# Remote control of smart meters: friend or foe?

Mihai Costache*, Valentin Tudor*, Magnus Almgren*, Marina Papatriantafilou*, Christopher Saunders†
*Department of Computer Science and Engineering
†Department of Energy and Environment
Chalmers University of Technology, SE–412 96 Gothenburg, Sweden

***Abstract*—The traditional electrical grid is transitioning into the *smart grid*. New equipment is being installed to simplify the process of monitoring and managing the grid, making the system more transparent to use but also introducing new security problems. Smart meters are replacing the traditional electrical utility meters, offering new functionalities such as remote reading, automatic error reporting, and the possibility for remote shutoff. This last feature is studied in this paper through two scenarios where the effects are outlined, both on a theoretical level and through a simulation. In the first scenario, the *frequency* property of the grid is the target to possibly cause a blackout. In the second scenario, the *voltage* is driven out of bounds by the adversary.**

***Index Terms*—smart meters; smart grid security; denial of service**

## I. Introduction

The electrical distribution grid is being transitioned from the traditional grid into the new so-called *smart grid*, partly to become more flexible and to be able to accommodate large energy production from renewable sources. This transition involves, among other steps, the installation of advanced equipment in places where it previously was not found, including *smart meters* replacing the traditional domestic electrical meters. Even though this transition offers new functionalities, it also brings security concerns in how the technology can be misused by a malicious adversary. Many of the new security issues in the smart grid are well-known problems in the information and communication technology (ICT) domain, such as buffer overflows in devices and sloppy implementations of cryptographic protocols, but some issues originate from the electrical and power engineering domain (device tampering). There are also new challenging problems, requiring an interdisciplinary approach for the analysis of possible solutions. In this paper we describe and analyze two scenarios where the adversary targets the smart meters installed in the electrical distribution network. Our main focus is not on the attack on the smart meters themselves, but rather on the impact (and resulting damage) that the adversary can cause to the electric grid *if* he would manage to control a number of smart meters in a single neighborhood or even several cities within a country.

While the current definition of a smart grid is abstract, overall it can be summarized as "electricity networks that can intelligently integrate the behavior and actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies" [1]. Simply put, the main purpose is to extend the traditional network so it becomes more flexible by adding new equipment and a management layer; this layer controls the equipment, making the system robust, flexible and easier to administer. This change is necessary to, among other reasons, accommodate the use of more renewable energy sources. Today the primary globally-consumed resource to produce electrical energy is coal, which together with natural gas and oil account for 67% of the total energy produced in 2009 [2]. Nuclear power covers another 13%, while the main source of renewable energy comes from hydroelectric plants (16%). Solar, wind and geothermal energy cover only 3% of the energy production. However, the long-term strategy of many countries is to use more renewable energy production. Germany, for example, has recently announced that all nuclear plants operational from before 1980 will be shut down this year, and by 2022 all the nuclear power production should be ceased [3]. The plan is to replace the nuclear energy with renewable energy, which by 2020 should count for 35% of the national energy production, i.e. double than what it is today, as well as to decrease the electricity consumption by 10%. The migration to use more renewable energy is one factor driving the adoption of the smart grid, together with the expected wide adoption of hybrid vehicles as well as a better utilization of produced energy, meaning that both the traditional energy transmission and distribution networks are being upgraded.

As part of this process, the EU mandates that all the metering devices present in the traditional energy distribution network should be replaced with smart meters by 2020, in an attempt to better control and monitor the energy consumption. Some countries have already completed the installation of smart meters in the distribution network, such as Sweden, Germany, Italy, and UK. The smart meter allows remote reading of consumption, hopefully influencing consumer behavior with near-real-time measurements. However, meters will also have other functions such as promptly alerting the distribution company of electrical problems occurring at the site of the customer (such as power outages), and maybe even controlling when consumer devices may be allowed to run.

The smart meter is a small embedded system, with the ability to measure, process, and communicate with other meters, data concentrators, or the central system as shown in Figure 1 and Figure 2. As such, these integrated ICT components bring many new functionalities to the grid, but also lead to many security problems already present in traditional ICT systems, albeit with a big difference: the electricity network is a critical infrastructure in society and if it fails, many other

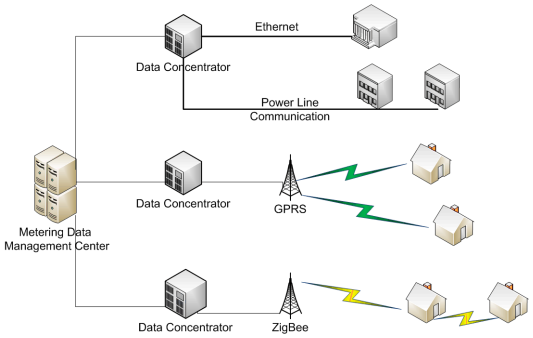


Figure 1. Smart meter communication model

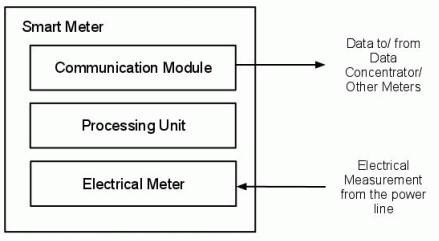


Figure 2. Smart meter components

systems will in turn cease to function correctly. Problems also stem from different underlying assumptions in the ICT domain compared to the electrical engineering (EE) domain. In electricity networks, equipments are expected to have an extended life span (about 20 years), while within the ICT domain it is not unusual to patch systems on a weekly basis. Replacing a large number of smart meters after they are installed, or simply updating their firmware might be very costly. For that reason, the systems must be planned well from the beginning with a good security model. Unfortunately, as explained later in the paper, several vulnerabilities in these systems have already been discovered.

