Computer Networks 86 (2015) 14–26

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A blind processing framework to facilitate openness in smart grid communications

Mehmet Hadi Gunes [a,*], Murat Yuksel [a], Hayreddin Ceker [b]

[a] University of Nevada – Reno, Reno, NV 89557, USA
[b] University at Buffalo, The State University of New York, Buffalo, NY 14260, USA

ARTICLE INFO

Article history:
Received 21 April 2014
Revised 27 December 2014
Accepted 4 May 2015
Available online 18 May 2015

Keywords:
Open cyber architecture
Power grid
Privacy

ABSTRACT

Smart grid has diverse stakeholders that often require varying levels of access to grid state and measurements. At the distribution level (i.e., MAN), smart grid provides two way communication between households and utilities. At the transmission level (i.e., WAN), multiple organizations need to share the transmission lines and cooperate with participants in their region. In this paper, we propose secure communication and computation services for smart grid to transform the current "closed cyber architecture" to an "open cyber architecture". In order to ensure the privacy and integrity of communicating parties at the distribution level, we propose to utilize the smart meters as a gateway between intra-network (i.e., HAN) and inter-network (i.e., WAN) communications, and manage incoming and outgoing traffic and mediate household devices based on the instructions from the electric utility or contracted service providers. To enhance data sharing between operators at the transmission level, we propose an open cyber architecture that utilizes *blind processing* service, in which sensitive data is transmitted through the secured channel and used in computations running in an isolated environment while the outcome is rendered only to a dedicated user or process. The "open" communication between the smart substructures and "blind" computation at operation centers will increase data sharing, minimize human intervention, and mitigate cascading events. In the paper, we provide and discuss underlying mechanisms to achieve an open cyber architecture.

1. Introduction

Power grid is a crucial infrastructure for public health, safety and welfare. Proliferation of renewable energy-based electric power production, increased use of electric vehicles, and upgrading the aging electricity infrastructure for more efficient grid operations are only viable with smarter monitoring, control and consumption of the electrical energy. It is not possible to achieve the nationwide visions for a smarter grid, if the current control, monitoring, and consumption practices are not significantly changed in high voltage transmission and medium/low voltage distribution levels.

A key factor of the power infrastructure is its multi-owner property at the *transmission level* of high-voltage interconnected grids. The power transmission networks are physically inter-connected; however, the electrical and financial energy markets are governed by independent system operators (ISOs) in different *markets*. Each ISO monitors (i.e., *operations* domain) and controls (i.e., *service provider* domain) its own region and only provides power flow information on tie-lines between other transmission regions. The existing cyber-architecture in the power grid provides limited information exchange among domain owners and ISOs due to energy market constraints and trust boundaries. This "closed" cyber-architecture leaves the power grid vulnerable to

* Corresponding author. Tel.: +1 775 784 4313.
E-mail addresses: mgunes@unr.edu (M.H. Gunes), yuksem@cse.unr.edu (M. Yuksel), hayreddi@buffalo.edu (H. Ceker).

http://dx.doi.org/10.1016/j.comnet.2015.05.004
1389-1286/

cascading events and makes it difficult to detect potential problems and can lead to catastrophic failures [1–3]. As emphasized in the NARC's report [1], one of the primary weaknesses in need of attention is *"communications within the ISO and with its neighboring control areas and reliability coordinators"*. Additionally, potential coordinated attacks on these systems require the infrastructures to be more automated and self-healing [4]. As the power grid becomes more dynamic with renewable resources that provides intermittent energy, accurate monitoring and reporting is required [5–7]. The increased information sharing will thus enhance the adaptability of the power transmission grid with the proliferation of distributed renewable energy generation.

