Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities

Ismail Butun[1], Alexios Lekidis[2], and Daniel Ricardo dos Santos[3]
[1]*Chalmers University of Technology,* [2]*Eindhoven University of Technology,* [3]*Forescout Technologies*
ismail.butun@chalmers.se, a.lekidis@tue.nl, daniel.dossantos@forescout.com

Keywords: Smart Grid, Cybersecurity, Network Intrusion Detection, Advanced Metering Infrastructure

Abstract: Smart grids are a promising upgrade to legacy power grids due to enhanced cooperation of involved parties, such as consumers and utility providers. These newer grids improve the efficiency of electricity generation and distribution by leveraging communication networks to exchange information between those different parties. However, the increased connection and communication also expose the control networks of the power grid to the possibility of cyber-attacks. Therefore, research on cybersecurity for smart grids is crucial to ensure the safe operation of the power grid and to protect the privacy of consumers. In this paper, we investigate the security and privacy challenges of the smart grid; present current solutions to these challenges, especially in the light of intrusion detection systems; and discuss how future grids will create new opportunities for cybersecurity.

1 INTRODUCTION

Smart grids are electric power systems that provide automation, remote sensing, and remote control capabilities. They are a promising upgrade to legacy power grids due to enhanced cooperation of involved parties, such as consumers, utility providers, and distributed generators (Abdallah and Shen, 2018).

Smart grids improve electricity generation and distribution through optimization and projection of electricity consumption by leveraging communication networks to exchange information between those different parties. However, increased connection and communication also expose the control networks of the power grid to the possibility of cyber-attacks. At the same time, cyber-attacks on industrial networks are becoming more frequent and more critical. Therefore, research on cybersecurity for smart grids is crucial to ensure the safe operation of the power grid as well as to protect the privacy of consumers.

In this paper, we investigate the security and privacy challenges of the smart grid; present current solutions to these challenges, especially in the light of Intrusion Detection Systems (IDS); and discuss how future grids will create new opportunities for cybersecurity.

In particular, the following are the main contributions of this paper. In Section 2, we present the key points of smart grids: network architectures, use cases, and network communication protocols. In Section 3, we describe security and privacy issues in the smart grid. In Section 4, we discuss secure protocols, IDS, and privacy regulations as current solutions to the security and privacy challenges. In Section 5, we consider new opportunities for cybersecurity in future grids.

2 SMART GRIDS AND AMI

A smart grid consists of four segments: *Generation*, *Transmission*, *Distribution*, and *Consumption*. Each of these segments, especially the first three, relies on complex control signaling which is explained below.

The Generation control signals consist of 3 branches. (1) *Automatic Voltage Regulator*, where generator exciter control is used to improve power system stability by controlling the amount of reactive power being absorbed or injected into the system. (2) *Governor Control* is the primary frequency control mechanism that detects disturbances and accordingly alters settings to change the power output from a generator. (3) *Automatic Generation Control (AGC)* is a secondary frequency control loop that fine tunes the system frequency to its nominal value.

The Transmission control signals consist of 2 branches. (1) *State Estimation* estimates system variables, such as voltage, magnitude, and phase angle, by projecting faulty measurements from field devices. (2) *Volt-Ampere Reactive (VAR) Compensation* controls reactive power injection or absorption to improve the performance of transmission.

The Distribution control signals consist of 2 branches. (1) *Load Shedding* helps in preventing a system collapse during emergency operating conditions.

