LOAD OSCILLATING SMART METER ATTACK

Carter Lassetter, Eduardo Cotilla-Sanchez, Jinsub Kim

Oregon State University

ABSTRACT

This paper investigates the potential impacts of load oscillating attacks in a microgrid to the stability of the main power grid. The adversary is assumed to be able to control switches within compromised smart meters and thus is able to dynamically connect or disconnect the corresponding loads within the microgrid. Using the commercial PSS/e time-domain simulator with the IEEE Reliability Test System (RTS-96), we demonstrate the impacts of attacks cycling the total load of the microgrid. Cycling attacks with different load oscillation frequencies and magnitudes are considered. We found that for certain oscillation frequencies, oscillating 30 percent of the total microgrid load can significantly harm the main grid stability.

Index Terms— Smart meter, load oscillating attack, power system stability, microgrid

1. INTRODUCTION

The power network is trending towards a smarter and more intelligent entity due to developments in *smart grid* over the past several years. These advancements occur at the transmission, distribution, and consumer levels. Distribution networks have seen a multitude of developments including communication system upgrades, automation of distribution elements, load control, and Advanced Metering Infrastructure (AMI) [1]. With such improvements, the potential to dynamically control and protect distributed networks becomes more feasible. Unfortunately with the broadening of said improvements, new attack surfaces are introduced to the power grid [11]. For instance, attackers may intrude into AMI and manipulate the data or inject false control data in order to remotely control switches. This paper focuses on studying whether such attacks launched at a distribution network can affect the main grid stability.

Monitoring of the distribution level has been difficult in the past, but with the introduction of smart meters in AMI, the ability to dynamically track load details becomes possible. Smart meters not only provide power system operators with real-time information of individual customer load (*e.g.*, single house load) but also allow operators to remotely control switches in order to connect or disconnect individual loads [13]. Such two-way communication creates a new security concern because compromised smart meters (or compromised channels between smart meters and the operators) may not only cause the leak of measurements, but also allow the adversary to connect or disconnect the corresponding customer loads [2].

There have been reported successful hacking of smart meters allowing one to sniff data or even inject commands into the device. The ability to control the devices and shut down power is a real possibility and may have harmful outcomes pertaining to wide grid stability [6]. The diverse ways to hack smart meters could be as simple as reverse engineering one or using software radio programmed to mimic communication devices to learn how to communicate with the meter. Compromised meters could be used to spread *malware* to other smart meters allowing easier accessibility for smart meter based attacks for adversaries [5]. The spreading of software with malicious intent has already been tested and successfully carried out by researchers in which a worm was created and traveled through other meters [9]. As a result, it is possible that a few compromised smart meters could lead to a large network of compromised meters.

Such security risks of meters are becoming more concerning due to the deployment of such systems outpacing security efforts [10]. Such deployments stem from sources such as the Smart Grid Recovery Act in which $4.5 billion dollars were directed toward modernizing the power grid. These changes are occurring very quickly. In 2014, the U.S. had 58,545,938 AMI installations with 88% being residential customer installations [3]. It is expected that the number of smart meters installed worldwide will grow from 313 million, in 2013, to nearly 1.1 billion in 2022 [12]. With the rapid growth of such network based systems and lack of research on such security risks, major consequences may occur from compromised systems.

The immediate thought of smart meter attacks would seem to be price fraud in which meters are tampered with allowing setting changes. In 2009 many reports of such fraud were reported in Puerto Rico where utility employees changed meter settings such that customers were charged less [5]. Main security research in regards to smart meters have focused on privacy or fraud, however more intelligent based attacks could create more serious consequences, *e.g.,* disrupting control of power grid [4]. Other attacks may rely on oscillating portions of the grid to disrupt power delivery. Such attacks have been developed and tested on small test cases as seen in [7], [8]. These coordinated attacks may have significant impact on grid stability depending on the source of said switching.

