SMART METER: APPLICATIONS, SECURITY ISSUES AND CHALLENGES

Imen Aouini[1] and Lamia Ben Azzouz[2]

[1,2]University of Manouba, ENSI CRISTAL Laboratory, Tunisia
[1]imen.aouini@ensi-uma.tn; [2]lamia.benazzouz@ensi.rnu.tn

ABSTRACT. The smart meter is an important intelligent device on the Smart Grid that has the capability to report information related to power consumption, billing and other significant readings. The protection of smart meter communications against attacks is essential to ensure reliable operations of the Smart Grid. In this paper, we give an overview of smart meter applications, and we discuss the security issues and attacks that can be performed on the smart meter and that may have severe impacts on the global Smart Grid network.

Keywords: smart grid, smart meter, home area network (HAN), neighborhood area network (NAN), security

INTRODUCTION

The Smart Grid is an intelligent electric network that aims to improve the current energy delivery in terms of efficiency, reliability and economics. It remotely and rapidly repairs faults, maintains and restores stability for more reliable delivery of the electric power. Also, it permits a flexible usage of renewable energy resources. Moreover, it allows customers to reduce and manage their energy consumption based on their own preferences. In order to harmonize Smart Grid architectures, the National Institute of Standards and Technologies (NIST) issued an architecture that defines heterogeneous systems and devices over various domains: Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Provider (National Institute of Standards and Technology, 2010). To adapt this architecture to the European model of the electrical grid, IEEE introduced a new domain called distributed energy resources that provide the capability to control and monitor the distributed energy resources. Furthermore, the IEEE established the standard 2030-2011that defines the Smart Grid Interoperability References Model (SGIRM) (IEEE Standards Coordinating Committee, 2011). This model defines a set of networks that allows domains to communicate. The Home Area Network (HAN) allows the communication of smart meter and intelligent devices such as thermostats, lighting for energy management. The Neighborhood Area Network (NAN) involves neighboring meters as relays if no direct uplink exists to a concentrator node that collect periodic information of HAN such as price information, energy consumption. The Field Area Network (FAN) contains the communication of a large number of Intelligent Electronic Devices IED devices (Feeder, switcher, closer, transformer) (Skopik, Ma, Bleier, & Grüneis., 2012). The Wide Area Network (WAN) connects concentrators and substations to the operation domain (Kuzlu, Pipattanasomporn, Rahman, 2014). The Smart Grid introduces new security issues due to architecture characteristics and the critical nature of applications in terms of delay, sensitive and personal data exchanged. Many works in the literature showed that several attacks can be performed on devices and systems involved in the Smart Grid (Wang & Lu, 2013; Aloul, Al-Ali, Al-Dalky, Al-Mardini, El-Hajj, 2012; Skopik et al., 2012). The NIST report7628 (The Smart Grid Interoperability Panel, 2011) identified the impact level (low, moderate or high) of security requirements (confidentiality, integrity and availability) for Smart Grid communications. In the customer's domain, a fundamental device called smart meter is connected to the control center and allows the remote collection of metering readings. In addition, it is able to balance the usage of energy inside home in order to avoid energy peaks and it allows consumers to adapt their energy use in line based on accurate information and cut down on energy waste to provide financial savings. Few works in the literature were interested on the security issues of the smart meter. Works of (Aloul et al., 2012; Sophia, Sekercioglu & Ahmet, 2012; Temple, Binbin & Nils-Ole, 2013; Namboodiri, Aravinthan, Mohapatra, Karimi, & Jewell, 2013; Skopik et al., 2012) identified some attacks on smart meter and showed that attacks against this device can have several impacts on the electricity grid. Identifying smart meter applications and the data flow exchanged can constitute a good starting point to study the security of this critical device. In this paper, we discuss security issues of the smart meter. We first present an overview of Smart meter applications and data exchanged by the smart meter with several devices and systems. In a second section, we present an overview of works dealing with the smart meter security issues. Then we identify and classify additional attacks that can be performed on the smart meter. A conclusion addresses the smart meter security challenges and future works.

