ASTORIA: A Framework for Attack Simulation and Evaluation in Smart Grids

Alexandre Gustavo Wermann, Marcelo Cardoso Bortolozzo, Eduardo Germano da Silva,
Alberto Schaeffer-Filho, Luciano Paschoal Gaspary, Marinho Barcellos
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
Email: {agwermann, marcelo.bortolozzo, eduardo.germano, alberto, paschoal, marinho}@inf.ufrgs.br

***Abstract*—Electric power grids are undergoing a modernization process. By relying on the ICT infrastructure and on Internet connectivity, these so-called Smart Grids are now able to provide new functionalities and to become more efficient. However, despite the existence of a few standards that aim to specify the secure operation of Smart Grids, utility companies do not have a comprehensive set of metrics and evaluation tools for assessing security properties in these infrastructures. Thus, it is necessary to develop new toolsets to provide support for vulnerability analysis in Smart Grids. This paper proposes ASTORIA, a framework developed to allow the simulation of attacks and the evaluation of their impact on Smart Grid infrastructures, using closely-related real devices and real topologies comprising both power grid elements as well as ICT and networking equipment. We anticipate that ASTORIA can be used by Smart Grid operators not only to analyze the impact of malicious attacks and other security threats in different components, but also to permit the development and evaluation of anomaly detection techniques in a simulation environment. Further, we present evaluation scenarios illustrating customizable Smart Grid topologies, comprising sensors, master and remote stations, and using an extensible set of attack profiles.**

I. Introduction

Electric power grids are part of a complex critical system that encompasses energy generation, transmission and distribution. These systems are undergoing a modernization process and, by relying on the ICT infrastructure and on Internet connectivity, are now able to provide new functionalities and to become more efficient. This new generation of power grids is called *Smart Grids*. According to the Department of Homeland Security of the United States, Smart Grids are classified as one of the eighteen critical infrastructures [1], supporting essential services to sustain society. Consequently, these systems need to be protected against an increasing range of security attacks. In this context, SCADA (Supervisory Control and Data Acquisition) power systems are a prime target for different kinds of attacks and need to ensure high levels of confidentiality, integrity and availability.

The number of attacks against SCADA systems in general has doubled in 2014 compared with the previous year, according to Dell Security Annual Threat Report 2015 [2]. Only in Finland, United Kingdom and United States, which are countries where SCADA systems are more likely to be connected to the Internet, 202,322 attacks were registered in 2014. These numbers take into account not only power system vulnerabilities but also attacks in all kinds of SCADA systems such as petroleum refineries, factory control systems and water and gas distribution centers. According to the report, buffer overflow vulnerabilities are the primary attack method, corresponding to 25% of the attacks. Improper input validation and information exposure follow in second with about 9% each. Because some organizations prefer to hide the occurrence of attacks, and some may not be even detected, the number of incidents is likely to be higher.

Further, numerous events have been reported about attacks against SCADA systems specifically in the electricity sector. In 1999, a system administrator hacked into computers of a power distribution center in Wisconsin, U.S. He provoked twenty eight power outages and twenty other services interruptions causing about $800,000 in damage in thirteen Wisconsin provinces [3]. In 2003, a virus attack in a European utility compromised the management of several distribution substations for three days. It took approximately 40 person-week to solve the problem. There was no electric power loss; therefore there is no official acknowledgment of this incident [3]. More recently, in 2014, the Russian hacker group Dragonfly has compromised over 1,000 energy companies in North America and Europe [3], [4]. The group gained access to power plant control systems primarily by malware in emails, websites and third-party programs. The primary objective of the attack was cyber espionage. The incident was discovered before the group could cause damage or disruption to energy supplies in affected places. Despite the existence of a few standards that aim to specify the secure operation of Smart Grids, utility companies do not have a comprehensive set of metrics and evaluation tools for assessing security properties in these infrastructures [5]. Thus, it is necessary to develop new toolsets to provide support for vulnerability analysis in Smart Grids.

In this context, this paper proposes ASTORIA (**A**ttack **S**imulation **TO**olset for Smart G**R**id **I**nfr**A**structures), a framework that enables the specification of Smart Grid networks, as well as the simulation of attacks and the evaluation of their impact in these infrastructures. ASTORIA supports the simulation of customized topologies for Smart Grid infrastructures, comprising both power grid elements as well as ICT and networking equipment. The framework allows the instantiation of different Smart Grid devices to build realistic configurations. It is possible to associate consumption and production profiles to devices in geographically dispersed areas and generation power plants. The simulator provides a set of built-in attack profiles and allows the development of new ones to be explored by researchers or utility companies interested in improving the

security of Smart Grids. We anticipate that ASTORIA can be used by Smart Grid operators not only to analyze different kinds of vulnerabilities, but also to permit the development and evaluation of anomaly detection and mitigation techniques in a simulation environment.

This paper is organized as follows: Section II presents background on the Smart Grid architecture and its most common protocols. Section III discusses the primary vulnerabilities found in SCADA systems. Section IV describes the functionalities of the proposed framework and provides an overview of the attack simulation toolset. Section V presents the evaluation results of our tool combining real scenarios from specialized industry and academic papers. Section VI describes related work in simulation and evaluation of Smart Grids attacks. Section VII concludes the paper.

