Gap Analysis of Intrusion Detection in Smart Grids

Kush, Nishchal and Foo, Ernest and Ahmed, Ejaz and Ahmed, Irfan and Clark, Andrew
Information Security Institute, Queensland University of Technology
{n.kush, e.foo, e.ahmed, irfan.ahmed, a.clark}@qut.edu.au

Abstract

Given the recent emergence of the smart grid and smart grid related technologies, their security is a prime concern. Intrusion detection provides a second line of defense. However, conventional intrusion detection systems (IDSs) are unable to adequately address the unique requirements of the smart grid. This paper presents a gap analysis of contemporary IDSs from a smart grid perspective. This paper highlights the lack of adequate intrusion detection within the smart grid and discusses the limitations of current IDSs approaches. The gap analysis identifies current IDSs as being unsuited to smart grid application without significant changes to address smart grid specific requirements.

Keywords: *smart grid, intrusion detection*

1 Introduction

The smart grid is the integration of modern information and communication technology (ICT) technology to supervisory control and data acquisition (SCADA) networks. It uses digital data communication to enhance the delivery of electricity to consumers. Due to increasing demand for interoperability and cost reductions, conventional hardware, commercial–off–the–shelf (COTS) software, and open communication standards are increasingly being utilised in the smart grid. Therefore they are more susceptible to attacks.

intrusion detection systems (IDSs) used in conventional networks cannot be readily deployed on the smart grid and SCADA networks for a variety of technical and operational reasons (Lauf, Peters, & Robinson, 2010; Zhu & Sastry, 2010). This paper presents the gap analysis of intrusion detection in smart grids. This work is closely related to the research conducted by Zhu and Sastry (Zhu & Sastry, 2010). The latter focuses on IDSs for SCADA networks, whereas this research focuses on IDSs for smart grid environments. This paper contributes by;

1. Identifying and presenting the key functional requirements of smart grid environments based on its key characteristics and attributes.
2. Investigating and presenting a survey of existing intrusion detection methods and techniques for smart grids.
3. Evaluating and presenting results of the existing intrusion detection solutions against the key functional requirements identified.

The structure of the remainder of this paper is as follows: Section 3 identifies and summarises the characteristics of the smart grid network. The key functional requirements are described in Section 4. Section 5 describes the related work in existing intrusion detection techniques in the supply–side and demand–side networks. The research identified in the related work section are then compared and discussed in Section 6, and finally a conclusion is presented in Section 7.

2 Smart Grids

The smart grid is an integration of the traditional electrical power network to modern ICTs. The objective of this integration is to yield a system capable of self–healing and self–organising. The latter is intended to provide higher efficiency and resilience to aging critical infrastructure. The smart grid integrates the *physical* electrical SCADA network components with the logical *cyber* ICTs.

To achieve additional benefits from electrical SCADA networks, there has been a recent trend towards integrating electrical SCADA networks to corporate and enterprise networks. To better facilitate data communications, modern ICT technology is adapted. This has given rise to the concept of a *smart grid*. The traditional electrical power grid is composed of three primary electrical networks: the generation, transmission and distribution networks. However the smart grid network is intended to extend the electrical distribution network to include the *home area network (HAN)* (Fabro, Roxey, & Assante, 2010). The HAN is comprised of smart meters and smart appliances. Thus the smart grid merges the *supply–side* and *demand–side* electrical networks. A high level overview of the modern electricity networks is presented in Figure 1 below.