SMART METER: APPLICATIONS AND DATA FLOW

We give, in this section, an overview of smart meter applications and the data flow.

Smart home applications

Automated Control of Home Appliances (ACHA): the energy management in HAN is performed by the smart meter to balance loads between home devices over time and avoid overloading (Ahmad, 2011). For example, the smart meter allows the charging of an Electronic Vehicle (EV) only when energy consumption is low. The smart meter takes the decision to turn on a device depending on dynamic pricing and energy availability.

Management of Energy Storage (MES): Energy can be stored in storage sources and delivered to the electrical grid when it is required (Kenneth, Budka Jayant & Thottan, 2014). For example, vehicle batteries can be used to store energy when prices are low and sell it back to the grid when prices are higher.

Smart meter control applications

Automated Meter Reading (AMR): The smart Meter provides energy measurement (consumption amounts, time of consumption, devices, energy of renewable resources…) and automatic remote data in a regular interval (between 5 to 15 minutes) to the control center (Kenneth et al., 2014).

Pricing and Billing Services *(PBS):* Distributed utilities communicate frequently electricity prices to smart meters. Therefore, customers can use electronic devices that need large loads (e.g. Electronic vehicle, stove, and washer) when power supply costs are relatively low. Furthermore, the control center is able to disconnect the smart meter from the electricity network when a customer does not pay the electricity bill.

Outage Detection (OD): By gathering data and outage notifications from smart meters, the Outage Management System (OMS) can quickly analyses and determines if an outage is within the private residence or not. This is will reduce outage times and costs.

Smart meter distribution applications

Demand Response (DR): the demand response application helps to improve the balance between energy supply and demand on the distribution grid (Romer, Reichhart, Kranz, & Picot, 2012; Kenneth et al., 2014). For that, the distribution substation can request from smart meters in a district to reduce energy consumption by shutting down some home electronic devices to reduce peak power.

Electronic Vehicle Charging (EVC): The Electronic Vehicle Supply Equipment (EVSE) can interact with the smart meter over NAN to allow EV charging at public charging stations.

Renewable Energy Production (REP): when the home distributed energy resource generates more electricity than usual consumer needs, the electricity goes into the electric grid to be used elsewhere. The power provider generally pays the producer for the renewable electricity.

Smart meter data flow

Some works in the literature (IEEE Standards Coordinating Committee, 2011; Namboodiri, Aravinthan, Mohapatra, Karimi, Jewell, 2013) identified data exchanged between Smart Grid elements. We classified smart meter data flow in seven groups as shown in Table 1.

Table1. Smart meter data flow

	Group	Interfaces	Data
Smart meter	G1	Neighbors meters	Meter reading, Pricing data, Billing,
	G2	Concentrators/aggregator	Metering reading, voltage,
	G3	Home Appliance	Energy management,Devices control
	G4	Plug-in Electronic vehicles	Load shedding, Storage, Positioning
	G5	Distributed Energy Resources	Generation, storage,
	G6	Workforce Mobile	Geographic position, maintenance
	G7	Internet	Energy profile, billing

Each group (G) represents data exchanged through a specific smart meter interface (see Table1). The group G1 represents communications of smart meter with his neighbors' meters. The smart meter sends over a neighbor's meter a set of information to the concentrator (G2). Several types of data (Time of use, energy consumption…) are exchanged between the smart meter and home devices (G3). Authors of (Namboodiri, et al, 2013) showed that home appliances can be classified into four groups. Group 1 contains devices (e.g. Television, refrigerator) that need to inform the smart meter only when they are connected and disconnected from the system. Devices in group 2 (e.g. Stove) will need to send its power usage and expected duration of usage whenever possible. Group 3 contains devices (e.g. Air-conditioner and washer/dryer) that request the smart meter and wait for its acceptance to be switched on. Electronic vehicles are classified in group 4 due to the expensive load and need timely and adequate control. The smart meter communicates with the electronic vehicle (G4) when it is plugged into an on-site charging station. Distributed energy Resources (DER) communicates with the smart meter (G5) in order to use energy of this type of resources. Workforce mobile access the smart meter (G6) and provide faster diagnosis and performs repair work. The smart meter uses the Internet connection (G7) as the home to communicate with the service provider.