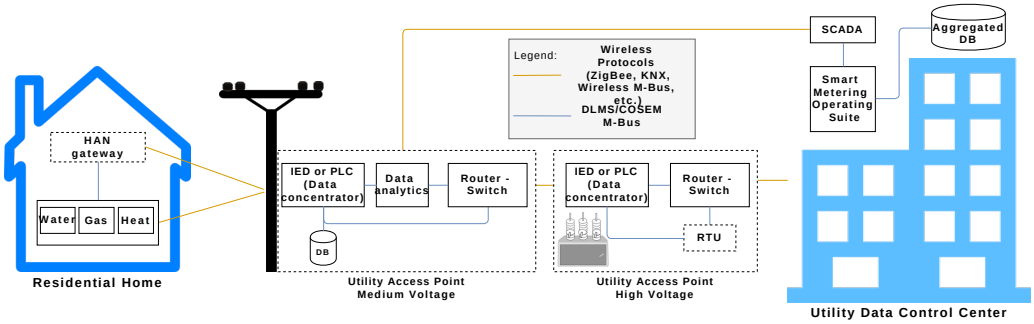

Figure 1: AMI architecture

These systems can be manual or use automatic relays. (2) the *Advanced Metering Infrastructure (AMI)* is responsible for collecting, measuring, and analyzing electric energy consumption data, as well as transmitting this data to a central collection facility. In a smart grid, the electricity usage of consumers is measured by an enhanced metering device (called a smart meter) that can transmit its measurement data to the operators via a network connection.

2.1 Architecture

Figure 1 presents the architecture of a smart grid, focusing on the AMI and its networking protocols.

In the *Residential Home*, a Home Area Network (HAN) connects smart meters and end-user applications in the same building to a local data collector and gateway between access and local network. This segment has a *HAN gateway* where the data of smart meters and other smart devices is centrally stored to be forwarded to a *Data Concentrator*. The HAN is optional, since many devices can directly connect to substations of the energy distribution company. In this segment, we can find the DLMS/COSEM (DLMS UA, 2019) protocol for configuring, reading information from, and writing information to smart meters. Many European meters also use M-Bus (EU, 2019) for meter reading, which is compatible with the DLMS/COSEM application layer and includes a radio-assisted extension, called Wireless M-Bus, to transmit meter data over GSM/GPRS interfaces.

The *Utility Access Point of Medium Voltage* represents a substation of the energy distribution company. It contains *Intelligent Electronic Devices* (IEDs) or *Programmable Logic Controllers* (PLCs), which are industrial computers that enable advanced power automation. These devices receive smart meter information via a wireless connection and serve as data concentrators by aggregating the data of multiple smart meters and storing them in dedicated databases. They then calculate actual energy consumption, based on the meter readings, and compare it to an estimated consumption associated with historical data for each house and climate conditions in the neighborhood. Both the actual and the estimated energy consumption are then forwarded to the next part of the AMI by a dedicated *Router*. These substations can also have a *Data Analytics* module to provide consumption reports to the operators.

The *Utility Access Point of High Voltage* also contains IEDs, PLCs and Routers to forward aggregated data to a centralized location of the electricity provider, called Utility Data Control Center.

The *Utility Data Control Center* is the management system of the energy distribution company, which has an overview of aggregated data from each consumer, as well as the center for utility and customer-related services through the *Smart Metering Operating Suite*. In this center, we can also find the *Supervisory Control and Data Acquisition* (SCADA) system that receives all the required analytics from the dedicated components of the Utility Access Point of Medium Voltage. The communication with the previous three segments was initially via the Power Line Communication (PLC) protocol (Galli et al., 2011), which relies on existing power lines to transmit data signals. But as the amount of data transferred increased exponentially over the last years, the PLC medium was found to be difficult and noisy, thus adding unpredictable delays to transmissions and disturbances. Additionally, in residential neighborhoods the average bandwidth is very low. Hence, wireless or cellular technologies started to be used in the communication with the Utility Access Point of Medium Voltage, especially ZigBee, KNX, and Wireless M-bus (Mahmood et al., 2015).

2.2 Use Cases

The AMI is the main enabler for the smart grid. Thus, we present below two use cases derived from (but not limited to) it.

Distribution. Smart meters can quickly notify electricity distributors if the power is out in a certain area, thus enabling early-stage fault identification and location. Problems can be located faster, repair crews

Figure 2: Distribution use case

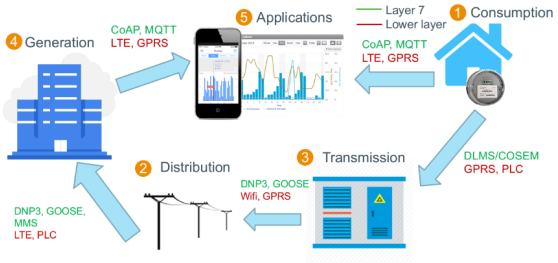

Figure 3: Billing use case

can be prioritized, and repairs can begin sooner. Customers can also receive information about outages in their area and estimated repair times.

