Modeling Power Distribution to Heterogenous Customers in the Presence of a Strategic Adversary

Nathan Burow, Saurabh Bagchi
Purdue University
{nburow, sbagchi}@purdue.edu

***Abstract*—One of the key benefits of the smart grid is the ability to integrate new power sources, most notably renewables. However, these sources produces variable amounts of power, which makes fulfilling consumer demands challenging. To offset this however, the smart grid will allow consumers to add flexibility to their demands. This added flexibility will let the utility smooth demand and reduce peak demand by rescheduling flexible consumers to off peak times. All of this will rely on the cyber component of the smart grid, which means that it is susceptible to malicious manipulation. This paper examines a system with variable power supply and flexible consumer demand in the face of a limited, strategic adversary. We model the game between the utility and the adversary and the utility to find the impact of various attacks, and who how much effect strategic defensive investments can have. We find that the attacker can increase standby power usage by 50%, and that our defensive strategy can halve this to 25%.**

I. Introduction

It is trite but true that the power grid underlies most of modern civilization. Traditionally the power grid has had a few fixed producers that sell power to utilities, who in turn distribute it to their customers. Traditionally these customers have not coordinated with the utility, but simply bought whatever power they needed at the prevailing price. Similarily, utilities have simply ensured that they have enough power to meet their customer's demands. With the advent of the smart grid, this picture is giving way to dynamic supply and dynamic demand, incentivized in part by dynamic changes in price of energy. Renewables like wind and solar will enter the supply side of the equation in greater numbers and will contribute to the variation in available supply, in somewhat unpredictable manner. Increased connectivity through the smart grid will allow consumers (and more specifically, the smart appliances) to be aware of the prevailing price of energy and calibrate its usage accordingly.

In the smart grid, consumers can also communicate their power demands and constraints to the utility, who can then schedule power dispatch to them accordingly. For example, if the communicated demand over the next time window (15 minutes out, one hour out, etc.) exceeds the anticipated supply, the utility may decide to fire up an expensive generator using fossil fuel. One crucial observation enabling this kind of dynamic demand-supply negotiation is that some demand loads are flexible ("elastic" in economic-speak) in that they can be scheduled to run at any time within a time window. For example, running the dishwasher or charging an electric vehicle is flexible as long as it is completed by a certain time. Other kinds of loads, such as running the AC in the summer, are not flexible. In aggregate though, the presence of elastic loads will enable consumers to indicate flexible usage periods to the utility, and the utility to schedule its various sources of electricity in a price-optimal manner. This beneficial aspect of the smart grid has been expressed in many publications and even mainstream books (such as, Thomas Friedman's "Hot, Flat, and Crowded" from 2009). The scheduling problem for the utility has been investigated in many publications, many of which provide a theoretically rigorous treatment of the problem [**?**].

However, no prior work has investigated the impact of security attacks on such scheduling. Security attacks in the smart grid are widely anticipated [1] and many demonstrations have been done in laboratory settings [2]. It is till now unknown how security attacks — jamming, false data injection, and delays in the communication channel — affect the scheduling problem. The ultimate possible impact could be in the form of brownouts or blackouts and in our evaluation, we bring this out in the form of instantaneous mismatches between the demand the supply. A mismatch is undesriable in both directions — if the demand is larger, this may lead to brownouts or blackouts, and if the supply is larger, then this may mean that the utility had to use more expensive sources of energy to fill a perceived (but ultimately incorrect) demand. The attacks could result in these impacts by disrupting the communication of the actual demand. Due to the interconnected nature of the smart grid, there are many possible entry points for such attacks — the smart meters, the connection of these to the neighborhood data collection unit (DCU), the connection between the DCU and the control station at the local sub-station, etc. In addition to demonstrating the effect of such attacks, we take well-known security controls and evaluate how using them in our smart grid setting will mitigate the effects of some of these attacks. For example, we show that transient denial of service can be sucessfully "fought through" by using historical data of demand, even when the demand is somewhat fluctuating from day-to-day, provided a good characterization of the elasticity of the loads can be done.