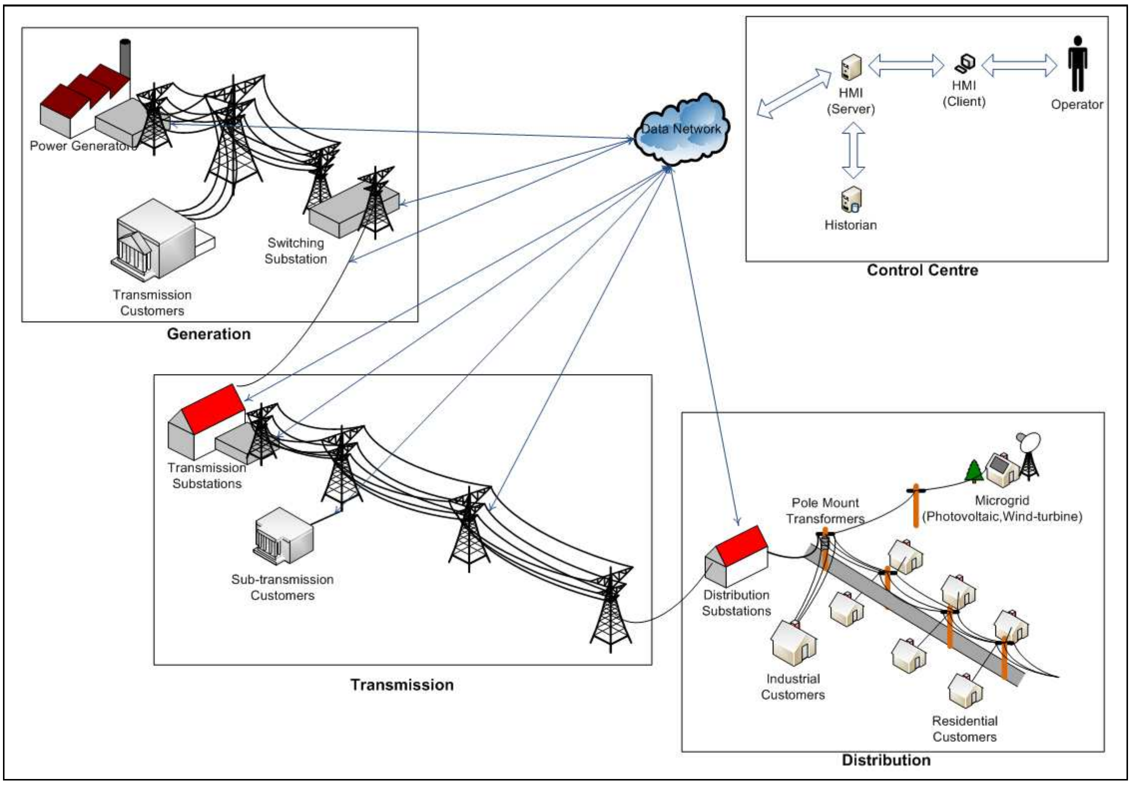

Figure 1: High-level overview of the modern electricity network.

Although there are several definitions for smart grid (Reed, Philip, & Ansel Barchowsky, Christopher J. Lippert, 2010; Aggarwal, Kunta, & Verma, 2010) driven by multiple stake holders, the overall objectives of the conceptual smart grid are often identical (Aggarwal et al., 2010; Hassan & Radman, 2010; Momoh, 2009; Cohen, 2010). These objectives are intended to provide benefits such as;

1. Greater efficiency in production and consumption
2. Higher resistance to disturbances
3. Better recovery capabilities from disturbances
4. Better control of electrical consumption in distribution networks
5. Higher quality of electrical power production
6. Integration of micro-grids for distributed generation

7. Increase network observability

The expected benefits and objectives of the smart grid described above provide a basis for the characteristics and attributes of the smart grid. Such characteristics are discussed in detail in the following section.

3 Characteristics

In an effort to identify the key functional requirements of an IDS for smart grid environments, it is essential to first characterise the attributes and behaviour of the environment within which the IDS is to be deployed. The identification of the characteristics is essential to establish exactly how SCADA networks are different from smart grid environments. Such a distinction is essential for the effective detection of incidents.

C1 – Legacy Communication Protocols Although the smart grid is the adaptation of modern ICT to traditional SCADA technology. A large aspect of traditional SCADA design remains, i.e. legacy communication protocols would lack security in terms of confidentiality, authentication and non-repudiation. With the introduction of smart grid and digital communication the security goals of *confidentiality, integrity, availability, authentication and non-repudiation* must be addressed.

C2 – Scale of Network An obvious attribute of the smart grid is the scale of the smart grid network. Conventional corporate and enterprise networks may have thousands of network nodes, however the smart grid network is composed of potentially "tens of billions" (Cohen, 2010) of network nodes. With HAN; smart meters; smart appliances and electric vehicles integrating to extend the distribution network as part of the smart grid.