Figure 2 depicts the distribution use case as follows. Power plants generate energy, which is transferred through poles and wires to substations. Substations use their transformers to reduce the voltage and distribute energy to neighborhoods. They also use data concentrators to estimate and forecast energy consumption based on historical data and environmental conditions. Finally, to perform more accurate estimations, concentrators may initiate read requests to the smart meters. Each step of the use case uses different protocols, shown in green (for application layer protocols) and red (for lower-layer protocols) in the Figure. The PLC and DLMS/COSEM protocols were presented above. LTE, WiFi, GPRS, and LoWPAN are lower-layer wireless protocols that are not the focus of our analysis; the interested reader is referred to (Mahmood et al., 2015) for details. DNP3, GOOSE, and MMS are application-layer protocols that will be described in details in Section 2.3 (GOOSE and MMS are mappings of the abstract data model defined in the IEC 61850 standard, which is detailed in that Section).

Billing. Billing is a use-case that directly leverages the collection of consumption profiles at customer households and the tariff data from the respective customer's contract to calculate a final electricity bill, thus allowing flexible pricing plans where the cost of electricity changes according to when it is used.

This use case is shown in Figure 3. Smart meters periodically record the consumption profile at the customer's household, which is transmitted via network packets to the data concentrators that are usually located in substations. Concentrators use the poles and wires to transmit the consumption profile to the utility control center. Energy providers use the consumption profile and their tariff rates to calculate the actual energy price that the customer must pay for the time period covered by the profile. Finally, the energy price along with energy analytics is made available to the consumer, who can compare it with statistics from other consumers and use it to manage more efficiently its energy consumption. As before, the communication protocols shown in the Figure will be explained in Section 2.3, with the exception of MQTT and CoAP, which are IoT protocols for data exchange between resource-constrained devices (Naik, 2017).

2.3 Communication Protocols

The control signals that enable the use cases discussed above are communicated in a smart grid via network protocols that have already been cited. In this Section, we describe in details the most important application-layer protocols used in a smart grid.

DLMS/COSEM. DLMS/COSEM (DLMS UA, 2019) is the de-facto standard for reading and configuring smart meters in Europe. The protocol is based on a common data model and application layer used over different communication media. DLMS/COSEM is a client-server protocol where the server is a meter and the client can be a gateway or central office. The standard specifies the data model and commands to control smart meters. The COSEM object model specifies the smart metering functions in different applications, e.g., Data storage, Access control and management, Time and event bound control, and Payment metering.

The DLMS/COSEM standard provides two security mechanisms: authentication (also called security level) and encryption (also called security suite). The two mechanisms often use the same keys, but they can be chosen independently of each other and can be used in any combination. The following authentication mechanisms exist: Lowest Level Security (0), where no authentication is used; Low Level Security (1), where only the client is authenticated using a plain text password; and High Level Security (> 1), where both client and server are authenticated. The cryptographic algorithm used for authentication depends on the HLS level (e.g., level 2 is for vendor-specific algorithm, whereas levels 3-7 are for MD5, SHA-1, GMAC, SHA-256, and ECDSA, respectively). The encryption mechanism is used to encrypt messages and add authentication tags to individual messages. The commonly implemented encryption mechanism in DLMS/COSEM is based on AES-GCM-128. It uses

the global unicast encryption key and, if available, the authentication key. Optionally, a client may send a so-called dedicated session key to the server during connection setup. The dedicated key is then used instead of the global encryption key for the remaining communication of this connection. The dedicated key is a temporary key that is usually generated ad-hoc at connection time.

M-Bus. M-Bus is based on the European standard EN 13757-2 (EU, 2019) for the remote reading of gas, electricity, and other meters. M-Bus is a binary protocol, where the commands are contained in so-called M-Bus telegrams. The protocol is based on a master/slave communication model and can be operated as a line, star or tree topology. The master powers the serial bus and processes the data of the M-Bus slaves (measurement devices). The main benefits of M-Bus are: a single bus cable connects all meters to a central system; bus nodes are supplied directly via the two-wire bus; and devices from different manufacturers can be connected to a bus system.

