An Overview of the Firewall Systems in the Smart Grid Paradigm

Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Thanasis Liatifis, Tryfon Apostolakos, Spyridon Oikonomou
University of Western Macedonia,
Department of Informatics & Telecommunications Engineering
{pradoglou, psarigiannidis}@uowm.gr, {st1027, st1137, st1199}@icte.uowm.gr

***Abstract*—The multiple interconnections and the heterogeneity of the devices and technologies into the Smart Grid (SG) generate possible cyber-physical security vulnerabilities that can be exploited by various cyberattackers. The cyberattacks in SG, usually target the availability and the information integrity of the systems. Replay attacks, Denial of Service (DoS), Distributed DoS (DDoS) and botnets are typical examples. Furthermore, the hacking tools have been largely automated, so even a novice can execute destructive cyberattacks. These situations make it necessary to develop efficient firewall systems that can prevent possible cyberattacks. In this paper, we present an overview of the various firewall systems in the SG paradigm and also we provide new research directions in this field.**

***Index Terms*—Advanced Metering Infrastructure, Cyberattacks, Firewall, SCADA, Security, Smart Grid, Substation**

I. Introduction

The traditional electrical grid mainly consists of three processes: a) energy generation, b) transmission and c) distribution. The SG paradigm introduces to the electrical grid Information and Communication Technology (ICT) services, thereby offering significant advantages for both utilities and energy consumers. On the one side, the energy providers can utilize ICT operations in order to manage, control and automate the aforementioned processes of the electrical grid efficiently. On the other hand, the energy consumers have the ability to monitor the energy consumption in real-time, thus achieving more cost-effective pricing.

Although SG promises multiple benefits, such as, increased reliability, better energy management, sustainability, resilience and self-healing, it also introduces significant cybersecurity issues as it combines multiple heterogeneous technologies that are characterized by several vulnerabilities. The cyberattackers can exploit the weak points of the SG paradigm, such as Supervisory Control and Data Acquisition (SCADA) systems, thereby causing disastrous consequences. For instance, in December 2015 a Ukraine power grid was attacked, and electricity knocked out for 225,000 people [1].

A basic and necessary countermeasure against cyberattacks is the firewall systems. A firewall can be considered as a mechanism which controls the network traffic and determines through specific rules the authorized internal and external communications. In this paper, we provide a study of the firewall systems in the SG paradigm, by analyzing various instances and providing new research directions in this field.

In particular the remainder of the paper is organized as follows. Section II provides the motivation and the contribution of this work. Section III and IV introduce an overview regarding the SG paradigm and the firewall systems respectively. Section V analyzes various firewall instances. Section VI discusses the previous analysis and provides new research directions in this field. Finally, Section VII concludes this paper.

II. Motivation and Contribution

Several papers have examined the security issues in the SG paradigm, by mainly analyzing the security requirements, the potential threats and the corresponding countermeasures. Some of them are listed in [3]–[6]. Other works investigate the security issues of common industrial protocols that are used widely in the SG paradigm [7]–[9]. Moreover, in [10], [11] the authors provide an analysis of Intrusion Detection Systems (IDS) for the Advanced Metering Infrastructure (AMI) protection. Furthermore, in [12] the authors present a comparison among various Security Information and Event Management (SIEM) tools regarding their capabilities in SG. Nevertheless, although firewalls constitute crucial systems for the overall security of the Information Technology (IT) and industrial environments, we did not find any survey or review paper that examines or evaluates these systems in the concept of SG. Therefore, in this paper, we provide an analysis of various firewall systems in SG, by discussing and assessing their capabilities and providing new research directions in this field.