The smart meter and other technological advances enable further changes to the electrical grid. From having been a centralized system with a few large energy producers, where energy is *broadcast* to the consumers, local renewable energy production through solar or wind power turns the grid into a more distributed structure [4], by creating local power generation areas called *power islands* or *micro grids*. Some islands then become self sufficient, and may even inject (sell) their surplus energy back into the distribution network.

In this paper, we present two scenarios where a similar type of distributed attack is used against smart meters but executed on two different scales. In the first scenario, we focus on the electrical distribution network from a large geographical region (several large cities) where the adversary tries to take control over a very large number of smart meters. By using the remote capability to turn power on or off, the adversary can tamper with the frequency of the electrical grid. The second scenario is localized to a neighborhood modeled as a power island. Here, the attacker's purpose is to create havoc and damage the electrical appliances in the neighborhood by changing the voltage in the network through his control over the smart meters. We also include a simulation modeled on the second scenario, as well as analyzing the possible impact based on this simulation.

The rest of the paper is organized as follows. In Section II we describe the capabilities of smart meters and their communication infrastructure. We also include some electrical concepts that is necessary to understand the simulation of the second scenario. In Section III, we outline the two scenarios and the possible consequences. We further study the second scenario in Section IV through a simulation. In Section V, related work is described and the paper is concluded in Section VI.

## II. Background

For an easier understanding of the attack scenarios described in Section III, we present a brief overview of the smart meter's main features and its communication model. We also include a short summary of important terms and formulas used for the simulation of the electrical network.

### A. Smart meters

A smart meter is an embedded system whose main current functionality is to automate the collection of consumption indexes by minimizing the need for an operator to manually read each meter. Conceptually, it can be seen as having three components: the electrical meter, the processing unit and the communication module, as shown in Figure 2.

The electrical meter has the role of measuring the electricity consumption at the power line and to translate the readings into data that can be used by the processing unit. The processing unit's role is to process and store the information and to control both the electrical meter and the communication module. The communication module can be embedded in the smart meter or installed in an extension slot, meaning that the same smart meter equipment can use different communication modules depending on the circumstances. In some deployments, a ZigBee network is used in urban neighborhoods while GPRS is used in rural environments.

The smart meters can send data via different communication channels (IP, GSM, GPRS, PLC, ZigBee) to so-called *data concentrators*, to aggregate data and then dispatch it to the central system, the *metering data management system*, as shown in Figure 1.

The electrical meter part of the smart meter is usually highly regulated and must conform to a set of national standards. The other two parts vary in their functionalities, but the more advanced ones may have an indoor module to inform the customer of their instantaneous electricity consumption, energy consumed so far (translated into a currency), or the current tariff based on time of day utilization. One key feature of the smart meter is the remote ON/OFF switch. The distribution company can, for example, cut the power from customers that have defaulted on their payments by simply issuing a remote command to the smart meter.

Real-time reporting of energy usage of the end-customers will also enable a better management of the distribution grid by reducing electricity loss and maintaining efficiency of electricity production. Smart meters have the capability to report information to the data concentrators at different intervals (daily/hourly), but this may change to real time reporting in the future. Some meters can be queried about the current load, raising some privacy concerns as such data can be used to identify what appliances are currently in use.

Finally, customers can choose to install renewable energy production facilities in the premises of their homes (such as solar panels) and some customers may then produce more energy than they consume. The smart meter is responsible for keeping track of the energy consumed from the electricity network as well as for the energy injected back into the grid.

### B. Transmission and distribution networks

Power generating facilities are usually placed in remote locations and therefore a transport network is necessary to deliver electricity the end consumers. A typical electric grid has two components: the *transmission section* and the *distribution section*. The transmission section transports the electricity from the generator to the distribution section and the distribution section delivers it to the end customers. Transporting over long distances requires electricity to be converted to a high voltage alternating current form (HVAC) that enables efficient delivery with an acceptable loss. This is done by using a step-up transformer that outputs voltages in the range of $50-350$kV (depending on the line capacity) into the transmission grid. Before reaching the end consumer, the transmission grid is connected to a series of step-down transformers that feed lower voltage electricity to the distribution grid (typically $0.4 - 50$kV).