C3 – Resource Constraints Unlike conventional network nodes, smart grid nodes may be severely resource constrained. Devices would perform specific low level functionality or have customised firmware. In addition to traditional SCADA nodes e.g. intelligent electronic devices (IEDs), programmable logic controllers (PLCs), etc. the communication devices such as microwave radios, etc. would also have resource constrained capabilities.

C4 – Maintenance Cycle Although maintenance cycle of the physical SCADA network is an operational consideration, it is still considered an important characteristic. Due to network dimension; geographical dislocation, and mission critical nature, smart grid networks typically have a maintenance cycle of 15 to 50 years, as opposed to 1 to 5 years for conventional networks. The smart grid would need to facilitate these variant maintenance and management cycles.

C5 – Emerging Standards Work on smart grid standards are being undertaken by the Institute of Electrical and Electronic Engineers (IEEE), National Institute of Standards and Technology (NIST) and International Electrotechnical Commission (IEC). Well established standards are essential "to ensure a highly secure, scalable, consistently deployed smart grid system" (Metke & Ekl, 2010). The evolving smart grid standards present an important challenge for security researchers within the smart grid security space.

C6 – Topology A large part of the smart grid has a relatively static network topology, i.e. the physical network, only the HAN, specifically the integration of electric vehicles adds mobility to the network. However, the smart grid network topology is also expected to provide real–time performance for self–healing and self–organising capabilities, and thus become dynamic, see C9 below.

C7 - Traffic Patterns The traditional SCADA networks would demonstrate regular traffic patterns (Zhu & Sastry, 2010). However, with the emergence of the smart grid, such determinism cannot be taken for granted. With two–way communication and increased customer and market interactions, smart grid related traffic is expected to be more dynamic and less predicable in the demand–side networks.

C8 – **Nature of Network** Smart grid networks provide mission critical functionality, this has specific performance requirements, in terms of latency, reliability and resilience. The field environment were expected to have real–time performance; be highly reliable and delivery very high uptime; and implement recovery mechanisms to mitigate any disturbances within the network. The smart grid is intended to enhance and support such characteristics.

C9 – **Adaptive** Given the objectives of the smart grid for higher resilience to disturbances and better recovery capabilities, the smart grid needs to be adaptive. This relates to the C6 capability discussed above, where the topology may change dynamically based on events within the smart grid.

The characteristics identified can be evaluated using metrics such as "reliability, and power quality, dynamic optimisation, scheduling and prediction, data management, data mining measurements, state estimation and devices for real-time analysis, and analytical ability" (Hassan & Radman, 2010).

4 Key Functional Requirements

The characteristics discussed in Section 3 highlight how the SCADA network is altered to function as a smart grid. Given the overview of the benefits and objectives of the smart grid and the key characteristics and attributes of the envisioned smart grid, key functional requirements of the smart grid in respect to IDSs can be extrapolated.

This section identifies and extrapolates specific high–level smart grid functional requirements that relate directly to the characteristics and attributes identified above (Section 3) in the context of an IDS for the smart grids. Therefore the requirements are drawn directly from, and support the characteristics of the smart grid.

Another benefit of developing such requirement from the characteristics and attributes identified is to present a uniform mechanism for evaluating existing IDS approaches. Different techniques address different characteristics of the smart grid, but an effective means to uniformly compare these techniques does not exist.

R1 – **Support Legacy Protocols** The proposed IDS shall effectively handle legacy communication protocols without adversely affecting real–time performance requirements and design goals of reliability and resilience. Although there are emerging modern smart grid communication protocols that include additional security goals such as confidentiality and authentication, the smart grid may still largely operate over legacy protocols. Any IDS must be capable of handling legacy protocols and their inherent lack of security. This requirement directly related to the C1 characteristic identified in Section 3.

R2 – **Scalable** The proposed IDS shall be scalable, to effectively handle the relatively large number of network communication nodes present in the smart grid network. Unlike conventional networks that are limited to thousands of nodes, the smart grid comprises of billions of nodes, such as smart meters and smart appliances within the distribution and HANs. The proposed solution must be capable of deployment and scalability to such dimensions. Additionally due to increasing electrical energy demands, the smart grid would grow to accommodate such demands. This requirement related directly to the C2 characteristic.

