

Cyber attacks in Power Grid ICT systems leading to financial disturbance

Yannis Soupionis and Thierry Benoist

European Commission, Joint Research Centre (JRC)
Institute for the Protection and Security of the Citizen (IPSC)
Security Technology Assessment Unit
Via E. Fermi, 2749, 21027 Ispra, Italy
{yannis.soupionis,thierry.benoist}@jrc.ec.europa.eu

Abstract. Decentralized Critical infrastructure management systems will play a key role in reducing costs and improving the quality of service of industrial processes, such as electricity production. In this paper, we focus on the security issues on the communication channel between the main entities of a smart grid, like generators, consumers and transmission/distribution operators and the energy market. We simulate the energy (spot) market auctions and the power grid network, but we emulate the ICT information part which is the focus of our work. We set in motion a well-known attack, Denial-of-Service (DoS), in Cyber-Physical systems and we are able to identify the consequences not only in power distribution network but also in financial area.

Keywords: Cyber physical, cyber security, DoS attack, energy market

1 Introduction

Information and Communication Technologies (ICT) is a key component of the current Critical Infrastructures (CI), since their operation is dependent on communication between the CI components. Moreover, ICT involvement in CI management is being promoted by most regulators, since it can lead to cost reduction, greater efficiency and interoperability between components. So the time that the CIs were isolated environments has passed and we have reached a state where most of them are interconnected and the lack of communication can lead to serious problems. Moreover, the isolation of the CIs has many functional limitations, e.g. higher installation, maintenance and operational costs coming from not infrastructure sharing. Therefore the reliance of CIs on distributed Networked Industrial Control Systems (NICS) brings a lot of positive attributes, but it makes them vulnerable to significant cyber-threats [1], [2].

The CIs interdependency [3], [4] and uncertainty/implications in the Cyber-Physical environment, as cyber attacks and errors in physical devices, make ensuring overall system robustness, security, and safety a critical challenge. A well-established cyber threat is the Distributed Denial of Service (DDoS) attacks,

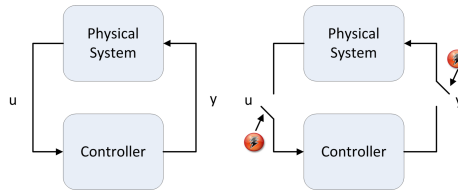


Fig. 1. Overview of normal operation (left) and under DoS attack (right).

which is one of the most effective form of attacks known today. By flooding a network element of the NCIS from many different sources, DDoS attacks can make part of the ICT infrastructure to be separated from important information for the operation of the CIs. This is depicted in Fig. 1, where either the control or the physical equipment is not able to communicate with the other infrastructure element.

Nowadays, CIs are very familiar with DDoS attacks. A McAfee report in November 2010 [15] shows energy providers are getting hit by some serious DDoS attacks. Across 200 industry executives over 14 countries revealed that 8 in 10 CIs had faced a significant DDoS attack in 2010. The full report has shown the sheer scale of attacks, with 29 per cent of critical infrastructure providers surveyed saying they were being hit by large scale DDoS attacks multiple times each month. Stuxnet [16] was listed as the most significant threat affecting CIs to date, which has been proven wrong about the possibilities of cyber attacks. Moreover, the last report [13] of the European Network and Information Security Agency (ENISA) shows clearly that a significant increase of Denial of Service attacks has been detected. The main reason is the DNS reflection attacks, which target poorly configured DNS servers. Additionally, there are tools which embrace DoS attack capabilities and can be obtained without any extreme cost [12]. The most destructive DDoS to date was not recorded against a CI but against the Spamhaus in 2013. Thanks to many misconfigured DNS servers (Open resolvers) worldwide, the hosting service CyberBunker performed a DNS-amplified DDoS on Spamhaus with bursts of up to 300Gbps.

An important communication channel for the smart grid is the exchanging data between the power production elements and the power market, especially when the power management system is centralized. The main feature of this model is that at the physical layer, the grid is designed for a one-way flow of the electricity. More precisely, this is presented in Fig. 2 from the left part of the figure, where the electricity is generated in large power plants and transported to local substations, to the right part, where it is in the delivery of electricity to end users. An abstract view of the communication between the main elements of the power grid is also illustrated in Fig. 2 and it is obvious that any communication interruption can lead to unexpected results.