Such inter- and intra-ISO communication capabilities necessitate mechanisms to securely and efficiently exchange sensitive data for system modeling and monitoring. In order to protect both the electric utility and the user against adversaries including malicious users or external cyber attackers, we need to enhance the privacy of the user and ensure the integrity of the communication. We propose a system model that creates a symbiotic relationship between all actors within the power grid using *blind processing* [8]. In our "open cyber architecture" model, sensitive data will be transmitted through the secured channel and used in computations running in an isolated environment while the outcome will be rendered only to a dedicated user or process. Traditionally, security mechanisms are deployed to protect the transmission channel and the execution environment from third parties based on the security requirements of the data. In *blind processing*, we establish a secure channel between trusted processes which are concealed from the rest of the system, including the root processes [6].

At the *transmission level*, we propose development of an "open cyber architecture" where information sharing is the norm for ISO operations. However, such openness requires handling of various market and trust conflicts. In order to achieve open communications and promote information sharing, we develop *blind processing* service that provides authentication, privacy, and integrity assurances. Blind processing will enable the advantages of additional information exchange while respecting electrical energy market constraints and trust boundaries over the operation of the power grid infrastructure.

At the *distribution level*, we aim to revolutionize the relationship between the utility and customers via privacy protecting smart meters. The utility will be able to monitor the electricity consumption of the customer in a more detailed manner while the customers can be well informed with the cost and the amount of energy they are consuming. Secure communication can also help the utilities to inform their customers of price change during peak consumption times. Moreover, power generated at home (by solar panels, wind turbines, etc.) will better be integrated to the system.

Contributions of this paper are in two directions (i) *open cyber architecture* in Section 2 (we provide an assessment of open versus closed cyber architecture in Section 2.1 and discuss issues in the power grid communications in Section 2.2) and (ii) *blind processing prototype* in Section 3 (we provide a prototype for blind processing systems that will enable increased information sharing in an open manner by power operators in Section 3.1, and then analyze performance overhead in Section 3.2 and security issues in Section 3.3). We conclude the paper in Section 4.

2. Information sharing via open cyber-architecture

The main goal of proposed open cyber-architecture is to enhance reliability and efficiency of the large-scale multi-owner power grid infrastructure. The existing systems typically use a centralized cyber-architecture and strictly hide proprietary information from other owners. Though a "closed" approach (as in Fig. 1) hiding proprietary information makes sense in terms of business goals, the technical viability of the overall system depends on safe and sufficient sharing of basic technical information in a relatively "open" manner (as in Fig. 2). Information sharing among owners is critical to attain the needed robustness for power grid. A key proposition is to increase information sharing through more regulated means and essentially make it part of the physical system itself even to the extent that the owners may not be able to avoid sharing of some of the market related information.

The basic idea of sharing crucial information has successfully been implemented in some large-scale systems. For instance, the Internet requires its participants to provide basic connectivity information. Otherwise, the participant cannot be part of the connected network. This implicit reinforcement of information sharing is mainly driven by the "fate sharing" that naturally exists in the overall system. Participants become willing to share the information (and potentially other resources) in order to make "the whole ship float". Through trusted computing mechanisms, we aim to extend this paradigm to power grid communication infrastructure.

We abstract components of "open" communication as follows:

- **Integrated secure communication:** In order to provide means to share information, subsystems (or components) of the power grid must have secure communication capabilities integrated with the physical substrate.
- **Self-healing via automated control:** Usage of the shared information must respect the market rules and policies set forth by the domain owners. Thus, components must control the underlying systems based on domain owners' desires. Further, the system should be automated and reduce dependency on humans to resolve crisis situations. This is critical since the time required to respond to a crisis is mostly much shorter than human operation timescales.
- **Distributed planning via smart subsystems:** Since robustness of the power grid is crucial, individual components must have the planning and learning capability to be ready for unexpected events.

At transport layer, we can utilize *data aggregation* mechanisms [9,10] to minimize grid management overhead due to small-sized periodic grid measurement data as in Fig. 3. Providing GPRS/WiMAX capability for every smart meter is not cost-effective as WiFi technology is much cheaper to operate than GPRS/WiMAX. Additionally, we need to filter some of the critical proprietary information from other domains and data aggregation help enhancing data privacy.