Promoting Resiliency in Emergency Communication Networks: A Network Interdiction Stylized Initial Case Study Model of a Miami-Dade County Network

Michael R. Bartolacci, Information Sciences and Technology
Penn State University-Berks, Reading, PA, USA

Stanko Dimitrov, Management Sciences, University of Waterloo
Waterloo, Ontario, Canada

ABSTRACT

Police, fire, and emergency personnel rely on wireless networks to serve the public. Whether it is during a natural disaster, or just an ordinary calendar day, wireless nodes of varying types form the infrastructure that local, regional, and even national scale agencies use to communicate while keeping the population served safe and secure. We present a network interdiction modeling approach that can be utilized for analyzing vulnerabilities in public service wireless networks subject to hacking, terrorism, or destruction from natural disasters. We develop a case study for the wireless network utilized by the sheriff's department of Miami-Dade County in Florida in the United States. Our modeling approach, given theoretical budgets for the "hardening" of wireless network nodes and for would-be destroyers of such nodes, highlights parts of the network where further investment may prevent damage and loss of capacity.

Key Words: *Network Interdiction, Wireless Network, Model Optimization, Network Hardening*

INTRODUCTION

Wireless networks play an ever-increasing role in the lives of most countries across the globe. Whether utilized for personal voice and data communications, the exchange of various forms of business traffic, or governmental/public service uses, such networks are expected to remain operational in the face of natural and manmade disasters. One of the authors has previously published work related to the lack of wireless infrastructure in rural areas of China and the tremendous destruction and lack of resilience that occurred in those same areas when faced with natural disasters such as floods and earthquakes (Ozceylan & Bartolacci, 2012). Even during disasters such as Hurricane Katrina and Superstorm Sandy in the U.S., the loss of the cellular network, in addition to power outages or direct wind/flood damage, created chaos and hindered the ability of responding emergency personnel to assist the affected populace. When the possibility of deliberate sabotage or the hacking of wireless networks is added to the seeming eventuality of natural and manmade disasters, one can see the need for risk management with respect to such network infrastructures.

Risk management for such networks would necessarily include the determination of possible failure modes and their associated probabilities for network nodes. While the damaging effects of natural disasters are difficult to predict and even more difficult to assess their specific costs, it is a necessary exercise for governmental agencies, network operators, and other associated entities. In order to ascertain where a network may be "hardened" through the addition of such elements as backup power generators, redundant equipment, and wind-resistant antenna masts, a budget along with potential costs for damage and the equipment necessary to maintain connectivity must be determined *a priori*. Although portable nodes exist for cellular networks and temporary RF (radio frequency) networks can be set up for other forms of emergency wireless communications, the time to move such secondary forms of network nodes into place and become operational could entail the cost of much destruction of lives and property (Bartolacci, et al., 2013). Costs and procedures for hardening a network against hacking or terrorism would be similar in scope, but the probabilities of various failure scenarios may be more difficult to define in that unlike natural disasters, terrorists or hackers can damage multiple nodes without warning and accomplish such in a pattern that intends to inflict the most damage on the network subject to their budget constraints. This tradeoff of the ability of a network's operator to invest resources to make network less susceptible to damage from natural or manmade events versus the ability of terrorists, hackers or "mother nature" to inflict damage on a network can be modeled through network interdiction modeling.

NETWORK INTERDICTION MODELING

Network interdiction models fall under the general category of game theory models. Such models attempt to capture the interplay between two or more actors, each seeking some goal. Various types of game theory models exist with most models having an assumption that each actor involved intends to maximize their reward within the "game" for him or herself as it plays out. The term "interdiction" is seen throughout optimization research literature, particularly with respect to modeling military and governmental processes such as supply logistics as utilized in the work by McMasters and Mustin (1970). Its military definition broadly deals with the destruction or disruption of supplies and the processes used to deliver them. One of the first applications of deterministic network interdiction modeling was conducted by Wood (1993) on the flow of raw materials for illicit drug production into various regions in South America. Network interdiction models tend to follow the process outlined by Smith (2008). Dimitrov and Morton (2013) describe four applications of network interdiction modeling, including one that is similar to the case study model, in this work: identifying vulnerabilities in an electric power system. Work that utilized the notion of network interdiction for analyzing source-destination path availability in a network infrastructure was conducted by Murray, et al. (2007) and Matisziw and Murray (2009). A description of the basic workings of an interdiction model is necessary to fully understand its applicability to our case study.