II. Background

Smart Grids are divided into seven complex domains [6]: Markets, Operations, Service Provider, Bulk Generation, Transmission, Distribution and Customer. ASTORIA covers the last three of them. Before describing in detail the framework functionality, this section presents background information on the Smart Grid architecture and its most common protocols.

A. Smart Grid Architecture

The typical Smart Grid power distribution architecture is composed of a Supervisory Control and Data Acquisition (SCADA) system, which includes the control center of the utility company and a set of distribution substations [7]. The control center is organized in a Control Network and the Corporate Network of the power distribution company. The main component of the control center is the Master Terminal Unit (MTU), which gathers real-time information from geographically dispersed substations and provides the management of the SCADA power distribution system from a control room. The Control Network also includes a Human-Machine Interface (HMI) whereby operators have access to all supervisory data system, SCADA servers and databases that store operational and financial information. The electrical distribution substations have a Remote Terminal Unit (RTU), usually implemented with Programmable Logic Controllers (PLCs), which communicate with hundreds of field devices located in substations, including sensors and actuators. PLCs and field devices are often referred to Intelligent Electronic Devices (IEDs). Substation components compose the Field Network. Figure 1 illustrates this Smart Grid architecture.

The power grid distribution system interacts with the transmission and customer domains [6]. Transmission lines are responsible for forwarding electricity from power plants to substations. These lines operate with high voltages in order to reduce energy dissipation. Substations deliver energy to customers in closely located areas. Sometimes, there are remote intermediary stations in poles between a substation and a region of customers.

B. SCADA Protocols

SCADA protocols follow a simple request-reply pattern between a master and a set of remote stations. While legacy

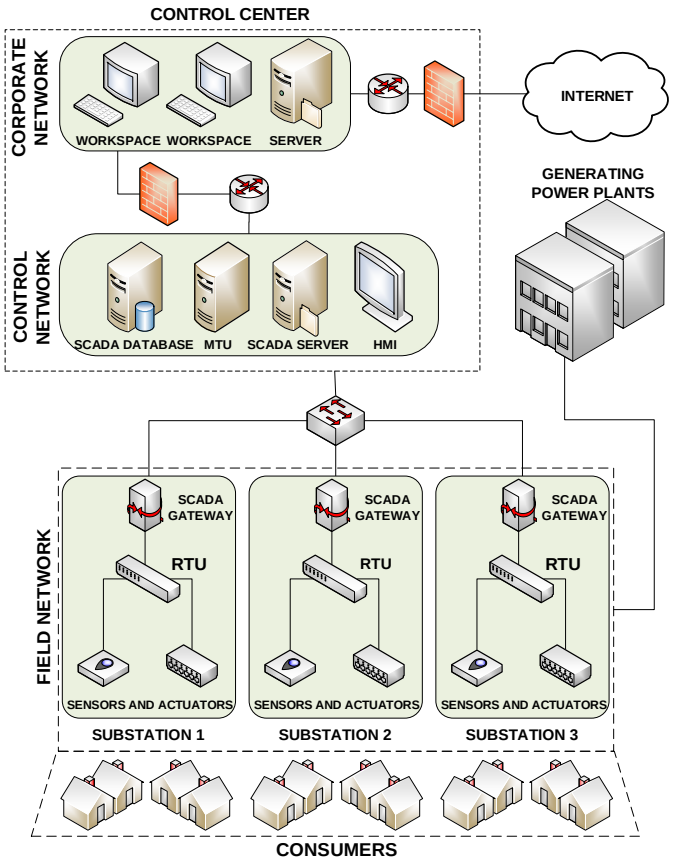


Fig. 1. Smart Grid architecture

protocols rely on serial communication, the vast majority of protocols currently in use is based on TCP/IP. Modbus [8] and DNP3 [9] are examples of protocols widely used in SCADA systems.

Modbus is a standard application layer protocol in industrial automation. The protocol works as follows: the master station sends a message with a function code that specifies the action to be taken, such as read sensor data or operate an actuator, and the slave station replies with the requested data. Initially, Modbus only supported serial communication, but with the advance of SCADA systems it was extended to a TCP/IP version. Modbus TCP/IP Application Data Unit (ADU) has a 7-byte header, the message function code and a field to additional data. The ADU is embedded into the data field of a TCP frame and sent via port 502 [8]. Although Modbus is a very simple protocol, it is still widely used in different SCADA applications.

DNP3 (Distributed Network Protocol) is a more advanced protocol. It was designed by a North American manufacturer specifically for SCADA systems and provides efficient communication between a master control computer and a remote outstation [10]. DNP3 supports master-slave communication in different network topologies such as One-on-One, Multi-drop, Hierarchical and Data Concentrator [11]. The protocol has two application layers: the top one is the DNP3 user's application and the bottom layer corresponds to the DNP3

protocol software that offers basic communication functions.