M-Bus does not define any transport or network layer protocol, but instead uses the application layer to define the messages that are exchanged in the Master-Slave architectural model. The architectural model can be either based on the EN 13757-3 (EU, 2019) standard or the DLMS/COSEM application layer. There are four types of messages in the data link layer and, depending on their type, some fields are vendor-specific.

M-Bus offers password authentication before sensitive commands are executed and EN 13575-4 (EU, 2019) introduced the use of AES encryption. A comprehensive security analysis of M-Bus was conducted in (Brunschwiler, 2013).

DNP3. Distributed Network Protocol-3 (DNP3) (IEEE, 2010) is a set of communication protocols used in process automation systems, especially utility distribution, such as electricity and water. The protocol was developed for communications between various types of data acquisition and control equipment, such as SCADA control centers, Remote Terminal Units (RTUs), and IEDs. Competing standards include the newer IEC 61850 protocol, discussed below.

IEC 61850. IEC 61850 is a standard defining communication protocols for IEDs at electrical substations, which is a part of the IEC TC 57 reference architecture for electric power systems. The abstract data models defined in IEC 61850 can be mapped to a number of protocols (TC57, 2019). IEC 61850 was intended to replace DNP3 in substation communications. However, current IEC 61850 is only limited within a power substation. It is projected that IEC 61850 would be used for outside substation communications as well in the near future (Wang and Lu, 2013).

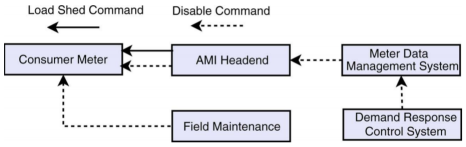

Figure 4: AMI control functions (Sridhar et al., 2011)

3 CHALLENGES

In cyber-physical systems, such as smart grids, the goal of cybersecurity is to protect the confidentiality, integrity, and availability of systems, information, and related assets, with privacy usually mentioned as an additional desirable property (Butun, 2017). In this Section, we discuss the challenges of protecting the security and privacy of smart grids.

3.1 Security

The security of an AMI is fundamental in the deployment of smart grids (Faisal et al., 2014). Figure 4 depicts AMI control functions that can halt the operation of a single smart meter or the whole network, depending on the source and type of the control signal. Therefore, these control signals should be secured to prevent malicious manipulation. Smart meters have three main types of interfaces on which attacks can be launched: optical, wireless, and cellular. Below, we describe potential attack scenarios on each interface.

Attacks via the optical interface. A smart meter's optical interface can be connected to a laptop through a dedicated cable connected to a dedicated port, which varies across different countries. An attacker can use specialized tools to analyze or set the values of a connected smart meter. By connecting a physical device (e.g., Raspberry Pi), a malicious actor can launch attacks to control different parts of the Residential Home. These attacks are feasible as a physical connection to the meter directly bypasses encryption. However, such attacks require physical access of a malicious actor to the residential home.

Attacks via wireless networks. A smart meter's wireless interface is used for periodic data collection to calculate daily energy consumption from each HAN. The periodic nature of data collection makes the packet flow on the network predictable. Thus, malicious actors can tamper with the normal behavior by, for instance, blocking the periodic transmissions. Wireless attacks can have an effect in the Residential Home, where a malicious actor needs to be in proximity (i.e. positioned in the neighborhood between the meter and the Utility Access Point). A potential scenario leveraging ZigBee is as follows. First, use radio jamming (Algin et al., 2017) over the ZigBee frequencies to jam the communication between the meter and the Util-

ity Access Point and wait for the users to re-pair the device. Then, eavesdrop the communication and navigate to the DLMS/COSEM part of a message (Kistler et al., 2009). From there, the attacker can, e.g., eavesdrop requests and send responses that disable power connection. Wireless attacks mostly affect the Residential Home or the Utility Access Point segments and they can have consequences on electricity, hardware, and data loss or leakage for the customers.

