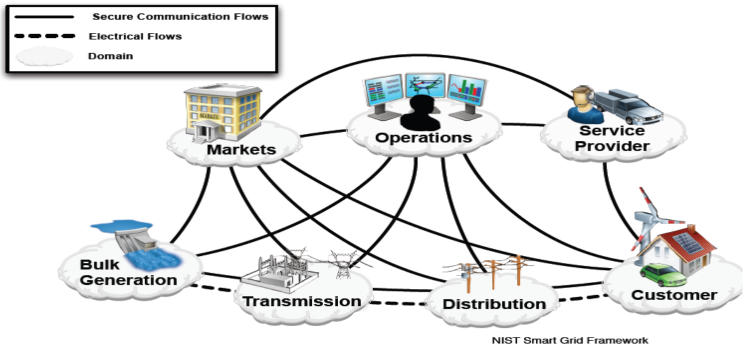

Fig. 1. Conceptual Overview of the Smart Grid [1]

Bulk Generation is responsible for generating electricity. It consists of electrical equipment, remote terminal units, programmable logical controllers, equipment monitors and fault recorders. It also communicates with the market and the operation domains sending important information such as generation capacity and scarcity.

Transmission domain is responsible for passing the amount of generated electricity sent from the bulk generation domain to distribution with the usage of a number of substations and transmission lines and self-healing when needed.

Distribution communicates with the customer domain in order to deliver electricity to the end users according to demands and electricity availability. Also, distribution communicates with distributed energy resources, plug-in electrical vehicles and advanced metering infrastructures.

Operation ensures the efficient and optimal operation of transmission and distribution domains. It uses the field and wide area networks located in both transmission and distribution domains to collect valuable information about the grid's state using supervisory control and data acquisition (SCADA) systems.

Market maintains the balance between the supply and the demand of electricity. This is operated by constantly and effectively communicating with the bulk generators and the distributed energy resources.

Customer is about who can consume, store and generate electricity. Home, commercial and industrial buildings fall into this domain. This domain communicates with the distribution, market, service provider and operation domains. With the introduction of the two-way communication in the smart grid, the customers can participate actively in the smart grid, using an entity installed in their premises called Energy Services Interfaces (ESI), and directly communicate with the utility centres and exchange information. Also, another entity installed, the smart meter (SM), can actively send metering data for billing purposes to the appropriate service providers for operating the data received.

Service Provider is responsible for offering electricity to the customers and the utilities. They operate functions such as billing and management of customer accounts. It receives the metering information by communicating with the operation domain and it provides smart services for the customer.

B. *Smart Grid Vulnerabilities*

Smart Grid is a state of the art set of interconnected systems which makes heavy usage of two-way communications and high speed exchange of information for the most efficient to the customers and environmentally-friendly usage of electricity. To achieve that, it uses a wide range of different types of equipment, each one with its own requirements, demands and operations, giving the infrastructure dynamic and interactive capabilities. However, the tradeoff in this situation is clear; in order to provide these remarkable services the smart grid has gained many and different vulnerabilities, each one with its own distinct characteristics. These vulnerabilities expose the smart grid to a plethora of threats that can damage the smart grid from a low to high degree. Below a set of high-level vulnerabilities threatening the smart grid is presented as the authors in [2] have defined.

Security of the Customers: Smart meter and Energy Services Interface (ESI) are responsible for collecting and transmitting massive amounts of data constantly and continuously. These data are considered to be private and confidential.

Deployment of many intelligent devices: The usage of a great number of intelligent devices for the normal operation of the smart grid indicates their connection to the Internet making them an ideal case of attack entry points.

Size of Smart Grid: It is estimated that smart grid is 100 to 1000 times larger in size of the Internet. A size like this makes it management and network monitoring even more complex.

Physical Security: The smart grid, in contrast to its predecessor, consists of many scattered components, outside of the utility centres, that are not monitored by staff making them physically reachable by anyone.

Power Systems Lifetime: Power Systems in general consist of legacy systems that are probably outdated compared to the IT systems. For that reason, they might act as weak points in the system in general.