III. Vulnerability Analysis

Early power distribution communication networks were real-time air-gapped systems. They needed to offer high performance, while security was not the main concern. Despite the benefits provided by Smart Grids, such as two-way communication, improved energy management, and micro generation [12], these systems rely on legacy components and protocols and are thus subject to a number of vulnerabilities. Another concern is that Smart Grids are connected to the Internet and consequently present similar security threats. These vulnerabilities can be exploited by malicious users, to cause financial losses to the utility company, allowing blackmail, or benefit a particular person, enemy nations and even terrorist groups. In this section, we present some of the most common vulnerabilities encountered in Smart Grid components, classified according to Table I.

TABLE I. Smart Grid Vulnerabilities

	Confidentiality	**Integrity**	**Availability**
Control Center	Malicious Software, Phishing, Ping Sweeps, Port Scanning, Spyware	Malicious Software, SQL Injection, Unauthorized Access, Spoofing, Replay	Denial of Service, Malicious Software
RTU	Malicious Software, Ping Sweeps, Port Scanning	Malicious Software, Replay, Spoofing Unauthorized Access,	Denial of Service, Malicious Software
Field Devices	Denial of Service	Denial of Service Replay	Denial of Service, Buffer Overflow
Communication Protocols	Eavesdropping, Sniffing	Man-in-the-Middle, Sniffing	Denial of Service, Replay

A. Control Center

The control network of the SCADA distribution system is the front door to many types of cyber-attacks since it is connected to the corporate network and typically to the Internet. Considering that SCADA systems rarely make use of updated anti-virus [13], malicious software arising from the Internet can infect components of the control, corporate and field networks, and compromise communication between substations and the control center. Moreover, keeping operational systems and applications updated is demanding or even impossible [13]. Typically, the lifetime of SCADA equipment is about 15-20 years, which is much longer than traditional IT components; therefore, software is rarely updated to prevent incompatibilities that may cause the instability of the SCADA operation. The lack of updates is also a problem because network components are unsafe to a wide range of virus and malware.

The control center's databases are vulnerable to attacks against the integrity and confidentiality of critical data. In this context, an SQL Injection attack can access and modify confidential data of SCADA databases, such as overload network and energy costs, in order to damage equipment or benefit a particular user. The centralized control is another major problem of SCADA networks, given the fact that an intruder with access to the control center can easily operate the entire distribution system, potentially causing its collapse.

B. Field Network

The field network is composed of thousands of devices that measure and control the power distribution. These components usually run for many years without rebooting and accumulate memory fragmentation. Since field devices have constrained memory, an attacker can compromise their availability and cause component crashes through a buffer overflow attack. The problem can be reduced by adopting a more secure programming technique that includes fixed memory allocation and checking process memory borders. Buffer overflow is a common vulnerability in field devices, but is also present in control network components.

Another major challenge for security is that field components have limited computing resources. Encryption algorithms are generally computing intensive, and SCADA systems need to operate in real-time. This makes the use of cryptography difficult. Thus, eavesdropping and man-in-the-middle attacks can be readily exploited to cause financial or operational losses to the distribution company. A well-known technique to overcome this problem is called Bump-in-the-Wire [14]. It is widely used in different SCADA systems including those used for power distribution. It consists of additional gateways between the field and control networks, which encrypt and decrypt all transmitted and received data.

C. Communication Protocols

Because SCADA protocols are unable to support cryptography, the communication between master and slave components is subject to eavesdropping and sniffing attacks. Captured information can be used by attackers in different ways, such as to determine the power consumption of a particular area, breaching privacy, or as an enabler to cause Denial of Service attacks, *e.g.*, leading to power outages.

Further, the majority of protocols fail to offer a robust authentication technique. This vulnerability can be exploited by invaders in replay attacks to forge fake messages and send them to a particular component in order to reboot or shut it down. The lack of endpoint authentication can lead to Man-in-the-Middle attacks that aim to tamper operational or consumption messages. In contrast, some protocols adopt simple authentication methods and provide a higher level of authenticity, such as DNP3 [15].

IV. Attack Simulation and Evaluation in Smart Grids

Given the considerable number of security vulnerabilities that may afflict Smart Grids, and the fact that utility companies do not have a comprehensive set of metrics and evaluation tools for assessing security properties in these infrastructures, this paper proposes the ASTORIA Framework. ASTORIA allows the simulation of attacks and the evaluation of their impact on Smart Grid infrastructures, comprising both power grid elements as well as ICT and networking equipment. The framework permits the specification of accurate Smart Grid topologies, the creation of different types of attack profiles, and

the injection of attack instances during runtime. We anticipate that this toolset can help SCADA operators to understand the effects of malicious attacks in the Smart Grid, and assist in the implementation and evaluation of new attack detection and mitigation strategies. The next sections will present a description of the framework requirements, the system architecture and an overview of the possible attack profiles.

A. Framework Requirements

The framework is based on the integration of a communication network simulator with a power flow simulator, which correspond to the SCADA control and the power grid systems, respectively. There is a large number of power flow and network simulators, but to the best of our knowledge none can individually provide the attack simulation environment that we propose in this paper. We investigated tools that could attain the following requirements:

- ***Accurate power grid simulation:*** the framework needs to provide a power grid simulation close to the reality, including the grid infrastructure, as well as authentic energy production and consumption profiles;
- ***Network extensibility:*** the communication network has to be extensible to allow the instantiation of new components and protocols;
- ***Run-time information exchange:*** the power grid simulator needs to provide the measurement system found in field devices, and provide sampled data to the communication simulator;
- ***Scalability:*** the simulation environment should be scalable to support large-scale and realistic topologies with thousands of devices;
- ***Attack development:*** the toolset should allow the implementation and customization of different types of attacks against components or protocols.