III. SG Overview

The SG paradigm constitutes a combination of multiple and heterogeneous technologies that are integrated into the traditional electrical grid, thereby providing remote control and management capabilities that offered significant benefits to both utilities and energy consumers. Some of these technological entities are AMI, SCADA systems, substations, microgrids and synchrophasor systems (Fig. 1). AMI is the most critical characteristic of the modern electrical grid, enabling the real-time and remote interaction between the energy utilities and consumers. In particular, AMI consists of three primary devices: a) smart meters, b) data collector and c) AMI Headend. The SCADA systems constitute an industrial type of systems and their main operation is to monitor and control automation processes. They usually consist of a) Master Terminal Unit (MTU), b) Remote Terminal Units (RTUs) or Programming Logic Controllers (PLCs), c) communication network and d)

P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos,and S. Oikonomou, “An overview of the firewall systems in the smart grid paradigm,” in2018 Global Information Infrastructure and Networking Symposium (GIIS), Oct 2018, pp. 1–4.

The published version is available at IEEE Xplore, October 2018, pp. 1-4, DOI: 10.1109/GIIS.2018.8635747

Human Machine Interface (HMI).The substations constitute a crucial system for the functionality of the electrical grid, as they are used for the transmission and distribution processes. A substation can incorporate various components such as RTUs, PLCs, Intelligent Electronic Devices (IEDs). A microgrid is an independent distribution grid which can operate in conjunction with the main electrical grid, but usually employs Distributed Energy Resources (DERs) to operate autonomously. Finally, synchrophasor systems usually perform various measurements from current/voltage waveforms, such as phase angle, frequency, active power and reactive power.

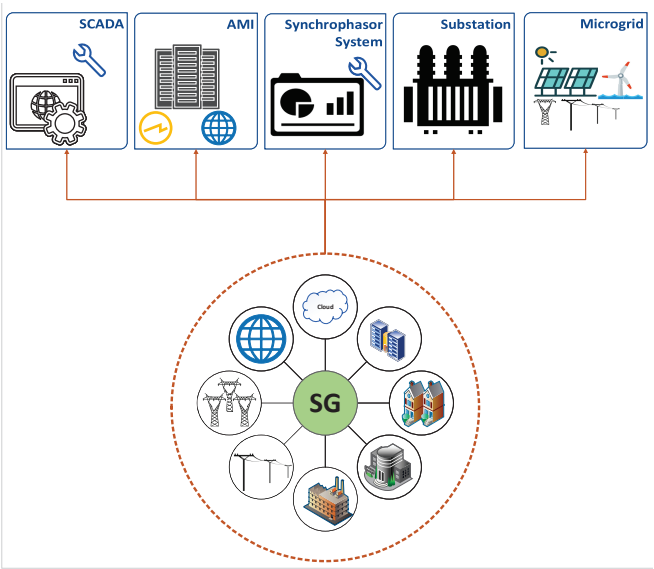

Fig. 1: SG Technologies.

IV. Firewall Overview

A firewall is a hardware or software protection system which continuously monitors and controls the network traffic, which is exchanged between the target systems utilizing a specific predetermined security policy as well as control rules. In particular, this security policy can be classified into two categories: a) negative policy and b) positive policy. On the one hand, the negative policy rejects all the internal or external communications and utilizing specific rules determines the authorized connections. On the other hand, the positive policy allows all the communications and by using control rules defines what connections will be dropped. Furthermore, the firewall systems can be categorized either by their functionality or by their placement. In the first case, four categories can be defined: a) Packet filtering firewall, b) Stateful inspection firewall, c) Application-level gateway, and d) Circuit-level gateway. In the second case, according to the security management and risk assessment processes, there can be various architecture combinations. Finally, it is noteworthy that a firewall cannot provide protection services against cyberattacks that bypass it. For example, a firewall may not be able to cope with malicious insiders.

V. Firewall Systems in the SG Paradigm

In this section, we examine either the functionality of various firewall systems for the protection of SG or other works that focus on providing appropriate instructions and specifications for the firewall systems in the electricity industry sector. More specifically, we analyze 12 cases, classifying them based on what devices and technologies they include. Consequently, based on our search, the papers related to the firewall systems in SG, can be classified into four categories: a) SG, b) AMI, c) SCADA and d) Substations.

