Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 34 (2014) 532 – 537

Procedia Computer Science

International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA-2104)

Security Issues and Challenges for the IoT-based Smart Grid

Chakib BEKARA*

* *Centre de Développement des Technologies Avancés, Cité 20 Aout 1956, Baba Hassen, Alger, ALGERIA*

Abstract

Internet of Things (IoT) is the next step evolution of our today Internet, where any physical object/thing having/equipped with computation and communication capabilities could be seamlessly integrated, at different levels, to the Internet. The Smart Grid (SG), which is considered as one of the most critical Infrastructures, is defined as the classical power grid augmented with a large-scale ICT and renewable energy integration, can be seen as one of the largest IoT network. The SG will involve billions of smart objects/things: smart meters, smart appliances, sensors, actuators-cars, etc. in addition to several communication infrastructures whether public (most often) or private. However, security is seen as one of the major factors hampering the rapid and large scale adoption and deployment of both the IoT vision and the Smart Grid.

In this paper we investigate the security issues and challenges on the IoT-based SG, and define the major security services that we should consider when dealing with SG security

Selection and peer-review under responsibility of Conference Program Chairs

Keywords: Internet of Things, Smart Grid, Security, Cyber Physical Systems, Advanced Metering Infrastructure

1. Introduction

Internet of Things (IoT)[1] is a recent new concept, on which Internet evolves from connecting machines and peoples towards connecting (*smart*) *objects/things*. Thus, we can say that IoT communications is the evolution of M2M communications. According to Cisco, by 2020 there will be over 50 billion connected objects against a population of 7 billion[1]. An object can be *any* thing/device/entity equipped/embedded with computation, storage

* Corresponding author. Tel.: +213-6691-841-29; fax: +213-213-510-39.
E-mail address: cbekara@cdta.dz

Selection and peer-review under responsibility of Conference Program Chairs
doi:10.1016/j.procs.2014.07.064

and communication capabilities with *different capacities* (sensor, actuator, mobile phone, desktop, laptop, printer, car, fridge, oven, etc.). While smart objects are already connected through *proprietary non*-IP solutions in different applications (Zigbee, HART/ Wireless HART, Z-Wave, etc.) and at a *small* scale, IoT aims at connecting the objects at a *large* scale using *IP-based* solutions (IP, TCP/UDP, etc.), directly or through gateways if IP support is not possible, while allowing them to interact with any other communicating party on/over the Internet.

The Smart Grid (SG)[2], the intelligent power grid, could be seen as the largest instantiation of the IoT network in the next future[7]. The whole power grid chain, from the energy power plant generation to the final electricity consumers (houses, building, factories, public lightning, electric vehicles, smart appliances, etc.), including transmission and distribution power networks, will be filled with intelligence and two-way communication capabilities to monitor and control the power grid anywhere, at a fine granularity and a high accuracy. For instance, smart houses, will be equipped with smart meters and smart appliances, whereas power generators and electric transmission and distribution networks will be equipped with various sensors and actuators. The aim of the SG is to keep a *real-time balance* between energy generation and consumption, by allowing a fine-grained monitoring and control over the power chain, thanks to the huge number of the two-way communicating smart objects (smart meters, smart appliances, sensors, actuators, etc.)

While the use of IoT is very prominent in the context of the SG, it could also lead to disasters. Indeed, as a *critical infrastructure*, the SG will now be more attractive to *cyber-attacks*, since its monitoring and control could be done over standard internet-based protocols and solutions, and may rely on public communication infrastructure. As a consequence, an attacker could cause financial loses to the utility and make damage to the electric assets, by *breaking* the real-time balance between energy consumption/production, through manipulating data generated by the smart objects or sent from the utility.