In this paper, we focus on attacks that exploit compromised smart meters in order to introduce load oscillation *within* a single microgrid. In general, perturbation at a distribution level is considered to have a negligible impact and is ignored in the main grid control. The potential impacts of *elaborately designed* perturbation at a distribution level on the main grid stability have not been well understood. This paper aims to fill this gap by providing case studies with load oscillating attacks.

2. ATTACK MODEL

In this paper, we consider an adversary who compromised a subset of smart meters within a microgrid and is capable of controlling switches associated with them. A straightforward attack could involve a one time dropping of the entire adversarial load, however this may not capture the worst case result as the network may recover from the single instance as opposed to a more intelligent attack.

With a more intricate attack, an adversary may choose to cycle

C. Lassetter, E. Cotilla-Sanchez, and J. Kim are with the School of Electrical Engineering & Computer Science, Oregon State University, Corvallis, OR, 97331 USA e-mail: {lassettc,ecs,kimjinsu}@oregonstate.edu

loads to confuse the system and create potential problems with protective device operation. In this case, the cycling would pertain to actual load manipulation, not just the meter readings. With a cycling attack, the adversary may control loads and switch them on and off at a frequency potentially harmful to the network. With such an attack, network convergence issues may result from component stress or protective schemes occurring to aid in the current cycled state whilst being detrimental to the next cycled state. Consistent cycling may result in compounded consequences leading to instability. As a result, this attack would change the actual operating point of the network.

We modeled such an attack in a microgrid setting. With the RTS-96 case [14], we assumed the third zone to be our microgrid. We set up an attack model by choosing all loads in the microgrid to be susceptible to attacks. All initial load models on buses are split into 10 individual feeder representations with identical values. We choose the amount of load the microgrid may cycle and pick adversarial feeders for each bus based on this information. For example, if we allow 50 % of the total microgrid load to be cycled, we represent this by cycling 5 adversarial feeders at each bus in the microgrid. The adversarial feeders for each bus are chosen at random and independently to ensure diversity. We perform attacks that vary in the set of adversarial feeders, the cycling frequency, and the attack duration. This attack is performed when the microgrid is interconnected to the main grid to determine the impact of load oscillation within the microgrid on the main grid.

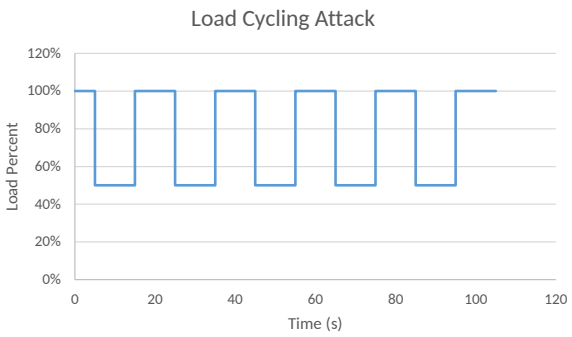

Fig. 1. Example microgrid attack cycling half of the load

An example attack on the microgrid is shown in Figure 1. This attack controls 50 % of the microgrid load and cycles them at a frequency of 0.05 Hz. The attack lasts for 100 seconds with loads oscillating from 50 % to 100 % of the microgrid load. It is important to note that the absolute total load of the grid may decrease as the attack goes on because some uncompromised feeders can be disconnected due the protective scheme triggered by load oscillation.

For clarity, an example is described and the expected outcomes are discussed. We use the attack seen in Figure 1. The network begins with the main grid and microgrid interconnected and operating at the precomputed steady state. At 5 seconds the adversarial loads are switched off in the microgrid leading to only 50 % of the microgrid load remaining. The network will then be exposed to transients and attempt to converge to a new stable point of operation. Relays will operate if their thresholds are exceeded for a pre-set time. These relays are discussed in more detail in Section 3. Relay operation may result in load shedding, line tripping, or machine tripping. The attack will then restore the adversarial loads at 15 seconds. It is important to note that the load shedding from the protection scheme does not discern between adversarial and non-adversarial feeders. The load shedding may shed adversarial load even when it has been switched off. As a result, when an adversarial load is restored, it may no longer be served. The attack may then decrease in magnitude as adversarial load is shed throughout the attack period.