Attacks via cellular networks. Cellular attacks can be launched when having remote access to the Utility Access Point of Medium/High Voltage. In this scenario, a malicious actor needs to eavesdrop the GSM communication between the Utility Access Point and the Utility Data Control Center. This can happen as follows. First, the attacker can use a radio sniffer to listen to GSM traffic. If the data on this traffic is encrypted, the key can be recovered using the Barkan-Biham-Keller attack scheme (Barkan et al., 2008). Then, the attacker can connect to the RTU at the substation gateway and finally open the circuit breakers of the substation to stop power transmission. Alternatively, a malicious actor could rely on physical access of a utility access point. The utility access points may be accessed only occasionally by the utility operators and this increases their insecurity by making them vulnerable to malicious physical access, which would allow an attacker to connect to the RTU directly. These attacks target the Utility Access Point of Medium/High Voltage segment, but they have devastating economic consequences for the utility company as well as may cause data loss for its customers.

Other attacks. Traditional attack classes that can affect smart grids include Denial of Service, Replay, Brute forcing, Radio Jamming, and Identity Spoofing. The possible consequences of such attacks include: power outage, data leakage, bricked devices, loss of trust from customers and financial loss for utilities.

3.2 Privacy

Metering data can be privacy-sensitive, such as energy usage readings, or non-sensitive, such as voltage quality data and information about the meter itself. Utilities must protect the privacy of consumers by safekeeping this data. However, in the smart grid, consumers may have to share their data with their utilities, which in turn might share them with other entities that want to use them, such as advisory or insurance companies. This leads to data leakage issues. Below, we explain how data is shared in smart meters and how other data can be inferred.

Data from smart meters. Metering data can be accessed through four smart meter ports (P0-P3), as shown in Figure 5. P0 is used for local connection

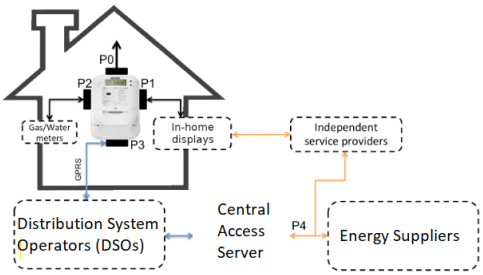

Figure 5: Smart meter ports that generate data

during installation and maintenance work. P1, also called the consumer port, allows for communication with third party equipment locally installed at the consumer's house. The port only supports communication from the meter to this equipment, not the other way around. Via P1, the meter provides real-time measurements in periodic intervals and it can be used to display messages on the connected equipment. P2 connects to other local metering equipment, e.g., water and gas meter. This port can be wired or wireless. Water and gas meters send their measurements to the electricity meter periodically and afterwards it can remain with the electricity meter or be forwarded. P3 communicates with the utility company to send meter readings, status checks, power quality and outage measurements, and remote updates. Unlike P1, P3 supports two-way communication. P3 energy data are not available in real-time. There is an additional P4 port that allows the utility company to provide metering information to third parties.

Data inference. Using the data transmitted by smart meters, there are two methods to infer more user data.

The first method, called Non-Intrusive Load Monitoring (NILM) (Lisovich et al., 2010), allows to infer information such as location and behavior of users (e.g., if they are at home), the amount of energy they consume, and the type of devices they own. NILM separates the energy data into categories, such as heating, appliances, entertainment, lighting, hot water, and cooking. Based on these categories, the utility company can use disaggregation techniques to infer details on the energy fingerprint of each appliance. Anyone who gets hold of this data gets a glimpse of what appliances are used and how often they are used. This allows to get details on the electricity consumption of an individual household or an entire neighborhood. NILM is successful in the HAN and small businesses because of the low event generation rate and number of loads at these sites. Larger commercial and industrial facilities require a more sophisticated approach, due in part to high rates of event generation, load balancing, and power factor correction.

The second method relies on the real-time monitor-

ing capabilities of energy consumption profiles from smartphone applications. This method can be used to infer total energy consumption data. Based on the total energy consumption data, an adversary may infer presence information i.e. if the consumer is at home. Nevertheless, it is difficult to derive energy consumption profiles for the house appliances, as this information is available from the utility company.

4 CURRENT SOLUTIONS

Cybersecurity systems should be layered and combine Prevention, Detection and Mitigation (Butun and Österberg, 2019). This Section discusses current solutions to the challenges presented in Section 3, especially in the form of secure communication protocols (for Prevention), network monitoring (for Detection) and privacy regulations (for Mitigation).