The power flow simulator must allow the production and consumption of electricity data obtained from the distribution grid. The network simulator, in turn, must use the information obtained from the distribution grid to simulate the SCADA system and its communication infrastructure. The integration between both simulators needs to be performed by a middleware that can coordinate and manage the information exchange. Moreover, the simulator parameters configuration, the grid topology, as well as energy and attack profiles need to be simple and easy to build.

B. Framework Conceptual Architecture

Figure 2 shows the conceptual architecture of ASTORIA. The power flow simulator has specific nodes for power distribution, consumption and production. These nodes are responsible for generating power information in the proposed framework. The network communication simulator contains components to reproduce the behaviors of the MTU, RTUs and field devices. These components are associated in pairs for reproducing a Smart Grid distribution environment, *i.e*, each power simulator node has its correlated network simulator node, except for the MTU, since it is an exclusive SCADA component. The matching between elements of the SCADA network and power grid nodes is illustrated in Figure 2: while RTU is associated with distribution nodes, field devices are associated with consumption and production nodes. RTUs store data from field devices. This data contains the power consumption of the respective geographical area being monitored. The MTU requests data from RTUs and the field data from their respective sensors. In other words, the MTU stores data from sensors of the power distribution system.

The integration between both simulators is supported by a middleware layer. This middleware manages the communication between the network simulator and the power flow simulator, and allows a synchronized simulation in configurable time steps. It also provides the initialization of both simulators, configuring the grid topology, the energy profiles and the simulators parameters.

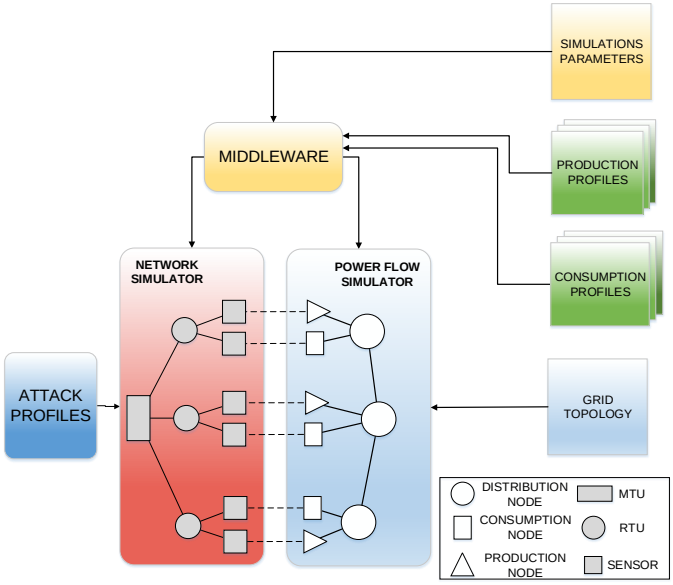


Fig. 2. ASTORIA framework conceptual architecture.

The ASTORIA framework facilitates the specification of customized simulations that can be configured by four input datasets: *Simulation Parameters*, *Grid Topology*, *Consumption Profile* and *Production Profile*. These configuration datasets provide ASTORIA with information about: the simulation step time, the number of field devices connected to each substation; the number of residences associated to each sensor; and the amount of final users in each residence. It is also possible to set the consumption and production data to be managed by the power flow simulator, and the interconnection between all network components, including production nodes and the MTU.

C. Attack Profiles Simulation

ASTORIA permits the injection of attacks and the evaluation of their impact through a simulated environment. These attacks are instantiated via *Attack Profiles*. An attack profile consists of a generic formatted configuration file, to facilitate the specification of different kinds of attack behaviors. It enables the setting of different attack parameters, such as attack type, source and target components, frequency/intensity, and