Absolute trust between power devices: Machine to machine communications in the power systems are vulnerable against data spoofing in cases which the state of one machine directly affects the actions of another machine.

No clear communication between the different teams: Due to different backgrounds of the teams involved, makes the communication between them inefficient and unorganized. As a result, bad decisions might be taken increasing the vulnerability.

Usage of Internet Protocol: The usage of Internet Protocol makes the smart grid compatible with various components. Due to that though, all these devices using IP become vulnerable to attacks such as spoofing, teardrop, denial of service and so on.

Increase in stakeholders: The large number of different stakeholders makes the system vulnerable to insider attacks.

The vulnerabilities identified above, illustrate the need for ensuring security in multiple levels in the smart grid network. Over the years, the need to protect the traditional IT networks has pushed the professional and industrial community to design and develop appropriate solutions for them. Since the smart grid has implemented various concepts from them, it would seem logical to use the solutions already defined as well. However, as the authors in [3,4] have accurately described that the smart grid network differs greatly from the IT networks. Specifically, they differ in their architecture, the technology used and their quality of service. The need for individual smart grid security solutions is essential.

C. Smart Grid Security Objectives

As CISCO [5] and IEEE [6] have established, the three main security objectives are confidentiality, integrity and availability. *Confidentiality* involves the protection of personal information and ensuring the correct authorisation to disclosed information. *Integrity* involves the protection of information against unauthorised modification or even destruction. *Availability* involves the continuous and reliable access and usage of information and services.

III. Current Attacks at the Smart Grid

In this section, a classification of the different attacks on different layers, consisting of all three objectives, is defined and a literature review of the already attack scenarios established with the consequences they can have.

A. *Attacks at the Physical Layer*

The most usual attack in the physical layer regarding *availability* is Jamming. To perform a jamming attack the attacker only needs to connect to a communication channel, which makes the launch of the attack easier. The authors in [7] have focused on Denial of Service (DoS) attacks from the remote terminal unit to the control centre. The attacker can jam the communication channels or attack the protocols or even just sent huge amounts of traffic to flood the network. This results into packets being lost and the control centre being unable to process the legitimate traffic it receives.

Regarding *confidentiality*, eavesdropping can occur. It is a form of passive attack and as the name implies it involves of an adversary being able to overhear messages exchanged between two nodes over a communication channel. The authors in [8] discussed the attack scenario of an adversary eavesdropping data from Data Concentrator Nodes that forward the messages from the smart meters to the utilities, violating the customer's privacy. Regarding integrity, the smart meter can be physically tampered from an adversary as the authors in [9] have stated.

B. *Attacks at the MAC Layer*

A passive-confidentiality attack is traffic analysis, in which adversaries is able to sniff/intercept and examine the messages in order to extract useful information about possible patterns of the communication between two nodes.

Furthermore, an illegal modification of the MAC parameters, targets confidentiality again but in a more active way, masquerading, also called MAC/ARP Spoofing. This leads to the attacker having the freedom to launch more serious kinds of attacks such as the illegal modification of data before they are forwarded by using a Man-in-the-Middle attack (MITM). In [10], an adversary after performing ARP Spoofing succeeding into injecting false data or by using MITM attack succeeds into sniffing data. This can have severe consequences since the injection of false data can lead to disruption of the normal functioning of the network. Considering integrity, the data concentrator unit is directly connected to a home area network's smart meter. A compromise of one can cause the blocking of information due to illegal modification of data [8] or a MITM attack between the data concentrator unit and the smart meter.

C. *Attacks at the Transport/Network Layer*

Attacks in these two layers, targeting *availability*, aim to disrupt the end-to-end communications by exhausting the resources, resulting into the destination device being unable to accept any legitimate traffic after a while. Some common examples are TCP and UDP Flooding Attacks. Regarding *integrity*, possible replay attack can occur, in which the adversary's aim is to retransmit or delay messages; after obtaining them through a masquerading attack. Finally, for *confidentiality*, a possible MITM attack can occur as the adversary can perform IP-Spoofing to intercept malicious data. According to the possible attack scenarios above, authors in [11], discussed about two attack-scenarios in SCADA networks. The first consisted of an attack on a SCADA substation from four different IP Spoofed Intelligent Electronic Devices. The attacker send compromised packets in order to gather information for the SCADA protocol used, DNP (although its is Layer-2 protocol). The modified packets' aim is to corrupt the commands from a substation to an IED. The second consisted of an attack that aims to disrupt the control centre from again four IP spoofed substations in order to send random overload DNP packets so the control centre would be unable to respond fully to requests, as part of a replay attack.

