Security Issues and Solutions in Smart Grid: FUSE-IT European Project Use-case

Mohamed Attia, Sidi Mohammed Senouci, Shohrer Avhar, Jen Rossey, Luc Lutin, Isabel Praça

Security Issues and Solutions in Smart Grid: FUSE-IT European Project Use-case

Mohamed Attia*, Sidi Mohammed Senouci*, Shohrer Avhar⊢, Jen Rossey±, Luc Lutin#, Isabel Praça⊣

**DRIVE EA1859, Univ. Bourgogne Franche Comté, F58000, Nevers France*
{Mohamed.Attia, Sidi-Mohammed.Senouci}@u-bourgogne.fr
⊢ Institut Mines-Telecom, Evry, France, shohreh.ahvar@telecom-sudparis.eu
±IMEC, Belgium, Jen.Rossey@UGent.be
 # NIKO, Belgium, Luc.lutin@niko.be

⊣GECAD, ISEP/IPP, Porto, Portugal, icp@isep.ipp.pt

Abstract

As we transition to more complex, higher performing and energy efficient buildings, it is apparent that traditional Building Management Systems (BMS) are not up to the task of monitoring and managing today's building operations. Therefore, the need for sustainable, reliable, user-friendly, efficient, safe and secure BMS in the context of smart critical sites is being crucial. FUSE-IT European project is the ICT experts' response that aims to develop a smart secured building system, incorporating secured share sensors, effectors and devices strongly interconnected through trusted federated energy & information networks, a core building data processing & analysis module, a smart unified building management interface and a full security dashboard. In this brief news letter, we provide an overview of the smart grid security challenges, the main FUSE-IT goals, depict its architecture and highlight potential achievements and realizations with a focus on the security aspects.

1. Introduction

Smart grid is an intelligent power network that aims to provide a reliable and economic system that handles power supply and consumption. Three communication levels are defined in the grid for metering-related functions, which are Wide Area Network (WAN), Neighborhood Area Network (NAN) and Home Area Network (HAN). Customer's appliances compose a HAN; we can cite laptop, electric vehicle, etc. These appliances are connected to the smart meter through a wireless or wired link. In each region, a collector collects the measurements delivered by the smart meters located within its range and forwards them to a control center. Smart meters and collector represent the NAN as presented in (Meng, 2014) (Mohammadi, Misic, Khazaei, & Misic). Finally, the WAN represents all NANs and the control center (Meng, 2014). According to several research reports (Meng, 2014) (Mohammadi, Misic, Khazaei, & Misic) (NIST, 2009), security in the grid is mandatory since it manages a vital information such as metering data and energy distribution, which could be a target for attackers. Contemporary security mechanisms, used in computer networks, do not have the ability to detect all malicious nodes due to the high number of communicating nodes (customers' appliances and smart meters) that are deployed in large and complex geographical areas (Mohammadi, Misic, Khazaei, & Misic). Thereby, an efficient security mechanism suiting the smart grid requirements should be deployed. Current security approaches for NAN (M. Badra and S. Zeadally, 2014) (Nayak, 2014) are based on cryptography mechanism to assure smart meters authentication and their privacy. The Intrusion Detection System (IDS) is

defined as a second layer of security that uses special agents to detect if there is an attack or not and triggers an alert when an intruder launches an attack (Raya, Papadimitratos, Aad, & Hubaux, 2007) (Sedjelmaci, Senouci, & Feham, 2013).

The remainder of this news letter is described as follows: State of the art about smart grid security is introduced in section 2. Then, a general description of the FUSE-IT project is presented in section 3. Section 4 is devoted to FUSE-IT security solutions. Finally, section 5 concludes this paper.

1) Security in Smart Grid: State of the art

In literature, there are several techniques used in Intrusion Detection Systems (IDS). They rely basically on one of the two following approaches: anomaly-based detection (Tylman, 2008) (Maxion & Tan, 2000) or/and rule-based detection (Mitchell & Chen, 2013) (Yang, McLaughlin, Littler, & Sezer, 2013). On one side, the first is generally more sophisticated, robust and rejoices by its highest detection rate among all the security mechanisms. However, it requires a high computation & energy capabilities and generates a high false positive rate (Hai, Huh, & Jo, 2010). On the other side, rule-based detection system is lighter in terms of computing complexity and energy consumption. This system (i.e. rule-based detection) is based on a number of well-defined rules and thresholds where each overtake is announced as an attack. That is why it is characterized by its low false positive rate unlike learning algorithms.

