A Smart Grid Security Architecture for Wireless Advanced Metering Infrastructure (AMI)

Aftab Ahmad, John Jay College of Criminal Justice, City University of New York (CUNY), New York, NY, USA

ABSTRACT

The authors present a protocol and security architecture for the smart grid in an advanced metering infrastructure (AMI). Various levels of the hierarchical grid are isolated in protocol planes for preventing propagation of attacks. The utility meters are interconnected via the wireless technologies in order for metering functions, as well as location identification and reporting for attackers. An amended version of Bell Labs security framework (aka, ITU-X.805) protects every component with added first response security apparatus, forensic component and a location determination algorithm for fortifying the PHY of WLAN interconnecting the meters.

KEYWORDS

Advanced Metering Infrastructure, PHY, Smart Grid, Smart Meter, WLAN Attacks

1. INTRODUCTION

Advanced Metering Infrastructure (AMI) is set to meet multiple objectives for utility companies, regulatory agencies, government energy planners, and the consumers. There are challenges is every sectors but the gains outweigh the obstacles by a mile. In terms of technology, the advancements in IP-based networking have moved our goals of internet of things to wireless access for things, and AMI is no exception. Even though we have a wireless infrastructure that is as trust-worthy as it takes to be deployed in a classified environment (DoD, 2009), two issues remain unresolved for an infrastructure that can place a sensitive wireless device, such as a wireless smart meter, in the supervision of a common user. These are the physical layer being open to denial or service (DOS) attacks and the possibility of propagation of higher layer attacks to the energy grid with a potential nation-wide breakdown. In this position paper, we present a security architecture with these two challenges as the highest priority. The rest of the paper is organized as follows. In Section 2, we describe components of a wireless AMI. As we will see in this section, ‘wireless’ does not have to apply to the backbone grid. It really implies the link from a smart meter to utility network node being wireless. However, as we have shown in (Thomas, 2012), this is not sufficient. Multiple wireless interfaces may be needed to fortify the physical layer using mechanisms such as in (Cebula, 2011). In Section 3, we describe currently available proposals and frameworks for securing large infrastructures along with their strengths and weaknesses. These include the one proposed in (Cleveland, 2008), (NIST, 2014), (Cisco, 2009) and (ITU, 2003). In this section, we justify the need for a new security architecture that is proposed in Section 4. In Section 5, we discuss the tradeoffs for the proposed security architecture and its comparison with the existing solutions. We conclude in Section 6 followed by references in Section 7.
2. WIRELESS AMI

Figure 1 depicts one way to implement the Wireless AMI.

As seen from the figure, the grid consists of four hierarchies from the meters at the lowest level connected via three local network interfaces; the interface $I_{MM}$ between meters, $I_{MU}$ between meter and home appliances and $I_{UM}$ between the meter and the utility node. The same ‘multi-homing’ paradigm repeats up the hierarchy with the utility network nodes having additional interface $I_{UU}$ with each other and $I_{UG}$ with the local grid, the local grid nodes connected via interfaces $I_{GG}$ with each other and $I_{GG}$ with the main backbone grid (the National Grid). The national grid consists of segments, shown as $i$ and $j$ in figure that connect to each other via the common interfaces $I_{GG}$.

The interfaces $I_{MM}$, $I_{MU}$ and $I_{UM}$ are wireless in nature while the remaining interfaces could be wired or wireless. In a robust design keeping man-wrought and natural calamities in view, a wired interface at higher levels of the hierarchy will be well-supported by wireless standbys.

2.1. Protocol Architectures

In order to keep the focus of the discussion on the most vulnerable component of the hierarchy, the meter, we will discuss the protocol architectures for only the interfaces $I_{UM}$, $I_{MM}$ and $I_{MU}$. We dub these as utility network, smart meter network and home appliances network, respectively.

2.1.1. Utility network

The utility network consists of a high speed metropolitan area network that interconnects trusted utility nodes, with each utility node providing a wireless local area network (WLAN) service to the meters in a neighborhood. Thus, $I_{UM}$ will be a high-speed WLAN, such as IEEE 802.11.

The $I_{UU}$ could be based on optical fiber with a backup provided by IEEE 802.16 or similar. Figure 2 (a) and (b) show these interfaces.
E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems
[www.igi-global.com/article/voting-risk-assessment/58980?camid=4v1a](www.igi-global.com/article/voting-risk-assessment/58980?camid=4v1a)

Scanning and Enumeration Phase
(2019). *Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention* (pp. 149-177).
[www.igi-global.com/chapter/scanning-and-enumeration-phase/218418?camid=4v1a](www.igi-global.com/chapter/scanning-and-enumeration-phase/218418?camid=4v1a)