Network Security Monitoring in a Small-Scale Smart-Grid Laboratory

Matti Mantere, Sami Noponen, Pia Olli, Jarno Salonen
VTT Technical Research Centre of Finland
Email: firstname.lastname@vtt.fi

***Abstract*—Smart grids are the next generation of electrical grids, enabling the better management and leveling of power consumption by suppliers. Via the use of automatic meter reading, smart grid also provides better information to the end-users, making it possible to enhance their energy consumption and adapt it according to the current energy price, availability and other factors. As the grid becomes more and more reliant to ICT and communication networks, risks related to cybersecurity and privacy have to be taken into account. The link between automatic meters and the distribution operator has to be protected from security breaches that may lead to false billing and the transferred data has to be protected as it contains sensitive information about household and business behavior. In this article we present a limited state-of-the-art review as well as a network security monitoring setup for small-scale laboratory that is in essence a small scale smart grid environment. We discuss about the challenges and threats that are possible in the smart grid environment and the feasibility of using network security monitoring techniques that represent our work-in-progress research in this context.**

I. Introduction

The broad topic of this paper is the smart grid (SG) cybersecurity. It is an extremely important issue for several reasons. Vulnerabilities and weaknesses in this part of the national critical infrastructures (CI) can have serious consequences if exploited. The forms of exploitation possibilities are numerous. Among them are acts by those seeking economic gains, and by those trying to impress their peers or to cause distress for political ends as in the case of terrorism. [31]

The term smart grid is used in this work to describe the overall evolving electrical grid which is incorporating increasing amount of intelligene and number of communications and control equipment spanning over wide areas connected through different network solutions. Smart grid is a combination of several technologies with interdependencies spanning over various other critical infrastructures. The entwined nature of different infrastructures provides a wide selection of attack surfaces. A particular CI can be attacked by attacking another CI on which it depends. As the potential attacker can select any of these infrastructures with dependencies, any particular CI is only as strong as the most weakly protected CI on which it depends on.

Protecting the smart grid itself therefore requires the protection of all the CI's it depends on as well as hardening the grid itself. In this paper we provide a review on the current state of cybersecurity research concerning smart grids. A good number of studies and reviews have been published on the matter and research is moving forward; the most important ones will be presented in Section II.

Finland is a nation with highly advanced technology sector. The deployment of electrical grid with smart grid components, such as remote metering, is well under way. The correct implementation of cybersecurity mechanisms, safeguards, and preventative actions is a paramount to the preservation of national security and critical services of the society. At the VTT Technical Research Centre of Finland Oulu premises a miniature smart grid test laboratory has been developed and deployed. In this paper we investigate the possibilities of network security monitoring of smart grid communication in the context of this smart grid test lab. We use the term industrial control system (ICS) as an umbrella term which includes supervisory control and data acquisition (SCADA) systems.

The physical protection of various smart grid components that are critical to the grid security is not in the scope of this paper. The physical security will be discussed in a more abstract manner, mostly concerning the physical access to various components. The physical security of the various smart grid components is also a very mature engineering subject.

Monitoring the control and communication of the various industrial control system components and human-machine interfaces for security critical deviations requires specialized equipment. Commercial off-the-shelf (COTS) monitoring systems, such as the various intrusion detection systems (IDS) and their like rarely include support for the various protocols used. This is not always the case, as for example the Bro Network Security Monitoring system (Bro NSM) [32] currently includes support for distributed network protocol (DNP3) over transmission control protocol (TCP) [24] and Modbus over TCP.

This paper presents work-in-progress and is intended as the introduction of our current efforts to implement new cybersecurity monitoring approaches for a smart grid environment. The paper is divided into the separate sections as follows: We begin by presenting a review of the current cybersecurity situation of smart grids, along with privacy concerns related to them and the relevant standardization. Then we describe the smart grid laboratory setup used in our research for network security monitoring and discuss about the differences to the real smart grid environment. We also discuss about the network statistics collected during the recording and analysis phase as well as the monitoring challenges and possibilities that

978-1-4799-4223-7/14 $31.00 © 2014 IEEE
DOI 10.1109/ARES.2014.48

the laboratory setup enables for network security monitoring research.

II. Background and Related Work

In this section we present a brief review of the current cybersecurity and privacy situation concerning smart grids and the relevant standardization.