In this paper, we investigate the security issues and challenges of the IoT-based SG. In section 2 we briefly describe IoT, SG and the link between them. In section 3 we investigate security issues and challenges in the IoT-based SG. In section 4 we consider the security services for the SG, and we conclude our work in section **5.**

2. Internet Of Things And Smart Grid

2.1. Internet of Things

The term IoT often makes reference to the integration of (*resource-constrained*) objects, such as sensors, actuators, RFID tags or any device involving a communicating interface and a computing capability, into the Internet. Objects of the physical world (fridge, window, heater, switch, washing-machine, etc.) could now be easily accessible, manageable and communicate through Internet using internet-based protocols (IPv6, UDP/TCP, HTTP, etc.). For the most resource-constrained devices, especially those compliant with the IEEE 802.15.4 standard, the IETF (Internet Engineering Task Forces), proposed several protocols for their *efficient* integration and at different layer to the Internet:

- *6LowPAN*[4]: IPv6 over Low Power Wireless Personal Area Networks, an adaptation layer to support the IPv6 protocol on IEEE 802.15.4 networks
- *RPL*[4] Routing Protocol for Low-Power and Lossy Networks
- *CoAP*[4]: Constrained Application Protocol, is a specialized web transfer protocol for use with constrained nodes and constrained networks

Even for those objects that still couldn't support IP natively, or updated to support it (due to extremely resources constraint or other considerations like preserving legacy systems), integration to the global Internet network is still possible through gateways, where proprietary non-IP stack protocols (Zigbee v1, HART, Z-Wave, etc.), are translated to/from IP stack protocols, but at a highly cost and without achieving and end-to-end communication.

2.2. Smart Grid

The SG can be seen, in its simple form, as the classical power grid augmented with the massive use of *ICT*

technologies (software, hardware, networks), in addition to the integration of distributed renewable energy generation and storage capacities[6]. As seen in Figure 1, in the SG there are two flows:

- ***Electric flow*** (dashed line) from the plant generation to the end customer, which is the main flow of the classical power grid. However, in the vision of the SG, the electric flow could be bidirectional, where the end-customer will buy and could also sell energy.
- ***Information flow*** (regular lines): A large-scale *two-way* communication flow between the different shareholder and components of the SG. Most of the communication flow is due to the massive use of sensors/actuators and other smart objects alongside the transmission and distribution areas, in addition to the use of smart meters and other smart objects (smart appliances, electric vehicles, etc.) at the end-customer side.

Figure 1 The Smart Grid Conceptual Model[2]

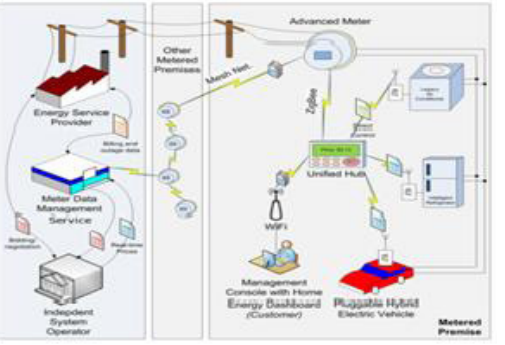

Figure 2 General View of The AMI[9]

The SG involves, amongst others, two key elements, which are Smart Meters and Advanced Metering Infrastructure:

- Smart/Advanced meters (SMs)[2], equip houses, factories, institutions, etc. (see Figure 2). They record energy consumption data and other information for billing or management purposes. They can report data periodically, upon request or in response to some events to the utility and also respond to *requests* from the utility (e.g., software update, real-time pricing, load shedding, energy cut-off, etc.), thanks to their two-way communication capability. They may optionally play the role of local energy management system, by controlling/managing the energy consumption of the smart devices on the house (fridge, oven, air-conditioner, electric cars, etc.)
- Advanced Metering Infrastructure (AMI)[9], as shown in Figure 2, is responsible for collecting, analysing, storing and providing the metering data sent by the SMs to the appropriate authorized parties (e.g., energy provider, utility, SG's operator, Meter Data Management Service, etc.), so they can proceed them (billing, outage management, demand forecasting, etc.). The AMI is also responsible for transmitting requests, commands, pricing-information and software updates from the authorized parties to the SMs. Figure1 presents a simplified view of the AMI as a part of the whole SG,

2.3. IoT-based SG

Compared to classical power grid, the SG highly integrates *ICT* on the whole energy chain (from producers to end-consumers), through the *large-scale* deployment of different kind of sensing, actuating and other embedded devices, in addition to the use of smart meters, smart appliances and e-cars, all of them sharing the capacities of *computing* and *communication*.