The authors in [12] have focused on attacks SCADA networks which use the IEC-104 Protocol. Specifically, they discussed about an attack scenario called 'Spontaneous Message Storm' consists of an enormous amount of data being sent from a server in either a control room operator or a control server in an attempt to flood them and reduce their availability to legitimate requests.

Similarly, the authors in [13] have discussed about the possibility of a DoS TCP-SYN Flood attack, attack performed in substation IED devices that use the IEC-61850 protocol.

The authors in [14,15] have discussed of a distributed or simple DoS attack from smart meter/s to the data concentrator unit. The compromise of the meter can begin with compromising the device/s and proceeding to inject malicious traffic to the concentrator unit, resulting into its flooding and its unavailability to accept legitimate traffic. Such scenarios are not focused on stealing energy but disrupting the service of the area. The consequences of such cases can vary, from a 'simple' service disruption to a major blackout, depending on the smart meters or data concentrators compromised. In case the adversary wants to trick the smart grid and pay less, the data is tampered during transmission to the utility, aiming for energy theft as the authors in [16] have discussed.

Another attack that can be performed in the network layer, regarding *availability* and *integrity*, is the wormhole attack. The authors in [17] have also focused on cyber attacks between the smart meter data transmission to the data concentrator unit and from the utility centre to the data concentrator unit. Specifically, they have discussed about the possibility of a wormhole attack at this part of the smart grid. A compromised meter can drop all or most of the packets it receives from the concentrator node to achieve the attack resulting into the smart grid becoming unstable.

Also, in the transport layer buffer overwhelming can be performed threatening the smart grid's availability. The authors in [12] have also stated an attack scenario called 'Potential Buffer Overflow' in which the attacker generates and sends packets whose length is bigger of normal packets so the destination's buffers can be filled faster and become unresponsive in SCADA systems using the IEC-104 Protocol.

D. *Attacks at the Application Layer*

Application layer attack's main aim is to exhaust the target's CPU and memory by flooding it with intensive periods of requests in application level. Also, selective message forwarding can be a threat in the application layer; the adversaries succeed in including themselves in a data communication channel and dropping certain packets, thus preventing them from reaching their destination. Sometimes, instead of selective packets the adversary might drop packets from certain sources or follow a random pattern. The authors in [18] have discussed about cyber attacks in industrial control systems. In particular, they discuss a DoS scenario in application level. It is called 'Invalid Cyclic Redundancy Code (CRC)' and aims to send large in number of MODBUS (serial communication protocol to transmit data between two electronic devices) packets with a faulty CRC. The target device is forced to check every packet's CRC so in our case the target device is flooded or even crashed so the communication is majorly disrupted and unable to accept any legitimate traffic. The authors in [19] have simulated a selective forwarding attack where multiple meters were compromised, resulting into a number of packets being dropped while other being forwarded normally.

TABLE I. ATTACKS ACROSS DIFFERENT LAYERS

OSI Layer	Type of Attack
Physical Layer	Jamming, Eavesdropping, Meter Tampering
MAC Layer	MAC DoS, Traffic Analysis, MAC/ARP Spoofing, Jamming
Transport/Network Layer	Buffer Flooding, TCP/UDP Flooding, Replay Attack, IP-Spoofing, Data Injection, Wormhole
Application Layer	HTTP Flooding, Protocol Attacks, Selective Message Forwarding
Multiple Layers	MITM

IV. FUTURE ATTACKS AT THE SMART GRID

As it has been highlighted from the previous section, the two main parts of the smart grid the research is focused on securing the AMI and the entities located in the distribution and transmission domains. However, little focus has been put into the 'last mile', the home area network. The majority of research targets into threats in HAN where the smart meter is the main target of the attack. Mainly its compromise aims to disrupt the normal activity of the HAN, or in some cases to attack the data concentrator unit. As a result, HAN tends to be treated as an isolated network. However, that is clearly not the case. The HAN is also connected to the smart grid and an attack can be initiated from it. Hence, various smart grid services can be damaged more that can be estimated. Moreover, even the studies that have focused on this aspect of attacks have just stayed up to the Headend and have not gone deep into the different services and the possible consequences of their potential malicious disruption.