R3 – Support Legacy Hardware The proposed IDS shall be deployable on networks utilising resource limited nodes such as IEDs and PLCs. Such hardware usually have long maintenance cycles and are distributed in nature. The proposed solution must be capable of being deployed on such a distributed environment, with nodes that lack the capability to perform high–level or computationally intensive operations. This requirement related to the C3 and C4 requirements.

R4 – Standards Compliant The proposed IDS shall be based on existing ICT and SCADA standards as well have capabilities to accommodate and facilitate emerging smart grid standards. Since ICT and SCADA standards are well established, and many smart grid standards are still under development, the proposed solution must be capable of working with existing standards as well as handle additional standards as and when they become available. This is based on the C5 characteristics.

R5 – Adaptive The proposed solution shall dynamically maintain a topological model of the smart grid network and facilitate the monitoring and control of network elements in real–time. Due to the scale of the smart grid network, the proposed solution must be capable of effectively handling any changes to the topology of the smart grid. This requirement supports the C6, C8 and C9 characteristics of the smart grid.

R6 – Deterministic The proposed IDS in addition to facilitating and ensuring real–time performance shall ensure that the deterministic nature of the underlying SCADA networks is not adversely affected. Due to the mission critical nature of the smart grid, this is probably the most important requirement and directly related to the C8 characteristic identified in Section 3. Further the level of network traffic regularity within the smart grid is subject to change depending on smart grid applications, (refer C7), but the performance of the IDS should remain deterministic.

R7 – Reliable Due to the mission critical nature of the smart grid and the underlying SCADA environment, the proposed solution must be highly reliable. The IDS must resist accidental failure as well as malicious attacks and not adversely affect the performance of the system being monitored in case of failure. Again this is requirement is related to the C8 characteristic relating to the nature of the smart grid network.

The requirements identified here are not intended to be a comprehensive list, but instead as a high–level set of key functional requirements to guide the design of an appropriate IDS for smart grid environments. In the following section we examine the IDSs as a technical security control for incident detection, i.e. for the effective identification and characterisation of disturbances within smart grid networks.

5 Related Work

Intrusion detection is the process of monitoring a system to identify incidents. Such *incidents* may be a result of various operations or activities, such as malicious software execution, cyber attacks, accidental or intentional misuse, etc. that compromise the security goals of a system, i.e. compromise to confidentiality, integrity, availability, authentication or non–repudiation.

Generally IDSs have three main components, sensors, that collect appropriate data for analysis; analysers that receive data from sensors or other analysers for further analysis; and an interface, that presents the output from the analyser for further action.

IDSs are classified based on the deployment of its sensors or analysis method. Based on source input the IDS may be classified as (Lin, Zhang, & Ou, 2010; Sabahi & Movaghar, 2008); Host–based, these IDSs deploy sensors to monitor characteristics and behaviours of single host; Network–based, these IDSs deploy sensors to collect network traffic for network segments of interest or network traffic from specific hosts; and Hybrid IDSs, that deploy sensors to collect network traffic as well as host inputs from monitored hosts.

IDSs are also classified based on the analysis component of the IDS, i.e. based on the processing of the data collected from the sensors (Sabahi & Movaghar, 2008). Common analysis methods are signature–based or anomaly–based detection. A third, less common detection method based on stateful protocol examination.

The remainder of this section provides a survey of current research relating to IDS within smart grids. Current work in IDS for the smart grid can be divided into two categories, i.e intrusion detection on the supply–side and intrusion detection on the demand–side networks.

This distinction is important, since, prior to the smart grid there was limited visibility into the demand–side network. SCADA systems provided access up until distribution substations networks. The supply–side network deals with production, and the demand–side networks facilitate consumption.

5.1 Supply–side Intrusion Detection

A number of IDS for SCADA networks have been surveyed and presented by Zhu and Sastry (Zhu & Sastry, 2010). These are readily applied to the physical SCADA network, but are inadequate for the smart grid environment. The integration of ICT solutions alters the characteristics of the SCADA network as discussed in Section 3. However, IDSs for SCADA networks is still considered an emerging research area (Carcano, Fovino, Masera, & Trombetta, 2010)

Naess et. al. (Naess, Frincke, McKinnon, & Bakken, 2005) identify embedded systems as being very application specific, and thus implemented a configurable middle–ware based IDS framework. The rationale for the approach was the availability of; all communication flow between nodes to the middle–ware and the application logic employed within the network. Thus the proposed IDS was able to interface the application logic with the communication flow using middle–ware. The analysis intelligence is implemented as application policies, which are used by the middle–ware to detect incidences and implement corrective action. This design is useful as it would support legacy hardware (R3).