RELATED WORKS

Some works in the literature identified threats and attacks that can be performed on smart meters. Some of them focused on networks where the smart meter is involved while others studied its interactions with devices and systems in various domains. Works in (Namboodiri, et al, 2013; Sophia et al., 2012) give a survey of smart meter security problems and challenges. Authors of (Namboodiri, et al, 2013) focused on HAN scenarios and identified four types of attacks (Jamming, replay, non-repudiation and equipment impersonation attacks). For example, the smart meter cannot responds to electronic devices commands when an attacker performs a jamming attack on the shared medium. It can also act inappropriately or disrupts critical home appliance (e.g. Switches on/off devices) when it responds to a false or replayed requests. Authors of (Wang, Xu, & Khanna, 2011) pointed also that attackers can manipulate smart meter hardware and firmware. For example, an attacker can stop meter reading by shielding the antenna of the wireless module of the smart meter. Works on (Sophia et al., 2012; Wang et al, 2012) describes several attacks that can be launched on the NAN network and may affect routing protocols (NAN sniffing, black hole attack, spoofing data). For example, an attacker can claim having a nearest path to the concentrator node and then he can drop or alter all incoming packets while the network cannot guarantee that it has transferred the original packet. Authors of (Kenneth et al., 2014; Efthymiou & Kalogridis, 2010) addressed the privacy problem for smart meters. The smart meter data can be manipulated by a malicious node to get personal and critical information such as when customers are at home which could be inferred from energy consumption information. Authors of (Mohassel, Fung, Mohammadi, & Raahemifar, 2014) give a survey of security challenges of the Advanced Metering Infrastructure (AMI) system. This infrastructure includes smart meters, communication networks and Meter Data Management Systems (MDMS) and allows collecting metering data. Once an attacker has access to the AMI data, he will also have access to information collected for billing purposes. Authors of (Temple et al., 2013) showed that attackers may use the Remote Connect Disconnect (RCD) commands to cause a widespread blackout. This attack may simplify the access of criminals to homes.

ATTACKS ON SMART METERING

In this section, we highlight additional attacks that can be performed on the smart meter and we define five clusters of attacks having different kinds of impacts as shown in Table 2.

Table 2. Attacks on Smart meters

Cluster (C)	Attacks
Energy management (C1)	Forgery, Replay, Spoofing, Jamming
Customer benefits (C2)	Forgery, Spoofing, Dropping, Denial of Service
Financial gains (C3)	Spoofing, Impersonation for billing energy, Forgery and replay
Routing Data (C4)	Modification and black forwarding

Privacy (C5)	Eavesdropping, tracking

Attacks impacting energy management

Forgery attacks*:* Sending false messages to inform the smart meter that a device is connected could lead the smart meter to take the decision to stop other home devices or prevent some devices turning on while energy is available. For example an attacker sends a false request to the smart meter to turn on the air conditioning. In order to balance the energy in the home and avoid the overloading, the smart meter switches off the charging of the electronic vehicle. Distributed energy resources (DER) inform the smart meter about the amount of energy generated that can be used to satisfy an increase home demand. An attacker can send false information about the energy generated by DER. If the quantity announced is bigger than the energy produced by DER, the smart meter uses the energy of the storage station and then it could not respond to the home energy demands. Moreover, the control center can remote disconnect the smart meter when a customer did not pay energy bills or for a remote maintenance work. An attacker can exploit these kinds of commands to stop the smart meter and prevent home appliance from energy. This attack can have a serious impact if it is performed against a smart meter of a critical Building (hospital, police station….) or performed on a large scale to disconnect all meters of a district. Additionally, the outage management system can send to the smart meter outage notifications to reduce energy consumption. An attacker can send a false outage notification, so the smart meter stops some devices at home while energy consumption is low.