What has made Internet universally *popular* is the use of *standard* communication protocols, mainly the *TCP/IP stack*. Any two computers situated anywhere in the world, could easily have an *end-to-end communication*, regardless their access technology. IoT extends the *reachability* of Internet to reach, through standardized communication protocols (or a gateway in the extreme case), *everything* that could communicate and be individually

addressed. This copes with the *huge* number of *devices/objects* deployed on the SG and the crucial need of *near-real time communication* with them through unified standard-based communication protocols (based on the TCP/IP stack), rather than proprietary solutions (Zigbee v1, (W)HART, Z-Wave, etc.).

Assuming that the SG of a country involves *20 million* smart meters, in addition to *40 million sensors* and actuators deployed to monitor the whole power grid infrastructure. For the SG's operator, it will be interesting to remotely manage and configure the smart meters and the sensors/actuators– regardless their manufacturer- in addition to get information on the last mile grid's status. For the energy providers, it will be interesting to get remotely energy consumption from SMs in-order to accurately bill the customers, in addition to detect attempts of tampering with the SMs (ex, energy theft). For the end-user, it will be also interesting to get up-to date prices (assuming dynamic pricing), to well manage its consumption, in addition to get early alerts about planed disconnection. Obviously, all these bidirectional *end-to-end* interactions and communications, will highly benefit from *IP based communication protocols* (unless it is impossible or not appropriate), and even *public communication infrastructures* to make them easily scalable and to make induced costs lower.

3. IoT-based Smart Grid's Security Issues And Challenges

The added *ICT* dimension to the classical power grid, introduced new *security issues and challenges* that were *not* (or rarely) *present* on the classical power grid. Those security issues and challenges could hamper the rapid deployment and adoption by end-users of the IoT-based SG. Hereafter, we briefly describe the most important security issues and challenges faced on the IoT-based SG.

3.1. Security Issues

As a cyber-physical system, the IoT-based SG will face several security issues:

- ***Impersonation*/Identity *Spoofing*:** This attack aims at communicating *on behalf* of a legitimate *thing* in an unauthorized way, by making use of its identity. An attacker could spoof the identity of some one's smart Meter, in-order to make it paying for its energy consumption.
- ***Eavesdropping*:** Since objects/devices on the IoT-based SG communicate, often using public communication infrastructure, an attacker can easily have *access* to their exchanged data. An attacker can easily know the energy consumption of households
- ***Data tampering***: An attacker can *modify* exchanged data, such as dynamic prices sent prior to peak periods, making them lowest prices. As a consequence, this could make households increasing their consumption (charging e-cars, etc.) instead of reducing them, thus resulting in overloaded power network.
- ***Authorization and Control Access issues*:** Since several devices could be monitored and configured *remotely*, such as smart meters, or field deployed sensors and actuators in distribution substations, an attacker or even an angry employee, could try to gain an unauthorized access rights, to manipulate them, thus damaging physical assets (ex, transformers) or leading to power outages.
- ***Privacy issue*:** Smart meters and smart appliances in residential houses, could tell more than the energy consumption. Their generated fine-grained data could harm the privacy of the end-user, by divulging information about their habits (wake up, sleeping and dinner times, etc.), if they are in or away from house, if they are on vacation, etc.
- ***Compromising and Malicious code*:** Since objects of the SG are *computation* and *communication* enabled, they are target to compromising physically or remotely. Moreover, since they run different kind of software, they could be target of different kind of software infection or malicious code infection in-order to control and manipulate them (ex, targeting smart meters, or smart appliances in households). Moreover, massively deployed objects with constrained devices (sensors, etc.) are usually non-tamper-resistant devices, making physical compromising an easy task
- ***Availability and DoS issues*:** In the classical power grid, it was difficult, if not impossible, to target the *availability* of assets (electricity meters, substations, etc.), especially at a large scale. In the SG, ICT will be *integrated* even in the vital assets of the power grid, thus making it possible to target them, making them partially

or totally unavailable resulting on DoS attack. Moreover, assuming that most devices/things are IP-enabled and do not run proprietary protocols stacks, the task of a familiar Internet attacker will be easier.