Recently, some detection frameworks are proposed for smart grid to prevent and detect the occurrence of the most lethal cyber-attacks (Yang, ve diğerleri, 2014) (Ma, Liu, Song, & Han, 2015) (Sargolzaei, Yen, & Abdelghani, 2014) (Yu & Chin, 2015). Specifically, in (Yang, ve diğerleri, 2014), the authors develop an algorithm to identify the optimal number of smart meters to manipulate in order to find the optimal attack strategy, which aims to perturb the state estimation of the grid system and bother its stability. Then, to defend against this attack, they proposed a rule-based detection to identify the stealthy false data injection in the network using Cusum (Cumulative sum: a sequential analysis technique used for monitoring change detection) technique (Yang, ve diğerleri, 2014). The drawback of this work is that this algorithm is embedded in a centralized fashion at the control center units and so it can't detect all the attackers. In addition, the control center cannot monitor the entire network and especially when a huge number of connected equipment and devices like smart meters and sensors are connected. A centralized monitoring system generates also a high overhead since it has to collect all the packets and then analyze them.

In (Ma, Liu, Song, & Han, 2015), the authors proposed a multiact dynamic game between the attacker and defender, in which the optimal strategies are taken by the two sides to maximize their own profits. Here, the attacker would proceed to jam a certain number of signal channels carrying measurement information. It has the goal to manipulate the electricity price in order to create an opportunity for gaining profit. In this paper, the authors do not evaluate their approach in terms of detection rate as well as false positive rate to test the performance and robustness of the model.

Recently, the authors in (Sargolzaei, Yen, & Abdelghani, 2014) modeled a Time Delay Switch (TDS) attack. This attack consists on putting a random delay on the power Load Frequency Control (LFC) system. They proved the impact of this attack and they demonstrated the damage and risks that can leave this attack on the power system and the instability that could create. Besides, they don't propose a countermeasure to prevent the intrusion caused by this attack that aims to perturb the well-functioning of the smart grid. In (Yu & Chin, 2015), the authors aim to detect the blind false data injection attack by using the Principal Component Analysis (PCA) approach. The drawback of this work is that the authors suppose that the malicious attacker has knowledge of the grid topology. This assumption is not evident especially with the extreme

extension and complexity of the smart grid. Moreover, like the previous work, there is no defensive mechanism to avoid those stealthy attacks and ensure the protection of the state estimation.

2) FUSE-IT Project: General Description

In the coming years, corporate and administrative buildings will be expected to meet strengthened regulations and company policies in matters of energy efficiency, facility management, information systems and security. In the context of a smart critical site, a site manager and a security manager may face incompatible objectives and constraints as well as dramatic overcosts if no substantial effort is done to optimize, federate and rationalize the legacy building management chains. In the following, we introduce the project goals and final demonstrators.

3.1 FUSE-IT goals

FUSE-IT (Future Unified System for Energy and Information Technology, 2013-2017) is a European project with four countries (France, Turkey, Belgium and Portugal). The project aim is to address the need of sustainable, reliable, user-friendly, efficient, safe and secure Building Management System (BMS) in the context of Smart Critical Sites. It is the sole initiative addressing Sustainability and Security & Safety challenges from a site management perspective. It will benefit to both challenges by solving the dilemma between efficiency and security in intelligent buildings. An overview of FUSE-IT architecture is presented in Fig 1. A BMS is defined here as a computer based system that controls and monitors the building facilities such as ventilation, lighting, power systems, fire detection and security. A Smart Site is a facility or infrastructure implementing intelligent building and energy control & monitoring technologies such as micro-grids, smart sensors or communicating devices. A micro-grid is intended here as a local electrical system that includes multiple loads and distributed energy resources that can be operated in parallel with the broader utility grid or as an electrical island. A Critical Site is a facility or infrastructure which has to meet higher grade safety and security requirements, whether this is for national / business-strategic or public health and safety reasons.