In this paper we present the development of an infrastructure which is composed of an IEEE simulated power grid, a simulated power market and the emulated network connecting those elements. We experimentally show that there are

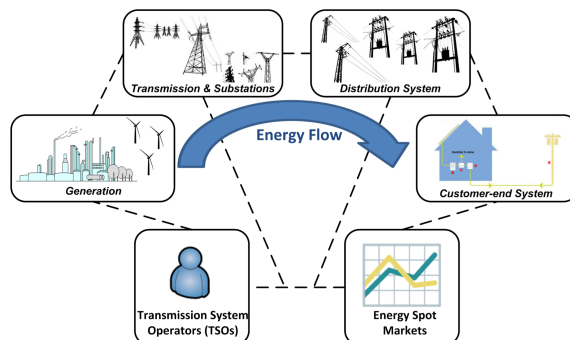


Fig. 2. Information and energy flow in Smart Grid infrastructure.

serious consequences on the power grid stability and on the market, by attacking solely on the provided communication data between the SCADA systems, the local Programmable Logic Controllers (PLCs) of the power grid nodes and the market. This research work provides a preliminary effort to a) integrate those three smart grid elements (power, ICT infrastructure and power market) in a real-time experimental platform and b) indicate the lack of models/approaches to reproduce the state of the network in extreme conditions such as DDoS attacks

Nevertheless, simple topology changes can have a significant impact on the network's resilience which is going to be presented in experimental section. Such solutions can already be deployed using existing routing hardware and software which can render DDoS attacks ineffective even with default configurations.

The paper is organized as follows: Section 2 describes the related work while in Section 3 we present the main elements of our research work. In section 4 we explain the proposed the created experimental framework, which includes the emulated and simulated elements of the infrastructure. Section 5 illustrates the impact of the DDoS attacks onto a power grid and describes the experimental results. Finally, section 6 concludes this work and identifies some open subjects for future work.

2 Related work

In this section, we briefly survey some techniques and approaches, which focus on the financial impact of cyber attacks on cyber-physical infrastructures.

Article [8] illustrates an able to be approximated the cyber-attack impact in financial terms. The papers focus on integrity cyber attacks occurring on electric power market operations. They focus on a different kind of attack which is based on the knowledge of the system's parameters. We propose a brute force attack, which can target directly our infrastructure and affect it by limiting the communication resources between the participating entities. Moreover, in [9] the authors show the impact of integrity attacks, as well. The attack's impact is

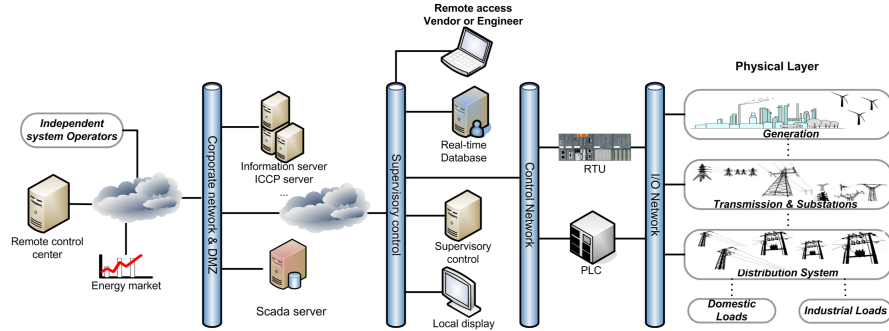


Fig. 3. The layers of the ICT power grid controlling system.

well illustrated but not only do they focus on a different kind of attack, they concentrate mainly on attack detection and identification procedures.

The financial impact is studied via a game theoretical approach in [10]. The effect of compromising measurements on the price of electricity is expressed as a zero-sum game between the attacker and the defender. The game identifies the effectiveness as well as the properties of the participants' strategy, justifies them through a detailed simulation, but fails to reach an equilibrium that is the best point for the operator/defender for designing a proper detection method. This work is a nice approach for the operators in order to draw their financial strategy but does not take into account any specific security issues.