In [13], adopting the white-list approach, the authors introduced a self-learning method in order to generate and optimize industrial firewall rules. More specifically, the proposed method includes three modules: a) data preprocessing, b) self-learning, and c) optimizing. The first module includes packet capturing and decoding processes. The second module determines and generates the white-list rules, by using an algorithm which processes the communication paths. Finally, the third module aims at reducing the number of rules in order to improve the performance of the firewall. According to the evaluation analysis, while the number of rules is increased, the rate of packet matching time is decreased exponentially. Therefore the efficiency of the rule matching is improved and the reliability of the rule base is increased.

In [14], the authors introduce a firewall system for the energy sector focusing on the Distributed Network Protocol 3 (DNP3). Their implementation is based on the iptables firewall and specifically on the u32 byte-matching module which is used to identify common cyberattacks in the payload of the DNP3 packets. The evaluation process was held on a scaled-down electric power substation, in which the communication between MTU and the field devices is carried out through the DNP3 protocol. Based on the experimental results, they demonstrate the efficiency of the u32 byte-matching module.

In [15] H. Eslava et al. present a firewall system which aims at managing and controlling the data flows of a substation, which utilizes the IEC 61850 protocol. Firstly, the authors examined the main features of a substation and identified those that can be affected by a security threat. The functionality of the proposed firewall is based on the matching of the network traffic with specific access control rules. If the characteristics of the network traffic do not meet the specific rules, then they are dropped. In order to evaluate their implementation, they simulated the network traffic of a SCADA system including PLCs, RTUs and HMI. However, it is noteworthy that the authors provide neither numerical results nor the rules mentioned above.

In [16], the authors presented a novel firewall system for industrial networks that utilize the Modbus protocol. Their methodology consists of three main steps. The first step is to divide the network into individual areas that are specified by a different security level. These areas can be a) an internal network which includes the Process Control Network (PCN), b) an external network which usually comprises the IT enterprise network and finally c) a demilitarized zone (DMZ).

The second step is to determine an appropriate whitelist policy. The use of a whitelist policy provides the capability to investigate the network packets by examining only the application layer header, thereby reducing the possible firewall overhead. Moreover, the stability of the industrial systems makes the configuring of the whitelist a simple process, unlike the IT environment. The third step constitutes a deep packet inspection process, which checks whether the network packets are included in the whitelist rules or not. In the second case, their system examines further the attributes of these packets and decides whether or not these packets will be dropped. Finally, it is worth to mention, that the authors demonstrate the efficiency of their system carrying out an experimental analysis, which was based on DoS attacks.

In [17], R.C Diovu and J.T Agee introduce an innovative firewall which not only can detect, but also prevent the AMI network from DDoS attacks. The most significant attribute of the proposed Grid OpenFlow Firewall (GOF) is that it minimizes the data processing load and the storage required for its processes. More specifically, GOF is responsible for reducing the effect of a DDoS attack, regarding the bandwidth of the AMI network. The authors claim that the firewall is able to improve to the Quality of Service of (QoS) of SG and maintain the operational status of the AMI network even when it is under attack. The GOF is developed with C++ libraries using the Riverbed Modeler Engine 17.5 suite. Concerning the evaluation of their firewall, they measured the resource utilization, network throughput, and the network latency responses. Furthermore, they compared its performance with a non-GOF firewall. According to the experimental results, the proposed firewall overtook the performance of the non-GOF firewall system. Finally, the authors note that their architecture is cost-effective and scalable.