Fig. 1. FUSE-IT architecture.

The trend towards global competition and supranational regulation forces nations to flow down more and more environmental, economical, national-critical and safety-critical requirements on key public and private actors. These actors need to upgrade their facilities and assets accordingly. In the context of a Smart Critical site, a Site Manager and a Security Manager may face incompatible objectives and constraints. A Site Manager would likely focus on manageability, automation, energy efficiency, sustainability and global cost of building operation. A Security Manager would more likely focus on anti-intrusion at physical and logical level, relying on dedicated equipment and segregated networks, whatever the infrastructure, staff & power required.

From a technological point of view, however, with ICT enhancing all legacy building equipment and automation, a number of synergies emerge which may help solving this dilemma. Through connection to enterprise network and the internet, building energy and automation systems become more flexible, powerful and upgradable. They also get exposed to new threats, a reason why, from its original focus on information networks, cyber-security has moved towards a more comprehensive scope involving security of cyber-physical systems. A striking rationale for that is that attacks on cyber-physical systems do not only harm national / business strategic information security. They can ramp up into industrial, environmental or public health and safety catastrophe.

A way to success is to stimulate cross-domain innovation between activities which are traditionally very segmented. Advanced data processing and analysis is the key capability required to meet all challenges above. Therefore, the main achievement of Fuse-IT shall be the development of a Core Building Data Processing & Analysis module. It will process data reported by Secured Share Sensors, Effectors and Devices strongly interconnected through Trusted Federated Energy & Information Networks. It will display the building & security status based on common Key Performance Indicators (KPIs). At user-level, a Smart Unified Building Management Interface will enable daily monitoring and controlling with a “view of god” on buildings, while a Full Security Management Interface will enable supervision of both physical and logical security throughout the premises and the enterprise network.

The result of Fuse-IT will be a Smart Secured Building System, incorporating the above described modules. They will be marketable as standalone components or fully integrated system in order to address either existing or new Smart Critical Sites. A service offering will also be set up to enable trusted building management and/or security management operation under rental price. Besides lower investment cost, this enables expertise federation and full benefit from big data analytics advantage.

3.2 FUSE-IT Demonstrators

The results of the FUSE -IT project are promoted through demonstrators and prototypes. These demonstrations are organized through the various FUSE-IT project countries as described below.

A. Gazi Technopark

Gazi Teknopark is the Turkish demonstrator, focusing on the Unified Building Management Interface. It is established as 5th Technology Development Zone of Ankara in October 2007. It is located at Gazi University Golbasi Campus, on 58.813m^2. Gazi Technopark is one of the first and largest installations producing electricity from renewable sources, specifically solar energy. It is also the first solar park over 100kW in Turkey, actually it is near 300 kW. Besides, it has the largest solar tracking panel system. Last but not least, it provides the first electric vehicles charging station powered by solar energy.

B. Elancourt Demonstrator

Airbus Defense and Space site in Elancourt is the French demonstrator and will host a demonstration mainly focused on the Unified Security of buildings, using as much information as

possible from the four main domains of site supervision, including forecast capabilities, to detect any threats regarding the building assets, and have a better understanding of the attack final objectives. The implementation of FUSE-IT framework will show that cross domain indicators are an added value to security supervision to categorize a threat, and apply the appropriate reaction to ensure the integrity and confidentiality of building assets.

C. CHSJ Demonstrator

Centro Hospitalar São João(CHSJ) is the Portuguese demonstrator and the one to address FUSE-IT innovations for the management of a complex and safety critical building. CHSJ building is a very old one, and the challenges coming from it are enormous: legacy equipment, several different equipment providers, disparate supervision of control areas, lack of a comprehensive view of the building, together with severe constraints and criticality of equipment and zones, and the need to be able to integrate the most advanced clinical technologies. The main focus of this demonstrator is on the unified and context awareness intelligent management of building resources.