HAN and its technologies are evolved rapidly every day. An important change that must be considered is that the customer gateway is no longer integrated with the smart meter device, instead it consists of a separate entity, called the ESI. A number of activities that used to be operated through the smart meters are not longer executed by it now. That means that the attacker is free to compromise more than one device, depending on what their aim is. Specifically, as authors in [20-22] have outlined smart meter now is only responsible for mainly the energy consumption data forward and reporting outage issues whereas the ESI is responsible for interacting with the HAN devices, communicating with the external service providers as well as handling any load shedding and demand/response signals and acting accordingly to the situation.

Additionally, the smart appliances used in the network become more and more 'intelligent'. Even if they don't consist of a usual graphical user interface they indeed use application layer protocols to communicate, such as the Constrained Application Protocol (CoAP) [23] thus being vulnerable to Application Layer attacks, including HTTP Flooding as well as the less common Low-Rate attack (LDoS).

Hence, it is clear that general flow of information and functionality of the various entities involved needs to be reviewed and reassessed so the potential vulnerabilities and threats can be realised. A set of possible attack scenarios have been identified and presented below regarding Availability and Integrity. Although confidentiality attacks, initiated from the smart home entity, they cannot directly harm the smart grid they can indirectly prepare the ground for major attacks. As it is shown in the following attack scenarios every attack is initiated with an impersonation of a key-entity inside the smart home. This consists of an attack targeting confidentiality. Below a set of detailed attack scenarios is outlined as well as a summary of them in Table II.

TABLE II. FUTURE THREATS IN SMART GRID

Source	Dest./data sent	Attack Type	Consequence	Security Goal
ESI	DRMS/LMS (DR ack.)	HTTP Flooding/LDoS	DRMS/LMS dysfunction	Availability
ESI	ESP (DR ack)	HTTP Flooding/LDoS	Dysfunction ESP servers	Availability
ESI	DRMS/LMS (DR ack)	Replay Attack/ Injection	Overload grid	Integrity
ESI	ESP (DR ack)	Replay Attack/ Injection	Overload grid	Integrity
ESI	DRMS/LMS (Load Shedding/Load Control Signals)	HTTP Flood/LDoS	DRMS/LMS dysfunction	Availability
ESI	DRMS/LMS (Load Shedding/Load Control Signals)	Replay Attack/ Injection	Overload grid	Integrity
ESI	Third Party Gas/Water Utilities (leak report)	HTTP Flood/ LDoS	Dysfunction utility	Availability
ESI	Third Party Gas/Water Utilities (leak report)	Replay Attack	Wasted time in false notifications	Integrity
SM	OMS (outage report)	HTTP Flood/LDoS	DRMS/LMS dysfunction	Availability
SM	OMS (outage report)	Replay Attack	Wasted time in false signals	Integrity
SM	OMS (DER shutdown)	HTTP Flood/LDoS	DRMS/LMS dysfunction	Availability
SM	OMS (DER shutdown)	Replay Attack	Wasted time in false signals	Integrity
ESI	OMS (traffic lights power outage)	HTTP Flood/LDoS	Dysfunction of the OMS	Availability
ESI	OMS (traffic lights power outage)	Replay Attack	Wasted time in false signals	Integrity
ESI	DRMS/LMS (DR ack for DER)	HTTP Flood/LDoS	DRMS/LMS dysfunction	Availability
ESI	DRMS/LMS (DR ack for DER)	Data Injection	Overloading the grid	Integrity