Smart grids are a combination of various different technologies but all include some form of ICS equipment communicating over Internet or some other channel. Usage of commercial-off-the-shelf systems is also bringing the same issues to the SG environment that are present in consumer environments. [17]

Smart grids are also geographically distributed to a wide extent. The power generation within the grid can also be distributed to the end-users who might also themselves be feeding electricity back to the grid. This functionality requires the metering infrastructure to support the small scale producer's activities. This requirement on smart meters for the measurement, reporting, and adaptation for the user-producers contribution requires caution, as it increases the surface-area of the attack plane.

A number of cybersecurity solutions have been proposed, such as the work presented in the paper [28] leveraging public key infrastructure (PKI). Cybersecurity is seen as a critical component of the overall SG structure, with requirements to build it in, rather than add it as an afterthought [29]. Documents such as [1] also strive to describe the cybersecurity requirements concerning SG architectures and overall strategy. However, there is currently no comprehensive cybersecurity solution that would have been implemented to an actual deployed smart grid environment. The insufficient built-in cybersecurity exacerbates the situation for all the CI's dependant on the electricity supply, and provides a weak point in the national security posture for potential exploitation [31].

A. Smart Grid Vulnerabilities

Smart grid depends on a complex network of computers, software, and communication interfaces. All complex systems have vulnerabilities and problems, and smart grid is no exception. Intelligent attacker has potential to cause great damage such as prolonged blackouts through the electricity grid [1]. Each communication path provides a potential attack path, and especially wireless communication is relatively easily disturbed. Several challenges and vulnerabilities will arise with the integration of cyber and physical systems [19].

1) Automatic Meter Reading: Automatic meter reading (AMR) refers to automatic gathering of electricity consumption data through varying communication networks. This requires new smart meters to be installed to the customers. Smart meters are increasingly being rolled out accross the world. Billing can be based on near real-time consumption rather than on estimates based on past or predicted consumption. AMR also provides a two-way communication channel between the consumer's electricity meter and the utility company. AMR brings the following cybersecurity challenges that are possible attack vectors or threats to the SG:

1) Utility can remotely shut off users
2) Wireless security/vulnerabilities
3) Authentication vulnerabilities
4) Over the air firmware updates to smart meters
5) Customer data and electricity consumption data is stored in various systems and shared between several companies

The smart metering systems are usually run as business networks by Distribution System Operators (DSO). The DSO is legally responsible for provision of customer usage data, managed in the subsequent refining steps by the DSO or the providers of energy market services. The data, initiating in the smart meter, is first transferred via mobile operator's network into the head-end system of the advanced metering infrastructure (AMI), and on into other information systems. The data is processed, stored, refined, combined with other data like customer and invoicing data and eventually delivered to the given market participants. The cybersecurity challenge originates in the variety of stakeholders, roles, and interfaces. The cybersecurity management and requirement implementation practices vary among the parties. Security in collaboration is thus hard to manage, and if one party fails, everybody has to bear the consequences. The interfaces are challenging also at the technical level; with a variety of interfaces, proprietary communication protocols and several versions complicating security analysis and remedies.

2) Industrial Control Systems: Industrial Control Systems are widely used in Smart Grid by electric utilities. ICS and SCADA cybersecurity has gained increasing attention in the recent years, especially after the Stuxnet case [23]. ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) has responded to over 200 incidents across all critical infrastructure sectors in the first half year of 2013 in U.S. The highest percentage of incidents reported to ICS-CERT occurred in the energy sector at 53% [12].

Project Shine [22] have collected over 1 million IP-addresses from ICS-related devices worldwide with their SHODAN-search engine and 2000-8000 devices are added daily. Large portions of the findings are not related to Smart Grid, but the project has revealed serious ICS cybersecurity issues in several countries.

3) Substations: Substations are basically a link between a power plant and the customer. Substations contain transmission and circuit breakers, power transformers, phase-shifting transformers, capacitor banks and disconnect switches. The level of automation in substations is increasing, and the level of automation is related to cybersecurity. Substations are generally controlled with ICS, but they can be also controlled with local wired or wireless connection [4].