D. HomeLab

Imec Homelab is a residential and home office test environment and innovation incubator that will be used as the Belgian demonstrator focusing on FUSE-IT capabilities to deal with flexible and reconfigurable buildings. The demonstration will focus on the ease-of-use and flexibility of installation and reconfiguring "smart" home features in the context of "flexible offices", and on the features of the open API that is supported by the Imec gateway. This demonstration will be showcased by adding a new device to the building using a different technology.

E. Final Demonstration

The overall Fuse-IT results will be demonstrated on 2 temporary events: The Digital Innovation Forum (DIF 2017) event, planned on 10-11 May 2017 in Amsterdam, and a final demonstration on a temporary event still to be confirmed. On these temporary events, a live demonstration is presented of a smart unified building facility, energy and security management system, integrating all results of the Fuse-IT project.

3) FUSE-IT security solutions

In this section, we present some security solutions proposed in the FUSE-IT project context.

3.1 Temporal and Spatial Based Detection Against Lethal Attacks in SG

The proposed algorithm relies on temporal and spatial attack detection, by monitoring the Number of Sent PacketsNSP and Jitter (i.e. the delay between exchanged packets). Our model follows the behavior of each node and detects any abnormal or unexpected behavior. A node here represents the smart meter, the actuator or even the control center. We note by $l_{Ni} = \{x_i(T_1), x_i(T_2), x_i(T_3), \dots x_i(T_k)\}$ the node i's vector where k represents the number of Time slots T. x(T) denotes either the NSP or the Jitter. We note n the number of nodes to be monitored (i.e. i=1…n). Therefore, we obtain an*k matrix size. The matrix is equal to: $M = \{l_{N1}, l_{N2}, l_{N3}, \dots l_{Nn}\}$. lNi denotes the ith line of the matrix M. In normal situation, each node follows normal distribution characterized by the couple (μ1(i),σ1(i)) where μ1(i) is the mean vector of the node i and σ1(i) is the standard deviation. In normal behavior, each value of the lNi should follow a normal distribution and should be within an interval of [μ1(i)- 3*σ1(i), μ1(i)+ 3*σ1(i)]. When x is out of the interval, the node is suspected as abnormal node.

3.2 Cyber Detection Mechanism to Detect Intruders in a Smart Grid Neighborhood Area Network

In this approach, three categories of IDS agents are proposed to monitor the behavior of appliances' costumers, smart meter and collector, and analyze the communication traffic. These agents are: (i) Low Level IDS (LLIDS). Embedded at each smart meter to monitor the behavior of

appliances' costumer. (ii) Medium Level IDS (MLIDS). Embedded at a collector level to monitor the meter data delivered by smart meters located within it neighborhood, verify the intrusion decision provided by LLIDSs and analyzes the communication traffic from these smart meters. (iii) High Level IDS (HLIDS). Embedded at the control center, it monitors the behaviors of collectors, verifies the intrusion decision provided by HLIDS and analyzes the communication traffic from collectors. These agents rely on rules-based intrusion detection and learning-based detection techniques to monitor the behaviors of a target node and analyze the communication. The proposed algorithm is aimed to detect jamming attack targeting to make smart grid resources unavailable. The characteristic of jamming attack is the high Signal Strength Intensity (SSI) that is generated to interfere with physical transmission and reception of wireless communication. Jamming attacks could occur at smart meters or/and collector nodes to disrupt wireless communications. LLID, MLIDS and HLIDS monitor the SSI related to each smart meter located within its radio range and collector, respectively. Furthermore, these agents analyze the distribution of SSI by using the Euclidean distance.