3 ICT infrastructure and Power/Spot Market

The main two elements for our implementation is the ICT infrastructure serving the communication channel and the power market which is based on auction algorithms for serving the optimal energy bids.

3.1 Networked Industrial Control Systems

In this section we provide a brief description of the NICS architecture used in this work. We present the standardized architecture and subsequently our implementation of the simulation/emulation framework.

The ICT infrastructure of a power grid system is consisted mainly by the automation control. It includes of control centers, which supervise the operation of the substations. The layers of the power grid controlling system are depicted in Fig. 3 and they perform all the controlling procedures and data collection.

The physical layer is composed of field devices, like sensors, meters, phase measuring units, which send raw information to the first layer. There we have Remote Terminal Unit (also called a SCADA slave), Programmable Logical Controllers (PLCs) and lower-level distributed controls. The higher layers contain

more advanced controlling processes as Supervisory Control and Data Acquisition (SCADA) server.

Moreover, in order to deliver electrical power from producers to consumers in a cost-effective way, the central power grid operators have to exchange information with various organization and devices, as Independent System Operators and Energy market. This data is collected at corporate and control center level (remote control center). Even though the communication at an operation center level is generally based on dedicated lines using ICCP (Inter Control Center Protocol), the link that is deployed between operation center and corporate/control relies on IP-based (Internet Protocol) protocols.

Traditionally, power grid automation systems have been physically isolated from the corporate network, often using proprietary protocols and legacy hardware and software. However, this has been changing to public infrastructures so as to reduce the operational cost [11]. From the financial point of view, it seems like a reasonable choice, however one should be aware of the fact that it definitely increases the vulnerability of power grids to cyber attacks and the associated implications.

3.2 Power Market

Electricity is an essential good in our society. Since more than one decade, a political change of mind has led to the liberalization of the power markets. Its goal: the creation of an internal European market which achieves security of supply and competitive prices and services for the customers. In this market, a growing variety of enterprises organizes the production, the trading, the marketing, the transmission and the supply of electricity, respecting appropriate regulation. Producers compete to sell energy at the best possible price. The suppliers which deliver electricity to the final consumers buy the energy on the wholesale market from the producers or the trading companies.

Power markets or spot markets offer trading platforms [18]- [20] to exchange members submitting bids for buying and selling power. They organize markets that are optional, anonymous and accessible to all participants satisfying admission requirements. The main objective of power exchanges is to ensure a transparent and reliable wholesale price formation mechanism on the power market by matching supply and demand at a fair price and ensure that the trades done at the exchange are finally delivered and paid. Summarizing, for the cyber security point of view the power market processes should guarantee fair and orderly execution of the orders of the exchange members. Therefore a possible interruption between the communication of the power grid and the power market can lead to financial disturbances and even to market/prices manipulation.

The main procedure of a power market, apart from the exchanging money and anonymization, is the auction, which is any set of trading rules for exchanging goods or services by offering them up for bid, taking bids, and then selling the item to the highest bidder. The auction type we implement for our research work is a one-sided auction, which is presented briefly in the next subsection.

One-Sided Auctions In a one-sided auction bids only inserted only from the producers, and are sorted in an ascending order based on the price per KW (power grid). The consumers demand is unelastic, meaning they have to absorb/consume the requested power. Offers are accepted beginning with the least expensive and continuing until the demand is satisfied. The uniform price is then set equal to either the last accepted offer. The offers by the producers are arranged by blocks which contain a certain amount of KW. Usually the last block is partially accepted, except for the special case where the quantity clears all the offered block. This block is taken as the last accepted block and its price corresponds to the incremental cost of additional demand. Moreover, the distance between the power grid buses (section 4.2) are included in the prices adjustment, which represents the cost of transmission between locations. Generalizing to a network with possible losses and congestion results in nodal prices λ^p which vary according to location. These λ^p values can be used to normalize all bids and offers to a reference location by multiplying by a locational scale factor. For bids and offers at bus i , this scale factor is $\lambda_{ref}^p / \lambda_i^p$, where ref is the nodal price at the reference bus. The desired uniform pricing rule can then be applied to the adjusted offers and bids to get the appropriate uniform price at the reference bus. For example, if the normalized uniform price at bus ref is u_{ref}^p , then the uniform price at each bus k is