Two main actors take part in a network interdiction model, the interdictor and the defender. When applied to networks such as wireless telecommunication ones, the interdictor performs some interdiction actions on the network in order to disable or destroy part or all of the network. Such actions may involve removing nodes or links, or at the very least reducing their ability to function as designed thereby reducing capacity and flow. The extent to which the interdictor can complete as many of these actions as possible is subject to a budget constraint. In other words, an interdictor does not have unlimited funds to spend on attacking a network and must attempt to inflict the most damage with what resources are available. A network defender has the opportunity to invest in preventing network damage through various actions such as adding redundant equipment or better security around network nodes. Such actions come with their associated costs. The goal or objective of the network defender is to retain as much original capacity (flow or traffic) in the network as possible through its defensive actions on the network subject to its budget constraint. This directly runs counter to the previously described goal of the network interdictor or attacker to reduce as much capacity or flow on the network as much as possible through attacks on network components subject to its budget constraint. This two-stage network interdiction model process is similar to a Stackelberg game as described by Smith (2020). In this type of interdiction model the actions of both a network provider and attacker can be viewed as nothing more than the equilibrium strategies of a two-player game. This is a zero-sum game in which the attacker (interdictor) is interested in lowering the operator's objective function as much as possible.

From a game-theoretic point of view, a network operator would want to spend the minimum amount of resources to operate a network to its full capacity. This would be the equivalent of operating the network as originally designed. On the other hand, a network attacker would want to maximize the amount of resources expended by the network operator required for full capacity by choosing network components to attack, thereby reducing capacity and the network’s functioning performance. This perspective results in the interdictor playing a maximin strategy while the operator playing a minimax strategy. One may extend the two-stage, maximin models, to three stage min-max-min models, in which the operator first designs and deploys the network, then the interdictor attacks the network, and finally the operator responds to the attack. This case study focuses on the investment of resources in order to prevent damage due to parts of the network. From both a disaster planning and a network risk analysis point of view, determining where to make investments in order to prevent network components from sustaining damage is the proper course of action. This is supported by the notion that responding to damage from a network interdictor can take time and resources that are not available in the context of a crisis.

For the purposes of this case study, a public service network in a hurricane-prone area such as Miami-Dade County in Southeastern Florida would have some “hardening” built into its original design to withstand the forces of Mother Nature. Unfortunately, such a design would not necessarily include the possibility of destruction or interference by terrorists or hackers. This case study illustrates how a network interdiction model can provide crucial decision support for a network operator in deciding where to invest additional resources in order to take these additional factors into account given a limited budget for such investments to prevent the damage in the first place. For the network interdiction model presented, a network interdictor only seeks to reduce capacity through an attack on a given network component. Although complete destruction of the component may be the ultimate result, the optimized model for this case study does not distinguish between capacity reduction and total capacity loss for a given component. In the "real world" context of an emergency or crisis, any reduction in capacity in the network may be considered catastrophic in nature and have potentially grave consequences.

If we consider the ability of the network to perform during and immediately after a disaster or emergency, then the following example may provide some additional insight on the application of a network interdiction model. Consider that an interdictor is interested in disrupting post-disaster telecommunications involving emergency responders thereby delaying or prevent their response to calls for assistance from the affected populace. Such disruptions only add to the myriad of difficulties already being encountered during a crisis such as a severe hurricane making landfall. Given a wireless emergency response network's architecture, the interdictor will have a budget that places an upper limit on the number of network components it may destroy or disable within a relatively short time window for a given crisis. For example, the attackers may bring down or reduce capacity at most *l* of n total nodes in the network due to this restriction. Also, it should be noted that at this point in the discussion, the model allows for heterogeneous nodes within the underlying network structure; thus they may vary in their functional nature and likewise their cost of removal or infliction of damage. As such, estimating that at most *l* nodes may be removed or damaged by the attacker, the operator may choose to expend resources to create a telecommunication network composition that is resilient to *l* node failures. An optimized network interdiction model will enable the provisioning of a hardened wireless network infrastructure that is resilient to such attacks from a given interdictor at the lowest possible cost. In fact, the resulting optimized model pinpoints where such investments should be made to harden the network against attacks from a given interdictor and their budget. The decision support properties behind the model and its optimization are that a given attacker will use its budget in such a way as to maximize the damage to the overall network while a network operator will use as much of its budget as necessary to harden the network against the resulting points of attack identified. Thus, the overall modeling approach, when optimized, can provide specific information on where to harden a wireless network and the costs involved to do so for a given attacker and their budget.

