Proceedings of the 2015 Winter Simulation Conference
L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds.

CYBER DEFENSE ECONOMETRIC OF A POWER GRID DISTRIBUTION INFRASTRUCTURE

Cory-Khoi Q. Nguyen, James Eric Dietz, Samuel Liles, Victor Raskin, John Springer

Purdue University
Knoy Hall
401 North Grant Street
West Lafayette, 47906, USA

ABSTRACT

In collaboration with a Midwest Utility Provider, we developed a cyber defense econometric model via Anylogic that not only simulates the operational process of the Utility's local distribution infrastructure, but also helps to minimize the cost of implementing security. By measuring the economic impact of various cyber attacks affecting disparate components of the distribution infrastructure, it was discovered that both extremes of the paradigm (no security measures implemented vs. securing every device) were unacceptable solutions in regards to protecting the business financially.

1 INTRODUCTION

Cybersecurity has been the topic of interest in not only the financial and government sectors, it has been a point of concern for the critical infrastructure sector as well. In our research in collaboration with a Midwest Utility Provider, we established an Cyber Defense Econometric model that helps utility provider make more inform decisions in regards to securing their distribution infrastructure.

By using real data provided by the utility company, we were able to simulate the real energy consumption as it flowed through the distribution infrastructure. Various components throughout the infrastructure are responsible in helping to regulate power to the consumers. Our model not only simulates the distribution grid of the provider, it also simulates the operational component - i.e. routine maintenance, repair and replacement time and cost of the devices.

Once we established a baseline of normal operations, we introduced the cyber component and the challenge of securing the devices responsible for regulating and delivering power successfully to the consumers. We introduce probabilistic cyber attacks in the model and measure the economic impact of a spectrum of cyber security practices (from ignoring security to securing every device). Through numerous simulation testing, we employed the AnyLogic Optimization engine to establish the best case scenario for the company given a set of cyber security implementations through various parameters.

The results of our study shows that depending on the cost of security, it would beneficial to secure certain devices over others, and in extreme cases when the cost of security is very high, it would be better for the company to risk not implementing security measures at all. We studied scenarios from one extreme to the other and concluded that there can be a compromise in "when to" and "when not" to implement security measures.

2 PROBLEM

The utility sector is not apt to change, their investment of equipment and infrastructure is envisioned to operate and function for the next 20+ to 50+ years. In order to more easily manage these devices, many have the ability to communicate over networks and inevitably the Internet. These embedded devices are then exposed to the same vulnerabilities and threats of traditional computing systems (desktop, servers, and etc..). However, unlike traditional computing systems which are quickly patched, the critical infra-

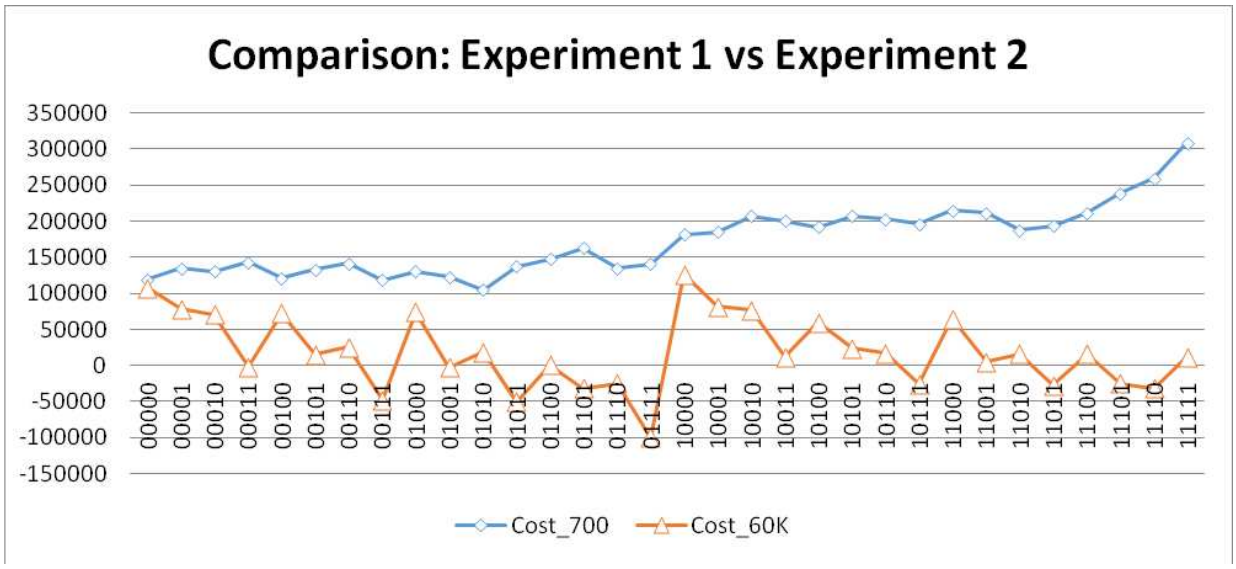
structure devices are not so easily patchable due to inherent architecture limitations and often required replacement by newer models. This is the point of contention and debate. At what point are utility companies willing to risk an attack through a known vulnerability of their device or invest in security measures to eliminate that risk. Our model with the given parameters aims to help providers answer this question better and not just be satisfy with ignoring all security risk, by not implementing any security in their devices and infrastructure.

3 SIMULATION METHOD

Our model employs both discrete and agent-based methods to more accurately represent the devices and infrastructure for the local distribution layer of the Utility Provider. Discrete method was used to help represent the flow of power usage from the source to the consumer. Agent based method was used to represent the devices (i.e. capacitors and reclosers) used to regulate power throughout the distribution infrastructure.

4 RESULTS

The model represents 2 reclosers and 3 capacitors. Experiment 1 set the security cost per device at $700 and Experiment 2 set the security cost per device at $60000. Experiment 1 sets the price to secure each device at a reasonable rate compared to the extreme case of Experiment 2 where the price to secure each device is very expensive. The results show that when the price of security of device was very high, the difference in financial gain of just securing 1 device as to no devices is not (~$20K difference) statistically significant performed by our One-Way ANOVA. Therefore in this case, the user of the model would lower the cost of security per device parameter of the model to gauge at one point it is affordable to secure at least one device.



5 IMPACT / BENEFITS

The impact and benefit of this study allows the utility provider to make better decisions of where and when and at what price to implement security solutions throughout their distribution infrastructure. They now have a clearer picture of how much it would cost their business when they decide or not to decide to implement security of their critical infrastructure devices.