SANDIA REPORT

SAND2016-9871
Unlimited Release
Printed September 2016

Game Theory for Proactive Dynamic Defense and Attack Mitigation in Cyber-Physical Systems

Joshua Letchford

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online ordering:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2016-9871
Unlimited Release
Printed September 2016

Game Theory for Proactive Dynamic Defense and Attack Mitigation in Cyber-Physical Systems

Joshua Letchford
Data Science & Cyber Analytics
Sandia National Laboratories
P.O. Box 969
Livermore, CA, 94551
jletchf@sandia.gov

Abstract

While there has been a great deal of security research focused on preventing attacks, there has been less work on how one should balance security and resilience investments. In this work we developed and evaluated models that captured both explicit defenses and other mitigations that reduce the impact of attacks. We examined these issues both in more broadly applicable general Stackelberg models and in more specific network and power grid settings. Finally, we compared these solutions to existing work in terms of both solution quality and computational overhead.

Contents

1 Introduction 7

2 Standard Stackelberg Security Model 9

3 Simple Network Model 17

4 Power Grid Models 21

Nomenclature 21

Model 23

Solving this Model 23

Additional models 27

5 Experiments 33

Runtime 33

Utility 34

References 37

Appendix

A Additional Models 39

Chapter 1

Introduction

It is clear that terrorist organizations take into account impact (economic and otherwise) when planning attacks. One prominent example of this is Osama ben Laden's interview with Al-Jazeera following 9/11, where he gave economic analysis suggesting that the impact of these attacks was in excess of one trillion dollars [16]. For this reason, there has been a great deal of recent work in security using game theory to account for the dynamic nature of an adversaries response when determining security policies, with deployed applications at sites such as airports and naval ports. While security investments alone may be the most economical way to deter attacks for some applications, for many of our larger cyber-physical systems this is unlikely to be true.

For systems of sufficient scale, complete immunity to failure is prohibitively expensive (if not impossible). For this reason, strategies for mitigating the effect of system failure have been studied, including limiting the spread of these failures, speeding the recovery of the system and maintaining critical infrastructure during failure [4]. However, in contrast with security policies, these mitigation solutions have generally been designed and evaluated only in terms of their direct effectiveness against threats, disregarding their potential for deterrence. One notable exception to this allows the defender to split a defense budget between protecting generators and substations, increasing generation or line capacity, and purchasing spare transformers however, their methodology has significant scalability issues and makes some problematic assumptions about the attacker [14]. Another adds a single investment area that globally reduces the time needed to repair all failures to a security model [2]. Additionally, in many of these models, the primary metric is amount of demand unsatisfied (load shed). While a reasonable starting point, in reality not all power outages are equivalent. The expected loss for a particular location losing power has been studied in a range of fields such as [13, 7]. The cost to stockpile redudant, replacement parts (to reduce the length of a potential outage) has also been studied [15].

We have focused on developing models that incorporate both security and damage mitigation of successful attacks in three settings:

- The standard Stackelberg security model with a single attacked target.
- An extended Stackelberg security model that allows for failure cascades, to abstractly

capture the interconnected nature of the possible targets.

- A model of the power grid using an underlying linear DC power flow model to evaluate the consequence of attacks. We first considered the case when a single target is attacked, and show how to transform this into the standard Stackelberg model. We then extend these concepts to a k-target framework, both individually and jointly allowing for a range of investments types such as demand reduction, alternative/repair preparation, new plants/increased generation, and transmission line defense.

Chapter 2

Standard Stackelberg Security Model

Our initial work focused on extensions to the standard Stackelberg security model proposed by Kiekintveld et al. [10]. In this model we have a defender who is interested in determining an optimal defense policy over a set of targets (T). The defender can choose to invest resources at any target to reduce the probability of a successful attack at that target, with the assumption that resources invested will lower the probability of a successful attack. Opposing the defender we have an adversary, who chooses one of these targets to attack, knowing the defense policy of the defender. In its simplest form, we can model the utility of the defender (attacker) for target $t \in T$ is $U_c^d(t)$ ($U_c^a(t)$) when the defender has invested resources into defending t (representing an attempted attack that was unsuccessful), and $U_u^d(t)$ ($U_u^a(t)$) otherwise. We will refer to this model and the corresponding extensions to other domains as the *Standard* or *Multiplicative* model.

One of the convenient properties of Stackelberg (security) games is that the follower (attacker) always has a *pure*-strategy (deterministic-strategy) best response, meaning that against any defense strategy available to the defender there will always exist at least one single target that they choose to attack that will give them at least as much utility as any possible *mixed*-strategy (randomized-strategy) available to them. This fact leads to the standard method for solving this model is to exploit the independence of the targets, separating the problem into a series of linear programs; one for each potential target [3]. This formulation, for a specific target $t^* \in T$ is depicted below:

$$Max\ p_{t^*}U_c^d(t^*) + (1 - p_{t^*})U_u^d(t^*) - \sum_t p_t c_t \tag{2.1a}$$

$$\text{s.t.} \tag{2.1b}$$

$$p_t U_c^a(t) + (1 - p_t)U_u^a(t) \leq p_{t^*}U_c^a(t^*) + (1 - p_{t^*})U_u^a(t^*), \qquad \forall t \in T \tag{2.1c}$$

At a high level, line 2.1c forces this LP to only consider defense strategies where target t^* is the optimal choice for the attacker by ensuring that the utility that the attacker would get from every target is at most the utility achieved if the attacker were to choose to attack target t^*. Given this restriction, the objective forces it to choose the defense strategy that optimizes utility for the defender. As neither player will be able to increase utility by changing targets, each of these LP's returns an equilibria. Finally, if we consider the set of solutions returned by this set of LP's (one for each possible target), it should be clear that the globally optimal solution for the defender exists in this set and is simple to locate (merely choose the target that has the highest objective value).

Next, we consider extending this model so that there are multiple types of mitigations from different sources interacting to determine the utilities of both the attacker and the defender. Unfortunately, difficulties arise in this multiplicative model if we are interested in combining multiple probabilistic defense options (e.g. [11] or [9]). An alternative is to consider a different relationship between security/mitigation options. The two options we will primarily explore here are an additive model, where the effect of a set of security options that all effect the same target is the sum of the individual effects, and a maximum model, where the effect on each target of a set of security options is the maximum of that set.

Our first alternative model, which we will refer to as the *Additive* (*Add*) model, we assume that we have a set M of mitigations, where $U^d_m(t)$ ($U^a_m(t)$) captures the effect of mitigation $m \in M$ on the utility of the defender (attacker). Below is the LP for finding the optimal mitigation choice for target t^*:

$$\begin{aligned}
&Max\ U^d_u(t^*) + \sum_m p_m U^d_m(t^*) - \sum_m p_m c_m && \text{(2.2a)}\\
&\text{s.t.} && \text{(2.2b)}\\
&U^a_u(t) + \sum_m p_m U^a_m(t) \leq U^a_u(t^*) + \sum_m p_m U^a_m(t^*), \qquad \forall t \in T && \text{(2.2c)}
\end{aligned}$$

Again, as with the SG model, line 2.2c ensures that the attacker prefers to attack target t^* and the objective searches within this feasible space to maximize defender utility.

Our next model, which we will refer to as a *Maximum* (*Max*) model is similar, but of course assumes that for each target, if more than one mitigation effects that target, only the mitigation with the largest effect has any effect. Unfortunately, are forced to add in one set of Binary variables (B) in the below Mixed-Integer program to solve for the optimal mitigation choice for target t^*:

$$\begin{aligned}
&Max\ U^d_u(t^*) + u^d_{m,t^*} - \sum_m p_m c_m && && \text{(2.3a)}\\
&\text{s.t.} && &&\\
&U^a_u(t) + u^a_{m,t} \leq U^a_u(t^*) + u^a_{m,t^*}, && \forall t \in T && \text{(2.3b)}\\
&u^a_{m,t} \leq p_m U^a_m(t) + L(1 - B^a_{m,t}), && \forall m \in M, t \in T && \text{(2.3c)}\\
&u^a_{m,t} \geq p_m U^a_m(t), && \forall m \in M, t \in T && \text{(2.3d)}\\
&\sum_m B^a_{m,t} = 1, && \forall t \in T && \text{(2.3e)}\\
&u^d_{m,t^*} \leq p_m U^d_m(t^*) + L(1 - B^d_{m,t^*}), && \forall m \in M && \text{(2.3f)}\\
&u^d_{m,t^*} \geq p_m U^d_m(t^*), && \forall m \in M && \text{(2.3g)}
\end{aligned}$$

$$\sum_m B^d_{m,t^*} = 1 \tag{2.3h}$$

Again, as with the previous models, line 2.3b ensures that the attacker prefers to attack target t^*. Lines 2.3c-2.3e (2.3f-2.3h) handle the generation of the max values for each target for the attacker, $u^a_{m,t}$ (defender, $u^d_{m,t}$).