We include in this section a formulation for a generic interdiction model. This mode seeks to determine the minimum cost network deployment strategy for a network operator with three different communication technologies $T = (A, B, C)$ that can be implemented in L locations for n nodes. The interdictor has a budget of k to remove nodes with a cost of k_i to remove a node of type i.

$$max_{x \in X} min_{y \in Y} \Sigma_{T,L} y_{i,j} \cdot c\_i$$

$$s.t. \sum_{i \in T} y_{i,j} = 1 - x_{i,j}, \quad \forall j \in L$$

$$\sum_{i \in T} k_i \cdot x_{i,j} \leq k,$$

$$x, y \in \{0,1\}^{|L| \cdot |T|}$$

$$connectivity\ constraints$$

Please note that above $X = Y = \{0,1\}^{|L| \cdot |T|}$, $y_{i,j} = 1$ if the node at location j uses technology i. Similarly, with respect to the decision variables, $x_{i,j} = 1$ if the node at location j using technology i is removed by the interdictor. The connectivity constraints are listed as the first set of constraints and are technology-specific (as explained above). As such, each must be added for a given network architecture. An example of such a constraint might be the maximum number of users a node using a particular technology can provide service for in a specific location. The second set of connectivity constraints deals with the limitation of the budget for the network interdictor. In other words there is a limit to the amount of nodes an interdictor can remove from the budget allocated.

To conclude this discussion of network interdiction models, we briefly describe our approach for optimizing such models. In order to facilitate the implementation of such models as decision support tools for network operators, we chose to utilize online open source optimizing software that would be readily available without cost. The general strategy for optimizing network interdiction models we followed is outlined in the tutorial by McLay (2015). Since this work focuses on the practical implications of decision support for network planners and operators, the optimization methodology encompassed in the software is not discussed. The optimization takes as inputs the number of nodes, the costs to harden such nodes, the costs to damage such nodes, the costs to move a network operations center to a new node, the budget of the network interdictor, and finally, the budget of the network operator. The optimization's output identifies which nodes were theoretically attacked and sustained damage (reduced capacity and flow) for a given set of inputs. Thus, "what if" analyses may be performed through a series of model instances, each with potentially different budgets and costs for both the network operator and interdictor.

NETWORK INTERDICTION FOR EMERGENCY RESPONSE NETWORKS

The scenario of interest in this work involves attackers, such as a terrorist or hacker organization, that seek to take advantage of the conditions following a natural disaster to inflict damage upon wireless communication networks used by emergency responders. The motivation for such attacks could be any one of several possible reasons, but we will focus strictly on the effect of the attack on the wireless network. The scenario could be easily adjusted to account for "mother nature" being the interdictor and seeking to damage the network, but for the purposes of this case study, we focused solely on human interdictors. Due to the fact that any nefarious organization or person, be it hackers or terrorists, attempting such an attack does not possess unlimited resources to carry out the attack, there exist restricting conditions on the nature and scope of the attack. The attacker would have a budget, as previously described, that limits the nature of the attack and the amount of possible damage that can be inflicted. The operator, on the other hand, takes actions to prevent damage to the network that would be caused by an attack by using resources to “harden” network components.

Emergency response wireless networks serve a variety of local, regional, national, and even international agencies and organizations including police, fire fighting personnel, and medical emergency personnel. A variety of fixed architecture and portable wireless networks exist to satisfy communication needs for such emergency responders and the affected populace before, during, and after a crisis. The most common type of wireless network utilized at the local level in the United States is a technology known as Trunked Radio. Typically, police, fire, and medical emergency personnel use a trunked radio system to communication between base stations and mobile units such as police cars, fire trucks, and ambulances. Centralized emergency services for a county or larger city in the U.S., known by their more common name related to the digits dialed to call the central base station as 911, also utilize trunked radio for communication and coordination. The premise of trunked radio is that it allows for sharing of frequencies among groups of users. One method for this sharing of frequencies can be accomplished through Time Division Multiple Access (TDMA) for a trunked radio network that uses digital channels. A standard developed in Europe, Terrestrial Trunked Radio (TETRA), utilizes this method of sharing capacity for both point-to-point and point-to-multipoint communications. These modes of sharing capacity and distributed communications increases the potential impact for an interdictor seeking to inflict damage on such a network. The ability to reduce capacity and limit communications for more than a single pair of network nodes during an attack represents the great potential for wreaking havoc on emergency responders and the affected populace. Although other types of wireless systems are used by emergency personnel for disaster-related communications, such as satellite-based ones and the cellular phone network, the focus of this work is on a trunked radio architecture.