4.1 Secure Communication Protocols

Secure protocols are crucial to avoid remote attacks in smart grids. DNP3 and IEC 61850, presented in Section 2.3, did not have inherent security from the beginning. Therefore, Secure DNP3 and Secure IEC 61850 (known as IEC 62351) are proposed to achieve end-to-end security for smart grid communications by adding an extra layer in the protocol stacks called "Encryption and Authentication" in between the Application and Network layers. As discussed in Section 2.3, DLMS has defined a data protection security layer that provides encryption and authentication mechanisms.

4.2 Network Monitoring

Network monitoring should be in place to detect complex attacks. IDSs implement network monitoring and they can be classified into three categories according to their detection methodology: misuse-based (also called signature-based), specification-based, and anomaly-based. Signature-based detection is difficult to apply to smart grids, since their ever-growing threat surface requires a constant rule-set update. Specification-based IDS is also challenging due to the difficulty of deriving specifications for the dynamically changing smart grid architectures. Finally, anomaly-based IDS can, in principle, detect any kind of bad (or anomalous) behavior by using either data-oriented or behavior-oriented (Kwon et al., 2015) mechanisms, tailored to the communication protocols of Section 2.3.

Architecture and deployment. To detect cyber-attacks effectively, it is important to know where and how to deploy network monitoring solutions on a smart grid. Below, we present three possibilities for deployment, using as a framework the architecture described in Figure 1. For each deployment option, we describe the placement of IDS components, their advantages and disadvantages.

Before describing the deployment of network monitoring solutions, we must define their components. Practical intrusion detection systems have at least two components: a *Monitoring Sensor* and a *Command Center*. The Monitoring Sensor is responsible for sniffing the network traffic (usually passively, without injecting any traffic, to avoid disrupting the network or delaying other packets) and either forwarding raw traffic or events (such as security alerts and operational anomalies) to a Command Center. The Command Center acts as a user interface with which a security analyst can interact. It also allows to connect multiple sensors, thus retrieving traffic or events from multiple locations (e.g., substations). This kind of architecture is followed by both commercial and open-source IDS.

It is also important to notice that modern commercially available network monitoring solutions for smart grids provide much more than just intrusion detection. These solutions usually embed asset visibility and management options, which allow network operators to see important information about all the devices in the network, such as hardware and software versions, protocols supported, and the presence of vulnerabilities. Additionally, intrusion detection in this domain has been extended with operational anomaly detection, which allows network operators to see abnormal or dangerous events that are not necessarily related to a security incident but may be indicative of a device failure. Other use cases include network traffic forensics (Corey et al., 2002), integration with Security Information and Event Management (SIEM) solutions (Bhatt et al., 2014), and support for network segmentation (Genge and Siaterlis, 2012).

Residential Home. The first deployment option places the monitoring sensor at the Residential Home, relying on the HAN gateway. The IP forwarding functionality of the HAN gateway can be leveraged by the monitoring sensor to monitor all the communication in the home network, which includes traffic from smart meters and other devices that have wireless interfaces. This deployment option allows to detect security and operational anomalies in the smart meters and devices in the home. The failures are reported through wireless event forwarding to a Command Center that is placed in the Utility Data Control Center. The main advantages of this deployment are full communication visibility inside the HAN and the detection of attacks targeting smart meters. The main disadvantages are: (i) limited scalability due to the high cost and effort for sensor configuration and maintenance; and (ii) no visibility of the Utility Access Points or the Utility Data Control Center.

Utility Access Point. The second deployment option

places the sensors at the Utility Access Points. When data is directly sent by the smart meters to a data concentrator (avoiding a HAN gateway), this is the only possibility to capture data and detect anomalies. This deployment has the following advantages: (i) full communication visibility of the smart meter communication, as well as network monitoring capabilities to ensure the integrity of data analysis; and (ii) detection of remote attacks for the smart meters. The main disadvantages are: (i) there may be many Utility Access Points, resulting in high deployment and maintenance effort; and (ii) it cannot detect attacks targeting the Utility Data Control Center.