Next we consider combining these models. Below is the necessary model for combining the traditional multiplicative and additive models, under the assumption that p_t is binary (p_t = 1 when t is defended and $p_t = 0$ when t is undefended) and that the additive mitigations only have an effect in the event of a successful attack (or rather that they have no effect against an attack that was prevented):

$$Max\ p_{t^*}U^d_c(t^*) + (1 - p_{t^*})U^d_u(t^*) + u^d_{m,t^*} - \sum_m p_m c_m \tag{2.4a}$$

s.t.

$$p_t U^a_c(t) + (1 - p_t)U^a_u(t) + u^a_{m,t} \leq p_{t^*}U^a_c(t^*) + (1 - p_{t^*})U^a_u(t^*) + u^a_{m,t^*}, \quad \forall t \in T \tag{2.4b}$$

$$u^a_m(t) \geq \sum_m p_m U^a_m(t) - p_t L, \quad \forall t \in T \tag{2.4c}$$

$$u^a_m(t) \geq 0, \quad \forall t \in T \tag{2.4d}$$

$$u^a_m(t) \leq \sum_m p_m U^a_m(t), \quad \forall t \in T \tag{2.4e}$$

$$u^a_m(t) \leq (1 - p_t)L, \quad \forall t \in T \tag{2.4f}$$

$$u^d_m(t^*) \geq \sum_m p_m U^d_m(t^*) - p_{t^*} L \tag{2.4g}$$

$$u^d_m(t^*) \geq 0 \tag{2.4h}$$

$$u^d_m(t^*) \leq \sum_m p_m U^d_m(t^*) \tag{2.4i}$$

$$u^d_m(t^*) \leq (1 - p_{t^*})L \tag{2.4j}$$

In short, Line 2.4b ensures that the attacker prefers target t^*, while Lines 2.4c-2.4f (2.4g-2.4j) allow us to correctly calculate the utility effect of the additive mitigations under the current security configuration for the attacker (defender).

Finally, the model that combines all three types of mitigations, again assuming that p_t is binary and that both additive and maximal mitigations have no benefit against prevented attacks:

$$Max\ U^d_c(t^*) + u^d_{m,t^*} + v^d_{m,t^*} - \sum_m p_m c_m \tag{2.5a}$$

s.t. (2.5b)

$$p_t U^a_c(t) + (1 - p_t)U^a_u(t) + u^a_{m,t} + v^a_{m,t} \leq p_{t^*}U^a_c(t^*)$$

$$+ (1 - p_{t^*})U_u^a(t^*) + u_{m,t^*}^a + v_{m,t^*}^a, \qquad \forall t \in T \tag{2.5c}$$

$$u_{m,t}^a \leq p_m U_m^a(t) + L(1 - B_{m,t}^a), \qquad \forall m \in M, t \in T \tag{2.5d}$$

$$u_{m,t}^a \leq L(1 - p_t), \qquad \forall m \in M, t \in T \tag{2.5e}$$

$$u_{m,t}^a \geq (p_m - p_t)U_m^a(t), \qquad \forall m \in M, t \in T \tag{2.5f}$$

$$u_{m,t}^a \geq 0, \forall m \in Mt \in T \tag{2.5g}$$

$$\sum_m B_{m,t}^a = 1, \qquad \forall t \in T \tag{2.5h}$$

$$u_{m,t^*}^d \leq p_m U_m^d(t^*) + L(1 - B_{m,t^*}^d), \qquad \forall m \in M \tag{2.5i}$$

$$u_{m,t^*}^d \leq p_m L(1 - p_{t^*}), \qquad \forall m \in M \tag{2.5j}$$

$$u_{m,t^*}^d \geq p_m U_m^d(t^*), \forall m \in M \tag{2.5k}$$

$$u_{m,t^*}^d \geq 0, \qquad \forall m \in M \tag{2.5l}$$

$$\sum_m B_{m,t^*}^d = 1 \tag{2.5m}$$

$$v_m^a(t) \geq \sum_m p_m V_m^a(t) - p_t L, \qquad \forall t \in T \tag{2.5n}$$

$$v_m^a(t) \geq 0, \qquad \forall t \in T \tag{2.5o}$$

$$v_m^a(t) \leq \sum_m p_m V_m^a(t), \qquad \forall t \in T \tag{2.5p}$$

$$v_m^a(t) \leq (1 - p_t)L, \qquad \forall_t \in T \tag{2.5q}$$

$$v_m^d(t^*) \geq \sum_m p_m V_m^d(t^*) - p_{t^*} L \tag{2.5r}$$

$$v_m^d(t^*) \geq 0 \tag{2.5s}$$

$$v_m^d(t^*) \leq \sum_m p_m V_m^d(t^*) \tag{2.5t}$$

$$v_m^d(t^*) \leq (1 - p_{t^*})L \tag{2.5u}$$

In short, Line 2.4b ensures that the attacker prefers target t^*, while Lines 2.5d-2.5h (2.5i-2.5m) allow us to correctly calculate the utility effect of the additive mitigations under the current security configuration for the attacker (defender) and Lines 2.5n-2.5q (2.5r-2.5u) allow us to correctly calculate the utility effect of the maximal mitigations under the current security configuration for the attacker (defender).

Combined models for the other two combinations ({Multiplicative,Max},{Additive,Max}) appear in Appendix A.

Next, we experimentally compared the computational aspects of these models on randomly generated problem instances. We found that the while the three simple models scaled relatively well, most of the combined models scaled fairly poorly. However, we found we could exploit the multiple LP/MIP nature of the problem, as we are solving a series of individual

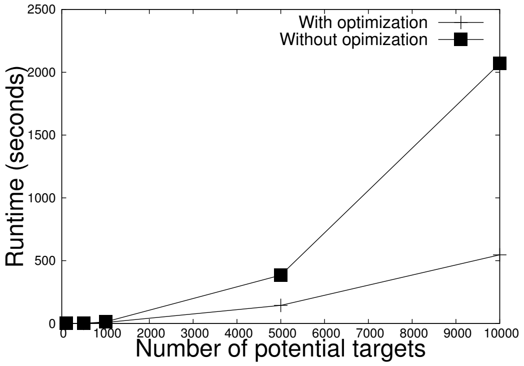

Figure 2.1: Average runtime:
Multiplicative model

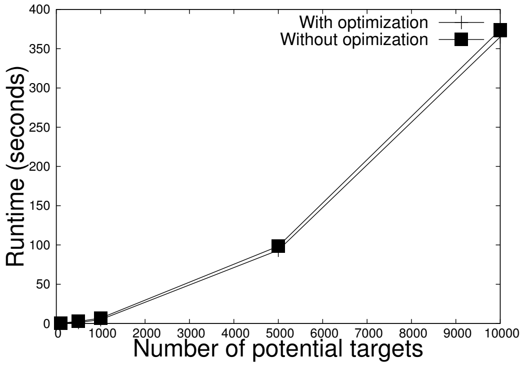

Figure 2.2: Average runtime:
Additive model

(but not independent) MIPs. We found that a simplified version of branch and bound, where we maintain the current best solution from the set of targets (which is a admissible upper bound on the optimal solution) we have already solved for, and terminate each LP/MIP whenever the lower bound for the solution is higher than our current upper bound. In other words, once the solver can prove that the solution for the current target cannot beat the best from the previously solved set of targets, we can move on to the next potential target. We found that this led to a significant speedup for the more complex models (the combined models). Figures 2.1-2.7 show the runtime both with and without this optimization for each of these models on problems between 100 and 10,000 targets solved via Gurobi 5.5.0 with 1-4 core 1.6Ghz processor and 6GB RAM (averaged over 10 runs). Points are omitted when runtime exceeded a day (such as in Figure 2.7 for 1,000 or more targets). Interestingly, this technique gave almost no improvement on the additive model (which was already the fastest model). The next smallest effect was on the other two simple models, at best it is reducing what appears to be a quadratic growth in runtime in the non-optimized case to a linear growth. Finally, in all of the combined models we see the largest increase in performance. Unsurprisingly, the effect is largest in the model that combines all three components, where even problems with only 1,000 targets fail to finish before our cutoff in the non-optimized case, but with the optimization 10,000 targets takes under four hours.