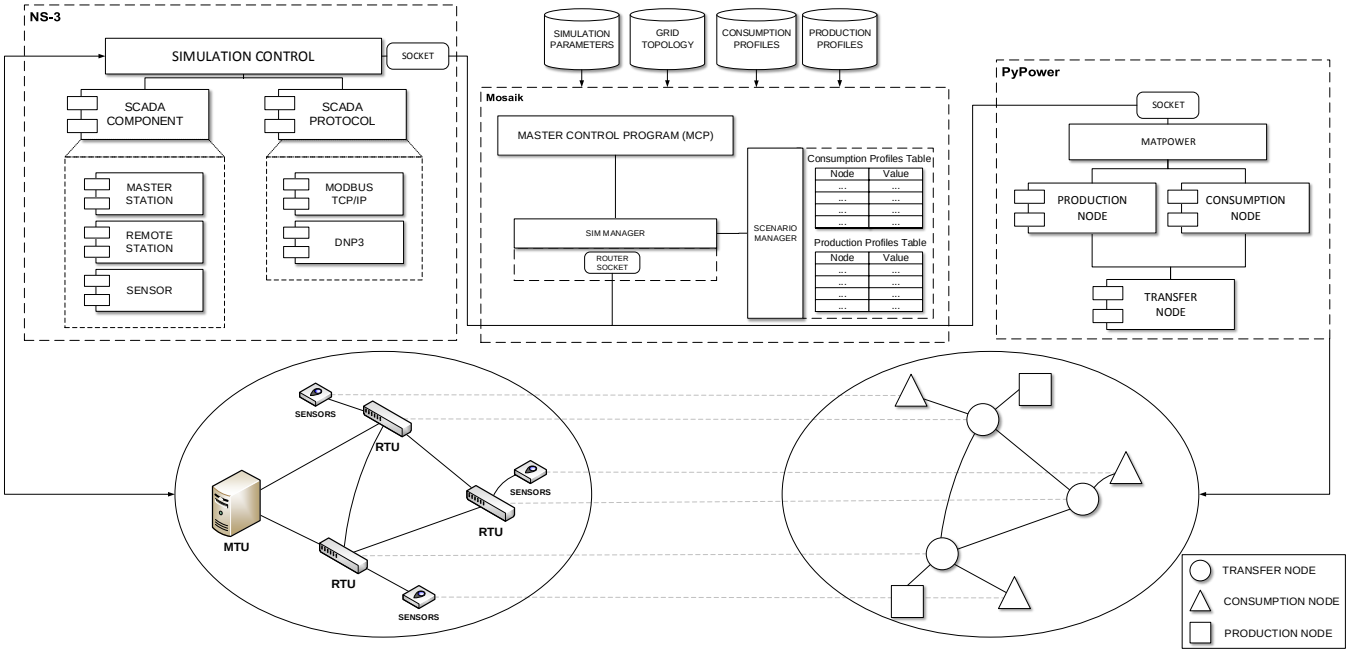


Fig. 4. ASTORIA prototype overview.

```
'AttackProfile': [

    'attack-type' : 'Denial-of-Service',
    'source-node' : 'RTU_X',
    'target-node' : 'RTU_Y',
    'step-size' : '2ms',
    'attack-start-time-hour' : '09:00:00',
    'attack-start-time-day' : '04-25-2016',
    'args' :
        [
        'packet-size': '1k'
        ]

]
```

Fig. 3. DoS Attack Profile configuration file.

the attack start time in the simulation. There are also optional parameters for specific types of attacks, such as the packet size of a buffer overflow attack. An example of a Denial-of-Service (DoS) Attack Profile is presented in Figure 3.

The attacks supported by the ASTORIA framework include the ones addressed in Section III: malicious software infection for tampering measurement information from sensors; DoS attacks against a SCADA device in order to cause a buffer overflow; and IP spoofing in the communication between devices, possibly leading to a man-in-the-middle attack. The framework also allows the installation of port scanner software in SCADA components to identify running services and compromise them, and replay attacks to transmit eavesdropped data to grid devices. Moreover, the library of attacks is extensible and new attacks can be readily implemented by developers interested in using and taking advantage of ASTORIA.

V. Implementation and Evaluation Results

In this section, we describe the proof-of-concept prototype of ASTORIA. Further, we present two types of attacks simulated using ASTORIA. Finally, we discuss the results achieved in our experiments.

A. ASTORIA Prototype Overview

ASTORIA is based on the integration between a power flow simulator and a network simulator. Figure 4 presents an overview of the implemented prototype. We chose PYPOWER[1] as the power flow simulator, which is an Alternating Current/Direct Current (AC/DC) Optimal Power Flow solver. It provides the structure for the simulation of a power grid and generates production and consumption information in real-time. PYPOWER can simulate realistic energy measurement data. This data is used as input to the communication network, and also enable the instantiation of the power grid topology. The power flow simulated by PYPOWER is based on production and consumption profiles, and each PYPOWER node has an ID number and its type (that can be production, consumption, or distribution node). Hence, each PYPOWER node is associated with a SCADA component in the network simulator.

For network simulation, we rely on NS-3. NS-3 allows the simulation of large-scale experiments and permits the development and instantiation of network components and protocols. It supports a large number of protocols, such as IP, IPv6, TCP, UDP, ARP and Ethernet. Typical SCADA communication protocols, such as Modbus TCP/IP and DNP3 over TCP, are not available. However, since NS-3 is extensible and permits adding extra components, we were able to develop and deploy these SCADA protocols in this simulator. We also

[1] https://pypi.python.org/pypi/PYPOWER

developed additional components in NS-3 to reproduce the behavior of MTU, RTU and field devices. Further, we created a *Simulation Control* component for managing the simulated SCADA network.

ASTORIA uses Mosaik[2] as the middleware for enabling the integration between PYPOWER and NS-3. Mosaik intermediates the communication between the two simulators through: *(i)* the use of socket connections; and *(ii)* the exchange of messages following the JSON format. Mosaik initializes both simulators and coordinates their execution by managing the simulation in time steps. Mosaik is also used to match the components of the two simulators, in order to collect data from the power grid and forward it to the communication network. The main component of Mosaik is the *Master Control Program (MCP)*, which is responsible for managing the simulation through the *Sim Manager* module. In turn, *Sim Manager* handles the communication with third-party simulators. Finally, the *Scenario Manager* component associates power grid and communication nodes, and manages the consumption and production profiles.