$$u_k^p = \left(\frac{u_{ref}^p}{\lambda_{ref}^p} \right) \lambda_k^p$$

A simple example for clarity reasons: Potential buyers submit the quantity desired and a price per unit in sealed bids. When all bids are collected, the seller gives the desired quantity to the bidder who offered the highest price, then the second highest, and so forth, until all available units are sold. All buyers pay the price per unit of the lowest bid that was awarded units. More specifically, suppose there are 1000 available units (KW) and three bidders. Bidder A offers 20 euros per unit and wants 600 units; Bidder B wants 400 units at 30 euros per unit. Finally, Bidder C wants 300 units at 35 euros per unit. Under this scenario, Bidders A and B both receive their desired units and they both pay 20 euros per unit. The proposed offered prices include the distance cost between buses.

Therefore by affecting the communication of a) a market's seller the available units may be affected, and b) a bidder can manipulate the final uniform price.

4 Experimental setup

In this section we briefly present the framework that was used for a) simulating the physical components of a smart grid and the power market, and b) emulating the cyber elements. An overview of the experimental setup is illustrated on figure 4.

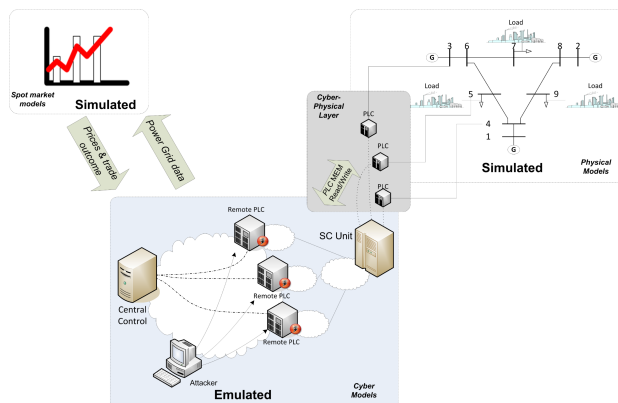


Fig. 4. The overall architecture of the simulation & emulation framework used in this work.

4.1 Network Emulation

In our laboratory we have installed an infrastructure using the Emulab [17] architecture and software, called EPIC [14]. The testbed of the NICS cyber part (SCADA servers, corporate network etc) facilitating the emulation of the ICT infrastructure is based on Emulab. We can automatically and dynamically map physical components, e.g., servers and switches, to a virtual topology and the communication channels between them. In other words, the Emulab software configures the physical topology in a way that it emulates the virtual topology as transparently as possible. This way we gain significant advantages in terms of repeatability, scalability and controllability of our experiments. Furthermore, the software configures network switches in order to recreate the virtual topology by connecting experimental nodes using multiple VLANs. Within the ICT network we used the Open Shortest Path First (OSPF) for traffic routing purposes.

A summary of experimental resources employed for the present study are:

- 3 Routers (Cisco 6503), which have four Gigabit experimental interfaces and one control interface (emulation).
- 14 virtual PCs (HP Proliant GL380p), which have Xeon(R) 4 CPUs @ 2.40GHz, 3GB RAM, two Gigabit experimental interfaces and one control interface. They were used as experimental nodes (attackers and simulated elements) and their operating system is FreeBSD8.2.
- 3 Switches(Cisco 3750G), which have 48 ports each. They were used for the communication network (emulation).

Finally, a network measurement revealed an average Round Trip Time (RTT) below 3ms. This means that the implementation exhibits the operational behavior of real communications systems where the delivery of high-speed messages must be below the maximum limit of 10ms, as stated by the IEEE 1646-2004 standard [21] on communications delays in substation automation.

4.2 Simulation Elements

The simulation elements constructed for our experimental environment are two: the physical systems (power grid) and the power/smart market system.