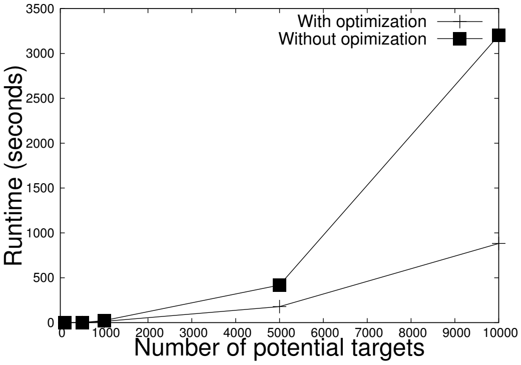

Figure 2.3: Average runtime: Maximal model

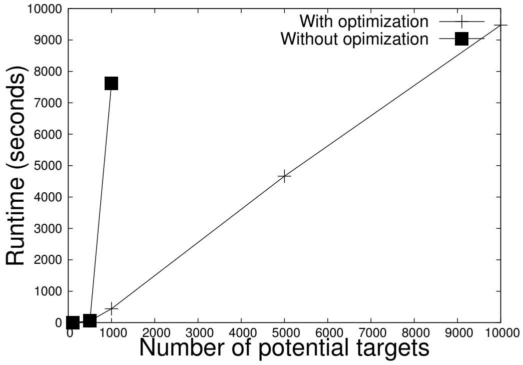

Figure 2.4: Average runtime: Mult & Add model

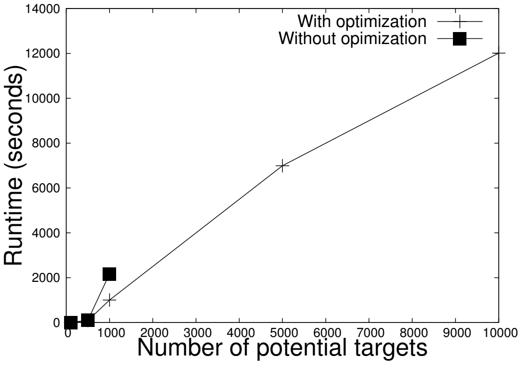

Figure 2.5: Average runtime: Mult & Max model

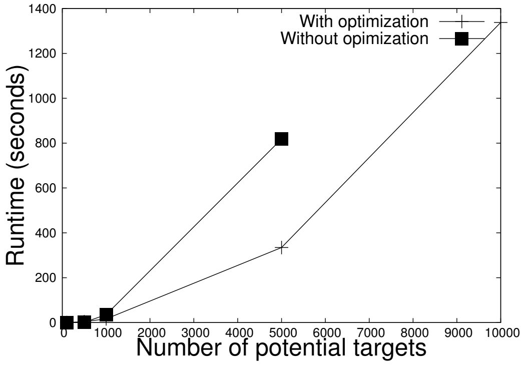

Figure 2.6: Average runtime: Add & Max model

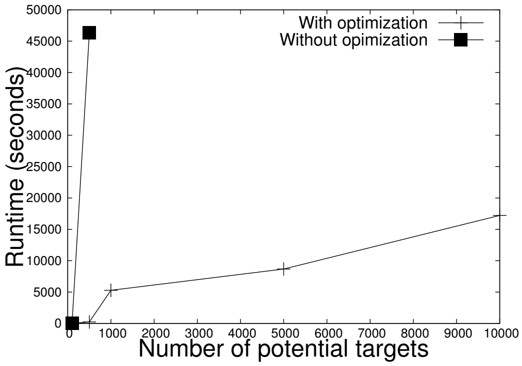

Figure 2.7: Average runtime:
Mult & Multi & Max model

Chapter 3

Simple Network Model

Here, rather than having a set of independent targets, we instead assume that we have a set of connected targets, represented by a graph ($G = (E, V)$). As in [12] we assume that the graph represents the ability of an attack at a specific node to spread to other nodes in the graph (with the value on edge (t^1,t^2) representing the probability that an attack that successfully effects t^1 to then spread and also effect t^2). Furthermore, we assume that once a target is compromised (either directly or indirectly), it can further spread to all as of yet uncompromised targets adjacent to the newly compromised node. While calculating the total effect of an attack was non-trivial, a simulation based approach was taken to determine the total utility for either players from an attack at each target. We will take a similar approach, but rather than condensing the simulation result for each target to a single number, instead have an $|T|^2$ relationship matrix that captures the probability of an attack at each target effecting each other target. To generate these value we adapted a well known approach for finding connected components [8].

- Iteratate over the following procedure:
  - Subsample the graph, including each edge with the probability that edge would spread an attack.
  - Calculate the connected components in this subsample.
  - For each pair of nodes, increment a counter if they are in the same connected component.

As the number of iterations increases, this count divided by the number of iterations will approach the probability of an attack starting at the first node spreading also compromising the second. This approach takes $|V| + |E|$ time in each iteration to calculate the connected components and $\sum_i |c_i|^2 \leq |V|^2$ to update the counts, where $c_i \in C$ is the set of connected components. The only step left is to know how many iterations to run. We choose a simple thresholding approach, where we kept increasing the number of iterations until the change was under a defined threshold.

Thus, we can reflect the utility for successfully attacking a given target is the sum of the probabilities times the value of each other target. This allows us to weight additive or max mitigation values differently for each target, proportional to the chance that the mitigation will effect an attack on that target.

The standard formulation is mainly unchanged, we substitute $U_t = \sum_{t^*} \gamma_{t,t^*} U_{t^*}$, where γ_{t,t^*} captures the probability that an attack originating at t will propagate to t^*.

For the additive models, we again substitute $U_t = \sum_{t^*} \gamma_{t,t^*} U_{t^*}$, but also need to change how we handle the mitigations. If we let $U_m^d(t)$ ($U_m^a(t)$) capture the effect of mitigation m on a successful attack that propagates to t for the defender (attacker), the additive model becomes:

$$Max \ \sum_{\hat{t}} \gamma_{t^*,\hat{t}} U_u^d(\hat{t}) + \sum_{\hat{t}} \gamma_{t^*,\hat{t}} \sum_m p_m U_m^d(\hat{t}) - \sum_m p_m c_m \tag{3.1a}$$

$$\text{s.t.} \tag{3.1b}$$

$$\sum_{\hat{t}} \gamma_{t,\hat{t}} U_u^a(\hat{t}) + \sum_{\hat{t}} \gamma_{t,\hat{t}} \sum_m p_m U_m^a(\hat{t}) \leq \sum_{\hat{t}} \gamma_{t^*,\hat{t}} U_u^a(\hat{t}) + \sum_{\hat{t}} \gamma_{t^*,\hat{t}} \sum_m p_m U_m^a(\hat{t}), \quad \forall_t \in T \tag{3.1c}$$

Similarily, the multiplicative model becomes:

$$Max \ \sum_{\hat{t}} \gamma_{t^*,\hat{t}} U_u^d(\hat{t}) + \sum_{\hat{t}} \gamma_{t^*,\hat{t}} u_{m,\hat{t}}^d - \sum_m p_m c_m \tag{3.2a}$$

s.t.

$$\sum_{\hat{t}} \gamma_{t,\hat{t}} U_u^a(\hat{t}) + \sum_{\hat{t}} \gamma_{t,\hat{t}} u_{m,\hat{t}}^a \leq \sum_{\hat{t}} \gamma_{t^*,\hat{t}} U_u^a(\hat{t}) + \sum_{\hat{t}} \gamma_{t^*,\hat{t}} u_{m,\hat{t}}^a, \qquad \forall t \in T \tag{3.2b}$$

$$u_{m,t}^a \leq p_m U_m^a(t) + L(1 - B_{m,t}^a), \qquad \forall m \in M, t \in T \tag{3.2c}$$

$$u_{m,t}^a \geq p_m U_m^a(t), \qquad \forall m \in M, t \in T \tag{3.2d}$$

$$\sum_m B_{m,t}^a = 1, \qquad \forall t \in T \tag{3.2e}$$

$$u_{m,t^*}^d \leq p_m U_m^d(t^*) + L(1 - B_{m,t^*}^d), \qquad \forall m \in M \tag{3.2f}$$

$$u_{m,t^*}^d \geq p_m U_m^d(t^*), \qquad \forall m \in M \tag{3.2g}$$

$$\sum_m B_{m,t^*}^d = 1 \tag{3.2h}$$

The combined models are updated similarly, but are omitted here for brevity.