B. Privacy Concerns

As the amount of data collected by smart meters increases, privacy of the so-called consumer-specific energy-usage data (CEUD) raises privacy implications that should be acknowledged. This is because the data may disclose detailed information about the activities and behaviour of a specific household that can be used for wrongful and even unlawful purposes. Khurana et al. state that electricity use patterns not only disclose how much energy a household uses, but also information about the household appliance types, home area or AMR network and even information about people being at home or at work may be detected [19]. This information may support criminal targeting of homes by someone who has access to this information either via the smart grid operator or using a man-in-the-middle attack. The benefit of using smart meter data versus maintaining privacy of the customer is one of the key issues of smart grid future. Among others Sankar et al. introduce the term "Competitive Privacy" stating that among regional transmission organisations there is a trade-off between sharing data for network reliability reasons and withholding data to ensure profitability and privacy [35]. This aforementioned privacy issue not only concerns individual homes, but information about electricity use patterns and their changes, for example increases in power draw for a company, might be valuable business intelligence information for competitors [19]. While new services are being developed for the smart grid that can e.g., detect the breakdown of a household device in advance based on its electronic signature change, this development enables a better detection of specific behaviour regarding energy consumption that might violate the privacy of the individual.

NIST defines privacy into four dimensions:

1) Privacy of personal information
2) Privacy of the person
3) Privacy of personal behaviour
4) Privacy of personal communications

According to NIST, most smart grid entities address the first dimension, based on the fact that most regulations and data protection laws cover privacy of personal information. However the other three dimensions should also be considered in the smart grid context, based on the new possibilities of smart grid data collection that enable for example the recognition of unique electronic signals at home or reveal the electronic vehicle charging station location information. Other examples of sensitive information potentially available through the smart grid are billing history (including late payments and failures to pay), name of the account holder, location of the household, usage patterns as well as the almost real-time meter reading that may be updated in less than 60 minute intervals. [2]

Another group, the Smart Grid Coordination Group consisting of members from the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI) define two levels of relevant data related to privacy; first of all personal data that means any information relating to an identified or identifiable natural person and sensitive data that consists among others of the origin, political, religious or philosophical views of a specific person. The group divides smart meter data into two categories; system information that includes revenue metering data, audit and log information, control signals etc. and personal information that can be either sensitive or non-sensitive, but may also consist of de-personalised information. [13]

Some potential smart grid privacy concerns described by NIST are:

1) Fraud e.g., by attributing energy consumption to another location or vehicle
2) Determination of personal behaviour patterns and personal household devices
3) Real-time remote surveillance
4) Non-grid commercial use of data by selling it to vendors or other organisations interested in the information

While many of the parties that are interested in using the smart grid data are legitimate, they should be aware of uses that impact privacy despite the benefit. For example insurance companies might be interested in their customers' sleeping behaviour and take into account the detection of erratic sleep that might indicate health problems. As another example law enforcement might be interested in identifying suspicious or illegal activities or even real-time surveillance of the target household through the grid data. [2] Probably due to these kinds of unclarified privacy concerns, the First Chamber in the Netherlands rejected two smart metering bills in 2009 that delayed the large-scale introduction of smart metering [16].

C. *Cyber Security and Standardization*

Smart grids are getting more and more involved with the IT and telecommunications sectors. Those sectors already have standards for cybersecurity to help with identifying vulnerabilities in the systems. However, those standards need to be assessed with the specific smart grid requirements, and also new, smart grid specific standards need to be developed. Smart grids are complex, highly time-sensitive systems that have several stakeholders; cybersecurity needs to be applied appropriately to ensure the privacy of customer information and the reliability of the smart grid. By developing and applying standards, the performance and interoperability of the systems is enhanced. [1], [9]

There are several standardisation bodies that are developing standards for smart grids at the moment. CEN, CENELEC and ETSI are examples of bodies that are developing standards for Europe [10], whereas NIST, ANSI and NERC, for example, are American standardisation associations. The same standards, concerning smart grid cybersecurity, are not directly applicable all around the world, because smart grids in Europe are not completely similar to those in US, for example. In Europe, energy theft and privacy are seen as the most important safety aspects of the smart grids, whereas in US malicious attacks raise more concern than privacy [6]. This is why NIST guidelines cannot be directly applied in Europe [10]. Despite of strong US focus on NIST publications, one of their target is to enhance the international interoperability [9]. An important publication in the US is the NIST Roadmap for Smart Grid Interoperability Standards, which highlights cybersecurity challenges to US authorities. There are not yet similar publications in Europe [33].