### C. Power quality

One of the important factors in the design of a distribution grid is power quality, i.e. limits for power supply frequency and voltage magnitude, so that electric and electronic equipments can function without damage when connected to the outlet. It is important to account for the transmission line's loss to ensure power quality standards for each *feeder*, where a feeder is a portion of the grid that provides power transportation capabilities to service areas. In real-world conditions with variable loads and unpredictable power generation levels, power quality issues need to be handled in order to respect the specification of appliances. According to the European "Voltage Characteristics in Public Distribution Systems" including EN 50160 and EN 61000 standards [5], there are specific voltage requirements and frequency regulations for different situations. There are requirements for an acceptable variation of voltage magnitude (from $220 - 240$V nominal value, depending on country) and power frequency ($50$Hz nominal value). Variations allowed for the frequency must be on average $\pm 1\%$ ($49.5 - 50.5$Hz) in $95\%$ of a week time and $-6\%$/+$4\%$ ($47 - 52$Hz) at all times. Voltage magnitude variation should be within $\pm 10\%$ of the nominal voltage in $95\%$ of a week time and all average values should not go outside $-15\%/+10\%$ of the nominal voltage. In the case that an energy provider does not respect power quality standards, grid problems may appear and cascade to unforeseen consequences. Therefore, power quality specification are enforced by financial penalties on the energy providers. Problems related to the quality of the voltage may manifest themselves as short interruptions, flickers, voltage dips, supply voltage variations and harmonic disturbances. For more information, we refer the reader to [6], which explains in detail how these phenomena manifest.

In the attack scenarios described in Section III, the electrical power frequency or the voltage magnitude, respectively, is pushed outside of the standard value limits. By inducing abrupt variations in the loads at precise points in time, for example when the grid becomes underloaded (too much available power), the voltage magnitude can be pushed outside the range of safe values. Formally, this is a consequence of the power flow equations relating individual nodes or bus power properties, used for the simulation in Section IV. These equations are briefly outlined below.

### D. Power flow equations

As previously mentioned, the electrical grid is composed of *nodes* or *buses*, where each node is connected by a *transmission line*. In order to model the electrical infrastructure and electricity flow, each transmission line is characterized by physical properties (resistance, capacity and inductance). The line's specific properties can be measured, and the loss characterizing the line, also known as impedance can be calculated. A square matrix, whose dimension depends on the number of nodes in the network, can be built to represent the impedance between nodes (the $Z$ matrix or impedance matrix). However, the $Y$ matrix (or admittance matrix), the inverse of the impedance matrix, is used in practice. With the following power flow equations, voltage magnitude and angle at each node, as well as real and reactive power flowing in and out each node, can be computed as:

$$\begin{aligned} P_i &= \sum_{i=1}^{N} Y_{ij} V_i V_j \cos\left(\theta_{ij} + \delta_j - \delta_i\right), \\ Q_i &= - \sum_{i=1}^{N} Y_{ij} V_i V_j \sin\left(\theta_{ij} + \delta_j - \delta_i\right), \end{aligned}$$

where $P_i$ and $Q_i$ are the real and the reactive power at node $i$, respectively; $Y_{ij}$ and $\theta_{ij}$ are the magnitude and angle of the admittance between node $i$ and node $j$; $V_i$ and $V_j$ are the voltage magnitudes at node $i$ and node $j$; $\delta_i$ and $\delta_j$ are the phase angles at node $i$ and node $j$.

Based on these values, voltage regulations can be enforced for each feeder in the grid [7]. Grid control and regulation in a centralized system can be solved by central operators in the SCADA (Supervisory Control And Data Acquisition) system. However, in the context of distributed generation where customers can produce their own energy, and thus become providers for their neighbors, serious problems may arise; this is the actual topic explored in Scenario 2. For

instance, since power injection into a grid is in some regions freely allowed (with the required standard specifications to be met), a node's voltage magnitude may vary even more due to abrupt changes in consumption.

### E. Power islands

One of the main changes involved in the transition to the smart grid is the distributed generation of energy. In [8], distributed generation is defined as: "[...] an electric power source connected directly to the distribution network or on the customer side of the meter". Many customers will opt for installing a renewable energy production facility on their domain, for example a wind turbine or photovoltaic panels, in order to obtain some independence from their main energy provider; some may even sell the surplus energy produced.

The traditional distribution network can be modeled as a tree-like structure, but with the changes of local producers of energy the best model is more flat, like interconnected power islands. The second scenario takes place in a power island (Figure 3), which has become self sufficient and surplus energy is injected back into the grid.

## III. Attack scenarios

With the overview given in Section II, let us now consider the two attack scenarios. Both scenarios are similar, in that the adversary takes control of a number of smart meters, but they differ in scale and the underlying property of the electricity network that the adversary will target. In the first scenario, the goal is to drive the frequency out of bounds – an attack that would require the adversary to control a significant number of smart meters, causing a serious imbalance that could propagate. In the second scenario, the goal is to vary the voltage in a small neighborhood – a simpler attack but where the consequences would also be more localized. The second scenario is then simulated and presented in further detail in Section IV.

Both of these scenarios require an interdisciplinary approach for the analysis of possible mitigation techniques and an understanding of their respective cost and weaknesses. For example, in the second scenario, one can either harden the smart meter (using security mechanisms known from the ICT domain) or one can install voltage regulators to mitigate the consequences of the attack (an electrical engineering solution).

