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

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

***Abstract*—Abstract goes here, especially once I get this in a better / more rigorous format. Bare bones for now.**

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 need at the prevailing price. Similarily, utilities have simply ensured that they have enough power to meet their customer's demands.

The future will be very different. More producers will enter the grid as renewables like wind and solar become more prevalent. Increased connectivity through the Smart Grid will allow consumers to be price sensitive, and put off demand during peak usage (and thus peak price) hours where possible. This will smooth the demand curve that utilities face, and make the grid more predictable.

In the smart grid, consumers will communicate their power demands and constraints to the utility, who will then schedule power dispatch to them accordingly. The crucial insight here is that some power consumption, such as running the dishwasher or charging an electric vehicle, is flexible as long as it is completed by a certain time. Other power consumption, such as running the AC in the summer is not flexible. In total though, this will give the utility more flexibility in dispatching power, and will smooth demand.

Offsetting the demand smoothing from increased consumer flexibility will be increased variation in power supply. More and more power will come from distributed and unpredictable sources: renewables such as wind and solar. These power supplies may flucuate during the day, and the level of power available from them at any given point is not knowable in advance.

This creates a coordination and scheduling problem for the utility. The utilities goal is to use all available power at any given time, constrained by the need to meet consumer's demands. If the utility faces a short fall, it has to turn to more expensive standby power sources to make up the difference. Any power that the utility cannot dispatch is wasted.

This scheduling problem is not the only difficulty facing the utility though. Information about consumer power demands and constraints as well as the amount of power being produced flows over a communications network, and it is tautological that any communications network can and will be attacked. We propose a malicious strategic adversary with strong abilities, whose goal is to destabilize the grid while remaining undetected.

TODO: Finish overview of our paper and results. Add citations. This introduction may well serve as the related works section if need be.

II. Model

A. Producer

We focus on renewable energy sources, which provide a fluctuating amount of power. Each sources produces a uniform random amount of power in a given interval. This amount of production is bounded by the minimum for the source and its maximum production capacity.

TODO: Is this the right way to go here?

B. Consumer

We model three different types of consumers, classified based on the flexibility of their demand. These follow the standard templates in literature for heterogenous consumers.

The first and most flexible class is buckets. Buckets are modeled after (... check the citation). As such, they can store power up to their maximum capacity. Buckets also consume power, and have a minimum floor that they cannot fall beneath.

The second class are batteries. Batteries have to be charged (receive a given amount of power) by a fixed end point. However, they do not have to charge continuously, and do not loose power when not being charged.

The least flexible class are bakeries. Like batteries, bakeries must receive a given amount of power, unlike batteries they must receive power continuously. Intutitively, think of baking bread. The over must remain on continuously for the bread to be properly baked (ie edible).

TODO: Give the equations, or maybe just say they are in the reference?

C. Utility

The utility's goal is to dispatch all power generated in a given time period. Each megawatt of power wasted incurs a penalty, ad does each megawatt of power that has to be used from standby sources.

TODO: Should these penalties be weighted? I'm inclined to say that standby should have a larger penalty: perhaps 2x.

III. Game

This section defines the game at a given time step. We work with both single and multi-round games in our analysis. The game is played between a strategic adversary that seeks to maximally disrupt the grid, within the constraints of his resources and the utility company whose objective is to dispatch all power at the time step.

A. Adversary

We consider X different adversary models:

- Jamming. The attacker can jam communication between the utility and producers / consumers. We consider scenarios where the attacker can jam 30% or 60% of communications between producers / consumers and the utility.

  TODO: This is not particuarly novel, there is prior work on jamming.
- False Data Injection - Load. The attacker can modify the communicated demand from consumers / supply from producers. Here the attacker is constrained to a small change of less than 50%. We analyses scenarios where the attacker can modify 30% or 60% of the communicated information.

  TODO: There is a lot of prior work on vanilla FDI, not novel. Though we could perhaps sell it in this context. TODO: Possbile novelty: What if any constraints to inject. IE the load is a new job, which of the 3 B's should it be? we could do the next two bullet points first to determine that, then move to this "more sophisticated" version of the attack.
- False Data Injection - Modify Constraints. Attacker can change the consumer's time constraints. The attacker can thereby decrease the flexibility available to the utility. The attacker would identify the largest loads possible and change their constraints so that they all have to receive power now. We constrain the attacker to only be able to modify the constraints of 30% or 60% of customers.

  TODO: This seems to be the novelty for having the heterogenous consumers.
- False Data Injection - Add Constraints. 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. The same constraints on the number of actions the attacker is allowed to perform apply.

  TODO: This is also novel. Should we change the rules s.t. there is a cost per constraint added vs per customer effected?

The attacker's goal is to maximize the cost to the utility.

TODO: Phrasing on that goal? It is important to have this nailed down. TODO: Flesh this section out, bare bones right now until we agree on everything.

B. Utility

The utilities 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.

- Jamming. Jamming is always detected. The utility corrects for this by using historical data. We examine the effects of the historical data being 5%, 20%, or 50% inaccurate.
- FDI - Load. Following prior work, we assume that this is undetectable given the attacker constraints. Consequently the utility has no strategy in this case because it cannot distinguish it from the default case of no attack.
- FDI - Modify Constraints. Utility's strategy here should be to only allow constraints to be relaxed. This will prevent the attacker from removing flexibility from the system.

  TODO: Justifiable? Realisitic? I think this is sellable: the user has to authenticate or do something more complicated like cancel the job and add a new one (also authenticated), but can't mutate the job.
- FDI - Add Constraints. Utility does not allow any constraints to be added.

  TODO: Justifiable? Realistic? seems too black and white. TODO: Is our contribution to show what the attacker could do if these things were allowed as justification for banning them? TODO: Do we only end up allowing the addition of new jobs, which throws us back to the FDI-load scenario, and detecting malicious injections? I guess we could comment on what constraints / mix of constraints the attacker would want to impose.

Need to comment on a cost function / equivalent for the utility.

Utility's scheduling algorithm is the Agile Balancing algorithm presented in ... We use this for evaluating the attacks.

TODO: We really ought to consider multiple scheduling algorithms, so that the results aren't dependent on the algorithm used. Likely a bridge too far though.

IV. Experimental Results

TODO: Need to show baseline (ie under the previously published scheduling algorithm) vs with attacker results. Probably do figures by attack class, and show the percentage degradation in performance. Have multiple lines for each level of attacker capability (ie how many customers / producers the attacker was able to effect).

TODO: Perhaps we should show with / without proposed defenses.

V. Related Work

TODO: I have the notes to write this up. Mainly waiting until I am on my laptop with Bibtex, or can get it installed at school.

VI. Conclusions

TODO: Filler! Huzzah now we are at 6 pages.