- **Cyber-attack:** The SG could be seen as the largest Cyber-Physical-System (CPS)[6], involving Physical systems representing the physical assets of the SG (transformers, circuit breakers, smart meters, cables, etc.) and ICT systems, where ICT elements *control/manage* physical entities. Now, a Cyber-attack could harm the physical assets - as was the case with the *Stuxnet attack* [7]-, which was difficult in the classical power grid.

3.2. Security Challenges

When dealing with security algorithms, protocols and policies for the IoT-based SG, several challenges need to be taken into consideration:

- ***Scalability*:** The SG could span over large areas (several cities or the entire country), and involves a large number of smart devices and objects. This will make it difficult to conceive scalable security solutions, such as key management and authentication[5].
- ***Mobility*:** with mobile devices/objects, such as e-cars and on-the field technical agents, there will be a *continuous* need for authentication and secure communication with a changing surrounding (smart meters, electric charging stations, etc.).
- ***Deployment***: Since the SG could span to the entire country, objects/devices are deployed at a large scale, work unattended, and could be placed on remote places with no physical perimeter protection, making them easily accessible. Security solutions should be able to detect any attempt to tamper with them.
- ***Legacy systems***: Already deployed systems and devices, could have a little or no support for security, since they were based mostly on proprietary solutions (hardware and software), deployed on isolated islands with no communication, or through private communication infrastructure. Integrating those legacy systems to the IoT-based SG is a real challenge, since in most cases there is no way to replace them with new systems, or update them so they can support the desired security solutions.
- ***Constrained Resources*:** several devices/objects of the SG, especially those massively deployed are resource constrained. Special care need to be taken when developing security solutions, to be sure that their limited resources could accommodate the solutions. This make applying classical security solutions, especially those based on public-key cryptography or on PKI, a challenge.
- ***Heterogeneity*:** Due to the discrepancy on the resources of the devices/objects on the SG (memory, computation, bandwidth, energy autonomy, time-sensitivity, etc.), and their implemented protocols and communication stacks (for non IP-based devices) achieving secure end-to-end communications is a challenging task, requiring the most often adaptation of existing solutions or even using gateways.
- ***Interoperability*:** It could be seen as **o**ne of the consequences of protocols and communication stacks heterogeneity, between devices/objects in the SG. Legacy system and devices/objects that couldn‘t support TCP/IP stack (ex, Zigbee v1, HART) couldn’t communicate with IP-based systems and devices/objects, unless through gateways, making end-to-end secure communication impossible. Interoperability could also be seen between two devices implementing the same protocols and communication stacks, but different feature capabilities: one with fully support, the other with partial support (ex, DTLS with/without certificate support)
- ***Bootstrapping*:** How to efficiently bootstrap the millions of devices/objects of SG with the necessary initial keying materials (cryptographic keys, cryptographic functions/algorithms and parameters, etc.)?
- ***Trust Management*:** Objects/devices on the SG could be managed by different entities (end-users for smart appliances, SG’s operator for smart meters and sensors, etc.). Objects/devices couldn’t communicate if a minimal trust level isn’t established. While objects/devices owned/managed by the same entity could easily establish a trust relationship, building trust between objects/devices owned/managed by different entities is a challenge, especially in such large-scale network.
- ***Latency/Time Constraint***: Some parts of the SG need to respond on a *real-time* basis to *events* and *messages*. For instance, electric SCADA (Supervisory Control and Data Acquisition) system[8], used on transmission and distribution sub-stations, must respond on a real-time basis to any variation on current, voltage or frequency *values* of the electricity in addition to other meteorological parameters influencing equipment’s functioning all

provided by different kind of smart objects (sensors, actuators, etc. etc.), in-order to keep the assets safe and prevent the propagation of anomalies (power overload or outage) to other parts of the power grid. This makes time-consuming operations (i.e. public-key operations) not suitable.