The main role of the simulation element (Sim) is to run the physical process model in real-time. This is done by coupling the model time to the system time in such a way to minimize the difference between the two. Models are constructed in Matlab Simulink from where the corresponding C code is generated using Matlab Real Time Workshop. These are then integrated using an XML configuration file that is flexible enough so that researchers do not need to modify the code. The generated code is then executed in real time and interacts with the real components of our emulation testbed. From a technical point of view, real-time simulation of IEEE grid models is implemented in AMICI [6], which is based on Matlab open-source libraries, i.e. MatPower [5] and MatDyn [7]. The IEEE model used for our experiments is the IEEE 9 buses, where 3 buses are the generators, 3 buses serve as connecting ones and the last three are the consumers.

The power market element is developed in Matlab simulink, as well, and is based on the principles presented in section 3.2. The communication channel with the power grid is presented in Fig. 4 and it interacts real time based on newly entered power demands from the consumers. Interaction with other simulation elements is enabled by implementing not only RPC (Remote Procedure Call) server-side operations but client-side calls as well. By using only the XML configuration file, the simulation element can be configured to read/write inputs/outputs of models run by remote ones. In our testbed, the two communicating elements via the cyber-emulated topology, are power market and power grid. Finally, the controller is based on the Matpower implemented functions.

4.3 DoS attack implementation

The DDoS attacks were implemented in the presence of an upto 100Mbit/s UDP-based background traffic, generated by either PathTest ¹ or Iperf ². We have installed these tools in all the attacker nodes.

We implemented two kind of DDoS attacks:

- the first one was going to be against specific equipment, meaning PLC or router. This is going to be implemented by bots sending large amount of network traffic (flood) to a specific IP or network interface.
- the second one was going to aim to minimize the network bandwidth between the physical equipment and the power market. Therefore there may be partial loss of communication between those entities.

The impact of the DDoS attacks was going to be expressed by measuring the Round Trip-Time (RTT). The RTT of a TCP segment is defined as the time it takes for the segment to reach the receiver and for a segment carrying the

¹ PathTest, Free Network Capacity Test tool , 2014

² Iperf: The TCP/UDP Bandwidth Measurement Tool, 2014

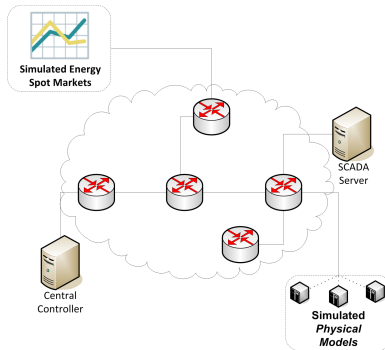


Fig. 5. The Emulab laboratory architecture for the experimental phase.

generated acknowledgment to return to the sender [22]. This technique expresses the latency of TCP communications.

To summarize this section, the important characteristics of the proposed framework are the following:

- The Matlab Simulink facilitates the integration of physical infrastructures/plants based on the a-priori known system’s analytical equations.
- The communication between the remote PLCs and the controlling units is based on the Modbus over TCP protocol. However, another protocol can be easily integrated due to the modularity provided by our implementation.
- There is a synchronization algorithm between the models execution time and the system clocks ensuring reliable exchange of data.
- The tools used for the DDoS attacks are well-established for this kind of experimentation.

5 Experimental results

In this section we evaluate the various network setups against DDoS attacks. The main scenario is that *there is an emergent need for energy from the customers. The producers (generators) place their bids and the consumers accept the offer according to the power market rules 3.2.* In all scenarios the consumers need a fixed amount of energy load, which have been already auctioned through power market (previous-day auction), but there is a sudden need for 10, 20 and 30 Mwh for each of three customers (1,2 and 3 respectively) and the bidders (3 generators) offer 30, 40 and 50 €/ MWh from generators 1 ,2 and 3 respectively (fig. 5). We attacked always bus 1, because this provides the maximum financial disturbance since generator 1 has the lowest price.