In this paper, we focus on the main steps of the scenarios and the impact of the final attack, and not particularly on the details of the actual attack against the smart meters themselves. For that reason, we describe known weaknesses of smart meters that have been documented elsewhere (and could be used by the adversary) before we describe the two scenarios.

### A. Prerequisite: Taking control of the smart meter

As the smart meter is a small embedded system, with three complex components (see Figure 2), it has quite a number of vulnerabilities. For example, some smart meters actually include a web server for query purposes. Given the number of exploits targeting web servers in a more traditional setting, it is expected that also the ones in the smart meter easily could be exploited. In [9], Carpenter et al. describe a methodology to extract and reverse engineer the firmware from a smart meter to obtain valuable information about its internals, such as passwords and communication encryption keys. Also the communication channel between the smart meters and the central system has been shown to contain weaknesses [10].

Security flaws have been discovered in the current implemention of smart meters and in [11], McLaughlin et al. discuss tampering with the measurement device and problems related to the communication module with interception and injection of false messages. They also present a scenario where the injection of false malicious data lets the adversary gain different benefits from the system.

In order to gain access to a large number of smart meters, even if a remote attack is not possible, the attacker can employ social engineering. She can advertise a product or a "jailbroken" firmware, which supposedly will reduce the electricity consumption by a certain amount.[1] The attacker will gain twice from this: the revenues generated by selling the cost -reduction device and the opportunity to gain access to a large number of smart meters.

As can be seen, there are already several methods documented in literature on how an adversary can control smart meters. Given that this is a relatively new area of research, it is expected there are many vulnerabilities that are not known at this point. Assuming the adversary controls a number of smart meters, we now turn to the actual scenarios.

### B. Scenario 1: Frequency variation

In the first scenario, the adversary targets the alternating current's *frequency*, which in Europe is 50 Hz. A stable frequency is required for the stability of the electrical grid, and the whole electrical grid must be synchronized at the same frequency. However, the frequency in the electrical grid is closely dependent on the instantaneous energy generation and consumption, which thus must be balanced. If the frequency goes outside the 48-52Hz range, total blackout may occur [12].

As was mentioned before, one of the functionalities implemented in the current generation of smart meters is the remote ON/OFF switch. In [13] Anderson and Fuloria raise and analyze the problem of improper use of the remote off switch. The ability to remotely turn electricity on or off for many customers simultaneously is new. Unfortunately, any capability can either be used as planned or misused by an adversary. Anderson and Fuloria point out that any vulnerability may lead terrorist organizations, environmental organizations and even individual criminals to be able to control this "feature," a feat possibly much simpler than to attack and destroy a power generation facility (the "traditional" way to cause a large blackout).

Controlling the power for a number of customers can cause severe havoc in society, but the question is whether the attacker

[1] See for example the following URL for an instruction video how to do this with the traditional meter: http://www.metacafe.com/watch/4659119/electricmeterhackhowtocutyourelectricitybillinhalf/

can force a larger blackout by having fine-grained control over the smart meters. The scenario setting is thus the following: an attacker takes control (using a remote exploit or through social engineering methods) of a number of smart meters in a *large geographical area*. By issuing synchronized commands to all smart meters to turn off their load, the result is an electrical network with excess generation, and no consumers. The central operators would at this point try to mitigate by reducing the power injection levels, but the attacker would in turn send a *turn on* command to all controlled smart meters, thus putting all the households back online very suddenly. By such a technique, the attacker would try to destabilize the electrical network which could lead to a complete blackout. The effect of a successful attack of this type and magnitude is considerable, because reestablishing the functionality of the electrical grid could take from several hours to a few days. During that period there will be large areas without electrical energy, lack of communications, lack of heating in the winter, significant economic losses which will cause distress among the population.

The question is then how likely the worst outcome would be. Frequency variation can be observed in classical electric networks, based on the behavior of the individual consumers and their utilization pattern.[2] To prevent frequency variation caused by a quick demand of electrical power in the grid, the electrical network has reserves that quickly can be injected. However, due to the significant cost of keeping these reserves in stand-by mode, the quantities available are usually estimated at the values required by specific standards/requirements. The success of the attack (in causing total blackout) is conditioned by its scale, i.e. the number of smart meters controlled (translated in volume of energy consumption) versus the number of energy producers (translated in volume of energy produced). Attempting this type of attack during the night would most likely not succeed – not much energy is consumed during the night and thus the attacker would not be able to control a critical mass – but the attack should be performed at times when there are already other stresses on the electrical grid (very warm summer day with air condition, or a very cold winter day for heating). The success also depends on the structure of the grid in the country, and where power can be injected. A country such as Sweden, where a large part of the energy is produced by hydro and gas turbines is more resistant as these generation facilities have better response time compared to coal and oil electrical generators [14].

Even though the individual steps are already known, the above compiled and complete scenario with its possible consequences should be useful to both the researcher in security and the electrical engineers designing the networks. The large scale deployment of smart meters in the electric grid with the remote ON/OFF feature can open the gates to new types of attacks. Research efforts into securing the smart grid is somewhat focused on the SCADA systems and the transmission network (see Section V), but even attacks originating from the distribution side can have significant effects.