Experimentally, we explored the computational aspects of these models as we did in the previous section. We evaluated these sampling techniques on Erdős-Reńyi (ER) [5] and

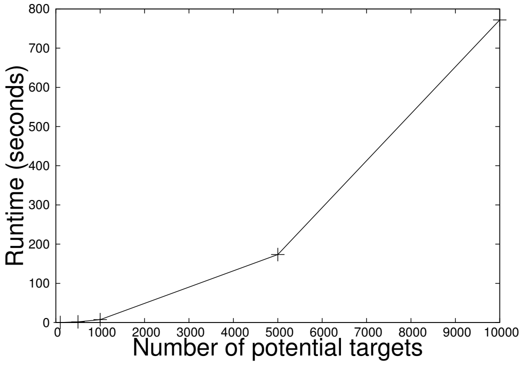

Figure 3.1: Average runtime: Utility propagation

BarabsiAlbert (BA) [1] random graphs. Luckly, even though we can only bound the runtime by $|V^2$, we found in practice that one of two things happened in these random graphs. Either the connected components were large, but fairly stable and the algorithm converged after a small number of iterations, or the connected components were fairly small and although a larger number of iterations was necessary, each iteration ran quickly. Figure 3.1 shows the runtime of just preprocessing step necessary to generate the models on an ER graph with $p = .25$ and spread chances randomly drawn for each edge uniformly from (.25,.75), the runtimes of the models themselves were effectively the same as in Figures 2.1-2.7.

Chapter 4

Power Grid Models

Here we explored the computational aspects of different extensions of the standard DC power flow models. These models extend the models discussed above by adding in the following elements:

- Constraints that force a balance of flow between the sources (generators) and the given demands.
- Kirchhoff voltage law enforcement between operational transmission elements.
- Thermal capacity constraints on operational transmission elements.

First, consider the simple case where the adversary is only allowed to attack one component of the power grid. A simple solution to this setting is to evaluate the system for each possible attack, effectively generating a normal form game as defined above. Unfortunately, while simple to solve, this approach scales poorly as we increase the number of targets the adversaries is able to attack, for 2 components this generates $\mathrm{O}(n^2)$ subproblems and for k components (n^k). To explore this setting for $k > 1$, we extend the defender-attacker-defender model proposed in [17] using a column-and-constraint generation technique. The approach proposed in [17] maps to the multiplicative setting we explored in Section 2. In the remainder of this section we first extend their model to handle utility weights on load shed, explain how to separate the problem to apply a column-and-constraint approach, and finally show both the model and column-and-constraint problem change as we add in additional defense options.

Nomenclature

Indicies and sets

N set of indicies of busses, indexed by n

J set of indicies of generators, index by j

Jn set of indicies of generators connected to bus n

L set of indicies of transmission assets, indexed by l

o(l) origin bus of transmission asset l

d(l) destination bus of transmission asset l

Z set of possible defense options

Parameters

S budget of attacker on out-of-service transmission assets

R budget of defender's protection decision

D_n demand at bus n (in megawatts)

U_n utility loss per megawata of load shed at bus n

$U_n^{z_n}$ reduction in utility loss per megawata at bus n with mitigation z_n

G_j generation capacity of generator j (in megawatts)

P_l power flow capacity of transmission line l (in megawatts)

x_l reactance at line l (Ω)

δ phase angle capacity of conneting bus

Decision Variables

z binary protection decision, 1 if chosen, 0 otherwise

v_l binary attack decision, 0 if line l is attacked, 1 otherwise

d_n load shed at node n

d_n^z load shed at node n partially mitigated by protection decision z

δ_n phase angle at node n

g_j generation level of generator j

p_l power flow on line l

Model

In our first, standard multiplicative model, we let set of possible defense actions be one per line ($z_l \in Z$).

$$Min_{z \in Z}\ Max_{v \in V}\ Min_{p_l, g_j, d_n, \delta_n} \quad \sum_{n \in N} U_n d_n \tag{4.1a}$$

$$s.t. \tag{4.1b}$$

$$\sum_{l \in L} z_l \leq R \tag{4.1c}$$

$$\sum_{l \in L} (1 - v_l) \leq S \tag{4.1d}$$

$$p_l x_l = (z_l + v_l - z_l v_l)[\delta_{o(l)} - \delta_{d(l)}] \qquad \forall l \in L \tag{4.1e}$$

$$\sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n = D_n \qquad \forall n \in N \tag{4.1f}$$

$$-P_l \leq p_l \leq P_l \qquad \forall l \in L \tag{4.1g}$$

$$-\delta \leq \delta_n \leq \delta \qquad \forall n \in N \tag{4.1h}$$

$$0 \leq g_j \leq G \qquad \forall j \in J \tag{4.1i}$$

$$0 \leq d_{\leq} D_n \qquad \forall n \in N \tag{4.1j}$$

Solving this Model

Consider the solution approach proposed in [17] (again with the minor addition of demand utility). This an standard constraint generation approach, iteratively using a master program to solve for the optimal defense choices against a restricted set of possible attacks, solving for the optimal attack against that defense, and then adding this new attack to the set of possible attacks (or ending when it fails to find a new attack).

$$Min\ \alpha \tag{4.2a}$$

$$s.t. \tag{4.2b}$$

$$\alpha \geq \sum_{n \in N} U_n d_n^i \qquad \forall i \in \{1, ..., k\} \tag{4.2c}$$

$$\sum_{l \in L} z_l \leq R \tag{4.2d}$$

$$p_l x_l = (z_l + v_l^i - z_l v_l^i)[\delta_{o(l)} - \delta_{d(l)}] \qquad \forall l \in L, i \in \{1, ..., k\} \tag{4.2e}$$

$$\sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n^i = D_n \qquad \forall n \in N, i \in \{1, ..., k\} \tag{4.2f}$$

$$-P_l \leq p_l^i \leq P_l \qquad \forall l \in L, i \in \{1, ..., k\} \tag{4.2g}$$

$$0 \leq g_j^i \leq G_j \qquad \forall j \in J, i \in \{1, ..., k\} \tag{4.2h}$$

$$0 \leq d_n^i \leq D_n \qquad \forall n \in N, i \in \{1, ..., k\} \tag{4.2i}$$

$$-\delta \leq \delta_n^i \leq \delta \qquad \forall n \in N, i \in \{1, ..., k\} \tag{4.2j}$$

Unfortunately, constraint 4.2e is nonlinear. However, in this subproblem, for a given value of i, we know exactly which lines have been attacked. Lines that have not been attacked are easy (as defense of that line does nothing against that particular attack), as we can simply write them as :

$$p_l^i x_l = \delta_{o(l)}^i - \delta_{d(l)}^i$$

For lines that have been attacked, we simply allow the defender to negate that attack (effectively turning that edge back on) with z. We can model this by introducing a large constant value (M):

$$p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \leq M(1 - z_l)$$
$$p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \geq M(z_l - 1)$$
$$-P_l z_l \leq p_l^i \leq P_l z_l$$

This allows us to generate the optimal defense against a restricted set of possible attacks. The next step is to develop an attacker oracle to populate this set. To do so we solve a two-level problem that finds for the optimal attack against a fixed defense strategy:

$$max\ min \sum_{n \in N} U_n d_n \tag{4.3a}$$

$$s.t. \tag{4.3b}$$

$$\sum_{l \in L} (1 - v_l) \leq S \tag{4.3c}$$

$$p_l x_l - (\hat{z}_l + v_l - \hat{z}_l v_l)[\delta_{o(l)} - \delta_{d(l)}] = 0, \qquad \forall l \in L \tag{4.3d}$$