Replay attacks: many commands and messages can fall into replay attacks and therefore affect the delivery of energy. In HAN, attackers can replay messages of home devices as a result some devices can shutdowns. For example, if an attacker replays a request of an electronic vehicle that need to be charged at home, the smart meter turn of other home devices to reduce energy consumption and avoid an overloading while the Plug-in Electronic Vehicle (PEV) is not connected. Additionally, replaying commands of control center can affect the delivery of energy. For example, to disconnect a smart meter from the energy network, an attacker can replay an old disconnect command.

Spoofing attacks: when an attacker spoofs the identity of a smart meter, smart appliances send requests to the hacker and may not have responses. Appliances that wait for the response of the smart meter such as air conditioning, electronic vehicles cannot turn on. The attacker that spoofed the smart meter identity can communicate with distributed substation and regulate energy voltage. As a result, the energy delivered into home will not be conformed to as devices demands. Moreover, the smart meter communicates with distribution substation to buy energy generated by DER. An attacker that has the identity of the smart meter can inform distribution substation that it has energy at storage stations. Therefore, the distribution substation purchases energy and delivered it elsewhere yet the victim smart meter needs this quantity of energy to satisfy energy demands at home.

Jamming attacks: when an attacker launches a jamming attack on the smart meter, he prevents it to send home energy demands to distribution substations. So, home devices could only work according to the energy available in a period where energy consumption was low.

Attacks impacting customer benefits

Forgery attacks: When a hacker sends a false dynamic pricing, it will make the smart meter turn on several electronic devices as well as the electronic vehicle while price is height and increase the customer's energy bill. An attacker can send a false quantity of energy generated by DER. When the quantity announced of energy is not sufficient for home energy needs, the smart meter will use the energy provided by the distribution network that is more expensive.

Spoofing attacks: A malicious node can spoof the identity of a legitimate smart meter in order to modify meter reading. As a result, the energy bill will not correspond to customer energy consumption. When an attacker spoof identity of a legitimate smart meter, it can send false position to workforce and it will not be able to reach the smart meter for repair work.

Dropping attacks: The attacker drops the pricing packets, so the smart meter cannot be informed by the variation of electricity prices. The smart meter stays using a large quantity of energy while the price of energy was increased.

Denial of service attacks: An attacker can perform a denial of service attack by continuously sending a large number of metering requests (outage information, metering reading…). This can result a prevent communicating to the smart meter.

Attacks to get financial benefits

Spoofing attacks: The electronic vehicle communicates with the smart meter in order to charge its battery using public charging stations. Malicious node can use the identity of an electronic vehicle to benefices of charging without be billed consumption on his associated smart meter.

Impersonation for billing energy: A malicious node can send energy consumption with false smart meter identity. In this case, a hacker gains the use of energy without billed it. However, the smart meter victim has an increased electricity bill.

***Forgery and replay attacks**:* Customers that do not pay their electricity bills can forge remote connect commands to be reconnected to the electricity network. In other hand, to benefice of energy for some time without paying a bill, the hacker can replay old messages of reconnect smart meter. An attacker can forge or replay message to tell substation that he will deliver energy generated by Distributed Energy Resources into the electricity grid. However, he does not deliver any quantity of energy. So, the power provider pays the attacker producer for the renewable electricity that is not delivered into the grid.

Attacks impacting routing protocols

Modification and black forwarding attacks: A malicious node can spoof the identity of a smart meter and modify the data before forwarding it to the destination. In addition, an attacker can claim that he has the best route and concentrator even though it does not have any valid routes to the destination.

Attacks on privacy

Attackers can collect private information and extract movements inside the house. For example, determine which medical devices are used, when the TV has just been turned on, which kitchen device is operating. In addition, by eavesdropping meter readings, attackers can find out when someone is or not at home and how long he stays there. Moreover, an attacker can track your displacements and get access to your geographic positions from information sent by an electronic vehicle when it charges its battery at a public infrastructure.