In 2011 Pearson stated in his article [33] that US seems to be ahead of Europe by most parts with smart grid cybersecurity. In the same year European Commission has given a mandate to European Standardisation Organisations to speed up the development of European standards for smart grids. Based on that mandate, CEN-CENELEC-ETSI Smart Grid Coordination Group has released a publication *First Set of Standards* in November 2012 [7], and a publication *Smart Grid Information Security* at the same time [8]. It is stated in the document [8] that the lack of a standard reference for the basic architecture of the smart grid itself has made it impossible to create a pervasive cybersecurity standards for smart grids. As the European smart grids are getting more and more interconnected, it is required to have similar cybersecurity standards between the connected stakeholders. Although a first document has been published, they want to highlight that creating and maintaining these standards cannot be done at once, but it requires a continuous effort. Therefore the standardisation work has continued strongly in Europe even after the mandate, and in 2013 an European project STARGRID has published its own report about the state of the smart grid standardisation both in Europe and International level [11]. It contains also some new and updated cybersecurity specific standards that have been released after CEN-CENELEC-ETSI's publications.

The lack of the standard definition of smart grid itself has also an impact on the smart grid specific standards defined in the NIST publication and by CEN-CENELEC-ETSI. NIST has defined a cybersecurity standard for AMIs, whereas CEN-CENELEC-ETSI has left AMIs out of the scope, at least in this first version. Otherwise CEN-CENELEC-ETSI's list of standards is more wide than NIST's. They both have defined the publication: *IEC 62351 parts 1-8, Power System Control and Associated Communications – Data and Communication Security*, as the first standard [5], [7]. Another mutual standard is *IEEE 1686, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*. Generally the standards defined by NIST are more extensive publications, like *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security* and *Cyber Security Procurement Language for Control Systems by Department of Homeland Security*, whereas CEN-CENELEC-ETSI have used those only as a base when creating their list of standards, and therefore defines more specific standards, like *IETFRFC 2617,HTTP Authentication: Basic and Digest Access Authentication* and *ETSI TR 102 419, Security analysis of IPv6 application in telecommunications standards*. However, these aforementioned standards are only a beginning, and it is expected that it requires hundreds of standards to build a safe, secure, and interoperable smart grid [5].

In Finland the responsible body of smart grid standardisation is called SESKO. It acts in the field of electrotechnical standards, and its mission is to act as a Finnish representative in the international standardisation body IEC and in CENELEC, and create national SFS-standards based on the results of those standardisation bodies. SESKO does not have any SFS-standards for smart grids at the moment, but it offers links to IEC's smart grid standards and to CENELEC's smart grid portal. [3]

III. Monitoring the Smart Grid Laboratory

Monitoring all of the portions of smart grid infrastructure needs to have a very high priority when security of the grid is desired. This monitoring requirement is needed to construct and upkeep a proper situational awareness. [21]. This paper discusses the monitoring of the network traffic of the smart grids and one laboratory environment particularly, but monitoring all the aspects of the smart grid is important for the bigger picture.

Monitoring the security state of data communications networks of smart grid systems has similar properties as monitoring the data communications of other ICS rich networks. Smart grid systems include various ICS equipment but they also include, for example, the end-user interfaces, that expand the surface area of the attack plane of the system. As the end-user will have the factual physical possession of the smart-meter portion of the infrastructure, additional caution must be exercised that the to-and-from communication channel cannot be penetrated.

Monitoring the end-user portion of the smart grid infrastructure would require sensors placed in either the end-user's smart-meter, between the server and the meter, or at the server. Adding monitoring capability to the smart-meter itself, would suffer from the fact that the monitoring sensor itself would then be in the hands of the same end-user, who might tamper with the sensor itself.

Depending on the network security monitoring sensor location, very different monitoring schemes might be required. Inside the communication network of the control traffic of the infrastructure, the ICS specific approaches can be used. For the parts of the environment that are facing Internet or are in user control and not directly communicating with the ICS equipment, these same methods are not feasible, or optimal.

The laboratory environment used as our monitoring case is of a limited scale. It is a realistic environment incorporating many of the systems that can be found in actual smart grid environments. The main components of the site are a wind mill, solar energy panels, power inverter and energy storage. The laboratory is VTT's renewable energy test site, that is used as a research environment. The energy produced with wind and solar power is used to power an apartment located at the VTT's premises. Energy production and consumption data are measured and stored in a database within the network. The test site is a good example of a distributed energy resources, local production in urban areas. A simplified diagram of the smart grid laboratory is depicted in Figure 2. All of the equipment and the apartment are located in the same building.