B. Evaluation Scenario

We simulated real scenarios in order to implements different kinds of attacks against a Smart Grid environment. These evaluation scenarios combine information from specialized industry and scientific literature. The power grid topology uses a peer-to-peer connection and was based on the IEEE 14 Bus Power Flow Test Case[3]. The protocol used was Modbus TCP/IP. The MTU requests real-time power consumption measurements of a geographic area from the corresponding RTU every 2 seconds, which is the default request time in typical SCADA systems. Figure 5 depicts the evaluation scenario, which is composed of 1 MTU, 14 RTUs, and 560 field devices.

Keeping in mind the vulnerabilities previously presented in Section III, we also reproduce a set of attacks by adding *Attacker* components. We simulated two common SCADA cyber-attacks: a Malicious Software Infection, for tampering power consumption information of a particular region; and a DoS attack targeting a set of SCADA components, in order to halt their operation due to a buffer overflow. The first one was implemented by creating an *MSIAttacker* application and installing it in a remote station. When the MTU requests sensor data from the infected RTU, the Malware intercepts the packet and informs a consumption measurement that is lower than the actual one. In the second attack, we created a *DOSAttacker* application to exploit buffer overflow vulnerabilities in four RTUs, disrupting the operation of the supplied regions.

C. Simulation Results

In this section, we demonstrate the results achieved in our experiments. They were analyzed to calculate the impact of the simulated cyber-attacks, in terms of: financial and operational losses to the power distribution company; and number of affected customers.

[2]https://mosaik.offis.de/

[3]https://www.ee.washington.edu/research/pstca/pf14/pg tca14bus.htm

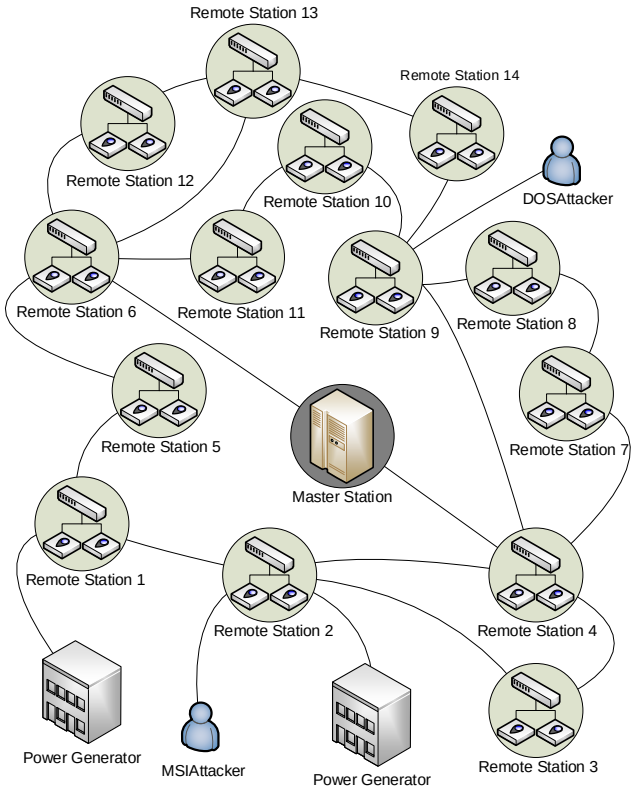
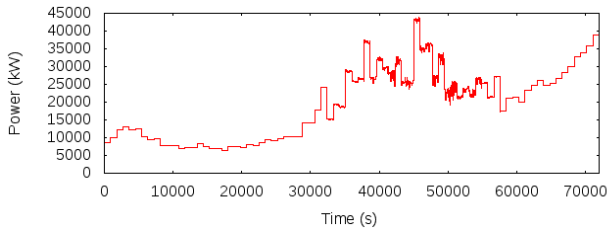


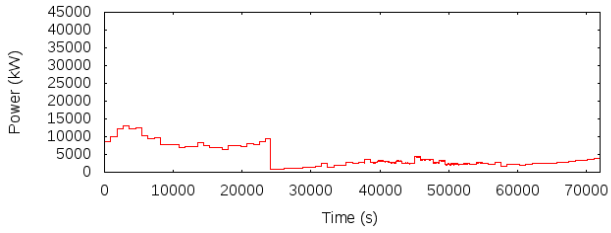
Fig. 5. Scenario adopted in the simulation.

1) Malicious Software Infection Attack: As already mentioned in Section III, the power grid is a prime target for malicious software attacks since anti-virus is rarely adopted. A virus can come from the Internet or be introduced physically via USB ports. Malware propagation can be performed by a person interested in causing financial or operational losses to the distribution company and reduce energy consumption in an area. The Malware application interferes the communication between the MTU and a RTU by sending tampered power measurements.