A different approach has been proposed by Valdes and Cheung (Valdes & Cheung, 2009), which is motivated by the move from proprietary infrastructure to COTS infrastructure. A multi–layered approach has been adopted, which includes monitoring at the host as well as network levels. The IDS uses a model–based approach, in which, the network behaviour is characterised using a model, and violations of the model are identified as intrusions. The analysis is based on specification–based, change detection and statistical anomaly detection methods. The approach was evaluated using Modicon communication bus (Modbus) transmission control protocol (TCP) and distributed network protocol version 3 (DNP3) over TCP/internet protocol (IP) based implementations. A conventional IDS, i.e. Snort was employed for the actual detection, based on rules developed to detect violations of the model.

An alternative approach for intrusion detection is provided by Barbosa and Pras (Barbosa & Pras, 2010), which is based on the network traffic flow analysis. The research exploits the deterministic behaviour of SCADA networks to detect anomalies. Any violation of a pre–generated flow–model are flagged as anomalies.

Lauf et. al. (Lauf et al., 2010) developed a two–stage IDS for ad–hoc mobile networks. They proposed an anomaly–based detection method that compared a set of predefined behaviour dynamically during network operation. The proposed IDS employed a two–stage analysis model in which the first stage employed a probability density function to identify anomalous behaviour on a per node basis, and a second stage, which cross-correlates multiple threats. The design allowed a scalable solution to be developed (R2). This approach can be transposed to SCADA networks as both environments employ embedded hardware with resource limitations (R3), and will be well suited to handle topology changes (R5).

5.2 Demand–side Intrusion Detection

The smart grid provides integration of the supply–side and demand–side networks as well as external enterprise networks. Traditional SCADA systems lacked such integration and remained logically and physically separate. With the emergence of the smart grid cyber attacks can be implemented more readily. The easiest point of access for cyber attackers would be via the HAN within the demand–side network.

Recent work by Berthier et. al. (Berthier, Sanders, & Khurana, 2010) examined intrusion detection for advanced metering infrastructure (AMI). They provided a detailed review of AMI communication networks and identified the requirements and constraints as a particular challenge for researchers given the "heterogeneity of communication technologies".

The paper reviewed existing IDSs in the context of AMI, and identified the robustness and seamless integration as another major challenge for IDSs for AMI. The same challenge needs to be addressed by IDSs for the wider smart grid environment.

Conventional IDSs for enterprise networks cannot be deployed on the smart grid for operational and functional reasons. The increased connectivity of ICT networks and SCADA networks increased the attack surface for cyber attacks on the smart grid. "Cyber attacks on the integrity of the grid, are increasingly a serious concern" (Rosenfield, 2010).

The security of the smart grid is beyond just the traditional ICT network and SCADA network security, but instead presents novel challenges for researchers and industry. Any proposed IDS needs to be reconciled with the key functional requirements of the smart grid as described in Section 4. A comparison of the research efforts is undertaken in Section 6. As part of the discussion limitations are also identified.

6 Discussion

Work undertaken by Metke and Elk (Metke & Ekl, 2010) identifies a number of stake holders working to identify security requirements for smart grids. Wang and Leung (Wang & Leung, 2011) focused in identifying technical requirements for IP network communication within the smart grid, specifically for implementing AMI solutions.

Requirements	Berthier	Lauf	Barbosa	Valdes	Naess
R1 – Legacy protocols	N/A	N/A	Y	Y	N/A
R2 – Scalable	Y	Y	N	Y	N
R3 – Embedded hardware	N	Y	N	N	Y
R4 – Standards compliant	N	N	N	N	N
R5 – Adaptive	N	Y	N	N	N
R6 – Deterministic	Y	N/A	N/A	N/A	N/A
R7 – Reliable	Y	N	N	N	N

Table 1: Comparison of IDS approaches against proposed requirements

Table 1 highlights the IDS approach proposed by researchers. The proposed IDSs are listed as meeting a specific high level requirement only if the approach explicitly addresses the requirement. Other requirements may be implicitly addressed by the research, however these are not recorded in the table (Table 1).