We build a discrete event simulator with two actors — a strategic adversary and a defender (can be taken to model a utility). The adversary has a budget for the attack, in terms of the number of assets she can simultaneously target, and performs a game-theoretic determination of which assets to target subject to the budget constraint. The defender also

performs a game-theoretic determination of which assets to make more secure against the above types of attacks. The discrete event simulation can model various intensities of attacks, different characteristics of loads, and different budgets for the adversary and the defender. For each configuration, it can provide the mismatch metric without any attack, with the attack and without any defense, and with the attack and with the defense controls in place.

We find that two new classes of attack - changing the time constraints of customer demand, and adding constraints to customer demand - can have a signficant impact, increasing the mismatch by up to 50%. These two attacks directly target the amount of flexibility available to the utility when dispatching power to the consumer, and so serve to hgihlight the critical importance of that flexiblity to the system. Our defensive strategy can halve the additional mismatch from the attack, which shows that systems designed with these new attack surfaces in mind can be robust to these new attack surfaces.

We have released our simulator as an open source project, along with our simulation datasets at Give URL. The rest of the paper is organized as follows: II surveys existing work in the field, III details our model of the customers, power producers, utility, and adversary, IV defines the strategic game between the adversary and the utility, V provides and overview of our simulator, VI gives the details of our results, and **??** concludes.

TODO: Finish overview of our paper and results. Add citations

II. Related Work

We build on the model for flexible consumer demand presented by Petersen et al [3]. There are three classes of consumers: Buckets, Batteries, and Bakeries. Buckets can both accept power from the grid, or push power back into the grid, and so are the most flexible class of consumer. Batteries must be charged to a certain level by given time, but do not need power constantly while charging (think of an Electric Vehicle: it needs to be charged by the next morning but it does not need to charge constantly). Bakeries are the most constrained class of customer: adding a requirement for constant charging to the Battery constraints.

Other prior works have looked at attacks made possible by the introduction of the smart grid, but they do not consider consumer diversity. Chen et al [4] present a scheme for detecting false data injection attacks through deviations in spatial / temporal relationships of data. Lin et al [5] examine the effects of false data injection on routing power in the smart grid. Yuan et al [6] examine similar attacks against the smart grid, and provide a set of equations that show how much and where an attacker can alter the load in the system while still remaining undetected. Sridhar et al [7] present a model-based attack detection scheme that focuses on modulating the frequency of the grid in the face of false data injections. Teixeira et al [8] provide a game theoretic model of a stealthy attacker who can alter line voltage readings, and present strategies for altering the configuration of substations to limit the set of stealthy attacks.

Other classes of attacks have been examined in the literature, agian without considering consumer diversity. The DETER testbed has been used to examine the effects of DDoS attacks against smart grids [2]. Gupta et al [9] presented a limited, strategic adversary who could jam a certain number of communications channels, and presented optimal strategies for such an adversasry.

Prior work has also considered how best to model risks introduced by the cyber component of smart grids. Ten et al [10] present a survey of existing work on the security of smart grids at the time, and present a risk assessment framework. Kundur et al [11] show a methodology for modeling the grid and its interdependencies as a graph, which allows automated impact analysis. In our prior work, we presented a tool for risk assessment of advanced metering infastructure [12].

III. Model

We examine the smart grid over the course of a given day, divided into arbitrary time steps. In this section we lay out the basic components of the grid, how we model them, and how they interact. In the next section we introduce the adversary. Our model has three components: Power Generation, Consumers, and the Utility. Each of these components is characterized by their behaviors, goals, and constraints. Additionally, our model for how they communicate is presented in this section.

A. Power Generation

We primarily consider power generated by renewable sources such as wind and solar. These sources have a high degree of individual variation. However, we assume that there are sufficient sources from a wide enough geographic area that in aggregate they produce a normally distributed amount of power. We also include a fossil fuel plant that is capable of making up any short fall in production for a given time period. The renewable sources provide their power to the utility continuously, however the fossil fuel backup is only used when needed.