$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.3e}$$

$$\sum_{j_J n} g_j - \sum_{l|o(l)=n} p_l + \sum_{l|d(l)=n} p_l + d_n = D_n, \qquad \forall n \in N \tag{4.3f}$$

$$0 \leq g_j \leq G_j, \qquad \forall j \in J \tag{4.3g}$$

$$0 \leq d_n \leq D_n, \qquad \forall n \in N \tag{4.3h}$$

$$-\delta \leq \delta_n \leq \delta \tag{4.3i}$$

$$v_l \in 0, 1, \qquad \forall l \in L \tag{4.3j}$$

Again, we first have to deal with the non-linearity in constraint 4.3d. The approach will be similar to how we dealt with this issue in Equation 4.2. We will break the set of lines into two sets, those lines that are currently unprotected by the defender (L_a) and those lines that are currently being defended by the defender (L_b). This allows us to rewrite constraint 4.3d&4.3e for L_a as:

$$p_l x_l - [\delta_{o(l)} - \delta d(l)] \leq M(1 - v_l), \qquad \forall l \in L_a \tag{4.4a}$$

$$p_l x_l - [\delta_{o(l)} - \delta d(l)] \geq M(1 - v_l), \qquad \forall l \in L_a \tag{4.4b}$$

$$-P_l v_l \leq p_l \leq P_l v_l \tag{4.4c}$$

and for L_b as:

$$p_l x_l = \delta_{o(l)} - \delta d(l), \qquad \forall l \in L_b \tag{4.4d}$$

$$-P_l \leq p_l \leq P_l v_l \tag{4.4e}$$

Next, since the lower level of this problem is guaranteed to have a feasible solution for any possible setting of V, we can rewrite this bi-level program as a single level program by taking the dual of the lower level and merging in the resulting maximization. If we assign the following {dual variables,constraint} pairs: {λ_n, 4.3f}, {γ_n, 4.3g}, {α_n, 4.3i}, {ξ_n & χ_n, 4.3i}, {β_l & τ_l, 4.4a & 4.4a}, {Θ_l & ρ_l,4.4c }, {μ_l, 4.4d}, and {phi_l & φ_l,4.4e}.

The resulting single level MIP becomes:

$$max \sum_{l \in L_b} P_l(\phi_l - \varphi_l) + \sum_{l \in L_a} M(\beta_l - \beta'_l - \tau_l + \tau'_l) + \sum_{j \in J} G_j \gamma_j$$

$$+ \sum_{n \in N} \delta(\xi_n - \chi_n) + \sum_{n \in N} D_n(\alpha_n + \lambda_n) + \sum_{l \in L_a} P_l(\Theta'_l - \rho'_l) \tag{4.5a}$$

$$s.t. \tag{4.5b}$$

$$\sum_{l \in L}(1 - v_l) \leq S \tag{4.5c}$$

$$x_l \mu_l + \phi_l + \varphi_l - \lambda_{n:o(l)=n} + \lambda_{n:d(l)=n} = 0, \qquad \forall l \in L_b \tag{4.5d}$$

$$x_l \beta_l + x_l \tau_l + \Theta_l + \rho_l - \lambda_{n:o(l)=n} + \lambda_{n:d(l)=n} = 0, \qquad \forall l \in L_a \tag{4.5e}$$

$$\gamma_j + \lambda_{n:j \in J_n} \leq 0, \qquad \forall j \in J \tag{4.5f}$$

$$\sum_{l \in L_b:d(l)=n} \mu_l - \sum_{l \in L_b:o(l)=n} \mu_l + \sum_{l \in L_a:d(l)=n} (\beta_l + \tau_l) - \sum_{l \in L_a:o(l)=n} (\beta_l + \tau_l)$$

$$+ (\xi_n + \chi_n) = 0, \qquad \forall n \in N \tag{4.5g}$$

$$\lambda_n + \alpha_n \leq U_n, \qquad \forall n \in N \tag{4.5h}$$

$$\beta'_l \leq \beta_l + M(1 - v_l), \qquad \forall l \in L \tag{4.5i}$$

$$\beta'_l \geq \beta_l - M(1 - v_l), \qquad \forall l \in L \tag{4.5j}$$

$$-Mv_l \leq \beta'_l \leq Mv_l, \qquad \forall l \in L \tag{4.5k}$$

$$\tau_l' \leq \tau_l + M(1 - v_l), \qquad \forall l \in L \tag{4.5l}$$

$$\tau_l' \geq \tau_l - M(1 - v_l), \qquad \forall l \in L \tag{4.5m}$$

$$-Mv_l \leq \tau_l' \leq Mv_l, \qquad \forall l \in L \tag{4.5n}$$

$$\Theta_l' \leq \Theta_l + M(1 - v_l), \qquad \forall l \in L \tag{4.5o}$$

$$\Theta_l' \geq \Theta_l - M(1 - v_l), \qquad \forall l \in L \tag{4.5p}$$

$$-Mv_l \leq \Theta_l' \leq Mv_l, \qquad \forall l \in L \tag{4.5q}$$

$$\rho_l' \leq \rho_l + M(1 - v_l), \qquad \forall l \in L \tag{4.5r}$$

$$\rho_l' \geq \rho_l - M(1 - v_l), \qquad \forall l \in L \tag{4.5s}$$

$$-Mv_l \leq \rho_l' \leq Mv_l, \qquad \forall l \in L \tag{4.5t}$$

$$\gamma_j \leq 0, \qquad \forall j \in J \tag{4.5u}$$

$$\xi_n \leq 0, \alpha_n \leq 0, \chi_n \leq 0, \lambda_n free, \qquad \forall n \in N \tag{4.5v}$$

$$\beta_l \leq 0, \Theta_l \leq 0, \tau_l \geq 0, \rho_l \geq 0, \qquad \forall l \in L_a \tag{4.5w}$$

$$\mu_l free, \phi_l \leq 0, \varphi_l \geq 0, \qquad \forall l \in L_b \tag{4.5x}$$

Note that β_l', τ_l', Θ_l', and ρ_l' are again created to deal with non-linearity in the direct dual formulation (as these values depend on v_l). Finally, we combine these two problems (the defender's master problem and the attacker's subproblem) in an iterative fashion as follows:

- Solve the attacker's subproblem against an empty defense and add this attack v^1 to a set of attack plans $\hat{V}$
- Until we try to add an attack v^k to $\hat{V}$ that it already contains:
  - Solve the defender's master problem against $\hat{V}$, let the optimal defense generated be $\hat{z}$
  - Solve the attacker's subproblem against $\hat{z}$, and add this attack v^k to $\hat{V}$

This approach is guaranteed to converge as it can add each possible attack set at most once and there are a finite set of possible attacks. Proving it will converge to an optimal equilibrium for the defender is also easy to show: First, the attacker is simply best responding to the most recent defense of the defender. If the attacker chooses a particular attack for the second time, it will be in $\hat{V}$, and thus the utility calculated by the defender's master problem in that will have taken that possible attack into consideration. Thus both the utilities calculated by the sub and master problems in that iteration will match and neither player will be able to deviated to increase their utility. Thus this solution will be optimal equilibrium solution for the defender.