4. Security Services for The IoT-Based Smart Grid

Hereafter, we briefly list the major security services that should be considered for the IoT-based SG:

- ***Authentication***: The capability to check/ensure the identity of any communicating device/object/ in the SG. For instance, the energy provider needs to authenticate each smart meter, in-order to bill the corresponding user.
- ***Data Integrity***: Ensures that (received) data were not modified in an unauthorized way. For instance, smart meters need to ensure the integrity of a software update, in addition to source origin.
- ***Confidentiality***: Ensures that data (stored or transmitted) is *accessible* only to the *intended* recipients. For instance, end-users' consumption need to be known by the SG's operator and the energy provider only.
- ***User's Privacy***: Guarantees that any data related to the user (energy consumer end-user) – brut, inferred or computed data- could not be obtained without its *explicit* approval, and will be used only for the intended purposes. For instance, energy consumption data used for billing purpose couldn't be used for other purposes
- ***Authorization and Control Access***: Guarantees that an authenticated object/person, is *authorized* to accomplish some tasks, or has been granted the necessary rights to access some resources. For Instance, an on-the field agent needs authorization and access control rights, to perform manual configuration on a smart meter.

5. Conclusion and Perspectives

Internet of Things, is the next step towards a globally and pervasive connection to any communication and computation enabled objects/devices, regardless their access technology, available resources and location. The Smart Grid can highly benefits from the IoT vision, where smart objects/devices are deployed alongside the energy path, from the generation plant to the end-customer. However, security is the main concern for the IoT, and the large-scale adoption and deployment of the SG.

In this paper, we briefly reviewed the main security issues and challenges for the SG, and dressed the major required security services. In the next future, we will study on-depth the security of a key-element of the SG, which is the AMI, where we focus on how we can securely integrate energy-aware smart home, equipped with smart meters and smart appliances, in the SG, so that end-customer could actively and securely participate in the energy consumption/production equilibrium.

6. References

1 D. Evans. "Internet of Things", Cisco, white paper, https://www.cisco.com/.../IoT_IBSG_0411FINAL.pdf (accessed on 5/02/2014)

2 NIST, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (last accessed April 10th, 2014)

3 O. Monnier. "Smarter grid with the Internet of Things", Texas Instrument, white paper, http://www.ti.com/lit/ml/slyb214/slyb214.pdf (accessed 05/02/2014)

4 Jurgen Schonwalder. "Internet of Things: 802.15.4, 6LoWPAN, RPL, COAP". http://www.utwente.nl/ewi/dacs/ Colloquium /archive 2010/ slides/2010-utwente-6lowpan-rpl-coap.pdf (last accessed April 10th, 2014)

5 C. Bekara, T. Luckenbach and K. Bekara. "A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service », 2nd IARIA ENERGY Conference, pp. 60-68, March 25-30, 2012, St Maarten, Netherlands Antilles.

6 J.E. Dagle. "Cyber-physical system security of smart grids". IEEE PES Innovative Smart Grid Technologies, pp. 1-2, Jan. 16-20 2012, Washington DC, USA

7 R. Langer. "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security&Privacy, Vol.9, N. 3, 20111

8 A. Sallam and O. Malik. "SCADA Systems and Smart Grid Vision". Book Chapter in "Electric Distribution System ", pp. 469-493, ISBN:9780470943854, 2011, Wiley-IEEE Press

9 AMI Security Lab, Illinois University, http://seclab.illinois.edu/ami-security (last accessed April, 10th, 2014)