1) ESI to Demand Response Management System/ Load Management System (DRMS/LMS) or Energy Service Providers (ESP) (DR Singals)

The DRMS/LMS services send demand/response (DR) signals to the customers either via the AMI Network or via external networks (e.g. Internet) either to help the customers manage their energy consumption in a more efficient way. The signals can consist of the price, urgency or level. In response, the ESI sends an acknowledgement of the DR signal. In a possible attack scenario (via the AMI network), the compromise of the ESI and the possible capture of old acknowledgment packets can be used to flood the DRMS/LMS services aiming to disrupt their functionality, thus violating the availability objective. In case of the signal being transmitted through external networks, it is the ESP, which sends the signals, and the acknowledgment response will be sent from the ESI back to it. The attack scenario follows the same procedure as explained above, and its aim is to disrupt the normal functioning of the ESP, again threatening the availability objective. Another scenario, again initiated by the impersonation of the ESI, is followed by either a replay attack or a data modification attack, both of them violating the integrity objective. The compromised ESI either replaces the signals received with older, or deletes/modifies them. This can have sever consequences in cases which the smart grid is highly loaded but the altered signals trick the appliances into functioning continuously draining the smart grid even more.

2) ESI to DRMS/LMS (Direct Load Control/Direct Load Shedding)

Direct Load Control and Direct Load Shedding use the same technologies. In the former, the DRMS/LMS send signals to start/stop the operation of smart appliances depending on the state of the grid and the appliances' state, so the customers can pre-cool their plenums during the morning and cycle off their air conditioning at peak times. In the latter, in case of an emergency, the facilities are shut down in order for the smart grid to be protected and not to collapse. In both cases, DRMS/LMS send a load control signal, for load shedding it also sends a "scram command", and the ESI responds back with an acknowledgement. ESI can be compromised and capture old acknowledgment packets can be used to flood the DRMS/LMS services aiming to disrupt their functionality and thus, putting the state of the smart grid into a critical condition, the availability objective being violated. Also, instead of flooding the services, the impersonation of the ESI can replay old messages or modify the signals contents and thus tricking the appliances into not functioning according to the smart grid's commands resulting into threatening its stability, violating the integrity objective.

3) ESI to Third Party Utility (gas/water utility)

In case of a possible leakage of either a gas or water meter the ESI is responsible for notifying the appropriate utility to ensure the safety of the customer by sending a leak notification. However, in a possible attack scenario, a compromised ESI can flood the utility with fake messages of a leak and making the utility unavailable to legitimate leak notifications from other ESIs, violating the availability objective. In a slightly different scenario, the compromised ESI sends old and outdated leak notification messages, as part of a replay attack, violating the integrity objective.

4) SM to Outage Management System (OMS) (power outage reports)

In case of power flow interruption; the smart meter is responsible for sending a power outage report to the Outage Management System to notify them about the issue so it can be fixed. However, an adversary can masquerade themselves in the smart meter and by capturing older messages, and even altering the messages, attempt to flood the OMS and overwhelming it, violating the availability objective. As a result, the OMS might become unavailable to legitimate reports being sent to it of real power outage. In a similar scenario, the adversary's goal is not to flood the OMS but rather send old power outage reports, as part of a replay attack. The impact is not severe, the utility wastes time in responding to fake outage requests, violating the integrity objective.

5) SM to OMS (DER-shut down signals)

In cases of an outage in the grid, the DER has to shutdown or island itself. However, the islanding/shutdown equipment can be either poorly installed or maintained. For that reason, the meter can detect whether the islanding operated correctly or not. If not, then the meter communicates with the OMS requesting its shutdown. A possible attack under this scenario is that the compromised meter will flood the OMS with DER shutdown messages threatening its stable functionality, violating the availability objective. In a slightly different scenario, after a compromise of the meter and a possible replay attack, the shutdown of DER occurs without really needing to, violating the integrity objective.

6) ESI to OMS (traffic lights power outage reports)

With the new technology integrated in the NAN part of the Smart Grid it is now possible to detect the outage of any streetlights in an area. In a possible attack scenario a compromised ESI can flood the OMS with fake outage reports of streetlights and disrupt its normal functioning and reduce its availability to legitimate incoming outage reports. Also, in the context of a replay attack old messages could be retransmitted, targeting integrity. Again, the impact is not severe but the utility wastes time into responding to fake outage requests.