Utility Data Control Center. The third deployment option places the sensors at the Utility Data Control Center when the number of Utility Access Point stations is sufficiently large. This deployment option has as main advantages low cost and effort, since only one sensor should be deployed to monitor the activities happening on the SCADA and logs in the aggregated database. The main disadvantage is that there is no visibility for attacks targeting the smart meters or the Utility Access Point.

Evaluation. The selection of deployment option must be tailored to the needs of each electricity company, depending, for instance, on the attacks it wants to detect and the geographical area that it covers. Even though state-of-the-art solutions in the academic literature usually use the first deployment option (in the Residential Home), we believe that this is neither scalable nor maintainable for larger residential areas. Moreover, it is disruptive to the end-user, who may not accept or trust it as a standalone technology. Instead, a configuration that is integrated to the HAN gateway may be more trustworthy. Our conclusion for the second and third deployment options is that they can be used in different settings. For an electricity company with a small number of Utility Access Point stations the best option may be the second, since it provides visibility and access on the entire network. For large energy providers, a deployment in the Utility Data Control Center (third option) is more suitable, as the second option will require substantial effort for maintenance.

4.3 Privacy Regulations

Encryption is common to protect the privacy of consumer data in smart grids. However, real scenarios have shown that utilities may use a shared key for their meters and, once this key is inferred, an adversary can have access to data from all the meters of the same utility (Burton, 2016). When attacks affecting the privacy of users happen, regulations are an effective way to ensure that users will be notified and that companies will take measures to avoid future incidents.

The General Data Protection Regulation (GDPR) went into effect in 2018 and has been formulated to protect the privacy of EU citizens. It requires online services that collect data to inform users about their data collection processes and obtain consent; and ensure that collected data is stored in a secure environment and is available to third parties or enforcement officials in defined time frames (Sharma, 2018). Smart grid operators are affected by the GDPR since they collect and process personal data and make it available to other stakeholders. A specific data protection and security framework for smart grids has been proposed in the *Electricity Directive*. The aim is to include relevant GDPR provisions in the new text and tailor those to the needs of smart meters. It follows that a new, comprehensive legal framework to ensure a high level of personal data protection in smart metering systems is being shaped, which is expected to lead to greater trust and confidence of energy consumers and, in turn, to their increased acceptance and participation in the smart grid (Fratini and Pizza, 2018).

5 FUTURE OPPORTUNITIES

Future smart grids are expected be different as the mass generation and distribution of electricity will be replaced by local renewable resources such as solar and wind. Besides, some of the solutions discussed above, such as encrypted communication protocols and strict regulations are expected to become more popular. Thus, this future scenario presents opportunities in 3 areas that we would like to highlight:

Unified security solution. Future security solutions should focus on identifying security incidents through indicators of suspicious behavior. Such indicators arise from monitoring the network as well as application logs from smart grid supervisory systems such as the Data Analytics or SCADA systems of Figure 1. Additionally, the presence of dedicated incident scoping and investigation scenarios will aid in reasoning about the incident's root cause and minimize false positives. Upon investigation, incident response actions shall be taken, which include next-generation firewalls to prevent unauthorized communications as well as containment and recovery actions for the involved smart grid assets. The final goal of security solutions should be to maintain the continuous smart grid operation.

Encryption. Encryption is an often advocated measure for data security and privacy, but it is not effective against several classes of attacks in industrial control systems, while it can severely decrease visibility and monitorability of smart grid networks (Fauri et al., 2017). As communication protocols for the smart grid evolve, encryption is a common additional capability. However, deciding what communications to encrypt

and when to encrypt them may be as important as deciding how and where to monitor network traffic in order to obtain the best results for intrusion detection. This creates an opportunity for the design of communication protocols that at the same time protect the information being communicated and allow for the monitoring of potentially malicious behavior.

Distributed grids. The more a grid becomes distributed, the more its attack surface is spread across its different parts. Monitoring a distributed grid requires a different deployment of sensors than what we presented above, since the threats are also different. For instance, it could be possible for future malicious actors to compromise the stability of the grid by attacking several small generation units. That would require a more distributed presence of sensors (such as the one described in our first deployment option). A similar attack scenario, but manipulating distributed electricity demand, instead of generation, has already been described in the literature (Soltan et al., 2018).