[2]Demand surges can be quite significant when many customers act simultaneously, such as reported for the British royal wedding http://www.guardian.co.uk/media/2011/apr/29/power-surge-royal-wedding-ratings

### C. Scenario 2: Voltage variation

As opposed to Scenario 1, the second scenario focuses on a small neighborhood, *a power island*, with only one power transformer. Some houses in the neighborhood produce their own renewable energy, and the excess energy is injected back into the network. Every customer has a smart meter installed, that in turn communicates with the data concentrator attached to the neighborhood power transformer. The power consumption is reported to the data concentrator once every 15 minutes, and the smart meters can receive commands to turn on or off the electricity for the customer at any moment.[3] All communication is encrypted with a symmetric encryption key but no other security mechanism is running on the smart meters. The neighborhood is shown in Figure 3.

A common misconception about security is that *if* encryption is used, the network and the devices are safe from attacks. However, the devices may still be vulnerable to an exploit (buffer overflow), the protocols may not be well implemented, an oversight may lead to no change of the default settings, or there might even be an inside leak from the electricity company in question. As a parallel, Stuxnet used valid signatures [15] in its infection.

Thus, the attacker is presumed to have a good knowledge of the smart meter deployment as well as its shared encryption key. The attacker can then take control over a number of smart meters in the neighborhood. Arbitrarily turning on or off electricity for customers would at least inconvenience customers, and cause a financial loss to the electricity company. However, the purpose of this scenario, further explored in the next section with a simulation, is to determine if an attacker can make the voltage of the network go outside the tolerance limits of +10% and -15% around the optimal value, being 230V for Europe.

## IV. Scenario 2: Simulating the effects

To demonstrate the viability of the voltage variation attack scenario, we use the PowerWorld Simulator software suite [16] to model a realistic grid configuration (e.g. modeling transmission lines, generators, loads and solving the resulting power flow equations). The upper of Figure 3 presents an intuitive overview of the neighborhood while the lower subfigure shows the overview of the resulting electrical network model used in the simulation.

### A. Simulation setup

The neighborhood is a typical country-side distribution grid, with several buildings and their facilities served by one power substation (marked as node one in the figure). The six buildings (numbered two to seven) have a relatively higher than normal individual instantaneous energy consumption from 10 to 50kW. There are three renewable energy production

[3]The smart meter has its own power supply, so it does not depend on whether the electricity in the house is on or off.

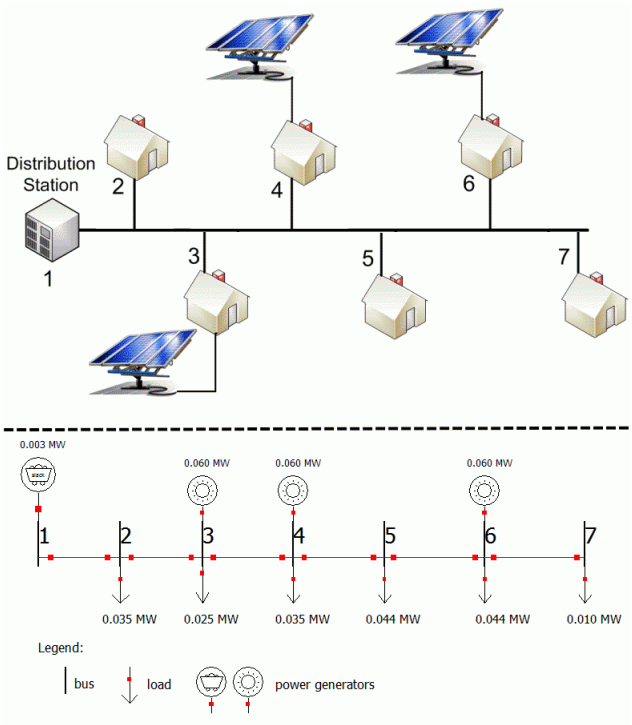


Figure 3. Neighborhood overview (top) and electrical network model overview (bottom)