A. Network statistics

Initial analysis was made to 17 days of recodred network traffic from the smart grid environment. The traffic

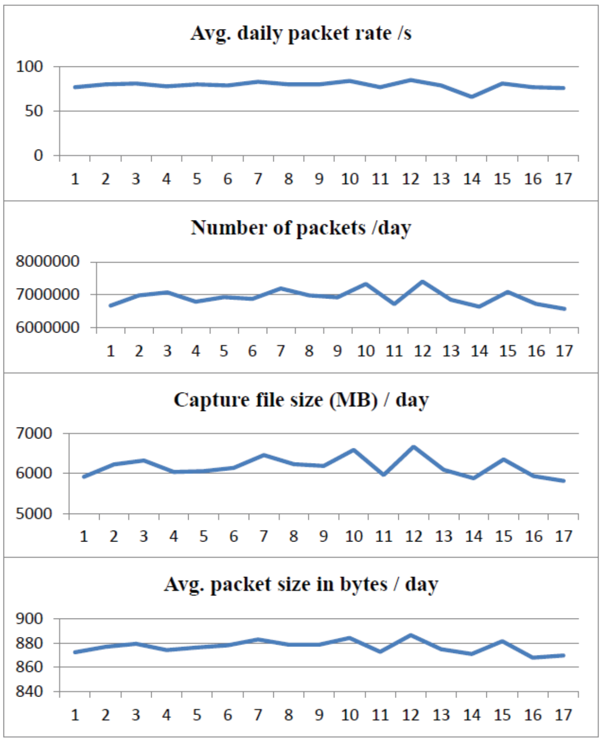

Fig. 1. Network traffic statistics

was recoded into daily captures files with tcpdump [37] and analysed with Wireshark [38]. The packet rate is between 0-20 packets/second most of the time. Exceptions to the previous are regular hourly bursts of 5000 packets and a 20 minute period at nighttime when several (4-5-gb/day so far) gigabytes of data is transferred regularly. The number of unique IP and MAC addresses remains at 11 during the analysis period. Contents of malformed packets and protocols such as NFS and RPC was not dissected. Most of the traffic - 80-90% of packets - is between just two hosts and covers over 99% of all data bytes. All of the traffic runs on IPv4, and 99% on TCP. The following protocols were found in the captures, not counting the lower level network protocols present:

1) Remote Procedure Call (RPC)
2) Network File System (NFS)
3) Used Datagram Protocol (UDP)
4) Netbios Datagram Service
5) Domain Name Service (DNS)
6) Internet Control Message protocol (ICMP)
7) Address Resolution Protocol (ARP)
8) Network Time Protocol (NTP)

The traffic remains relatively stable as seen as on daily analysis in Figure 1, in which the daily packet rate, daily packet count, capture file size and average packet size are visualized.