3. METHODOLOGY

A commercial dynamics simulator, PSS/e, was used to conduct experiments on the RTS-96 case. Due to the RTS-96 case being a set of three identical networks with two extra buses for interconnection of said zones, we selected the third zone to represent our makeshift microgrid. In order to adequately represent the the individual loads and the associated feeders at a distribution level, we broke each load model presented in the test case into 10 identical individual loads, each of which is connected to the substation by a different feeder. An example would be a 100 MW, 10 Mvar load on a certain bus. The load is broken into ten loads each with values of 10 MW and 1 Mvar.

In order to represent adequate cycling behavior, we allowed feeders to be either adversarial or non-adversarial. We first select the amount of load we wish to cycle in the microgrid, we then use this to determine how many adversarial feeders exist per bus. The representation was as follows: If we were to cycle load from between 40% and 100% of the total load, each bus in the microgrid would have 4 non-adversarial feeders and 6 adversarial feeders. It was important to create diversity throughout the case, thus we chose the adversarial feeders at each bus uniformly at random and independently. For each amount of load we cycle, we choose the adversaries at each bus as we stated before. For simulations using the same amount of load cycling, we use the same distribution of adversaries throughout the microgrid; this is to ensure that the same amount of load being cycled at different frequencies will result in different behavior due to this change in frequency, not due to the change of adversarial locations.

Dynamics were implemented in the case by using salient generator models along with the IEEE type 1 exciter and IEEE type 2 governor. Protective relays were also built for the case which included overcurrent line relays, undervoltage + underfrequency bus relays, and underfrequency machine relays. The initial pickup points for overcurrent line relays were synthesized by running the steady state solution and using the line currents at hand. The relay pickup time was chosen to be 140 % of the operating current in the steady state with a zero reset time of 5 seconds. Line relays would trip the associated branches if they timed out during operation. Table 1 shows the other setpoints for the line relays.

Table 1. Different operating points for overcurrent relays

	Percent of Pickup	Trip Time (s)
Point 1	100 %	5
Point 2	120 %	0.2
Point 3	140 %	0.15
Point 4	160 %	0.1
Point 5	180 %	0.05
Point 6	200 %	0

Undervoltage and underfrequency load shedding protection was produced by placing relays at each feeder previously created. For

the ten feeders per bus, five different setpoints were created to represent 20 % load shedding at a bus per setpoint; these are shown below in Table 2. In order to create variability in load sheds pertaining to frequency, we introduced four different types of setpoints that represent time until load shed. The time until operation for frequency points is a set value divided by a random variable, x, that can take on a value of 1, 2, 3, or 4. The relays for the ten feeders in the same bus shared the same value of x. This allows more diversity across bus relay configuration ensuring not all loads are shed at once due to common frequencies in smaller islands. Voltage points do not need such variability as their voltages differ enough throughout the network.

Table 2. Undervoltage/Underfrequency load shedding relays operating points

	Volt Pickup	Trip (s)	Freq Pickup (Hz)	Trip (s)
Pt 1	0.88 P.U.	3	59	4/x
Pt 2	0.85 P.U.	1	58.5	2/x
Pt 3	0.80 P.U.	0.5	58	1/x
Pt 4	0.75 P.U.	0.25	57.5	0.5/x
Pt 5	0.70 P.U.	0.1	57	0.25/x

A similar technique for machine relaying was used to ensure diverse frequency trips. We attach three underfrequency trip points for each machine in the case and introduce random time trips as shown in Table 3. We use a random variable, y, that can take on values of 1, 2, or 3.

