Smart Grid Cyber Security Research at Masdar Institute of Science and Technology

Davor Svetinovic and Zeyar Aung

Computing and Information Science Program, Masdar Institute of Science and Technology
Abu Dhabi, United Arab Emirates
Emails: {dsvetinovic, zaung}@masdar.ac.ae

Summary: Ensuring reliable power supply is the key to any country's economic growth and social welfare. But as our power grids adopt new technologies and becoming smart grids, they are also becoming more vulnerable. Cyber security is one of the major challenges in the smart grid development. Masdar Institute's Computing and Information Science Program is actively participating in smart grid cyber security research both from high-level systems engineering and low-level technical perspectives such as intrusion detection and design of new security/privacy protocols.

Keywords: Smart grid, cyber security, Masdar Institute of Science and Technology

Introduction

Masdar Institute of Science and Technology, located in Abu Dhabi, UAE, is a private, not-for-profit, independent, graduate-level, research-driven institute developed with the support and cooperation of Massachusetts Institute of Technology (MIT), USA. The goal of the Institute is to develop, over a period of years, indigenous R&D capacity in Abu Dhabi, addressing issues of importance to the region in critical areas such as: renewable energy, sustainability, environment, water resources and microelectronics.

Smart grids — intelligent electricity grids that use modern Information and Communication Technology (ICT) — have become a global trend. Masdar Institute is actively involved in various aspects of the smart grid research.

A smart grid is typically characterized by bi-directional flows of power and information between the utility and the customers. A cyber infrastructure is an integral part of the smart grid. Unfortunately, despite its significant benefits in providing greater efficiency, reliability and sustainability to the power system, the cyber infrastructure of the smart grid is susceptible to various types of security attacks like any other ICT system such as a large computer network or the Internet. Some of these attacks, if successful, can lead to disastrous consequences such as financial losses, nation-wide blackouts, and even vulnerability in national defence. Thus, cyber security is one of the major concerns in smart grid development.

In particular, our current smart grid cyber security research is focused on high-level systems security analysis, and on low-level intrusion detection and security/privacy protocols.

Systems Security Analysis

Our research aims to develop an integrated framework for systems security and privacy analysis, and for the execution of the security and privacy measures in the smart grid. To do this we are building a framework that includes the processes and tools for computer forensics to deal with the identifying, preserving, recovering, analyzing and presenting facts about security and privacy attacks in the smart grid.

Using the Security Quality Requirements Engineering method developed at Carnegie Mellon University (CMU) we are identifying and understanding the security requirements of the smart grids [6]. The reference architecture of the smart grid, with its components and communication interfaces used to exchange energy-related information, is integrated with the results of smart grid security threat analysis to produce comprehensive, integrated security models, including the smart grid control center and smart meters [7].

Our research also includes an inter-domain privacy analysis of complex dependencies and interactions among the domains of the smart grid [5]. We explore the way smart grid data is transformed, used and saved between different domains and actors in the smart grid in order to ensure security and privacy.

Intrusion Detection and Security/Privacy Protocols

We have proposed an intrusion detection system (IDS) framework for Advanced Metering Infrastructure (AMI) [1]. It uses data stream mining techniques to detect anonymous events in the AMI network (this work has won the best paper award at the PAISI 2012).

We have also designed an efficient authentication protocol for the data aggregation in AMI [3]. It uses signature aggregation, batch verification and signature amortization schemes to minimize the communication overhead, reduce numbers of signing and verification operations, and provide fault tolerance.

In addition, we have addressed the pressing issue of customers' privacy, and designed privacy preserving protocols for smart appliance control application [4], and multi-cast communication [2]. We investigated a privacy threat model and developed protocols that merely incur substantially light overheads in order to enable them to be practically used in resource-limited devices like smart meters.

References

[1] M. A. Faisal, Z. Aung, J. Williams, and A. Sanchez, "Securing advanced metering infrastructure using intrusion detection system with data stream mining," in *Proceedings of the 2012 Pacific Asia Workshop on Intelligence and Security Informatics (PAISI)*, LNCS 7299, pp. 96-111, 2012.

[2] D. Li, Z. Aung, S. Sampalli, J. Williams, and A. Sanchez, "Privacy preservation scheme for multicast communications in smart buildings of the smart grid," *Smart Grid and Renewable Energy*, 2013. In print.

[3] D. Li, Z. Aung, J. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," in *Proceedings of the 2012 IEEE Power and Energy Society Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1-8, 2012.

[4] D. Li, Z. Aung, J. Williams, and A. Sanchez, "P3: Privacy preservation protocol for appliance control application," in *Proceedings of the 3rd IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 294-299, 2012.

[5] H. Suleiman, A. Khaja, N. Zafar, E. Phillips, D. Svetinovic, and O. L. de Weck, "Inter-domain analysis of smart grid domain dependencies and mappings using domain-link matrices," *IEEE Transactions on Smart Grid*, vol. 3, pp. 692-709, 2011, DOI:10.1109/TSG.2011.2176151.

[6] H. Suleiman and D. Svetinovic, "Evaluating the effectiveness of the Security Quality Requirements Engineering (SQUARE) method: A case study using smart grid advanced metering infrastructure," *Requirements Engineering Journal*, 2012, DOI: 10.1007/s00766-012-0153-4.

[7] N. Zafar, E. Arnautovic, A. Diabat, and D. Svetinovic, "System security requirements analysis: A smart grid case study," *Systems Engineering (Wiley)*, 2012. In print.