Security analysis of Smart Grids

Joaquín Márquez Gabriel Rodríguez Gustavo Betarte Juan Diego Campo
Eduardo Grampín

Universidad de la República

Abstract

The benefits of Smart Grids are beyond doubt. However, thinking of a future where Smart Meters are ubiquitous raises a lot of concerns regarding security and privacy. Some of these concerns include the disclosure of the personal information of consumers, the provision of false consumption data to the utility, or even concerns of national security such as attacks to attempt to bring down parts of the grid or even the whole grid. The goal of our investigation is to identify and develop methodological proceedings and technical tools which aid in providing guarantees of the correctness of the adopted solutions for the design and implementation of a Smart Grid, in particular in relation with the security properties which must be guaranteed by those solutions.

1 Introduction

The deployment of Smart Grids has become a matter of great interest throughout the world, with some countries heavily investing in research regarding this topic due to all the benefits they could potentially provide to both Electric Utility Companies and their customers. The key feature of this type of system is the provision of near real-time information regarding the energy consumption in order to help in balancing its generation and distribution according to the demand and also to help the customers in dynamically adapting their consumption behavior.

Our investigation is framed within a collaboration between the Engineering School of the Universidad de la República(UdelaR) and UTE, the public electric utility company of Uruguay. This collaboration aims to identify and develop methodological proceedings and technical tools which aid in providing guarantees of the correctness of the adopted solutions for the design and implementation of a Smart Grid, in particular in relation with the security properties which must be guaranteed by those solutions. In this context our investigation aims mainly to contribute in the development of a threat model and in defining preventive and reactive measures to diminish the impact of the exploitation of those vulnerabilities.

We are still in an early stage of the investigation, studying the state of the art of Smart Grids and Smart Meters, with an emphasis on investigating the security issues in the context of an Advanced Metering Infrastructure (AMI).

2 Advanced Metering Infrastructure (AMI)

Usually, the network of transmission lines, substations, transformers and more that deliver electricity is known as the electric grid. An smart grid is the result of the integration between a grid and digital technology in order to provide the grid with more capabilities that optimize its operations.

In: Proceedings of the IV School of Systems and Networks (SSN 2018), Valdivia, Chile, October 29-31, 2018. Published at http://ceur-ws.org

In this context, an Advanced Metering Infrastructure is a crucial component of a smart grid, which handles the two way communication between smart meters and data management systems, allowing to send, receive and process consumption data of the clients, and also additional operations over the network.

The most common architecture used to address the features of smart metering systems is presented in the following diagram [Pop14]. It consists of:

- Smart meters (SM): local electronic meters
- Data concentrators (DC): process data from several meters
- Head End System (HES): central data collection point
- Local area network (HAN, NAN): allows bi-directional communication between the smart meters and a data concentrator
- Wide area network (WAN): allows bi-directional communication between the data concentrators and the head end system

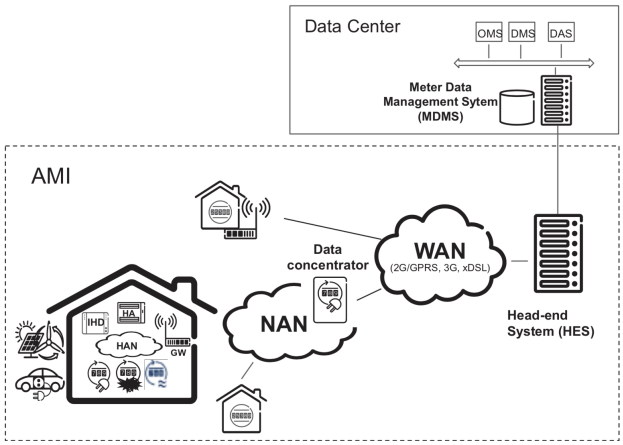

Figure 1: Example of AMI architecture [Pop14]

3 Security Concerns in Advance Metering Infrastructures

As with any communication network there are many security concerns that must be taken into consideration. Some of the possible attacks include[Ur-Reh15]:

1. *Eavesdropping*
   Resulting in the disclosure of personal information from costumers. It has been shown that a very accurate user profile can be extrapolated from the collected data [Mol10].
2. *Denial of Service attacks*
   With the purpose of shutting down parts of the grid or even the whole grid.
3. *Packet injection attacks*
   For example providing false billing information, generating costs for the customers or the utilities.
4. *Malware injection attacks*
   Affecting the communication between devices with the goal of compromising the billing and reporting process, disrupting the Demand/Consumption information affecting the load on the grid.
5. *Remote Connect/ Disconnect*
   Potentially leaving users without access to the service.
6. *Firmware manipulation*
   For example with the intention of manipulating the metering functionality to report false consumption data.
7. *Man-in-the-middle attacks*
   With the goal of providing false consumption information to the gateway or to send commands to the Smart Meters, potentially bringing down the whole grid.

The consequences of such attacks range from the disclosure of information affecting the privacy of customers, which can have legal consequences to utilities, to concerns of national security.

4 Security Countermeasures

Different countermeasures can be used to address the concerns presented in the previous section. Many of them may be familiar to the reader, as they are commonly used in general purpose networks.

1. *Encrypted Communication*
   Dual encryption is recommended, encrypting at the application layer to ensure end-to-end encryption and at the transport layer using existing protocols such as TLS.

2. *Integrity Protection*
   Integrity protection, such as using message authentication codes (MAC) to assure the integrity of the transmitted consumption data, is vital in the context of smart grids.

3. *Authenticity Verification*
   Standard approaches can be used, such as digital signatures.

4. *Gateway based Approach*
   This is a novel approach, proposed by European countries, such as Germany and the UK. It consists of having a Smart Metering Gateway to act as an intermediary in the communication between the Smart Meters installed in the customer's premises and the utility. The gateway receives the consumption measurements from the meters and communicates periodically, after a set interval, with the utility servers to send this data, being responsible of ensuring the privacy of the customer. Also, the gateway receives commands from the utility servers, such as instructions to act based on the load on the grid.

5. *Intrusion Detection and Prevention Systems*
   This type of systems help in the identification of intrusions, detection of rogue nodes and source of attacks and exclusion of these nodes from further communication in the network.

Apart from the presented countermeasures a security by design approach is worth taking into account[Ur-Reh15].

5 Conclusions

An introduction to our investigation was presented in this summary. Initial considerations on AMI and security were described as starting points on our research.

This topic has been proven of great importance nowadays, especially when security threats could have a wide range of unwanted consequences, where even national security is at risk.

We plan to continue this path, analyzing the security concerns in depth, reviewing the protocols involved and trying to propose security countermeasures specifically designed for the particular needs of UTE.

6 References

[Ur-Reh15] O. Ur-Rehman, N. Zivic and C. Ruland, "Security issues in smart metering systems," 2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2015.

[Pop14] Z. Popovic and V. Cackovic, "Advanced Metering Infrastructure in the context of Smart Grids," 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, 2014, pp. 1509-1514.

[Mol10] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smartmeter. In: Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, Zurich. ACM (2010).