7) SM to Meter Data Management System (MDMS)

A possible scenario is when the smart meter sends the energy consumption data acquired from the smart home to the MDMS (via the AMI Headend) so it can forward them for billing the customer. A possible compromise of the smart meter along with the capture of old metering messages can be used to flood the MDMS and disrupt its communication with the billing entity, violating the availability objective. In cases that the aiming of the adversary is to 'steal energy' they can modify the packets to pay less. A more sophisticated attack would involve the adversary into masquerading appliances that consume a large amount of energy as other appliances that consume less energy aiming for a cheaper bill, violating the integrity objective.

8) ESI to Demand Response Management System/ Load Management System (DRMS/LMS) (DR Signals for the DER Resources)

The smart grid has the option to manage energy using customers' Distributed Energy Resources (DER). The DRMS/LMS server sends Demand/Response signals either through the AMI Headend or directly to the ESI so it can act depending on the message, containing information about the urgency and level of import/export, received to forward it to the DER resources. In exchange, the ESI sends an acknowledgement of receiving the message. Again, in a possible attack scenario, the adversary after taking control of the ESI can send multiple acknowledgements back to the DRMS/LMS server, thus putting the grid intro critical state primarily from the attack itself and, but also in cases when the grid needs legitimate extra energy resources to support it from collapsing, violating the availability objective. Also, instead of causing flood attacks, the compromised ESI can drop the signals or illegally modify them so no the desired functioning by the DER resources is performed, violating the integrity objective.

V. What's Next

The threats described in section III, have managed to be detected successfully by a number of IDSs proposed. On the other hand, the threats, described in Section IV, are yet to be addressed in any way. Furthermore, the new emerging technologies and components used in HAN have made the bottom layer of the Smart Grid an entity that needs to be equally secured. The attack scenarios clearly illustrate the criticality of this entity the high likelihood of a possible attack affecting the Smart Grid being initiated from the Smart Home part. These two entities need to be considered as a whole and not as separate. One of the most effective security solutions in mitigating such types of threats is the usage of Intrusion Detection Systems (IDS). As a result, a potential IDS solution could be developed to detect these new threats. This IDS shall follow a distributed approach, due to the system's broadness and complexity, so the network can be effectively monitored. A vast amount of audit data shall be collected, focusing on the application layer, to detect any kind of potential unauthorised activity as soon as possible before it is spread to the higher layers of the network. In that way, the protection of such a critical infrastructure can be increased.

VI. Conclusion

In this paper, we outlined the three most important security objectives and how they are applied in the smart grid context. The potential vulnerabilities in the technologies integrated in the smart grid were identified, highlighting the smart grid being vulnerable as any other network infrastructure and high importance must be given on its proper security. Due to the grid's individual characteristics tailored solutions must be designed especially for its own needs. Hence, we also outlined on what that can be performed on various parts of this complex critical infrastructure from the research community in the form of scenarios and what consequences such attacks can bring. Due to the continuous improvement and change of smart grid technologies and the customer's active involvement, new security threats can rise. As a result, the need for more research on possible threats and attacks being initiated from the smart home and resulting affecting the smart grid has been highlighted. To support our views a set of new attack scenarios have been outlined illustrating the process in performing such attacks and the possible consequences their action brings to the smart grid's state. In future, it is essential that research shall focus on such new technologies as accurate and efficient security solutions will be designed and implemented to protect the smart grid.

References

[1] NIST- Office of the National Coordinator for Smart Grid Interoperability, *NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108* (2010) 1–145.

[2] F. Aloul et al., "Smart Grid Security: Threats, Vulnerabilities and Solutions,"*Int. J. Smart Grid Clean Energy*, vol. 1, no. 1, pp. 1–6, Sep. 2012.

[3] J. Liu et al., "Cyber Security and Privacy Issues in Smart Grids," *IEEE Comm. Surveys & Tutorials*, vol. 14, no. 4, pp. 981–996, 2012.