B. Consumer

We model three different types of consumers, classified based on the flexibility of their demand. These classes are the same as in [3]. These consumers are primarily categorized based on the flexibility of their power demand. Consumers have a maximum amount of power that they can accept in a given time step, as well as a maximum amount of energy demanded (the sum of all the power they receive).

The first and most flexible class is buckets. Buckets are conceptually a heat sink, or other store of power that can also be tapped. They are modelled as starting empty, and have both a positive and negative constraint on the amount of power they can accept from or provide to the grid. As such, they can provide a reserve against production shortfalls, or a place to store excess production for the future.

The second class is batteries. A good example of this class is an electric vehicle that has been plugged in to charge

overnight. As long as it has received a full charge by morning, you don't care when it charges. Further, it does not have to be charged continuously. More formally, a battery can only receive power from the grid, and is contrained by an amount of energy required, and a time by which that energy is required.

The final and least flexible class are bakeries. Taking the obvious example: a bakery must produce bread by a certain time. Bread must be baked for a certain amount of time, and furthermore must be baked continuously. This means that like batteries bakeries face time and total energy constraints, but add an additional constraint in that once they are started they must received power every time step until they have completed their job.

C. Communication

Before describing the utility, we first need to outline how the power generators and consumers communicate with the utility. The power generators communicate the amount of power they are currently producing to the utility at each time step. However, they have no forward knowledge of how much power they will produce at the next time step, and consequently neither does the utility. The consumer's communicate each power demand and its constraints to the utility when they create it. We simplify this by assuming that all jobs are created at the beginning of the day. However, customers are free to modify the job at any point.

D. Utility

The utility has two inputs: the amount of power generated by the renewable sources, and the demands from the consumers, which are communiated to it as described in III-C. The utility is required to meet all consumer demands. However, it is free to reschedule them to the greatest extent possible. Using this flexibility the utility's goal is simple: to ensure that all power generated is used, and to minimize the amount of power it has to receive from the fossil fuel backup. To do this, the utility uses the Agile Balancing scheduling algorithm in [3]. This first provides any required power, and then dispatches the rest based on flexibility.

IV. Game

This section defines the game between the adversary and the utility. This is a multistage game, with moves being made at each time step. We consider several variations on this game, which are differentiated by the adversary model. In general, the adversary seeks to maximally disrupt the grid by making strategic use of its limited resources to disrupt the grid. We play the game first with the utility only being allowed to follow its scheduling algorithm on the input it receives. We then replay the game after the utility has made strategic defensive investments based on the outcome of the first game. As such the game serves as an impact analysis platform that can guide defensive investments, and show the impact that they have against the adversary.

IV provides an overview of the adversary and utility strategies, explained in more depth below. When choosing which subset to attack or defend, the adversary and the utility weight individual bakeries / buckets by their agility factor [3] which encapsulates how much flexibility the customer is providing the system (higher agility = more flexibility). The proabilities are assigned according to 1.

Class	Adversary	Utility
Jamming	Attacker Jams a subset of the bakeries.	Utility uses historical data with accuracy +-20%
False Data Injection - Load	Attacker Increases the load of a subset of bakeries by 20%	Utility encrypts communications with a subset of bakeries, preventing them from being attacked
False Data Injection - Time	Attacker changes the timing constraint of a subset of bakeries such that they all must run at the same time	Utility encrypts communications with a subset of bakeries, preventing them from being attacked
False Data Injection - Class	Attacker permutes a subset of buckets into bakeries	Utility encrypts communications with a subset of the buckets such that they cannot be permuted

TABLE I
Attack and Defense Strategies

$$\sum_{i=1}^{n} \frac{i}{\frac{n*(n+1)}{2}} = 1 \tag{1}$$

A. Operational Rules

At the beginning of the day, the customer's send their demands to the utility. These are visible to the adversary, but he cannot modify them in transit (ie they are protected by HMAC or similar), other than by jamming the customer and causing the packet to be lost in transit. Once the customer messages are received, the adversary can inject any modification messages that he wants, subject to the model in IV-B. At that point the day begins, and the power producers send their production to the utility, who distributes it according to III-D. The power plant and utility continue in this fashion for every time step until the end of the day. At this point, the total cost that the adversary inflicted on the utility is determined.