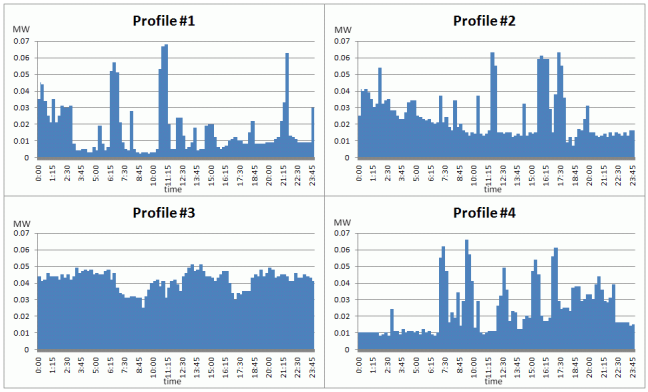


Figure 4. The consumption profiles for four different customers

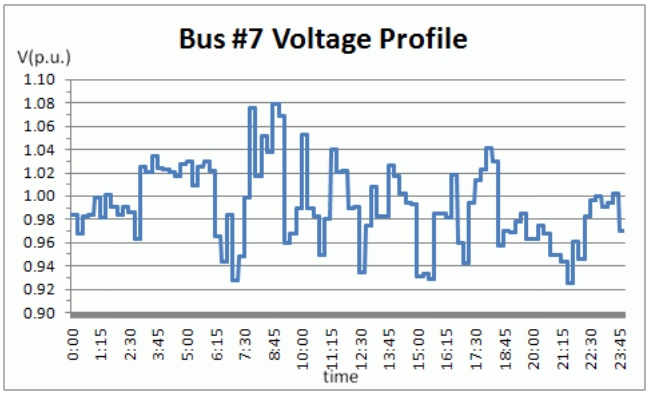


Figure 5. Voltage level at Bus #7 during the simulation

facilities in the neighborhood, connected at nodes three, four, and six respectively. These facilities can produce more energy than required for the local neighborhood, so sometimes the surplus is injected into the electrical network. The bars numbered from one to seven in the lower subfigure are called *buses*. Buses are points in the electrical system where certain electrical attributes such as voltage, power and current can be evaluated ("p.u." signifies the voltage per unit value of each bus). Every building that consumes energy is modeled as a load, every renewable energy facility is modeled as a generator and the electrical lines connecting the nodes are modeled as transmission lines with proper loss. We utilize four real-time daily consumption profiles for the customers according to [17]. In Figure 4, the consumption profiles are based on 24 hour consumption patterns with 15-minute interval measurements. These profiles are characterized by peaks during the rush hours (in the morning, at lunch and in the evening), depending on each household's appliances in use. We let customers #2 and #4 use the consumption profile one, customer #3 use profile two, customer #5 and #6 use profile three and finally customer #7 use profile four (chosen arbitrarily).

The simulation runs during 24 simulation seconds, equivalent to 24h with the load variation described above. Changing either the load profiles or the grid configuration will change the end result.

### B. Simulation results under normal conditions

In Figure 5 we present the voltage magnitude variation of Bus #7, i.e. the load for customer seven. The grid's behavior (loss, power injections, loads) is responsible for the voltage maximum and minimum points seen in the figure. The voltage peaks are the result of large amounts of power in the grid and few consumers, while the voltage minimum points are a result of many consumers and little available power. In normal running conditions, the voltage profile of Bus #7 respects regulations and the voltage magnitude never goes beyond $+8\%/-6\%$ of the nominal value.

### C. Simulation results while executing the attack

The goal of the adversary is to vary the voltage magnitude of Bus #7 outside the safety zone of $\pm 10\%$. This is achieved by manipulating the smart meters in the neighborhood to shut down power in only some parts. In a first attempt, the attacker gains control of the meter controlling the load on Bus #5. The attack is then launched at an appropriate point in time, for example at the voltage peak observed between time $7-10$ when the grid is vulnerable; there is then a high demand for energy (people are preparing for going to work) and the generators must compensate and push more power into the grid. If the attack is timed correctly, Load #5 will be interrupted during the established period, leading to more power being routed to the other buses. The result is shown in Figure 6, where the highlighted area represents the time of the attack. The voltage magnitude barely goes up 2% of the established barrier at 1.1 volts per unit and for very short

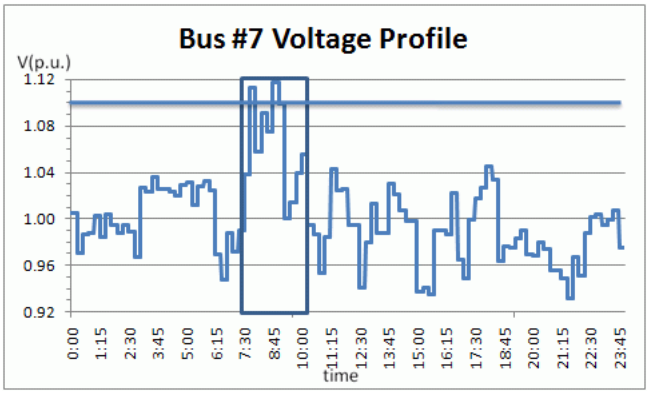


Figure 6. Bus #7 voltage after launching the attack on Bus #5 with the attack period emphasized with the square box. The safe voltage limit is at 1.1 V(p.u.) and the voltage is normalized.

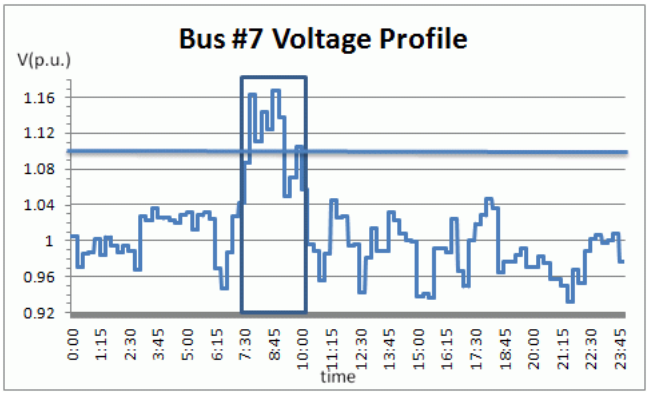


Figure 7. Bus #7 voltage after launching the attack on Bus #5 and #6 with the attack period emphasized with the square box. The safe voltage limit is at 1.1 V(p.u.) and the voltage is normalized.

period of times. This may not be enough to cause damage to the target and the attack cannot be deemed as a success.