Table 3. Points of operation for generator protection relays

	Frequency Pickup (Hz)	Time Until Trip (s)
Point 1	58.5	y
Point 2	57.5	y/2
Point 3	56	y/4

As stated earlier, a feeder can be adversarial or not. The protective scheme is setup such that adversarial loads may be shed even when cycled off. This adequately models an operator shedding a feeder during protective actions even if the feeder has been completely shut off by an adversary. We assume that the operator does not know the exact distribution of load on the bus, thus feeders are shed according the the predesigned protection schemes.

4. RESULTS

We performed tests on the RTS-96 case by allowing all buses in the microgrid to have a number of adversarial feeders. We tested on cases that cycled 30 %, 50 %, and 80 % of the microgrid load. We also cycled each attack at frequencies of 0.05 Hz, 0.1 Hz, 0.5 Hz, and 1 Hz. Attacks lasted for 100 seconds with the simulation terminating 75 seconds after the attacks end.

Interestingly, we observed that the oscillation of more load in the microgrid did not always correspond to the worst outcome; in fact we found that oscillating from 70 % to 100 % of the loads (*i.e.*, cycling 30% of the microgrid load) at 0.1 Hz in the microgrid caused a major loss in load, machines, buses and branches. Table 4 shows the remaining load after attacks lasted for 100 seconds.

The loads remaining are those that exist at stable islands after an attack occurs. Unstable islands are either directly disconnected due to protection or not counted as served if the island has not converged upon termination of the case. Similar behavior can be seen with the remaining machines after attacks shown by Table 4.

Normally high frequency-oscillation of feeders did not adversely effect machine tripping too much. We saw that low amplitude oscillation did not always result in less machine tripping. The cycling of half the loads seems to result in fewer machines tripping than cycling either 80 % or 30 %. We also observe a similar story for the remaining branches/transformers after each attack.

In Table 4, we track remaining load after an attack along with machines (generation), and branches (in service two winding transformers and bus tie lines). The remaining branches after attacks seem highly correlated with the remaining machines in the case. We see that the cycling of 50 % of microgrid loads results in less machine trips on average through differing frequency attacks. The remaining branches and transformers only represent ones that exist in stable islands upon completion of a test case. Normally high-frequency load oscillation caused only a small fraction of machines and branches to trip, however lower frequency coupled with high or low load oscillation removed a large portion of branches and transformers in the working case.

We also observe how many buses were lost after an attack ended in Table 4. The number of lost buses came from two different scenarios. The first cause was due to protective line tripping which isolated buses into separate islands. If an island were to lose all machines, the buses are set out of service due to the inability to serve as an active portion of the case. The other cause is due to islanding, however the island becomes unstable before losing all generation. If an island becomes unstable and reaches a point in which it cannot converge, the entire island is set out of service. The least number of buses that are disconnected come from a high frequency-oscillation, low amplitude-oscillation attack. We observe cycling half of the load in the microgrid seems to have less variability in terms of all parameters shown in Table 4 with respect to frequency, whilst frequency has a big impact on cycling 30% and 80% of the load. The worst case scenario again results from oscillating 30 % of the load at a frequency of 0.1 Hz.

One major result that was not immediately expected was the large impact small oscillations of load could cause as opposed to medium oscillations. The worst performance outcome was found when cycling only 30 % of the load at 0.1 Hz. We found that low amplitude oscillation allowed the perturbation to be felt by a large portion of the grid before protective islanding isolated the attack. As a result, the low oscillating attack at 0.1 Hz was able to cause enough distortion to cause a large island to become unstable before it broke into protected regions. In case of high-amplitude oscillation attack, the protective load shedding scheme was able to isolate the attacked region in the microgrid, however the microgrid and connected buses normally did not survive due to such an aggressive attack. The moderate-amplitude cycled load attack normally caused protection to isolate the fault, but some portions of the attacked microgrid still survived due to less drastic cycling. It is important to note that different protection schemes may result in differing behavior among the explored attack scenarios. The assumed testing did not account for an adversary knowing the protective layout of the system; as a result, more sophisticated attacks may cause further damage to the grid (in particular bypassing known protective operations isolating the attack).