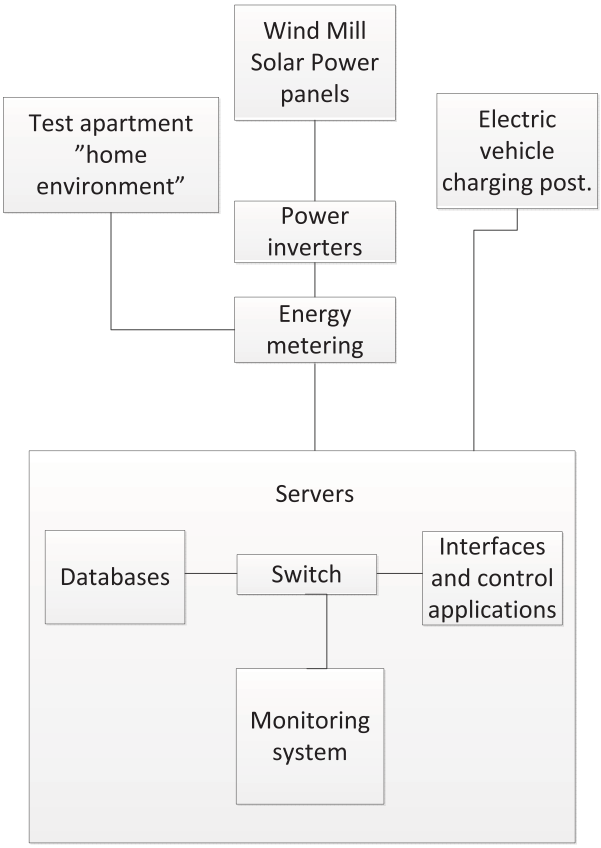

Fig. 2. Simplified diagram of the smart grid laboratory setup

TABLE I
STATISTICS OVER 17 DAY PERIOD

No.	pcap size	Uni. MAC's	Uni. IP's	Packets	avg. packet size	avg. packet rate
1	5921MB	11	11	6665K	872B	77
2	6228MB	11	11	6977K	877B	80
3	6327MB	11	11	7068K	879B	81
4	6038MB	11	11	6783K	874B	78
5	6064MB	11	11	6920K	876B	80
6	6143MB	11	11	6872K	878B	79
7	6462MB	11	11	7189K	883B	83
8	6238MB	11	11	6973K	878B	80
9	6190MB	11	11	6919K	878B	80
10	6594MB	11	11	7326K	884B	84
11	5966MB	11	11	6713K	873B	77
12	6675MB	11	11	7397K	886B	85
13	6097MB	11	11	6843K	874B	79
14	5880MB	11	11	6629K	871B	66
15	6356MB	11	11	7082K	881B	81
16	5938MB	11	11	6717K	868B	77
17	5816MB	11	11	6566K	870B	76

B. Monitoring possibilities

Monitoring setup consists of a server equipped with several network interfaces and running a FreeBSD 10.0. We capture the network traffic in two points through switch monitoring ports. This allows us to see the network traffic coming from the Internet and traffic moving inside the test network.

The network of the smart grid laboratory is in effect an ICS network. ICS networks that are correctly deployed and configured typically exhibit predictable attributes, and therefore can be monitored using slightly different approaches than traditional and more open networks [20], [26], [25]. The statistics presented in the Section III-A including the Figure 1 and Table I support an assumption that the traffic is quite stable at least over the period time monitored and investigated so far.

An example of network security monitoring in an environment such as this, is to use machine learning based anomaly detection. Such systems and their feasibility are investigated in several papers such as [30], [34], [18] to provide few examples. Challenges of machine learning systems are discussed in length in paper [36]. As the smart grid network is in effect an ICS network, all the typical solutions suitable for ICS networks would logically be feasible to some extent in them as well. Naturally some differences can occur and special cases might arise.

One of the many reasons for this presentation of the monitoring setup in this laboratory is the intended testing of our machine learning anomaly detection solution under development [27]. The network exhibits all the required attributes, such as predictability and static and restricted nature to a degree. Anomaly detection has been noted as appearing feasible for use in ICS networks, e.g., in [20].

A challenge with constant monitoring is the amount of network traffic [15]. High volume network captures will quickly fill hard drives. The high network throughput is also a challenge if computationally expensive monitoring techniques would be used. Even the experimental small scale laboratory environment monitored has a relatively high traffic throughput. This places demands on the performance of the monitoring equipment used. For computationally demanding monitoring approaches the high volume throughput might result in a situation where the traffic cannot be processed in real-time.

Machine learning based anomaly detection can be especially resource intensive if complicated algorithms are used. The available computing power dictates what type of an algorithm could be used and in what way. Handling every single packet using a system such as Bro [32] on which our own implementation is based, is already a resource intensive task. If such already intensive events are further handled using machine learning algorithms the issue is further excacerbated.

Figure 2 displays the monitoring location in the laboratory environment. The monitoring server is connected to the monitoring port of the switches. It is noteworthy that not all of the traffic inside the network is being captured. For example the traffic flowing between the energy metering and the test apartment is not visible from our monitoring location. However, all the traffic coming and going to the servers in the laboratory is being monitored.

Because all of the traffic coming and going to the servers is captured at the switches from their monitoring ports the setup is very unobtrusive. No changes to the laboratory systems or disconnects were needed. This would not be the case if network taps were to be used. Due to this unobtrusiveness the monitoring setup could be scaled to larger environments without much more difficulties. The main reasons for the monitoring system placement are listed in Table II.