This paper [18] extends the work of a previous paper [17] in which the authors developed a distributed firewall, called OpenFlow firewall, for AMI networks. Specifically, in this work, the authors investigate the efficiency of their previous work utilizing Markov stochastic processes and the PRISM software. By analyzing the effectiveness of the DDoS attacks against the firewall's detection probabilities and given a set of diagrams, the authors provide the best and the worst case performance of their implementation. In more detail, to model the AMI network, the authors utilize a square matrix of size n, where n denotes the number of the firewall systems. The AMI headends, as well as smart meters, are identified by three possible states, a) unaffected by the DDoS attacks, b) unaffected by the DDoS attacks, but the attacker was able to bypass the firewall system and c) affected by the DDoS attack. Two analysis scenarios were conducted with two different PRISM property parameters. In the first one, the authors calculate the minimum and maximum success rates of the DDoS attacks against various detection probabilities and for a set of Markov states. They conclude that as the detection probability increases, the attack success probability decreases. Although the number of Markov states increases, the firewall is unable to prevent the attacks, which means the detection probability is less effective. In the second analysis, they calculate the maximum and the minimum number of attacks until an AMI headend is successfully attacked against different detection probabilities. In both scenarios, the authors notice a difference between the maximum and minimum values. They justify these results due to the non-deterministic nature of the attacks.

In [19], I. N. Fovino et al. introduced the concept of the state analysis. The state term defines a vector with the real potential values of all the components of the industrial network. For instance, an unwanted, critical state is a state in which one or more industrial component does not work properly and is possible to cause extensive damage. It should be noted that when designing an industrial system, all the possible critical states have to be determined. Based on this concept, the authors developed a novel firewall system which possesses the ability to monitor the current state of the systems, alert the administrators once a system reaches a critical state and drop the malicious packets. Regarding the development process, the authors introduced two new languages that are named packet language and critical state language respectively. The packet language generates appropriate rules by combining the attributes of Transmission Control Protocol/Internet Protocol (TCP/IP) as well as data of industrial protocols. The critical state language generates corresponding rules on the basis of a condition which is formed by known critical states. It is noteworthy, that their firewall can calculate the distance of a system from a critical state, by using the Manhattan distance.

VI. Discussion

In this work, we aimed at providing a useful study concerning the firewall systems in SG. It should be noted that we are the first to attempt such a study. Our analysis was based on various papers that either develop a firewall system for the electricity industry sector or provide useful instructions for such systems. The firewall systems developed concern either the overall SG or individual networks such as AMI, SCADA systems and substations. Most of the firewalls in the literature concern the SCADA systems, while few efforts focus on AMI and substations.

Undoubtedly, the previous papers offer significant and useful efforts concerning the security of SG, by providing valuable methodologies, instructions and tools, that combine various technologies. However, we consider that the multiple interconnections and the heterogeneity of the devices and technologies into SG demand a distributed firewall approach that can efficiently control all entities of SG. It is worth mentioning that none of the previous firewalls examined take into consideration the interactions of the microgrids and the synchrophasor systems. Therefore, we consider that this distributed firewall framework should include individual modules that will possess the ability to inspect packets from all communication layers and also handle efficiently big data without reducing the performance of SG. In particular, it should manage various security events and identifies possible anomalies and critical states, informing the security administrator timely.

Furthermore, a crucial issue for the deployment of such a firewall, is to determine its location installation. Usually, a good practice is the distinction between the private and public networks, by monitoring and controlling their communication. Also, if there are entities, such as servers that need to be available to the public network, they should be placed in DMZ areas, thereby providing the isolation and protection of the private networks if an attacker can successfully access these entities. Finally, such a framework should be characterized by a simple configuration process including a quick installation and configuration process as well as appropriate diagnostic tools.

The Software Defined Network (SDN) technology can contribute significantly to the development of such a framework. By using suitable software controllers, SDN separates the control process from the forwarding processes, thereby providing efficient programmable interfaces and visibility capabilities. In particular, the global visibility offered by SDN enables the development of fine-grained monitoring mechanisms at different locations. Moreover, the dynamic programmability allows the development of appropriate preventive countermeasures such as isolating compromised devices, dropping malicious traffic and disconnecting or reconnecting sensors and meters. Finally, dynamic programmability can assure the timely detection and rapid response to disturbances.Therefore, by adopting an SDN-architecture for the SG paradigm, the deployment of a distributed firewall framework will be an easier process.