Additional models

We now propose the following alternative defensive models to this problem. Note that initially, we consider the changes necessary to replace the previous set of defense actions (of making lines immune to attacks), with a series of alternative defense models. We will defer discussion on how each of these changes effects the column-and-constraint method to the end of the section. First, we consider a model consisting of reducing the utility loss from load shed. Consider the case where multiple defense options combine cumulatively:

$$Min_{z \in Z}\ Max_{v \in V}\ Min_{p_l, g_j, d_n, \delta_n} \sum_{n \in N} U_n d_n - \sum_{n \in N, z \in Z} U_n^z d_n^z \tag{4.6a}$$

$$s.t. \tag{4.6b}$$

$$\sum_{i \in |Z|} z_i \leq R \tag{4.6c}$$

$$\sum_{l \in L} (1 - v_l) \leq S \tag{4.6d}$$

$$p_l x_l = (v_l)[\delta_{o(l)} - \delta_{d(l)}], \qquad \forall l \in L \tag{4.6e}$$

$$\sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n = D_n, \qquad \forall n \in N \tag{4.6f}$$

$$d_n^z \leq d_n, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.6g}$$

$$d_n^z \leq z, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.6h}$$

$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.6i}$$

$$-\delta \leq \delta_n \leq \delta, \qquad \forall n \in N \tag{4.6j}$$

$$0 \leq g_j \leq G, \qquad \forall j \in J \tag{4.6k}$$

$$0 \leq d_{\leq} D_n, \qquad \forall n \in N \tag{4.6l}$$

Note that this model differs from Eq. 4.1 in the objective, the attack constraints (4.6e) and with the addition of two sets of constraints to capture the amount load shed that is mitigated by each defense action (4.6g-4.6h). Next, consider the second alternative, where when multiple defense options overlap, we take pessimistically take only the maximial value:

$$Min_{z \in Z}\ Max_{v \in V}\ Min_{p_l, g_j, d_n, \delta_n} \sum_{n \in N} U_n d_n - \sum_{n \in N} U_n^m \tag{4.7a}$$

$$s.t. \tag{4.7b}$$

$$\sum_{i\in|Z|} z_i \leq R \tag{4.7c}$$

$$\sum_{l\in L}(1-v_l) \leq S \tag{4.7d}$$

$$p_l x_l = (v_l)[\delta_{o(l)} - \delta_{d(l)}], \qquad \forall l \in L \tag{4.7e}$$

$$\sum_{j\in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n = D_n, \qquad \forall n \in N \tag{4.7f}$$

$$d_n^z \leq d_n, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.7g}$$

$$d_n^z \leq z, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.7h}$$

$$U_n^m - Mz \leq U_n^z d_n^z, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.7i}$$

$$U_n^m \geq U_n^z d_n^z - M(1-b_n^z), \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.7j}$$

$$\sum_{z\in Z:U_n^z>0} b_n^z = 1, \qquad \forall n \in N \tag{4.7k}$$

$$b_n^z \leq z, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.7l}$$

$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.7m}$$

$$-\delta \leq \delta_n \leq \delta, \qquad \forall n \in N \tag{4.7n}$$

$$0 \leq g_j \leq G, \qquad \forall j \in J \tag{4.7o}$$

$$0 \leq d_{\leq} D_n, \qquad \forall n \in N \tag{4.7p}$$

This model differs from Eq. 4.1 in the objective, the attack constraints (4.7e) and with the addition of constraints that capture the total amount of load shed mitigated at each bus (4.7i-4.7l).

The next two models we consider are two different ways to modify the amount of power available/needed. Our first model here captures the case where the defender is able to invest their resources in increasing the available power at one or more of the buses:

$$Min_{z\in Z}\ Max_{v\in V}\ Min_{p_l,g_j,d_n,\delta_n} \sum_{n\in N} U_n d_n \tag{4.8a}$$

$$s.t. \tag{4.8b}$$

$$\sum_{l\in L} z_l \leq R \tag{4.8c}$$

$$\sum_{l\in L}(1-v_l) \leq S \tag{4.8d}$$

$$p_l x_l = (z_l + v_l - z_l v_l)[\delta_{o(l)} - \delta_{d(l)}], \qquad \forall l \in L \tag{4.8e}$$

$$\sum_{j\in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n = D_n, \qquad \forall n \in N \tag{4.8f}$$

$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.8g}$$
$$-\delta \leq \delta_n \leq \delta, \qquad \forall n \in N \tag{4.8h}$$
$$0 \leq g_j \leq G_j, \qquad \forall j \in J \tag{4.8i}$$
$$0 \leq g_j \leq z_j, \qquad \forall j \in J^z \tag{4.8j}$$
$$0 \leq d_n \leq D_n, \qquad \forall n \in N \tag{4.8k}$$

Here we simply add an extra set of generators (J_z), which the solution is not allowed to use unless z_j is 1. Next, we consider the converse side of the previous model, rather than adding in new generation supply, we instead allow the defender to invest in reducing demand at different nodes. One possible way this might be effected is through energy efficiency subsidies. While the effect of this model is fairly similar to the previous model (as our model does not consider explicitly consider generator costs), in some cases demand reduction is actually inferior to additional generation capacity, as with load shed being weighted, there are cases where additional generation at a bus would allow us to reduce load shed on another node, while demand reduction at that node only allows us to reduce load shed at that node. The model for this is:

$$Min_{z \in Z}\ Max_{v \in V}\ Min_{p_l, g_j, d_n, \delta_n} \sum_{n \in N} U_n d_n \tag{4.9a}$$
$$s.t. \tag{4.9b}$$
$$\sum_{n \in N} z_n \leq R \tag{4.9c}$$
$$\sum_{l \in L} (1 - v_l) \leq S \tag{4.9d}$$
$$p_l x_l = (v_l)[\delta_{o(l)} - \delta_{d(l)}], \qquad \forall l \in L \tag{4.9e}$$
$$\sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n + d_n^z z_n = D_n, \qquad \forall n \in N \tag{4.9f}$$
$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.9g}$$
$$-\delta \leq \delta_n \leq \delta, \qquad \forall n \in N \tag{4.9h}$$
$$0 \leq g_j \leq G, \qquad \forall j \in J \tag{4.9i}$$
$$0 \leq d_n + d_n^z z_n \leq D_n, \qquad \forall n \in N \tag{4.9j}$$

Next, we consider models that combine more than one of these five potential mitigation types. For brevity, we will jump straight to the fully combined model (utilizing all 5 types of mitigation, multiplicative (Z_l), additive (Z_a), maximal (Z_m), generator (Z_j) and demand (Z_d)). Similar constructions exist, but are omitted, for all subsets of these 5 mitigations. Notationally, we let $Z = Z_l + Z_a + Z_m + Z_j + Z_d$:

$$Min_{z \in Z}\ Max_{v \in V}\ Min_{p_l, g_j, d_n, \delta_n}\ \sum_{n \in N} U_n d_n - \sum_{n \in N, z \in Z_a} U_n^z d_n^z - \sum_{n \in N} U_n^m \tag{4.10a}$$

$$s.t. \tag{4.10b}$$

$$\sum_{i \in Z} z_i \leq R \tag{4.10c}$$

$$\sum_{l \in L} (1 - v_l) \leq S \tag{4.10d}$$

$$p_l x_l = (z_l + v_l - z_l v_l)[\delta_{o(l)} - \delta_{d(l)}], \qquad \forall l \in L \tag{4.10e}$$

$$\sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n + d_n^z z_n^d = D_n, \qquad \forall n \in N \tag{4.10f}$$

$$d_n^z \leq d_n, \qquad \forall z \in Z_a, n \in N : U_n^z > 0 \tag{4.10g}$$

$$d_n^z \leq z, \qquad \forall z \in Z_a, n \in N : U_n^z > 0 \tag{4.10h}$$

$$d_n^z \leq d_n, \qquad \forall z \in Z_m, n \in N : U_n^z > 0 \tag{4.10i}$$

$$d_n^z \leq z, \qquad \forall z \in Z_m, n \in N : U_n^z > 0 \tag{4.10j}$$

$$U_n^m - Mz \leq U_n^z d_n^z, \qquad \forall z \in Z_m, n \in N : U_n^z > 0 \tag{4.10k}$$

$$U_n^m \geq U_n^z d_n^z - M(1 - b_n^z), \qquad \forall z \in Z_m, n \in N : U_n^z > 0 \tag{4.10l}$$

$$\sum_{z \in Z : U_n^z > 0} b_n^z = 1, \qquad \forall n \in N \tag{4.10m}$$

$$b_n^z \leq z, \qquad \forall z \in Z, n \in N : U_n^z > 0 \tag{4.10n}$$

$$-P_l \leq p_l \leq P_l, \qquad \forall l \in L \tag{4.10o}$$

$$-\delta \leq \delta_n \leq \delta, \qquad \forall n \in N \tag{4.10p}$$

$$0 \leq g_j \leq G, \qquad \forall j \in J \tag{4.10q}$$

$$0 \leq g_j \leq z_j, \qquad \forall j \in J^z \qquad (4.10r)$$

$$0 \leq d_n + d_n^z z_n \leq D_n, \qquad \forall n \in N \qquad (4.10s)$$

Our approach for solving this combined model is similar to the approach for only the multiplicative model. The new master problem (after addressing the non-linearity issues) becomes:

$$
\begin{aligned}
& Min\, \alpha && && (4.11a)\\
s.t. & && && (4.11b)\\
& \alpha \geq \sum_{n \in N} \sum_{n \in N} U_n d_n^i - \sum_{n \in N, z \in Z_a} U_n^z d_n^{i,z} - \sum_{n \in N} U_n^{m,i}, && \forall i \in \{1, ..., k\} && (4.11c)\\
& \sum_{i \in Z} z_i \leq R && && (4.11d)\\
& p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \leq M(1 - z_l), && \forall l \in L_a^i, i \in \{1, ..., k\} && (4.11e)\\
& p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \geq M(z_l - 1), && \forall l \in L_a^i, i \in \{1, ..., k\} && (4.11f)\\
& -P_l z_l \leq p_l^i \leq P_l z_l, && \forall l \in L_a^i, i \in \{1, ..., k\} && (4.11g)\\
& p_l^i x_l = \delta_{o(l)}^i - \delta_{d(l)}^i, && \forall l \in L_b^i, i \in \{1, ..., k\} && (4.11h)\\
& \sum_{j \in Jn} g_j - \sum_{l:o(l)=n} p_l + \sum_{l:d(l)=n} p_l + d_n^i + d_n^{i,z} z_n^d = D_n, && \forall n \in N, i \in \{1, ..., k\} && (4.11i)\\
& -P_l \leq p_l^i \leq P_l, && \forall l \in L, i \in \{1, ..., k\} && (4.11j)\\
& 0 \leq g_j^i \leq G_j, && \forall j \in J, i \in \{1, ..., k\} && (4.11k)\\
& 0 \leq g_j^i \leq z_j, && \forall j \in J^z, i \in \{1, ..., k\} && (4.11l)\\
& 0 \leq d_n^i \leq D_n, && \forall n \in N, i \in \{1, ..., k\} && (4.11m)\\
& -\delta \leq \delta_n^i \leq \delta, && \forall n \in N, i \in \{1, ..., k\} && (4.11n)
\end{aligned}
$$

Interestingly, these new mitigations don't require new constraints in the subproblem, as by this time the defender's choices are fixed. Thus, we merely have to update some of the constant values in Eq. 4.3 in each iteration (as an example, consider demand reduction: if a particular defense allocation reduces demand for node n', then we replace D_n with $D'_n = D_n - d_n^z$ in Constraint 4.3f).

The only real concern is that the much larger space of potential defense actions will require a significant increase in the number of iterations. We look at this question experimentally in the next section.

Chapter 5

Experiments

We evaluated both the multiplicative model with utilities and the combined model on the IEEE one-area RTS-1996 system [6] with CPLEX 12.5 on a machine with 4-16 core 2.70 GHz processors and 512 GB RAM using a maximum of 16 threads. This system has 24 buses, 38 lines, 32 generators and 17 loads. Our goal was to prepare a pair of multiplicative and combined models that was as comparable as possible, to measure the effect of adding in new defense options on both runtime and utility. The bus demands, starting set of generators and line resistances are taken from the data available on the system. For both systems we assigned all low demand busses (those with at most 180) a utility weight of 2 with the option for the defender to reduce this utility loss back to 1 by spending defense resources in the combined system. In both systems all lines are available as targets for both the attacker and the defender. Finally, we for our combined model, we added an extra set of synthetically defense options, namely demand reduction for each bus and new potential generators (duplicates of existing generators) at existing generator locations. We solved both of these systems for the optimal set of mitigations (and the corresponding loss) for attack budgets (number of edges removed) between 1 and 12 and defense budgets between 0 and 6. In the following subsections we will discuss the effects that these additional defense resources had on both runtime and weighted Load shed.

Runtime

Tables 5.1&5.2 show the runtime in seconds for each attacker budget,defender budget pairing for these two models. Clearly, in both cases, while the problem becomes more complex as both attacker and defender resources increase, once we have a few attacker resources, increasing defense resources seems to have a larger effect on runtime. Of particular note is the fact that although the combined model is more complex, it doesn't perform noticeably worse. In fact, in some of the hardest cases, it significantly outperforms the simpler multiplicative model. While we would like to have had more time to follow up on this and fully explore why this is the case, we hypothesize that it due to the combined models ability to partially sidestep the combinatorial problem that the attacker and defender jointly face in determining what lines to attack/defend. If the attacker can cheaply guarantee that some small subset of buses will be disconnected unless the defender overcommits to defending that subset, then allocating demand or utility reduction to that subset effectively reduces the remaining problem to one with a smaller set of defense resources. This effective reduction in the number of free defense resources leads to an understandable reduction in runtime.

	0	1	2	3	4	5	6
1	0.84	0.75	0.93	0.85	0.84	0.85	0.88
2	2.31	4.44	6.74	10.46	11.43	12.49	19.50
3	1.98	3.73	12.14	18.34	26.37	31.48	51.18
4	2.07	4.57	11.73	27.74	46.13	28.737	65.79
5	2.55	7.07	13.43	28.38	46.00	52.39	88.11
6	5.69	16.69	23.09	75.12	62.16	87.03	108.59
7	2.46	11.10	59.74	75.62	123.61	205.76	190.36
8	5.44	17.69	40.82	107.08	228.51	287.07	289.82
9	3.53	18.94	35.31	98.62	118.74	382.52	683.07
10	4.81	13.51	45.08	73.22	164.91	511.09	937.05
11	5.19	18.53	47.01	86.28	221.31	387.52	1352.70
12	3.11	31.20	37.88	94.18	172.96	443.30	2688.05

Table 5.1: Runtime for Multiplicative Model

	0	1	2	3	4	5	6
1	1.66	2.60	2.18	3.32	2.80	3.18	2.11
2	4.44	6.83	11.97	13.61	21.76	23.36	34.63
3	3.77	6.42	12.64	16.61	30.42	36.75	50.89
4	4.12	7.27	16.91	31.61	53.08	54.55	70.53
5	4.98	13.43	14.86	34.17	52.97	68.50	135.56
6	11.97	26.30	30.12	61.65	42.31	164.53	156.65
7	5.02	16.64	56.02	97.44	166.04	212.22	378.11
8	10.08	25.36	44.18	106.20	188.35	212.98	352.36
9	6.90	19.30	32.87	144.90	122.63	318.21	472.43
10	9.31	16.58	46.83	67.01	153.48	378.66	509.76
11	10.43	32.46	50.77	110.04	267.37	462.42	1027.81
12	6.00	31.45	45.18	88.51	247.53	524.29	851.99

Table 5.2: Runtime for Combined Model

Utility

Tables 5.3&5.4 show the calculated attacker utility for each attacker budget,defender budget pairing for these two models (weighted load shed in MW). As the combined model contains a super-set of the defense options of multiplicative model, its utility is guaranteed to be at least as good as multiplicative model. Thus, what we are interested in is what in what cases we see an decrease in weighted load shed (and thus an increase in defender utility). Figures 5.1&5.2 show the difference in utility for each of these points. From this we can conclude that line defense is still the most important type of defense choice and when the defender's budget is low, there is generally no difference in utility. It is only when the defense budget climbs higher that these alternative defense options are chosen in addition to line, with the utility gap generally increasing as the defense budget increases. Finally, we can see the most significant increases when the attack budget is low (and where we can see significantly diminishing returns for more edge defenses in the multiplicative model).