From the comparison above it is evident that current research efforts fail to address all the high level functional requirements. Therefore the solutions proposed may be unsuitable for the smart grid without appropriate changes. The techniques identified for supply–side and demand–side network intrusion detection are discussed below.

The approach proposed by Naess et. al. (Naess et al., 2005) provides a good approach for interfacing embedded hardware with the detection logic. However, the use of middle–ware may limit the scalability (R1) of the approach. Further, the use of middle-ware and external analysis may also affect the determinism (R6) yielded by the approach. However the approach would be very useful if employed in an off–line mode.

The model–based approach presented by Valdes and Cheung (Valdes & Cheung, 2009) is quite useful and would adequately address emerging standards and modern protocols (R4). Another benefit of the proposed approach is the higher confidence level and coverage in the detection of incidences due to the use of correlation within the network (R7). A limiting factor of such an approach is the high costs involved in developing such models initially. However, a number of automated mechanisms are increasingly becoming available to address such concerns. The approach may have limited application in an adaptive (R5) environment such as the smart grid, as the models may need to change dynamically.

Flow-model based IDS as proposed by Barbosa and Pras (Barbosa & Pras, 2010) is useful in a static environment such as SCADA networks, however would be inadequate in the smart grid due to its fluid topology (R5) as a result of dynamic power routing, self–healing, high–resilience. The approach provides a useful starting point for approaches involving network traffic analysis.

The embedded systems approach implemented by Lauf et. al. (Lauf et al., 2010), albeit, in a different problem domain illustrated the use of distributed resource constrained nodes for intrusion detection. The approach is particularly appealing as it adequately addressed the issue of mobility (R5) within the network. Thus electric vehicles and dynamic power routing can be readily handles within the smart grid. The approach also presents a scalable solution that can handle future network growth.

The only demand–side approach by Berthier et. al. (Berthier et al., 2010) reviewed used a specification–based methods for intrusion detection. Although the approach is useful, just like model–based approaches, specification models have a high cost and given the emergence of new standards in both the demand–side as well as supply–side networks, a large number of specification models would need to be developed for the IDS to function universally. The work presented requirements that supported the requirements defined in Section 4. Specifically references were drawn to making the IDS scalable (R2) and the reliability of the IDS against accidental failure and malicious attacks (R7). It further, defined constraints of low overhead and minimal impact (R6).

Of all the approaches examined, the evaluation did not factor in the overall performance of the solution, i.e. for the proposed IDS to be deployed as an on–line system, it must yield deterministic (R6) performance to maintain the integrity of the smart grid and the underlying SCADA physical network, alternatively the IDS may be deployed in an off–line mode.

Conventional ICT network IDSs lack requirements such as scalability (R2), reliability (R7) and determinism (R6) as required in smart grid due to their mission critical nature. Any existing IDS tools may lack functionality to support legacy SCADA protocols (R1) and the implementation footprint to be deployed on legacy hardware and embedded systems (R3).

On the other hand SCADA IDSs that leverage off of the determinism in SCADA networks would be unable to handle the dynamic nature of the smart grid (R5). Further, such IDSs would be unable to support the multitude of application layer protocols that would be present in conventional ICT networks.

Any design must wholly support the requirements to adequately address the unique characteristics of the smart grid. A possible approach may be to design and develop an IDS with sensors in both the ICT and SCADA networks with separate analysis units for each, which then provide input to an integration analysis unit for correlating the analyses.

7 Conclusion

To achieve better intrusion detection, i.e. with better coverage, accurate detection and lower false positive rates, a holistic approach must be employed, which utilises correlation of events, to accurately monitor a system for incidents.

SCADA networks are very specific, thus depending on the application of the network, any IDS would need to be tailored to the specific application. This would be particularly relevant for model–based and specification–based approaches. Currently there is limited research in this area, a majority of recent control system IDS research appears to be focus on traditional SCADA systems or supply-side networks. There is a significant gap that needs to be addressed, i.e. an IDS for smart grid, which is capable of monitoring both the enterprise as well as SCADA networks, and operate in both the supply–side and demand–side parts of the smart grid.