SECURITY CHALLENGES AND FUTURE WORKS

Securing the Smart Grid, from the control center to the distributed substations, Intelligent Electronic Devices (IED) and even to customer meters, requires a global end-to-end security infrastructure. This infrastructure has to envisage security solutions for networks (HAN, NAN and FAN) and endpoints (Smart meters, IED, substations, control center) that tier network together. An end-to-end security architecture can be deployed by the provision of security mechanisms for wireless technologies of all smart grid networks. The Zigbee specification presents a number of security provisions for devices, but studying the performance of Zigbee security mechanisms for the HAN and NAN stays an open research topic. On the other hand, (CISCO, 2012) pointed out the use of IPsec protocol to provide an en-to-end security architecture for the Smart Grid network. In this case, a study of IPsec for Smart Grid networks has to be considered. The deployment of IPsec in the Smart Grid network may introduce some issues while Smart Grids present particular constraints (real-time data, delay…).

CONCLUSIONS

The Smart meter is an essential device of the Smart Grid that offers many kinds of applications. These applications aim to manage energy inside home, report significant energy information to the control center and provide the flexibility to use the renewable energy resource. The smart meter is vulnerable to many types of attacks (Eavesdropping, forgery, replay attack…). These attacks have many goals as impacting the energy flow, customer benefits, get financial gains and also obtain private information about customers. Communications of smart meter cross many domains and networks that use various communications technologies. To design security for the Smart Grid, it is important to study the deployment of an end-to-end security architecture.

REFERENCES

Ahmad, S., (2011). Smart Metering and Home Automation Solutions for the Next Decade. *International Conference on Emerging Trends in Networks and Computer Communications (ETNCC).*

Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*.

CISCO (2012). *Cisco and its affiliates; Cisco Connected Grid Security for Fiels Area Network* [Online]. Available:http://www.cisco.com/web/strategy/docs/energy/C11-696279-00_cgs_fan_white_paper.pdf.

Efthymiou, C. & Kalogridis, G. (2010). Smart Grid Privacy via Anonymization of Smart Metering Data. *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*.

IEEE Standards Coordinating Committee 21 (2011). *Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS)*, End-Use Applications, and Loads.

Kenneth, C., Budka Jayant, G., & Thottan, D.M. (2014). Communication Networks for Smart Grids Making Smart Grid Real. *Computer Communications and Networks*, 377.

Kuzlu, M., Pipattanasomporn, M., Rahman, S. (2014). Communication network requirements for major Smart Grid applications in HAN, NAN and WAN. *Computer Networks*, 67, 74–88.

Mohassel, R.R., Fung, A., Mohammadi, F., & Raahemifar, K., (2014). A survey on Advanced Metering Infrastructure. *Electrical Power and Energy Systems*, 63, 473–484.

Namboodiri, V., Aravinthan, V., Mohapatra, S., Karimi, B., & Jewell, W. (2013). Towards a Secure, Wireless-Based, Home Area Network for metering in Smart Grids. *Systems Journal*, 8(2).

National Institute of Standards and Technology (2010). *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0. January 2010

Romer, B., Reichhart, P., Kranz, J., & Picot, A. (2012). The role of smart metering and decentralized electricity storage for Smart Grids: The importance of positive externalities. *Energy Policy journal*, 486-495.

Skopik, F., Ma, Z., Bleier, T., & Grüneis, H. (2012). A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures. *International Journal of Smart Grid and Clean Energy*.

Sophia, K., Sekercioglu, & Ahmet. Y. (2012). Security and smart metering. *18th European Wireless Conference*.

Temple, W.G., Binbin, C., & Nils-Ole, T. (2013). Delay Makes a Difference: Smart Grid Resilience Under Remote Meter Disconnect Attack. *IEEE Smart Grid Comm Symposium-Smart Grid Cyber Security and Privacy*.

The Smart Grid Interoperability Panel (2011). *NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*.

Wang, W., & Lu, Z., (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57, 1344–1371

Wang, W., Xu, Y., & Khanna, M. (2011). A survey on the communication architectures in Smart Grid. *Computer Networks*, 55, 3604–3629.