Figure 6 presents the results of the malware attack experiment. Figure 6(a) shows the instantaneous power consumption sampled by a sensor in the compromised remote station. In turn, Figure 6(b) presents the tampered values forwarded to the MTU by the malware. There is no tampering occurring until 24,000 seconds of simulation, which is when the malicious application starts to report 10% of the actual consumption. The amount of energy being stolen is estimated by the difference between the two plot areas. Considering that the average real consumption between 24,000 and 70,000 seconds was approximately 250,00kW, we estimate 1.15TJ of actual energy consumption during 12 hours. Since the reported consumption was only 10% of the real one, the utility company registered only 1.15GJ of energy consumption. This corresponds to approximately 320,000kWh and 320kWh, respectively. Consequently, the energy not accounted for is approximately 319,680kWh. Considering a price of US$ 0.30/kWh, this attack can provoke a financial loss of US$ 95,904.00 to the power company in a short period of only 12 hours.



(a) Power consumption sampled by RTU sensors.



(b) Power consumption informed by the Malware software to MTU.

Fig. 6. Results of the Malware infection simulation.

Besides financial losses, this attack can impact not only the region supplied by the affected substation, but also geographically dispersed areas. Further, the compromise of data integrity can lead power grid operators to make wrong decisions, affecting the control of the power distribution system. The consequences can be devastating since the master station cannot detect the message tampering. In a real scenario, the control center may wrongly decide that the affected area has lower energy demands, which can result in power outages. A good alternative to avoid malware infection is the use of firewalls to protect the system against threats arising from the Internet and to restrict the access of third-party person to critical operated areas.

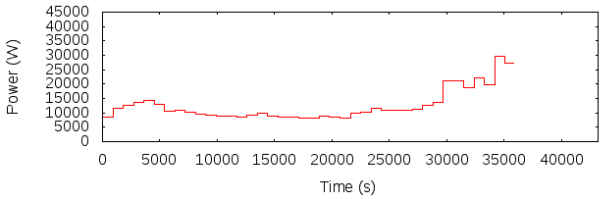
2) Denial of Service Attack: Considering that field devices have small memory capacity and are susceptible to fragmentation, the second attack implemented was a buffer overflow. We chose this attack because, as already mentioned, buffer overflow was the main vulnerability exploited in SCADA systems in 2014. A buffer overflow attack tries to delay or crash a SCADA component by exploiting bugs in the implementation of the protocol stack [16], input data queue or PLCs stack pointers. In this experiment, a set of RTUs halt their operation due to the overflow of the input value's queue caused by a DoS attack. We implemented a *DOSAttacker* component to send a high amount of valid sampled data to the remote stations. In the RTUs, we simulated a small input data queue. After some time of DoS attack, the input queue overflows and the RTU halts.

Figure 7 shows the results obtained in the DoS attack. In 7(a), we can see the real-time energy consumption sampled by the RTU sensors. Figure 7(b) demonstrates the number of packets per second sent by the attacker to RTU 4. The attack starts at 15,000 seconds of simulation when the number of packets per second increases from 1 (the request time of Modbus TCP/IP is 2 seconds) to 80 packets. The RTU is the target of the DoS until 36,000 seconds, which is when the input queue overflows and the component halts.

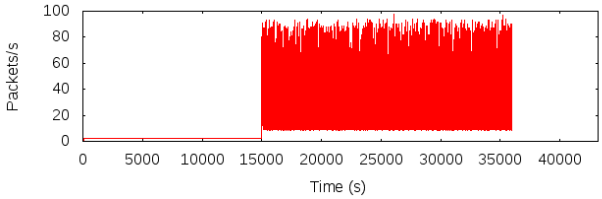
This experiment demonstrates that the consequences of a buffer overflow can be catastrophic since it can cause SCADA components to crash. The lack of consumption and production information has an impact on the control of the power grid, and may lead to power overloads, outages or even blackouts. Table II presents the estimated impact in terms of compromised sensors and affected households in our experiment. In seven hours, MTU loses the communication with three RTUs and 180 sensors. We also estimate a number of 1,125 households affected.

TABLE II. COMPONENTS AFFECTED BY THE DOS ATTACK

	Compromised sensors	Affected households	Simulation time (s)
RTU 4	40	250	35000
RTU 5	60	375	50000
RTU 9	80	500	60000



(a) Real-time power consumption sampled by RTU sensors.



(b) The number of packets per seconds sent by the attacker.

Fig. 7. Results of the buffer overflow attack.

VI. RELATED WORK

Recent attacks against SCADA and power grids have exposed vulnerabilities and the need of more robust and reliable security mechanisms. As such, it is necessary to analyze risks and vulnerabilities in these systems. However, given the importance, responsibility, and nature of Smart Grids, it is not feasible to conduct security experiments in real cyber-physical environments. Thus, the development of Smart Grid simulation frameworks is important, in order to enable the evaluation of security solutions before they are deployed in real systems. Queiroz *et al.* [17] presented SCADASim, a flexible SCADA simulator that supports the integration of real external field devices. SCADASim allows real-time communication between devices using SCADA protocols, *e.g.*, Modbus/TCP and DNP3. Almalawi *et al.* [18] proposed SCADAVT, a SCADA security simulation testbed for water distribution systems. In addition, the authors presented two case-studies to show how malicious attacks can disrupt supervised processes. There are also efforts that present specific Smart Grid simulators. Tan *et al.* [19] presents the Smart-Grid Common Open Research Emulator (SCORE), an integrated Smart Grid emulator of both power and communication network. This application enables solutions developed in this environment to be ported to embedded

devices with few or no modification. Finally, GECO *et al.* [20] is another existing power grid simulator, which was developed for dynamic simulations of WAMS (Wide Area Measurement Systems) applications. This simulator is a power system and communication network co-simulation framework, *i.e.*, it offers synchronized simulation of power system and communication network models.