VII. Conclusions

In this paper, we presented an analysis regarding the firewall systems in the SG paradigm. Our study was based on the analysis of various scientific works that either deploy a firewall or provide valuable information for these systems. According to our study, most of the research efforts in this field focus on SCADA systems without taking into account the heterogeneous nature of SG and its multiple interactions. For instance, no work was found concerning the firewalls in the microgrids or synchrophasor systems. Also, most of the papers examined focused on the Modbus and DNP3 protocols. However, there are many other industrial protocols used in SG, such as IEC 61850 and IEC 60870. Therefore, we proposed and determined the main attributes of a distributed firewall framework that will be able to solve the aforementioned weaknesses of the existing works.

In our future work, we intend to implement a decentralized firewall for the overall protection of SG following the directions of this work. Our implementation is going to be based on an SDN architecture of SG, through which will be possible the determination of suitable specifications and critical states as well as the development of efficient visualization mechanisms.

VIII. Acknowledgement

This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No. 787011 (SPEAR).

References

[1] C. Baylon, *Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare*. Cham: Springer International Publishing, 2017, pp. 213–229. [Online]. Available: https://doi.org/10.1007/978-3-319-45300-2_12

[2] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The cousins of stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 1 2012.

[3] B. B. Gupta and T. Akhtar, "A survey on smart power grid: frameworks, tools, security issues, and solutions," *Annals of Telecommunications*, vol. 72, no. 9, pp. 517–549, Oct 2017. [Online]. Available: https://doi.org/10.1007/s12243-017-0605-4

[4] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection*, vol. 18, pp. 3 – 19, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548217300495

[5] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45 – 56, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0142061517328946

[6] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933–1954, Fourthquarter 2014.

[7] B. Tare, S. Waghmare, I. Siddavatam, F. Kazi, and N. Singh, "Security analysis of dnp3 using cpn model with state space report representation using lda," in *2016 Indian Control Conference (ICC)*, Jan 2016, pp. 25–31.

[8] A. Elgargouri, R. Virrankoski, and M. Elmusrati, "Iec 61850 based smart grid security," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, March 2015, pp. 2461–2465.

[9] R. Nardone, R. J. Rodrguez, and S. Marrone, "Formal security assessment of modbus protocol," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2016, pp. 142–147.

[10] J. Jow, Y. Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," *International Journal of Sensor Networks*, vol. 23, no. 3, pp. 170–186, 2017.

[11] W. Tong, L. Lu, Z. Li, J. Lin, and X. Jin, "A survey on intrusion detection system for advanced metering infrastructure," in *2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC)*, July 2016, pp. 33–37.

[12] R. Leszczyna and M. R. Wrbel, "Evaluation of open source siem for situation awareness platform in the smart grid environment," in *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2015, pp. 1–4.

[13] W. Shang, M. Wan, P. Zeng, and Q. Qiao, "Research on self-learning method on generation and optimization of industrial firewall rules," in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Nov 2015, pp. 47–52.

[14] A. H. Khosroshahi and H. Shahinzadeh, "Security technology by using firewall for smart grid," *Bulletin of Electrical Engineering and Informatics*, vol. 5, no. 3, pp. 366–372, 2016.

[15] H. Eslava, L. A. Rojas, and D. Pineda, "An algorithm for optimal firewall placement in iec61850 substations," *Journal of Power and Energy Engineering*, vol. 3, no. 04, p. 16, 2015.

[16] W. Shang, Q. Qiao, M. Wan, and P. Zeng, "Design and implementation of industrial firewall for modbus/tcp." *JcP*, vol. 11, no. 5, pp. 432–438, 2016.

[17] R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks," in *2017 IEEE PES PowerAfrica*, June 2017, pp. 28–33.

[18] ——, "Quantitative analysis of firewall security under ddos attacks in smart grid ami networks," in *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, Nov 2017, pp. 696–701.

[19] I. Nai Fovino, A. Carcano, A. Coletta, M. Guglielmi, M. Masera, and A. Trombetta, "State-based firewall for industrial protocols with critical-state prediction monitor," in *Critical Information Infrastructures Security*, C. Xenakis and S. Wolthusen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 116–127.