B. Adversary

The adversary's goal is to force the utility to either waste power, or have to pull power from the backup. Either of these sources of wated power cost the utility money. This allows us to state the attacker's goal as to maximize the cost of the attack to the utility. To do this we present the following adversary model. Note that the idea of jamming [9], and false data injection on loads [5] [6] are established in the literature, though novel in this context. The false data injection on time constraints and consumer classification are new extensions on false data injection made possible by the presence of heterogenous customers.

- Jamming. The attacker can jam communication between the utility and producers / consumers. We model this in terms of the number of customers prevented from

communicating with the utility, divorced from any specific topology. We assume that the attacker can jam a percentage of the utility's customers, as detailed in V. This is not a stealthy attack: the utility can tell that the communication channel has been jammed.

- False Data Injection - Load. The attacker can modify the communicated demand from consumers / supply from producers. Here the attacker can remain stealthy. While the exact amount of noise the attacker can inject depends on a number of factors [6], for our purposes - exploring the effect of this attack given heterogenous customers - it is sufficient to assume that the attacker can increase the demand by 20%. This is a stealthy attack, with no known statistical method of detecting it [6].
- False Data Injection - Modify Time Constraints. Here the attacker can change the consumer's time constraints, ie he can cluster the demands more tightly. This can signfiicantly decrease the flexibility available to the utility by forcing power to be distributed to many customers at the same time. We assume a straightforward extension of [6] such that there is no known statistical method for detecting this attack. How the attacker clusters the demands is detailed in V.
- False Data Injection - Change Customer Class. Buckets are very useful to the utility in scheduling because they provide the most additional flexibility. The attacker could target them by adding constraints such that the buckets become bakeries. Here we allow the attacker to modify a percentage of the buckets, as detailed in V. We assume sufficient noise in the composition of the customers (ie buckets, bakeries, or batteries) that this modification cannot be detected with any known technique.

C. Utility

The utility's core strategy is to detect and correct for any malicious communications. This will allow its performance to be constrained solely by its scheduling algorithm (out baseline) and not by the attacker. However, only the jamming attack is detectable by the utility, assuming the attacker follows the constrainst set forth in [6]. Consequently, the best that the utility can do against the other attacks is to make defensive investments. The utility knows the attacker's strategy. Consequently, the utility can pick a subset of the same size of the attacker, chosen using the same criteria, and defend it. The utility's defense employ stronger (and therefor more expensive) cryptography when communicating with the defended customer. An example would be adding public key authentication. This defense is assumed to be too burdensome for general deployment, but practical enough for limited use as a defense. This defense allows the utility to significantly blunt the damage inflicted by the adversary **??**.

- Jamming. Jamming is always detected. The utility corrects for this by using historical data. The historical load data is accurate to within 20%. This means that the jamming attack may actually ease the scheduling problem (by decreasing load), though even in this case it would lead to brownouts as customers receive less power than they require (this effect is left for future work). Note that we assume that the constraints in the historical data are accurate. That is, if if a customer was a battery before being jammer, a customer is a battery afterwards, and has the same time constraint.
- False Data Injection - All Varieties. The utility cannot actively defend itself against this attack, because there is no known technique to detect it assuming the adversary stays within its limits. The utility can, however, model the adversary's likely targets and defend them against attack, as described in IV-C. This passive defense further limits the amount of damage that the attacker can inflict. If the utility were to institute a policy that all constraints (load, time, constant power) could only be relaxed (decreased, delayed, removed) then these attacks would become impossible (the attacker could only make the utility's scheduling job easier, not harder). However, we consider such policies to be too constraining on customers, and unlikely to be deployed.