TABLE II
REASONS FOR THE MONITORING PLACEMENT

1) No need to change network structure
2) No need to disconnect any devices
3) No added failure points
4) Good traffic visibility
5) Scalable

There are also downsides for this sensor placement. One of the important ones is the fact that we are now relying on the monitoring port functionality of the switches. The monitoring ports do not replicate everything, and under heavy loads there might be package drops [15]. Authors of [39] also note that using monitoring ports can cause timing differences and packet reordering in addition to packet loss. Some of the identified downsides of the sensor placement are listed in Table III.

TABLE III
DOWNSIDES OF THE MONITORING SETUP

1) Switch monitoring port issues: timing, reordering and packet loss
2) Everything is not captured
3) Attacks are seen only as they are already happening

An interesting issue presented in [14] is the absence of diurnal usage patterns in SCADA networks of water treatmet facilities. Whether this is true for smart grids is a interesting question that needs to be investigated. Electricity usage tends to vary according to the time of the day, and it is possible that diurnal or nocturnal usage patterns are present.

IV. DISCUSSION AND CONCLUSIONS

This paper represents the initial step in testing new methods and systems for a smart grid environment. The aim was to introduce the testing environment and context and further to investigate whether it will be suitable for testing the network security monitoring solutions. One such solution that will be investigated will be machine learning based anomaly detection systems.

The work presented is still very much work-in-progress and thus incomplete. However, it was deemed that publishing a separate work-in-progress paper on the setup and the possibilities before further investigations was mandated. We presented a review on different aspects of smart grid security, that provides a reasoning for our research. Currently, very much effort is put into enhancing the cybersecurity of smart grid through standardisation and research worldwide, but this work is still far from complete. Our approach to enhancing smart grid cybersecurity is through developing methods for network security monitoring in smart grid environments.

Smart grid environments require considerable monitoring arsenal to be deployed, including host based and network based solutions. However, these techniques are not yet commonly in use, and the smart grids are already partially in operation phase. [21]

The laboratory environment is suitable for testing a number of various monitoring techniques. Our initial work will be mainly targeted at the passive network monitoring based research, but we intend to investigate other venues as well. The laboratory environment and the network traffic also appear to conform to the expectations that using machine learning anomaly detection solutions would be feasible for use in smart grid control networks. The issues of the machine learning based anomaly detection and intrusion detection as presented in [36] are duly noted. However many of the issues are not present in ICS or smart grid network, or are at least significantly ameliorated. The possible temporal variances caused by changing electricity usage patterns can still produce additional challenges when compared to factory ICS network environment.

REFERENCES

[1] National Institute of Standards and Technologies. NISTIR 7628: Guidelines for smart grid cyber security: Vol. 1, Smart grid cyber security strategy, architecture, and high-level requirements. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

[2] National Institute of Standards and Technologies. NISTIR 7628: Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[3] SESKO. Älykkäisiin sähköverkkoihin liittyvä standardisointi. http://www.sesko.fi/portal/fi/standardeja_ja_direktiiveja/smart_grid/. Accessed on 20.1.2014.

[4] Idaho National Laboratory. National SCADA test bed substation automation evaluation report, 2009. http://www.inl.gov/technicalpublications/Documents/4374057.pdf.

[5] National Institute of Standards and Technology. NIST framework and roadmap for smart grid interoperability standards, 2010. http://www.nist.gov/public_affairs/releases/upload/smartgrid_ interoperability_final.pdf. Accessed on 18.12.2013.

[6] European Commission, Smart Grids Task Force. Regulatory recommendations for data safety, data handling and data protection, 2011. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2 .pdf. Accessed on 18.12.2013.

[7] CEN-CENELEC-ETSI Smart Grid Coordination Group. first set of standards, 2012. ftp://ftp.cen.eu/EN/EuropeanStandardization/ HotTopics/SmartGrids/First

[8] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart grid information security, 2012. http://ec.europa.eu/energy/gas_electricity/ smartgrids/doc/xpert_group1_security.pdf. Accessed on 20.1.2014.

[9] CLEEN Oy. Smart grid standardization analysis, 2012. http://www.cleen.fi/en/SitePages/publicdeliverables.aspx?fileId=1031&webpartid=g_1449a1fa_9f05_4750_900e_6294262dcbd4. Accessed on 21.1.2014.

[10] European Network and Information Security Agency, ENISA. Smart grid security: Recommendations for Europe and member states: Annex III. Survey and interview analysis, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/survey-and-interview-analysis.