Moreover, the response strategy for the controller during a DDoS attack is the last received data/signal as a current command:

$$c(t) = \begin{cases} c^{past}(t) \in T_{DoS} \\ c^{real}(t) \notin T_{DoS} \end{cases}$$

Table 1. Topology and results against a DDoS attack

| Topology | Outcome Description | Loss (€) | RTT (msec) |
|--|--|-----------|-------------------------|
| Public PLC | No data reached the market | 10.43/MWh | 1.2×10^6 |
| <i>Public Dedicated Router</i> | Data reached the controller, but critical situations existed. The market did not received adequate information | 10.43/MWh | $max(1.22 \times 10^4)$ |
| <i>Non-Public Dedicated Router Priority policy</i> | Data reached the controller - without issue. Data not always reached the market during repeatable experiments | 10.43/MWh | $max(3.45 \times 10^2)$ |

, where $c(t)$ is the values provided to the controller, T_{DoS} is the time period of the DDoS attack, $c^{past}(t)$ is the last received value of the PLC (stack-at fault), till a new value is received by the controller, and $c^{real}(t)$ is the real time values provided to the controller.

The proposed ICT network topologies and the outcomes are depicted briefly in Table 1. We sorted our results based on the network position of the PLC:

1. Public PLC: In this scenario we have a generator’s PLC to be reachable through Internet. This mean that a DoS attack can aim directly to a PLC’s port/interface. The attack duration was 20 minutes and the PLC was not able to provide any data through this period. Having implemented an exact replica of a PLC (memory-wise), we identified that the PLC crashed after only 2 minutes because its computational resources were exhausted. The outcome was that the market and the controller were unable to receive information. So when an urgent demand for additional energy was introduced, the specific generator was not able to verify its bid. Therefore there was a loss of 10.43 €/ MWh and a large increase to the voltage, where the connecting bus 2 reached its limit.

2. Public Dedicated Router: In this scenario we have a dedicated router connecting the main elements to be reachable through Internet. This means that a DDoS attack can aim directly to the router. The attack duration was 20 minutes. The outcome was that the controller received partially some data, but the market was unable to retrieve the appropriate data from the generator. So when an urgent demand for additional energy was introduced, the specific generator was not able to verify its bid. Therefore, the requested power was bought from another generator at a higher price and there was a loss of 10.43 €/ MWh. Moreover, a large increase to the voltage of the connecting bus 4 occurred (Fig. 6).

3. Non-Public Dedicated Router: In this scenario we have a dedicated router connecting the main elements, which is not reachable through Internet, but is used to pass communication for other services, as webservice, etc . This means that a DDoS attack cannot aim directly to the router, but by attacking a specific other service the network bandwidth is going to be limited. The attack duration was 20 minutes. The outcome was that the controller received partially

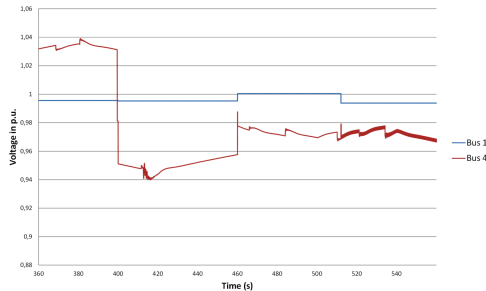


Fig. 6. The voltages (in p.u.) of buses 1 and 4, where bus 1 is under DDoS attack.

some data, meaning that there were a few voltage sudden increases but there was not a extreme situation for the specific time period. The market was unable to retrieve the appropriate data from the generator, unless there is a special router policy giving priority to specific IP ranges. So when an urgent demand for additional energy was introduced, the specific generator was not always able to verify its bid. Therefore the loss was from 0 to 10.43 €/ MWh.

6 Conclusions and Further research

In this paper we presented the financial disturbance and the affect on the voltage of a power grid due to a DDoS attack against the ICT communication system. We used a well-defined testbed in order to validate the outcome of these cyber attacks. We show that there are issues for the control schemes, which use public infrastructure due to operational costs without taking into consideration possible implications. Even though this architecture is advantageous, the stakeholders should think thoroughly how to setup their interface and use the public infrastructure.