V. Simulation

This section provides a brief overview of our open source simulator [XXXX], describing its parameters and use. The simulator takes as command line arguments how long the simulation is, a seed for its random number generator, which attack model to use, and what percent of the customers the attacker can effect. It outputs the amount of power either wasted (positive number) or required from backup sources (negative number). It gives three such results: the baseline result without the attack, the result with the attack, and the result with both the attack and defense.

Internally, the renewable energy producers are modeled collectively. We assume that there are sufficiently many of them that the central limit theorem applies and they are normally distributed in aggregate. Consequently, we sample from a normal distribution at each time step to find the amount of power produced. The mean and median of this distribution are tunable in the code, and are members of the Simulator class.

The number of Bakeries, Batteries, and Buckets is tunable in the code, with members of the Simulator class for each. When initializing them, we first calculate the total amount of power available, on average, over the simulation by multiplying the mean of the producers by the simulation run time. This is then divided by the total number of customers to get the mean power required per customer. We again assume that the customers in aggregate follow a normal distribution as per the central limit theorem. The standard deviation of this distribution, expressed as a percentage of the mean, is a user tunable member of the Simulator class. We sample this distribution once for each customer to get the amount of power actually required for the customer. Note that this implies that on average the amount of power demanded and supplied is equal, which makes the scheduling problem tractable. We then calculate the minimum amount of energy each customer must

receive per time step to statisfy his total demand. We increase this amount of energy by a random percentage, and based on this energy per time step compute the earliest time that the customer could be finished. We then select the actual required finish time (for Bakeries and Batteries) uniformly over [earliest, simulation end].

As mentioned abover, the percent of customers that can be attacked is a parameter to the simulator. This is used to calculated the actual number of customers attacked. We make the simplifying assumption that the number of customers attacked is less than the number of Bakeries for the Jam, False Data Injection - Load, and False Data Injection - Time attacks. This allows our adversary model to only consider Bakeries for those attacks. Bakeries are the most constrained customers, so attacks against them are the most damaging. For the False Data Injection - Class attack we assume that there are sufficient Buckets in the system so that only Buckets are attacked. As above, turning a Bucket into a Bakery (most flexible into least flexible) is the most damaging attack.

VI. Experimental Results

We used the simulator to examine the results of the game between the adversary and the utility described in IV. We examined the effectiveness of our four proposed adversarial strategies and our suggested defense techniques under two different scenarios. In the first, there are an equal number of each class of customer. In the second, 40% are Bakeries, 40% are Batteries, and 20% are Buckets. All of our results are over 15,000 total customers in order to make our distribution assumptions accurate. Further, the results presented here are average over 10 different random number seeds in order to eliminate any bias in a given sample from the distributions.

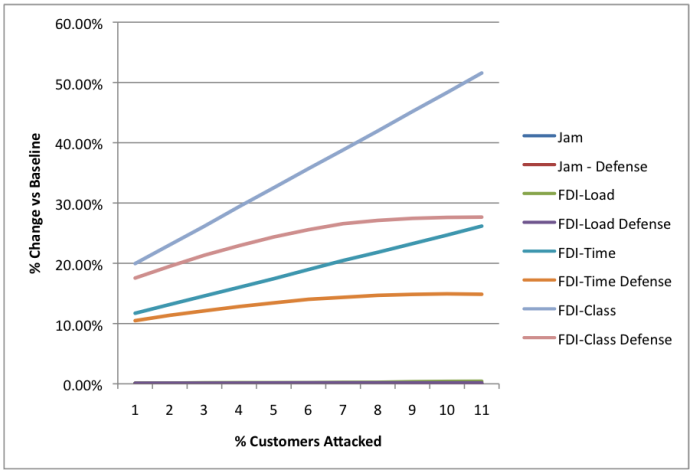

Fig. 1. Attack strategies with equal numbers of customers in each class

VI shows the results for the first scenario, with 5,000 Bakeries, Batteries, and Buckets. The first important thing to note is that in all cases the defense strategy halves the efficacy of the attack. It is also interesting ot compare the efficacy of the different classes of attack. Both the jamming attack and the false data injection - load attack are essentially ineffective. Both permute the load of a subset of bakeries by 20%, which is not enough to have a significant effect of the utility's scheduling problem, and shows the efficacy of existing techniques for dealing with this problem. However, the time and class injections had a large impact, at 26% and 52% respectively. Both of these attacks are only made possible by the advent of the smart grid and the addtional information that it communicates. Our defensive investment strategy was able to decrease the malicious effects to 14% and 27% respectively. This illustrates that these new vulnerabilities can be mitigated, and highlights the need to do so.