[4] W. Wang & Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks* , vol. 57, p. 1344–1371, 2013.

[5] Cisco, "Securing the Smart Grid," pp. 1–7, 2009. [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf. [Accessed Feb. 3, 2015].

[6] IEEE Standards Coordinating Committee 21, "IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads," *IEEE Std 2030tm-2011*, pp. 1–186, 2011. [Online]. Available: IEEE, http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6018237. [Accessed Feb. 3, 2015].

[7] S. Liu, X. Liu, and A. El Saddik, "Denial-of-Service (DoS) attacks on load frequency control in smart grids," in Proc. 2013 IEEE PES Innovative Smart Grid Technologies (ISGT), 2013, pp. 1–6.

[8] F. Skopik & Z. Ma, "Attack Vectors to Metering Data in Smart Grids under Security Constraints," *2012 IEEE 36th Int. Conf. Comput. Software Applications Workshops*, pp. 134–139, 2012.

[9] F.M. Cleveland, "Cyber security issues for Advanced Metering Infrastructure (AMI)," *Power Energy Society General Meeting - Conversion Delivery Elect. Energy 21st Century, 2008 Ieee*, pp. 1–5, Jul. 2008.

[10] Y. Yang et.al., "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," *IEEE Trans. Power Delivery*, vol. 29, no. 3, pp. 1092–1102, Jun. 2014.

[11] A. F. Shosha, P. Gladyshev, S. S. Wu, and C. C. Liu, "Detecting Cyber Intrusions in SCADA Networks Using Multi-Agent Collaboration," Int Symp Intelligent System Application to Power Systems (ISAP), Crete, 2011.

[12] Y. Yang, K. McLaughlin, T. Littler, S. Sezler, B. Pranggono, H Wang. "Intrusion detection system for iec 60870-5-104 based SCADA networks." In Power and Energy Society General Meeting (PES), 2013 IEEE (July 2013), pp. 1–5.

[13] IEC Standard, IEC 61850: Communication Networks and Systems in Substations.

[14] M. Q. Ali and E. Al-Shaer. Configuration-based ids for advanced metering infrastructure. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, pages 451–462, New York, NY, USA, 2013. ACM.

[15] D. Grochocki et. al, "AMI Threats, Intrusion Detection Requirements and Deployment Recommendations," *IEEE Smartgridcomm 2012 Symp. - Cyber Security Privacy*, pp. 395 – 400, Nov. 2012.

[16] P. Jokar, N. Arianpoo & V.C. Leung, "Intrusion Detection in Advanced Metering Infrastructure Based on Consumption Pattern," *IEEE Icc 2013 - Selected Areas Comm. Symp.*, pp. 1–5, 2013.

[17] N.B Mohammadi, et al. "An Intrusion Detection System for Smart Grid Neighborhood Area Network", in EEE ICC -Selected Areas in Communications Symposium, 2014.

[18] T.H. Morris & W.Gao, "Industrial Control System Cyber Attacks," *Proc. 1st Int. Symp. for Ics & Scada Cyber Security Research 2013*, pp. 22–29, 2013.

[19] S. Kaplantzis & Y.A. Sekercioglu, "Security and Smart Metering,"*European Wireless 2012*, pp. 1–8, Apr. 2012.

[20] D. Hardin, "Customer Energy Services Interface White Paper," *Grid-interop Forum 2011*, pp. 1–18, 2011.

[21] E.K. Lee, R. Gadh & M.Gerla, "Energy Service Interface: Accessing to Customer Energy Resources for Smart Grid Interoperation," I*EEE J. Selected Areas Comm.*, vol. 31, no. 7, pp. 1–10, Jul. 2013.

[22] National Institute of Standards and Technology "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0"," *Nist Special Publication 1108r2*, Feb. 2012.

[23] T.A. Alghamdi, A. Lasebae & M.Aiash, "Security analysis of the constrained application protocol in the Internet of Things," *Future Generation Communication Technology (fgct), 2013 Second Int. Conf.* , pp. 163 – 168, Nov. 2013.