[11] STARGRID.eu. Smart grid standardization documentation map, 2013. http://stargrid.eu/downloads/2013/11/STARGRID_WP2_D2.1_ v1.3_20131108.pdf. Accessed on 27.1.2014.

[12] ICS-CERT Monitor, (accessed 1/2/2014). http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf.

[13] Smart Grid Information Security, (accessed 23/1/2014). http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert _group1_security.pdf.

[14] R. Barbosa, R. Sadre, and A. Pras. Difficulties in modeling scada traffic: A comparative analysis. In N. Taft and F. Ricciato, editors, *Passive and Active Measurement*, volume 7192 of *Lecture Notes in Computer Science*, pages 126–135. Springer Berlin Heidelberg, 2012.

[15] R. Bejtlich. *The Tao Of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley Professional, 2004.

[16] C. Cuijpers and B.-J. Koops. Smart metering and privacy in europe: Lessons from the dutch case. In S. Gutwirth, R. Leenes, P. D. Hert, and Y. Poullet, editors, *European Data Protection*, pages 269–293. Springer, 2013.

[17] G. Ericsson. Cyber security and power system communication x2014;essential parts of a smart grid infrastructure. *Power Delivery, IEEE Transactions on*, 25(3):1501–1507, 2010.

[18] U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis. Network anomaly detection with the restricted boltzmann machine. *Neurocomputing*, 122(0):13 – 23, 2013. Advances in cognitive and ubiquitous computing.

[19] H. Khurana, M. Hadley, N. Lu, and D. Frincke. Smart-grid security issues. *Security Privacy, IEEE*, 8(1):81–85, 2010.

[20] E. Knapp. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier Science, 2011.

[21] E. Knapp and R. Samani. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Elsevier Science, 2013.

[22] I. N. Laboratory. Project shine shodan search engine.

[23] R. Langner. *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*. Momentum Press, 2011.

[24] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer. Adapting bro into scada: building a specification-based intrusion detection system for the dnp3 protocol. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, pages 5:1–5:4, New York, NY, USA, 2013. ACM.

[25] M. Mantere, M. Sailio, and S. Noponen. Network traffic features for anomaly detection in specific industrial control system network. *Future Internet*, 5(4):460–473, 2013.

[26] M. Mantere, I. Uusitalo, M. Sailio, and S. Noponen. Challenges of machine learning based monitoring for industrial control system networks. In *2012 26th International Conference on Advanced Information Networking and Applications Workshops*, march 2012.

[27] M. Mantere, I. Uusitalo, M. Sailio, and S. Noponen. A module for anomaly detection in ics networks. In *2014 3rd ACM International Conference on High Confidence Networked Systems*, april 2014. Accepted for publication.

[28] A. Metke and R. Ekl. Security technology for smart grid networks. *Smart Grid, IEEE Transactions on*, 1(1):99–107, 2010.

[29] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. *Smart Grid, IEEE Transactions on*, 1(1):57–64, 2010.

[30] S. Mukkamala, G. Janoski, and A. Sung. Intrusion detection using neural networks and support vector machines. In *Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on*, volume 2, pages 1702–1707, 2002.

[31] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. Scada security in the light of cyber-warfare. *Computers & Security*, 31(4):418 – 436, 2012.

[32] V. Paxson. Bro: a system for detecting network intruders in real-time. *Computer Networks*, 31(23-24):2435 – 2463, 1999.

[33] I. L. Pearson. Smart grid cyber security for europe. *Energy Policy*, 39(9):5211 – 5218, 2011.

[34] M. Ramadas, S. Ostermann, and B. Tjaden. Detecting anomalous network traffic with self-organizing maps. In *In Proceedings of the Sixth International Symposium on Recent Advances in Intrusion Detection, LNCS*, pages 36–54. Springer Verlag, 2003.

[35] L. Sankar, S. Kar, R. Tandon, and H. V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. *CoRR*, abs/1108.2237, 2011.

[36] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 305 –316, may 2010.

[37] Tcpdump. *[Online] http://www.tcpdump.org/*. Accessed 26/02/2014.

[38] Wireshark. *[Online] http://www.wireshark.org/*. Accessed 26/02/2014.

[39] J. Zhang and A. Moore. Traffic trace artifacts due to monitoring via port mirroring. In *End-to-End Monitoring Techniques and Services, 2007. E2EMON '07. Workshop on*, pages 1–8, Yearly 2007.