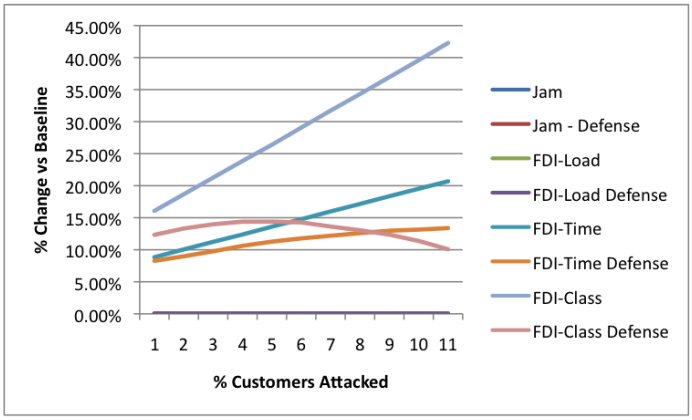

Fig. 2. Attack strategies with different numbers of customers in each class

VI shows the results for the second scenario with 6,000 Bakeries and Batteries, and 3,000 Buckets. The overall results here are roughly the same as for scenario one. The item of interest is that the defense for false data injection - class becomes more and more effective as more customers are attacked. This attack converts Buckets into Bakeries. The efficacy of the defense highlights the critical flexibility that Buckets provide for the utility.

VII. Conclusions

The smart grid provides greater flexiblity to the utility by recognizing inherent difference between customer's power demands, and this flexibility in turn helps the utility integrate new sources of energy, like renewables, that provide a fluctuating supply of power. The problem for the utility is to schedule customers' demands and make the best possible use of renewable power (by minimizing both the amount of standby power used, and the amount of generated power that is not dispatched). The additonal communication from customers to the utility - about their demand and its constraints - provides a new attack surface to malicious adversaries. We find that in the worst case even a strategically limited adversary can increase the amount of standby power requried by 50%. Our proposed defensive strategy for the utility - to model what the adversary will likely attack and protect those assets - can cut this worst case number by at least half.

REFERENCES

[1] (2015, May). [Online]. Available: http://www.nist.gov/el/smartgrid/cybersg.cfm

[2] A. Hussain and S. Amin, "Ncs security experimentation using deter," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 73–80.

[3] M. Petersen, K. Edlund, L. H. Hansen, J. Bendtsen, and J. Stoustrup, "A taxonomy for modeling flexibility and a computationally efficient algorithm for dispatch in smart grids," in *American Control Conference (ACC), 2013*. IEEE, 2013, pp. 1150–1156.

[4] P.-Y. Chen, S. Yang, J. McCann, J. Lin, X. Yang *et al.*, "Detection of false data injection attacks in smart-grid systems," *Communications Magazine, IEEE*, vol. 53, no. 2, pp. 206–213, 2015.

[5] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on*. IEEE, 2012, pp. 183–192.

[6] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 382–390, 2011.

[7] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *Smart Grid, IEEE Transactions on*, vol. 5, no. 2, pp. 580–591, 2014.

[8] A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *American Control Conference (ACC), 2014*. IEEE, 2014, pp. 4372–4378.

[9] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 1096–1101.

[10] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 40, no. 4, pp. 853–865, 2010.

[11] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 244–249.

[12] T. Shawly, J. Liu, N. Burow, S. Bagchi, R. Berthier, and R. B. Bobba, "A risk assessment tool for advanced metering infrastructures," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014, pp. 989–994.