	0	1	2	3	4	5	6
1	0	0	0	0	0	0	0
2	272	194	150.7	148	142	117.7	117.7
3	617.7	570.7	437	421.7	272	265.7	227.7
4	921.7	732.7	672.7	491.7	442	420	348
5	1036.7	969	787.7	709	657	464	463
6	1199	1057.7	868.7	858.7	678	639	503
7	1358.7	1199	979	898	810	748.7	600
8	1473.7	1274.7	1094	943.7	869	810	688
9	1636	1380	1196	1017.7	945.7	884.7	776.7
10	1636	1477	1247	1081.7	1004	942.7	830
11	1711.7	1477	1332	1152.7	1071.7	956.7	869
12	1786	1530	1441	1207.7	1071.7	997	923

Table 5.3: Utility (weighted Load shed in MW) for Multiplicative Model

	0	1	2	3	4	5	6
1	0	0	0	0	0	0	0
2	272	194	148	142	56	22	0
3	617.7	517.7	421.7	337	272	205.7	157.7
4	921.7	732.7	632.7	491.7	432.7	372.7	312.7
5	1036.7	936.7	787.7	687.7	609	464	403
6	1199	1057.7	868.7	768.7	597	597	499
7	1358.7	1199	979	863.7	783	687.7	590
8	1473.7	1274.7	1094	943.7	825	725	625
9	1636	1380	1196	1017.7	897.7	797.7	697.7
10	1636	1477	1247	1081.7	961.7	861.7	761.7
11	1711.7	1477	1332	1152.7	1032.7	932.7	832.7
12	1786	1530	1410	1207.7	1071.7	971.7	871.7

Table 5.4: Utility (weighted Load shed in MW) for Combined Model

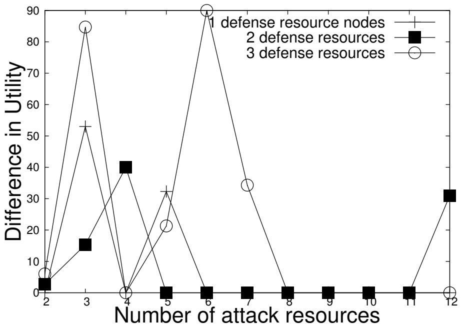

Figure 5.1: Difference in Utility (weighted Load shed in MW) between the two Models

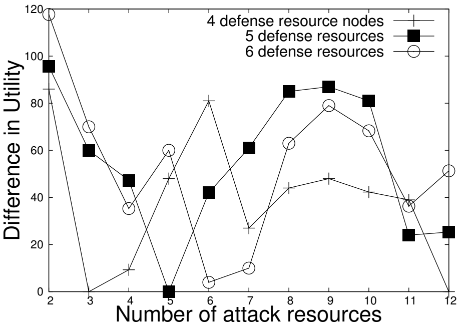

Figure 5.2: Difference in Utility (weighted Load shed in MW) between the two Models

References

[1] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.

[2] R. L. Y. Chen, A. Cohn, et al. Contingency-risk informed power system design. *IEEE Transactions on Power Systems*, 29(5):2087–2096, Sept 2014. ISSN 0885-8950.

[3] V. Conitzer and T. Sandholm. Computing the optimal strategy to commit to. In *Proceedings of the 7th ACM Conference on Electronic Commerce*, EC '06, pp. 82–90. 2006. ISBN 1-59593-236-4.

[4] N. R. Council. *Terrorism and the Electric Power Delivery System.* The National Academies Press, Washington, DC, 2012. ISBN 978-0-309-11404-2.

[5] P. ErdőS and A. Reńyi. On random graphs i. *Publ. Math. Debrecen*, 6:290–297, 1959.

[6] C. Grigg, P. Wong, et al. The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee. *IEEE Transactions on Power Systems*, 14(3):1010–1020, Aug 1999.

[7] P. Hines, J. Apt, et al. Large blackouts in north america: Historical trends and policy implications. *Energy Policy*, 37(12):5249 – 5259, 2009. ISSN 0301-4215.

[8] J. Hopcroft and R. Tarjan. Algorithm 447: Efficient algorithms for graph manipulation. *Commun. ACM*, 16(6):372–378, Jun. 1973. ISSN 0001-0782.

[9] M. Jain, V. Conitzer, et al. Security scheduling for real-world networks. In *In Proccedings of the Workshop on Multiagent Interaction Networks (MAIN 2013)*. 2013.

[10] C. Kiekintveld, M. Jain, et al. Computing optimal randomized resource allocations for massive security games. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems - Volume 1*, AAMAS '09, pp. 689–696. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2009. ISBN 978-0-9817381-6-1.

[11] D. Korzhyk, V. Conitzer, et al. Complexity of computing optimal stackelberg strategies in security resource allocation games. In *In Proceedings of the National Conference on Artificial Intelligence (AAAI)*, pp. 805–810. 2010.

[12] J. Letchford and Y. Vorobeychik. Computing randomized security strategies in networked domains. In *In Proceedings of the National Conference on Artificial Intelligence (AAAI)*. 2011.

[13] E. Mills and R. Jones. An insurance perspective on u.s. electric grid disruption costs. *Geneva Papers on Risk and Insurance Issues and Practice*, p. to appear, 2016.

[14] N. Romero, N. Xu, et al. Investment planning for electric power systems under terrorist threat. *IEEE Transactions on Power Systems*, 27(1):108–116, Feb 2012.

[15] J. Salmeron and R. K. Wood. The value of recovery transformers in protecting an electric transmission grid against attack. *IEEE Transactions on Power Systems*, 30(5):2396–2403, Sept 2015. ISSN 0885-8950.

[16] M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned.* Cambridge University Press, 2011. ISBN 9781139503662.

[17] W. Yuan, L. Zhao, et al. Optimal power grid protection through a defenderattackerdefender model. *Reliability Engineering & System Safety*, 121:83 – 89, 2014.

Appendix A

Additional Models

MAX + SG

$$Max\ p_{t^*}U_c^d(t^*) + (1-p_{t^*})U_u^d(t^*) + u_{m,t^*}^d - \sum_m p_m c_m \tag{A.1a}$$

s.t.

$$\forall_t \in T : p_t U_c^a(t) + (1-p_t)U_u^a(t) + u_{m,t}^a \leq p_{t^*}U_c^a(t^*) + (1-p_{t^*})U_u^a(t^*) + u_{m,t^*}^a \tag{A.1b}$$

$$\forall_m \in M, \forall_t \in T : u_{m,t}^a \leq p_m U_m^a(t) + L(1 - B_{m,t}^a) \tag{A.1c}$$

$$\forall_m \in M, \forall_t \in T : u_{m,t}^a \leq L(1-p_t) \tag{A.1d}$$

$$\forall_m \in M, \forall_t \in T : u_{m,t}^a \geq (p_m - p_t)U_m^a(t) \tag{A.1e}$$

$$\forall_m \in M, \forall_t \in T : u_{m,t}^a \geq 0 \tag{A.1f}$$

$$\forall_t \in T : \sum_m B_{m,t}^a = 1 \tag{A.1g}$$

$$\forall_m \in M : u_{m,t^*}^d \leq p_m U_m^d(t^*) + L(1 - B_{m,t^*}^d) \tag{A.1h}$$

$$\forall_m \in M : u_{m,t^*}^d \leq p_m L(1 - p_{t^*}) \tag{A.1i}$$

$$\forall_m \in M : u_{m,t^*}^d \geq (p_m - p_{t^*})U_m^d(t^*) \tag{A.1j}$$

$$\forall_m \in M : u_{m,t^*}^d \geq 0 \tag{A.1k}$$

$$\sum_m B_{m,t^*}^d = 1 \tag{A.1l}$$

ADD + MAX

$$Max\ U_c^d(t^*) + u_{m,t^*}^d + \sum_m p_m V_m^d(t^*) - \sum_m p_m c_m \tag{A.2a}$$

s.t.

$$\forall_t \in T : U^a(t) + u^a_{m,t} + \sum_m p_m V_m(t) \leq U^a(t^*) + u^a_{m,t^*} + \sum_m p_m V_m(t^*) \tag{A.2b}$$

$$\forall_m \in M, \forall_t \in T : u^a_{m,t} \leq p_m U^a_m(t) + L(1 - B^a_{m,t}) \tag{A.2c}$$

$$\forall_m \in M, \forall_t \in T : u^a_{m,t} \geq p_m U^a_m(t) \tag{A.2d}$$

$$\forall_t \in T : \sum_m B^a_{m,t} = 1 \tag{A.2e}$$

$$\forall_m \in M : u^d_{m,t^*} \leq p_m U^d_m(t^*) + L(1 - B^d_{m,t^*}) \tag{A.2f}$$

$$\forall_m \in M : u^d_{m,t^*} \geq p_m U_m(t^*) \tag{A.2g}$$

$$\sum_m B^d_{m,t^*} = 1 \tag{A.2h}$$

DISTRIBUTION:

1	MS 0899	Technical Library, 8944 (electronic copy)
1	MS 0359	D. Chavez, LDRD Office, 1911

Sandia National Laboratories