Future work includes a more detailed analysis of the behavior of real networking devices under other attacks, such as integrity attacks, and the introduction of additional monitoring attributes, such as frequency. We intend to develop a novel approach by integrating real physical infrastructure like PLCs and renewable energy generators, such as windmills and solar systems.

References

1. S. Sridhar, A. Hahn, and M. Govindarasu, Cyber - physical system security for the electric power grid, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan 2012.
2. Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, Cyber - physical security of a smart grid infrastructure, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan 2012.
3. P. Kotzanikolaou, M. Theoharidou, D. Gritzalis, "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructures*, Vol.9, No.1-2, pp.93-110, 2013.

4. M. Theoharidou, P. Kotzanikolaou, D. Gritzalis, A multi-layer Criticality Assessment methodology based on interdependencies, *Computers & Security*, Vol.29, No.6, pp.643-658, 2010.
5. R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, Matpower: Steady-state operations, planning, and analysis tools for power systems research and education, *Power Systems*, IEEE Transactions on, vol. 26, no. 1, pp. 12-19, Feb 2011.
6. B. Genge, C. Siaterlis, M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012.
7. S. Cole and R. Belmans, Matdyn, a new matlab-based toolbox for power system dynamic simulation, *Power Systems*, IEEE Transactions on, vol.26, no.3, pp. 1129-1136, Aug 2011.
8. F. Pasqualetti, F. Dorfler, and F. Bullo, Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design, in *Decision and Control and European Control Conference (CDC-ECC)*, 2011 50th IEEE Conference on, Dec 2011, pp. 2195-2201.
9. L. Xie, Y. Mo, and B. Sinopoli, Integrity data attacks in power market operations, *Smart Grid*, IEEE Transactions on, vol.2, no.4, pp. 659-666, Dec 2011.
10. M. Esmalifalak, G. Shi, Z. Han, and L. Song, Bad data injection attack and defense in electricity market using game theory study, *Smart Grid*, IEEE Transactions on, vol.4, no.1, pp. 160-169, March 2013.
11. Y. Yan, Y. Qian, H. Sharif, and D. Tipper, A survey on smart grid communication infrastructures: Motivations, requirements and challenges, *Comm. Surveys Tutorials*, IEEE, vol.15, no.1, pp. 5-20, First 2013.
12. Jon Thompson, Martin McKeay, Bill Brenner, Richard Mller, Mathias Sintorn and Geoff Huston, "Akamai's state of the internet", Q4 2013 Report, Vol. 6, Nm.4, Prolexic Quarterly Global DDoS Attack Report.
13. L. Marinos, "ENISA Threat Landscape Report 2013", European Union Agency for Network and Information Security, December 2013 (retrieved: April 2014)
14. C. Siaterlis, A. Garcia, and B. Genge, "On the use of Emulab testbeds for scientifically rigorous experiments", *IEEE Communications Surveys and Tutorials*, vol.15, no.2, pp. 1-14, 2012.
15. Stewart Baker, Natalia Filipiak and Katrina Timlin "In the Dark Crucial Industries Confront Cyber attacks mcafee" , McAfee second annual critical infrastructure protection report , 2010 (retrieved: April 2014)
16. R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security Privacy*, IEEE, vol. 9, no. 3, pp. 49-51, May 2011.
17. B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar, An integrated experimental environment for distributed systems and networks, in *OSDI02*, pp. 255-270, Dec. 2002, .
18. European Energy Exchange AG (<http://www.eex.com/en/market-data/natural-gas/spot-market>, last retrieved May 2014)
19. Epex Spot, (<http://www.epexspot.com/en/> , last retrieved May 2014)
20. APX Power spot exchange (<http://www.apxgroup.com/> , last retrieved May 2014)
21. Institute of Electrical and Electronics Engineers, IEEE, 1646-2004 standard: communication delivery time performance requirements for electric power substation automation, 2004.
22. Aikat, J., Kaur, J., Smith, F.D., Jeffay, K.: Variability in TCP Round-Trip Times. *Proc. of the 3rd ACM SIGCOMM on Internet Measurement Conference*, pp. 279-284, 2003.