Future work will involve the refinement of the high–level requirements to enable the design of an appropriate intrusion detection model for the smart grid environments to leverage off of the unique characteristics of such systems. Further, the design should involve the identification and use of multiple systems events for enhance correlation analysis to increase the confidence levels of incident detection. Specifically examining and correlating network related parameters with host specific parameters to enhance incident detection.

A number of research questions remain to be answered, such as; *how best to perform intrusion detection within the smart grid; how best to design an IDS for the smart grid; where best to deploy the IDS within the smart grid; what threat models to be used for the design of the IDS; how best to train and evaluate the IDS.*

References

Aggarwal, A., Kunta, S., & Verma, P. K. (2010, January). A proposed communications infrastructure for the smart grid. In *Proceedings of Innovative Smart Grid Technologies* (pp. 1–5). IEEE.

Barbosa, R., & Pras, A. (2010). Intrusion detection in SCADA networks. In *Proceedings of the Mechanisms for Autonomous Management of Networks and Services, and 4th International Conference on Autonomous Infrastructure, Management and Security* (pp. 163–166). Berlin, Heidelberg: Springer-Verlag.

Berthier, R., Sanders, W., & Khurana, H. (2010). Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In *Proceedings of the 1st IEEE International Conference on Smart Grid Communications* (pp. 350–355). IEEE.

Carcano, A., Fovino, I., Masera, M., & Trombetta, A. (2010). State-based network intrusion detection systems for SCADA protocols: a proof of concept. *Critical Information Infrastructures Security*, *6027*, 138–150.

Cohen, F. (2010, January). *The smarter grid* (No. 1).

Fabro, M., Roxey, T., & Assante, M. (2010, January). *No grid left behind* (No. 1).

Hassan, R., & Radman, G. (2010, March). Survey on smart grid. In *Proceedings of the IEEE SoutheastCon* (pp. 210–213). New York, New York, USA: IEEE.

Lauf, A. P., Peters, R. a., & Robinson, W. H. (2010, May). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. *Ad Hoc Networks*, *8*(3), 253–266.

Lin, Y., Zhang, Y., & Ou, Y.-j. (2010, April). The design and implementation of host-based intrusion detection system. In *Proceedings of the 3rd International Symposium on Intelligent Information Technology and Security Informatics* (pp. 595–598). IEEE.

Metke, A. R., & Ekl, R. L. (2010, January). Smart grid security technology. In *Proceeding of the Innovative Smart Grid Technologies* (pp. 1–7). New York, New York, USA: IEEE.

Momoh, J. A. (2009). Smart grid design for efficient and flexible power networks operation and control. In *Proceeding of the IEEE/PES Power Systems Conference and Exposition* (pp. 1–8). New York, New York, USA: IEEE.

Naess, E., Frincke, D. A., McKinnon, A. D., & Bakken, D. E. (2005, june). Configurable middleware-level intrusion detection for embedded systems. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops* (pp. 144–151). Washington, DC, USA: IEEE Computer Society.

Reed, G. F., Philip, P. A., & Ansel Barchowsky, Christopher J. Lippert, A. R. S. (2010). Sample survey of smart grid approaches and technology gap analysis. In *Proceedings of Innovative Smart Grid Technologies Conference* (pp. 1–10). IEEE.

Rosenfield, M. G. (2010). The smart grid and key research technical challenges. In *Proceedings of the Symposium on VLSI Technology* (pp. 3–8).

Sabahi, F., & Movaghar, a. (2008, October). Intrusion detection: A survey. In *Proceedings of the 3rd International Conference on Systems and Networks Communications* (pp. 23–26). New York, NY, USA: IEEE.

Valdes, A., & Cheung, S. (2009). Intrusion monitoring in process control systems. In *Proceedings of the 42nd Hawaii International Conference on System Sciences* (pp. 1–7). IEEE Computer Society.

Wang, J., & Leung, V. C. M. (2011). A survey of technical requirements and consumer application standards for ip-based smart grid AMI network. In *Proceedings of the International Conference on Information Networking* (pp. 114–119).

Zhu, B., & Sastry, S. (2010). SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. In *Proceedings of the 1st Workshop on Secure Control Systems (SCS).* Stockholm: Team for Research in Ubiquitous System Technology.