LTC Brian Axelsen
MAJ Steve Jones
OA4202 – Network Flows and Graphs
Red Team Modeling Project – Executive Summary

Interdicting Tradeflow on the U.S. Rail Network

The U.S. Rail Network is vital to moving large amounts of goods between large population centers. It covers over 140,000 miles and carries about 43% of intercity freight volume. In order to determine the economic impact of a "dirty bomb" attack on this network, we decided to simplify the problem by looking at just the two largest cities, which presumably have the largest economies, and how an attack would affect their tradeflow with the rest of the country. We designed a multi-commodity flow model that looked at how the generic New York City (NYC) and Los Angeles (LA) commodity flow would be impacted by an interdiction of the rail network that distributes a large part of those two commodities to the rest of the country.

We chose to model the tradeflow between our two supply cities (NYC and LA) and the demand cities (all major cities in the rest of the country) by using the economic gravity model. We got this idea from a thesis by a former NPS student, John P. Babick. The gravity model is commonly used and calculates the tradeflow between the supply and demand cities as a product of the economic mass of two cities proportional to their distance. We determined that in our simplified network the city's economic mass is roughly equal to its population. As an example, the demand of the LA commodity from, say, Des Moines, IA, is the population of LA multiplied by the population of Des Moines divided by the distance (squared) between the two cities.

We modeled the class 1 rail network of the U.S., which carries the majority of all rail traffic, using a coarse approach by first locating the largest 50 metropolitan statistical areas (MSAs) on the rail map and connecting them with edges that represent all of the rail lines that connect the two cities. In areas of the country where significant rail intersections occurred in MSAs smaller than the largest 50, we added those MSAs as nodes in the network. Additionally, we combined some MSAs to account for a very short edge between the two nodes. For example, LA and Riverside, CA were combined. In total, we accounted for ~55% of the US population using 63 nodes and connected those nodes together with 298 unidirectional edges. The cost to traverse an edge in the network (shipping cost) is one dollar per mile per unit of tradeflow. The supply from the supply nodes of each commodity equals the sum of the demands of all demand nodes for each commodity. The capacity of each edge is set to a level at which it will never impact the model in order to account for the fact that the U.S. rail network is operating at only 60% capacity and our edges correspond to multiple rail lines between cities.

The measure of effectiveness (MOE) for the network is the total economic cost of the supply and demand model for tradeflow. This includes the total shipping cost of moving both NYC and LA commodities along usable edges and the cost of unsatisfied demand (unused supply) for both commodities. The "operator" in this problem wants to satisfy all demand for each commodity from every demand node at the minimum cost. The "attacker" uses dirty bombs to maximize the cost of tradeflow between the two largest population centers and the rest of the country. Attacking an edge

represents the incapacitation of the rail network between two MSA's. Assuming heavy security at the port city, the model does not allow attacks on edges from NY or LA. We extended the model by removing this constraint (which will be discussed below).

The model was first run without interdiction to establish a base cost, and then with increasing attacks to determine the resiliency of the network. Solutions were not nested; the location of attacks depended on the number of attacks. Although this is a common feature of interdiction models, it highlighted a key feature of the network: there was neither a single point of failure nor excessive vulnerability. Results are presented in Figure 1.

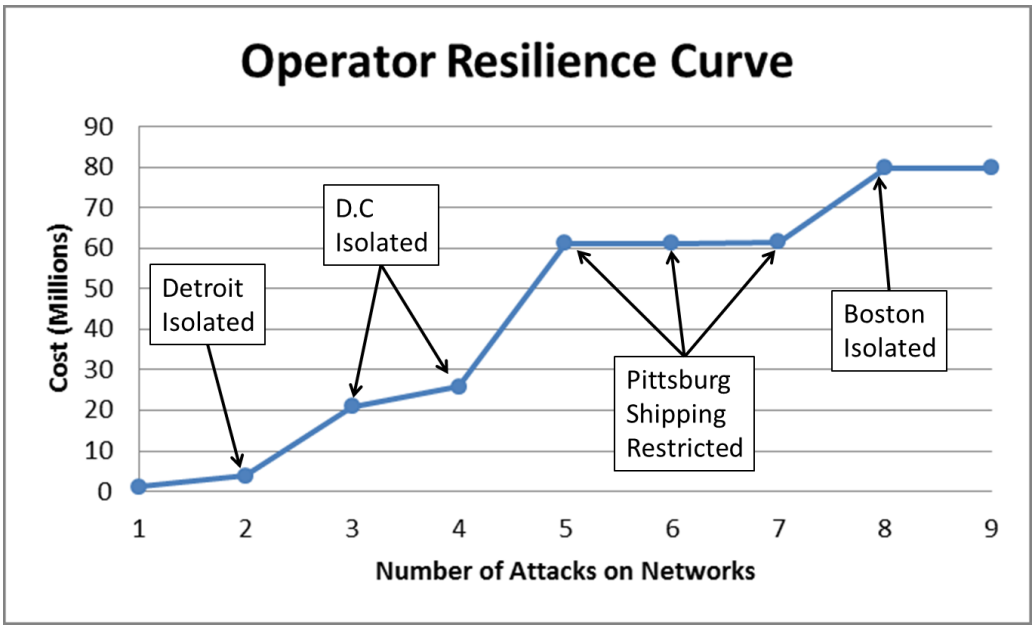

Figure 1. Operator Resilience Curve. The cost is in units of tradeflow per mile. The base case had costs of slightly less than 1 million, and 1 attack had costs of slightly more than 1 million, a relatively small increase. Increasing attacks do not cause a linear increase in user costs. Costs "jump" with increased attacker capability such as isolating a major city or restricting flow through a major transportation hub.

The model was extended to investigate the impact of allowing attacks on edges attached to the supply nodes, Los Angeles and New York. As could be expected, regardless of the number of attacks, an attack always occurred at edges attached to a port city. Also expected, once the attacker had a sufficient number attacks to completely disrupt one of the ports, costs increased dramatically. However, as seen in the constrained model, solutions were not nested; one attack interdicted tradeflow from New York, two attacks interdicted tradeflow from Las Angeles, etc. The dramatic increase in costs associated with attacks on ports validates the security focus on ports.

This work was limited in scope due to the compressed time to deliver results. Future work could significantly enhance the fidelity of the model solely by refining the data. Most simply, supply could be added to every major port city. Further, supply and demand could be added to each city to represent the actual flow of goods by rail (which would be a significant increase in data requirements). Similarly, the capacity between nodes in the current model is uniform; adjusting the capacity to reflect real capacities would be simple to implement (but somewhat tedious to support through data development). Finally, the cities could be remodeled as two nodes (one –in node and one –out node). This last

enhancement would be used to reassess the “dirty bomb” impact on shipping, and could complement and augment previous modeling efforts.

We conclude that based on our model, the U.S. class 1 rail network is fairly resilient to attack for several reasons. First, due to its high physical capacity, especially east of the Mississippi River, demand flowed around a small number of interdictions. There were also no single points of failure or extreme vulnerabilities, as demonstrated by the fact that the attackers’ solutions were not nested as they were allowed more interdictions. Finally, the greatest increase in cost incurred by the network came by isolating a transportation hub, not a city.