Table 4. Remaining load, machines, branches after an attack, and amount of buses lost

Attack	Active Load (MW)	Reactive Load (MVAR)	Machines	Branches	Lost buses
Normal Operation	9037	1737	99	120	0
80 % at 0.05 Hz	4201	845	57	49	38
80 % at 0.1 Hz	4745	901	66	62	26
80 % at 0.5 Hz	6220	1121	83	74	14
80 % at 1 Hz	6884	1259	90	77	13
50 % at 0.05 Hz	6454	1174	90	83	12
50 % at 0.1 Hz	6381	1157	89	75	13
50 % at 0.5 Hz	7097	1302	90	79	13
50 % at 1 Hz	7052	1299	90	76	13
30 % at 0.05 Hz	5685	1016	82	59	27
30 % at 0.1 Hz	3953	793	55	45	41
30 % at 0.5 Hz	6509	1260	86	86	5
30 % at 1 Hz	6741	1294	91	80	4

5. CONCLUSION

This paper investigated potential impacts of cyber attacks that exploit compromised smart meters to oscillate the total load of a microgrid. We found that an intelligent adversary could produce a small-amplitude load oscillation at a problematic frequency that can distort the grid and cause protective measures to take actions resulting in many losses and islanding. With presented material with respect to smart meter security exploitation, possible attacks on such systems could create harmful consequences that need to be addressed. No countermeasures to such attacks were explored in this paper, but remain a focal point for future research.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer

6. REFERENCES

[1] Estimating the costs and benefits of the smart grid. Technical report, Electric Power Research Institute (EPRI), 01 2011.

[2] Smart meters and smart meter systems: A metering industry perspective. Technical report, Edison Electric Institute and Association of Edison Illuminating Companies, 2011.

[3] Advanced metering infrastructure installations in the U.S.A. `http://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3/`, 2016.

[4] R. Anderson and S. Fuloria. Who controls the off switch? In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 96–101, Oct 2010.

[5] Aurora Geib. How privacy-conscious consumers are fooling, hacking smart meters. Natural News, July 2012.

[6] Kelly Higgin. Smart meter hack shuts off the lights. InformationWeek, October 2014.

[7] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry. Switched system models for coordinated cyber-physical attack construction and simulation. In *Smart Grid Modeling and Simulation (SGMS), 2011 IEEE First International Workshop on*, pages 49–54, Oct 2011.

[8] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry. A smart grid vulnerability analysis framework for coordinated variable structure switching attacks. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–6, July 2012.

[9] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security Privacy*, 7(3):75–77, May 2009.

[10] Stephen McLaughlin, Dmitry Podkuiko, Sergei Miadzvezhanka, Adam Delozier, and Patrick McDaniel. Multi-vendor penetration testing in the advanced metering infrastructure. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 107–116, New York, NY, USA, 2010. ACM.

[11] Anu Natarayan. *The Emerging Smart Grid: Opportunities for Increased System Reliability and Potential Security Risks*. PhD thesis, Carnegie Mellon University, 2012.

[12] Navigant Research. Number of smart meter installations, worldwide, 2013.

[13] Elhadi Shakshuki, Khaled Shuaib, Zouheir Trabelsi, Mohammad Abed-Hafez, Ahmed Gaouda, and Mahmoud Alahmad. Resiliency of smart power meters to common security attacks. *Procedia Computer Science*, 52:145 – 152, 2015.

[14] P. Wong, P. Albrecht, R. Allan, R. Billinton, Q. Chen, C. Fong, S. Haddad, W. Li, R. Mukerji, D. Patton, A. Schnei-

der, M. Shahidehpour, and C. Singh. The IEEE reliability test system-1996. *Power Systems, IEEE Transactions on*, 14(3):1010–1020, Aug 1999.