Unfortunately, the solutions currently available focus on particular parts of a power grid (*e.g.* GECO), or they address only the SCADA system (such as SCADASim and SCADAVT). Moreover, some of these simulators are not maintained by their developers, or they have been discontinued (such as SCADASim and SCORE). The ASTORIA framework aims to bridge this gap, by enabling the simulation of complex and accurate Smart Grid scenarios, comprising both the power infrastructure and the communication network. In addition, our framework allows the simulation and evaluation of cyber-attacks, which we expect that will help the development of specific resilience mechanisms for these environments.

VII. Conclusion

This paper presented ASTORIA, a framework for attack simulation in Smart Grids. It is based on the integration of a power flow and a network simulator to reproduce a real Smart Grid environment. Considering that utility companies do not have a comprehensive set of metrics and evaluation tools for assessing security properties in these infrastructures, ASTORIA can be used to support the simulation and evaluation of vulnerabilities in these systems.

Our primary contribution is a Smart Grid environment to simulate and analyze threats found in different components and protocols. Further, we expect that system operators will be able to use ASTORIA not only to evaluate the impact of malicious attacks, but also to allow the early development and assessment of new anomaly detection and mitigation techniques, prior to their deployment in a real system. Despite our efforts in trying to reproduce an accurate implementation of SCADA protocols and the real operation of SCADA components, we acknowledge that simulation environments have well-known limitations and may abstract some of the details found in an actual system implementation. Nevertheless, simulation environments are still important during the early stages of development or when the physical infrastructure cannot be easily prototyped in an actual testbed. We expect that the framework presented in this paper will support researchers, system administrators and SCADA operators in improving the security of Smart Grids.

Acknowledgement

This work is supported by ProSeG - Information Security, Protection and Resilience in Smart Grids, a research project funded by MCTI/CNPq/CT-ENERG # 33/2013.

References

[1] C. S. U. Sacramento, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks," California State University Sacramento, Tech. Rep., 2012.

[2] D. Incorporated, "Dell Security Annual Threat Report," Dell Incorporated, Tech. Rep., 2015. [Online]. Available: https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708

[3] E. Worldwide. (2015, July) RISIDATA - The Repository of Industrial Security Incidents. [Online]. Available: http://www.risidata.com

[4] The Hacker News. [Online]. Available: http://thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html

[5] U. S. G. A. Office, "Challenges in Securing the Electricity Grid," Tech. Rep., 2012.

[6] V. Igure, S. Laughter, and R. Williams, "Security Issues in SCADA Networks," *Computers & Security*, vol. 25, no. 7, pp. 498 – 506, 2006.

[7] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," *NIST special publication*, pp. 800–82, 2011.

[8] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack Taxonomies for the Modbus Protocols," *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37 – 44, 2008.

[9] S. East, J. Butts, M. Papa, and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in *Critical Infrastructure Protection III*. Springer, 2009, pp. 67–81.

[10] D. Bailey and E. Wright, "SCADA Systems, Software and Srotocols," in *Practical SCADA for Industry*, D. B. Wright, Ed. Oxford: Newnes, 2003, pp. 64 – 99.

[11] G. R. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.

[12] (2015, July) U.s. department of energy. [Online]. Available: http://energy.gov/oe/services/technology-development/smart-grid

[13] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Evaluating Security and Resilience of Critical Networked Infrastructures after Stuxnet," in *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. IGI Global, 2013, p. 153.

[14] P. Tsang and S. Smith, "YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," in *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, ser. IFIP The International Federation for Information Processing, S. Jajodia, P. Samarati, and S. Cimato, Eds. Springer US, 2008, vol. 278, pp. 445–459.

[15] X. Lu, Z. Lu, W. Wang, and J. Ma, "On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–6.

[16] R. Barbosa, "Anomaly Detection in SCADA Systems: A network based approach," Ph.D. dissertation, University of Twente, Enschede, April 2014. [Online]. Available: http://doc.utwente.nl/90271/

[17] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim: A Framework for Building SCADA Simulations," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 589–597, Dec 2011.

[18] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad, "SCADAVT-A framework for SCADA security testbed based on virtualization technology," in *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*, Oct 2013, pp. 639–646.

[19] S. Tan, W. Song, Q. Dong, and L. Tong, "SCORE: Smart-Grid common open research emulator," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, Nov 2012, pp. 282–287.

[20] H. Lin, S. Veda, S. Shukla, L. Mili, and J. Thorp, "GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1444–1456, Sept 2012.