In a second attempt, the attacker gains control of an additional smart meter (the one controlling Bus #6) and the result is showed in Figure 7. This time, the attacker manages to drive the voltage magnitude to peaks of +17% with a constant average value above the normal +10% between time 7 and 10. This increase in voltage should be enough to cause major damage, both physical and economical, to the customer in the absence of voltage regulators. As an observation, the number of smart meters that need to be compromised is not in direct relation to the total number of smart meters in the neighborhood, but with the power loads controlled by one of them. For example, a smart meter that controls a high-load household is more attractive for takeover since the strain it can reflect into the electrical grid is higher. The effect can be replicated any time by the attacker, by simply turning off the energy consumption in some buildings in a neighborhood, in turn damaging electric appliances in other buildings still connected to the network.

In the future, we would also like to explore possible economic losses caused by the attacker because even if no permanent damage is achieved, both customers and the electrical company may lose money when the attack is performed. Three ways to mitigate the attack is to either harden the smart meters, install voltage regulators at the customer's site or install adaptable renewable generation facilities.

## V. Related work

Many of the previous studies concerning this subject have either focused solely on computer security issues, or on problems related to the electrical power engineering domain, often with few references to the other domain.

There is a lot of significant research in the security of the central management systems (SCADA systems) [18], [19], [20] as these systems tend to become connected to the Internet and also govern power production, meaning that any attack here may have serious repercussions. Several groups have also investigated *the state estimators* [21], [22], because they can be used as a stepping stone for false data injection, in turn impacting the functional models created for the central management systems. For example, Liu et al. [21] present a type of attack targeting the sensors responsible of providing data for the state estimators in the SCADA system, and describe methods in which the measured data can be modified without triggering an alarm. Although it is mentioned that the attack poses great difficulties for the attacker, it is not impossible to be fulfilled. Specific attacks against the smart meters are outlined in Section III.

Within the literature, there are some proposals for protection mechanisms. Information security in the electrical network is well documented in [23], [24], [25] together with proposals for encryption schemes and their weaknesses [26], [27], [10]. As the Advanced Metering Infrastructure (AMI) can be modeled as a large interconnected network (similar to the Internet), some studies [28], [29], [30], [9] are covering the model and the functionalities of an Intrusion Detection System tailored for this new type of network, together with recommendations for the security measures regarding AMI. In [31], McLaughlin et al. present a solution which may stop a large-scale attack to compromise a large number of smart meters. It is a software solution and involves encrypting the functions' return addresses when they are pushed in the stack at function calls.

Other related work involves research focused on the stability of the electric grid, especially regarding frequency and voltage regulation in traditional electric network [5], [6], as well as data processing provided by the new devices installed in the smart grid (e.g. smart meters) to better control the electrical network [32], [33]. With the advent of the recent malware Stuxnet [15], it is clear that even very specific architectures may be targeted by attackers in the future.

## VI. Conclusion and future work

In this paper we present two scenarios where a skilled adversary may affect fundamental properties of the electrical grid by controlling a number of smart meters. By complementing and building on related research, we show how even attacks on the distribution network may affect grid stability. The first

scenario is presented from a theoretical view, and even though the necessary prerequisites of the scenario have been discussed in literature, the implications and limitations of the scenario are outlined here. The second scenario is studied in more detail, and a simulation is performed on a small *power island* to show feasibility. Mitigation and defense techniques against these attacks were only mentioned briefly in this paper but will be expanded upon in future work.

With the current push for massive installment of smart meters as well as a continuous development of their capabilities, it is only a question of time before the infrastructure is attacked. One goal of the paper is to look at the problems from an interdisciplinary point of view, considering both issues related to computer security and the electrical power domain. The smart grid straddles both these two domains and expertise on both areas are necessary to develop successful mitigation strategies.

## ACKNOWLEDGEMENTS

This work is supported by the Swedish Civil Contingencies Agency (MSB). The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 257007.

## REFERENCES

[1] SmartGrids – European Technology Platform. (2011, Jun.). [Online]. Available: http://www.smartgrids.eu/?q=node/163

[2] Observ'ER. (2010) Worldwide energy production from renewable energy sources, Stats and Figures Series. http://www.energies-renouvelables.org/observ-er/html/inventaire/pdf/12e-inventaire-Chap01-Eng.pdf.

[3] A. Breidthardt, "German government wants nuclear exit by 2022 at latest," http://uk.reuters.com/article/2011/05/30/us-germany-nuclear-idUKTRE74Q2P120110530, May 2011.

[4] European Commission. (2006, Apr.) European SmartGrids technology platform: Vision and strategy for Europe's electricity networks of the future. [Online]. Available: http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf

[5] H. Markiewicz and A. Klajn, "Standard EN 50160 - voltage characteristics in public distribution systems," 2004.