3.3 Ontology-based Model for Trusted Critical Site Supervision in FUSE-IT

To develop FUSE-IT BMS, there is a need for a common information base, which describes and defines formally all physical and conceptual building elements, their characteristics and interrelationships, as well as the constraints that apply to them. While current information bases are not integrated enough considering security and trust aspects along with other three domains (i.e., energy, ICT, facility) for critical site supervision, FUSE-IT ontology provides a unified view of smart buildings by merging security ontologies with IoT and BMS ontologies. The FUSE-IT base ontology considering the domain of ICT, facility and energy is built upon the Semantic Sensor Network (SSN) [17], Smart Appliances REFerence (SAREF) [18], Smart Energy Aware Systems (SEAS) [19], Industry Foundation Class 4 (IFC4) [20] and DogOnt [21]. In order to add the security domain along with other essential areas for critical site supervision, Ontology Web Language for web Services (OWL-S) [22], Intrusion Detection System (IDS) [23] and the Unified Cybersecurity Ontology (UCO) [24] ontologies are merged with the FUSE-IT base ontology. It is worth mentioning that in developing ontologies, while it is a major requirement to reuse, as much as possible publicly available ontologies, some of these heterogeneous ontologies share concepts with the same meaning leading to the need of ontology alignment that was done in FUSE-IT ontology to determine the correspondences between concepts and/or relations in the different ontologies.

4) Conclusion

FUSE-IT project aims to develop a Core Building Data Processing & Analysis module that will process data reported by secured share sensors, effectors and devices that are strongly interconnected through trusted federated energy and information networks. It will display the building and security status based on common key performance indicators. At user-level, a smart unified building management interface will enable daily monitoring and control of buildings while a full security management interface will enable supervision of both physical and logical security throughout the premises and the enterprise network. FUSE-IT will foster innovation by horizontal expertise sharing to create impact at sensor, network, management and security management level.

Références

Hai, T. H., Huh, E. N., & Jo, M. (2010). A lightweight intrusion detection framework for wireless sensor networks. *Wireless Communications and Mobile Computing, 10(4)*, 559-572.

M. Badra and S. Zeadally. (2014). *Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy.* IEEE Transactions on Information Forensics and Security Vol. 9, No. 2.

Ma, J., Liu, Y., Song, L., & Han, Z. (2015). Multiact Dynamic Game Strategy for Jamming Attack in Electricity Market. *IEEE Transactions on Smart Grid*, 99.

Maxion, R. A., & Tan, K. M. (2000). Benchmarking Anomaly-Based Detection Systems. *Proceedings International Conference on Dependable Systems and Networks*, (pp. 623-630).

Meng,]. (2014). *Smart Grid Neighborhood Area Networks: A Survey.* IEEE Network Vol 28, Issue 1, pp.24-32.

Mitchell, R., & Chen, I. R. (2013). Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications. *IEEE Trans. Smart Grid*, 1254-1263.

Mohammadi, N., Misic, J., Khazaei, H., & Misic, V. (s.d.). *An Intrusion Detection System for Smart Grid Neighborhood Area Network.* IEEE ICC, Sydney, Australia, pp. 4125 - 4130.

Nayak, S. R. (2014). *A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids.* IEEE Transactions on Smart Grid, Vol 4, Issue 1, pp. 196-205.

NIST. (2009). *Report to NIST on smart grid interoperability standards roadmap EPRI.*

Raya, M., Papadimitratos, P., Aad, I., & Hubaux, D. J.-P. (2007). *Eviction of Misbehaving and Faulty Nodes in Vehicular Networks.* IEEE Journal on Selected Areas in Communications, Vol.25, No.8, pp. 1557- 1568.

Sargolzaei, A., Yen, K., & Abdelghani, M. N. (2014). Delayed inputs attack on load frequency control in smart grid. *ISGT*, (pp. 1-5).

Sedjelmaci, H., Senouci, S., & Feham, a. M. (2013). *An efficient intrusion detection framework in cluster-based wireless sensor networks.* Security and Communication Networks, pp. 1211–1224.

Tylman, W. (2008). Anomaly-Based Intrusion Detection Using Bayesian Networks. *Third International conference on Dependability of Computer Systems*, (pp. 211-218).

Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., & Zhao, W. (2014). On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. *IEEE Trans. Parallel Distrib. Syst.*, 717-729.

Yang, Y., McLaughlin, K., Littler, T., & Sezer, S. (2013). Rule-based intrusion detection system for SCADA networks. *Renewable Power Generation Conference (RPG 2013), 2nd IET*, (pp. 1-4).

Yu, Z. H., & Chin, W. L. (2015). Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid. *IEEE Trans. Smart Grid*, 1219-1226.