6 CONCLUSIONS

As traditional power grids become smart grids, critical systems are connected to the users and potentially reachable from anywhere in the world. This brings benefits but also exposes a previously closed network to potentially malicious outsiders. This work presented security challenges, solutions and opportunities for smart grids in a comprehensive way, including definitions, architecture, use cases and networking protocols.

ACKNOWLEDGMENTS

This research has been partially supported by the Swedish Civil Contingencies Agency (MSB) through the projects RICS and by the EU Horizon 2020 Framework Programme under grant agreement 773717.

REFERENCES

Abdallah, A. and Shen, X. (2018). *Security and privacy in smart grid*. Springer.

Algin, R., Tan, H. O., and Akkaya, K. (2017). Mitigating selective jamming attacks in smart meter data collection using moving target defense. In *Proc. Q2SWinet*.

Barkan, E., Biham, E., and Keller, N. (2008). Instant ciphertext-only cryptanalysis of gsm encrypted communication. *Journal of Cryptology*, 21(3):392–429.

Bhatt, S., Manadhata, P. K., and Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE S&P*, 12(5):35–41.

Brunschwiler, C. (2013). Wireless m-bus security. Black Hat Briefings US.

Burton, G. (2016). Gchq intervenes to prevent catastrophically insecure uk smart meter plan. https://bit.ly/2QHAG1Y.

Butun, I. (2017). Privacy and trust relations in internet of things from the user point of view. In *Proc. CCWC*.

Butun, I. and Österberg, P. (2019). Detecting intrusions in cyber-physical systems of smart cities: Challenges and directions. In *Secure Cyber-Physical Systems for Smart Cities*, pages 74–102. IGI Global.

Corey, V., Peterman, C., Shearin, S., Greenberg, M. S., and Van Bokkelen, J. (2002). Network forensics analysis. *IEEE Internet Computing*, 6(6):60–66.

DLMS UA (2019). Dlms: Device language message specification. https://www.dlms.com/.

EU (2019). En 13757 - communication systems for meters.

Faisal, M. A., Aung, Z., Williams, J. R., and Sanchez, A. (2014). Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Systems journal*, 9(1):31–44.

Fauri, D., de Wijs, B., den Hartog, J., Costante, E., Zambon, E., and Etalle, S. (2017). Encryption in ics networks: A blessing or a curse? In *Proc. SmartGridComm*.

Fratini, A. and Pizza, G. (2018). Data protection and smart meters: the gdpr and the 'winter package' of eu clean energy law. https://bit.ly/36i9bCX.

Galli, S., Scaglione, A., and Wang, Z. (2011). For the grid and through the grid: The role of power line communications in the smart grid. *Proc. IEEE*, 99(6):998–1027.

Genge, B. and Siaterlis, C. (2012). An experimental study on the impact of network segmentation to the resilience of physical processes. In *Proc. NETWORKING*.

IEEE (2010). 1815-2010 - ieee standard for electric power systems communications - dnp3.

Kistler, R., Bieri, M., Wettstein, R., and Klapproth, A. (2009). Tunneling smart energy protocols over zigbee. In *Proc. ETFA*.

Kwon, Y., Kim, H. K., Lim, Y. H., and Lim, J. I. (2015). A behavior-based intrusion detection technique for smart grid infrastructure. In *IEEE Eindhoven PowerTech*.

Lisovich, M. A., Mulligan, D. K., and Wicker, S. B. (2010). Inferring personal information from demand-response systems. *IEEE Security Privacy*, 8(1):11–20.

Mahmood, A., Javaid, N., and Razzaq, S. (2015). A review of wireless communications for smart grid. *Renewable and Sustainable Energy Reviews*, 41:248 – 260.

Naik, N. (2017). Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http. In *Proc. ISSE*.

Sharma, R. (2018). How does gdpr affect smart grids? https://bit.ly/2QFE4uh.

Soltan, S., Mittal, P., and Poor, H. V. (2018). Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *Proc. USENIX Sec.*

Sridhar, S., Hahn, A., and Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. *Proc. IEEE*, 100(1):210–224.

TC57 (2019). Power systems management and associated information exchange.

Wang, W. and Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer networks*, 57(5):1344–1371.