[6] B. Franken, V. Ajodhia, K. Petrov, K. Keller, and C. Müller, "Regulation of Voltage Quality," in *9th International Conference "Electric Power, Quality and Utilisation", Barcelona*, 2007.

[7] N. Mithulananthan, M. M. A. Salama, C. A. Canizares, and J. Reeve, "Distribution system voltage regulation and var compensation for different static load models," in *International Journal of Electrical Engineering, vo1.37, no. 4, pp.384-395*, 2000.

[8] T. Ackermann, G. Andersson, and L. Söder, "Distributed generation: a definition," *Electric Power Systems Research*, vol. 57, no. 3, pp. 195 – 204, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378779601001018

[9] M. Carpenter, T. Goodspeed, B. Singletary, E. Skoudis, and J. Wright, "Advanced Metering Infrastructure Attack Methodology," http://inguardians.com/pubs/AMI_Attack_Methodology.pdf, 2009.

[10] T. Goodspeed, "Extracting Keys from Second Generation Zigbee Chips," in *Black Hat USA*, Las Vegas, Nevada, Jul. 2009.

[11] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," in *Proceedings of the 4th Workshop on Critical Information Infrastructures Security (CRITIS)*, 2009.

[12] DynamicDemand. (2011, June). [Online]. Available: http://www.dynamicdemand.co.uk/grid.htm

[13] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proceedings of the IEEE SmartGridComm*, June 2010.

[14] J. F. Prada and M. D. Ilic. (1999) The value of reliability in power systems - pricing operating reserves -. [Online]. Available: http://web.mit.edu/energylab/www/pubs/el99-005wp.pdf

[15] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.Stuxnet Dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[16] P. Corporation. (2011, Jun.). [Online]. Available: http://www.powerworld.com/products/simulator.asp

[17] W. H. Kersting, *Distribution System Modeling and Analysis*. CRC Press, 2002.

[18] R. R. R. Barbosa and A. Pras, "Intrusion detection in SCADA networks," in *Proceedings of the Mechanisms for autonomous management of networks and services, and 4th international conference on Autonomous infrastructure, management and security*, ser. AIMS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 163–166. [Online]. Available: http://portal.acm.org/citation.cfm?id=1875873.1875903

[19] H. Christiansson and E. Luiijf, "Creating a European SCADA security testbed," in *Critical Infrastructure Protection*, ser. IFIP International Federation for Information Processing, E. Goetz and S. Shenoi, Eds. Springer Boston, 2007, vol. 253, pp. 237–247. [Online]. Available: http://dx.doi.org/10.1007/978-0-387-75462-8_17

[20] E. Johansson, T. Sommestad, and M. Ekstedt, "Issues of Cyber Security in SCADA Systems. On the Importance of Awareness." in *20th International Conference on Electricity Distribution*, Jun. 2009.

[21] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois*, 2009.

[22] H. Sandberg, A. Teixeira, and K. H. Johansson, "On Security Indices for State Estimators in Power Networks," in *Preprints of the First Workshop on Secure Control Systems*, Stockholm, Sweden, 2010.

[23] G. Ericsson, "Toward a framework for managing information security for an electric power utility CIGRÉ experiences," *Power Delivery, IEEE Transactions on*, vol. 22, no. 3, pp. 1461–1469, Jul. 2007.

[24] ——, "Management of information security for an electric power utility – on security domains and use of ISO/IEC17799 standard," *IEEE Transactions on Power Delivery*, vol. 20, no. 2, pp. 683–690, Apr. 2005.

[25] ——, "Information security for electric power utilities (EPUs) – CIGRÉ developments on frameworks, risk assessment, and technology," *Power Delivery, IEEE Transactions on*, vol. 24, no. 3, pp. 1174–1181, Jul. 2009.

[26] H.-H. So, S. Kwok, E. Lam, and K.-S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 321–326.

[27] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 327–332.

[28] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 350–355.

[29] A. Metke and R. Ekl, "Security technology for smart grid networks," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[30] J. Zerbst, M. Schaefer, and I. Rinta-Jouppi, "Zone principles as cyber security architecture element for smart grids," in *IEEE PES Conference on Innovative Smart Grid Technologies Europe (ISGT Europe)*, Oct. 2010, pp. 1–8.

[31] S. Mclaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. Mcdaniel, "Embedded firmware diversity for smart electric meters," in *Proceedings of the 5th USENIX Workshop on Hot Topics in Security (HotSec 2010), Washington DC.*, Aug. 2010.

[32] K. Samarakoon and J. Ekanayake, "Demand side primary frequency response support through smart meter control," in *Proceedings of the 44th International Universities Power Engineering Conference (UPEC)*, Sep. 2009, pp. 1–5.

[33] D. Bergman, D. Jin, J. Juen, N. Tanaka, C. Gunter, and A. Wright, "Non-intrusive load-shed verification," *Pervasive Computing, IEEE*, vol. 10, no. 1, pp. 49–57, Jan.-Mars 2011.