The implementation of trunked radio for local and county emergency management involves the use of one or more base stations communicating with mobile units in a wireless fashion. Repeaters, remote unmanned stations that rebroadcast signals to expand the overall communication area are also used for larger cities and counties. For the purposes of our modeling, both base stations and repeaters represent fixed nodes on the wireless network that are potential targets for an interdictor. We do not consider individual mobile units, such as police cars or ambulances, as targets for interdictors due to the fact that they are single sources and destinations of traffic on the network and are transient in their operations. Targeting such nodes would represent significant logistical and technical challenges for an interdictor due to their mobility and ability to exit and rejoin the network in a haphazard fashion. In addition, during a large-scale emergency event, mobile units from various regions converge on the affected region. Thus, it may be difficult for an interdictor to account for all new units that may help during the event. In summary, in order for an interdictor to reduce overall network capacity, a large percentage of potentially unknown number of mobile nodes need to be targeted. While a single mobile node that is stationary for a period of time may represent a viable target, the same cannot be said for a large group of such nodes responding to a crisis.

Creating the logical network topology to be incorporated into a network interdiction model for a trunked radio network is therefore relatively simple if the network to be modeled has published information about the numbers and locations of its base nodes and repeaters. Once this information is determined, traffic flows must be ascertained for the links of the network. Since traffic flows both ways on such networks, estimates of flows must include not only traffic bound for mobile nodes, but also the traffic they generate. The estimation of traffic flows is important for the model because it is assumed that higher traffic portions of network represent areas with higher population, and therefore, greater needs for emergency services by the populace in those areas. Estimates are also needed on costs to "harden" various nodes in the network as well as the costs to bring down each node. These costs can be garnered from a typical risk analysis (Vose, 2008) that should be conducted for such networks by their operators. Creating a secondary base station node that would be used in the event of a nonfunctioning one is a cost that can be reasonably estimated and an example of how such costs would be derived. The destruction costs for nodes is more difficult in that one must envision how a terrorist or attacker would disable or interfere with a node's operation. We chose to create and optimize a network interdiction model for a given region as a "proof of concept" for the ease of analysis and applicability of the overall approach. The region chosen was Miami-Dade County in the state of Florida in the U.S.

MIAMI-DADE COUNTY EMERGENCY MANAGEMENT

Miami-Dade is a county in the southeastern portion of the state of Florida in the United States. The county includes the city of Miami and surrounding towns and cities along with a portion of the undeveloped rural area known as the Florida Everglades. The county employs a centralized 911 emergency management structure for its police (sheriff), fire, and emergency/rescue public service operations. This 911 emergency call center is the busiest in the Southeastern United States and employs over 200 personnel for all aspects of communications and dispatching emergency services including the sheriff, fire, medical and rescue personnel (Miami-Dade government website). The primary regional coverage of these services includes most of the county, but excludes certain areas that are served by city services such as those provided by the cities of Miami and Hialeah unless otherwise directed. The county's regional 911 emergency management center is located in Doral, one of thirty-four municipalities in the county, and has satellite offices/stations throughout the county. The overall scope of emergency management for the county includes a wide range of activities and services including those related to hurricane preparedness and response. In this work, we focus on a subset of the services provided by the county, namely, the sheriff's department for the county. The primary local law enforcement for the county, the Miami-Dade Sheriff's Department is considered one of the emergency response agencies that must deal with the aftermath of an emergency or disaster. Be it a natural disaster such as a hurricane, or a manmade one such as an act of terrorism, this department's duty is to ensure the safety of public and to uphold the law amid a possible range of resulting chaos and destruction.

The network we chose to focus on in this work is the eighteen node network used by the Miami-Dade Sheriff's Department. This network consists of the central node located at the central station in Doral, 15 other nodes located at various stations across the county, and two repeaters located within the county. The topology of the network can be consider a star topology (see Figure 1) due to the fact that all nodes are directly connected with the central 911 station. For the purposes of this analysis of potential attacks on wireless networking aspects of the emergency management network used by the sheriff's department, we are only considering wireless links between these nodes and take into account each mobile sheriff vehicle. The implied technological constraint of range of transmission and limitations of transmit power imply that each node covers a defined geographical range with information being relayed to the central 911 as needed from other stations and repeaters.

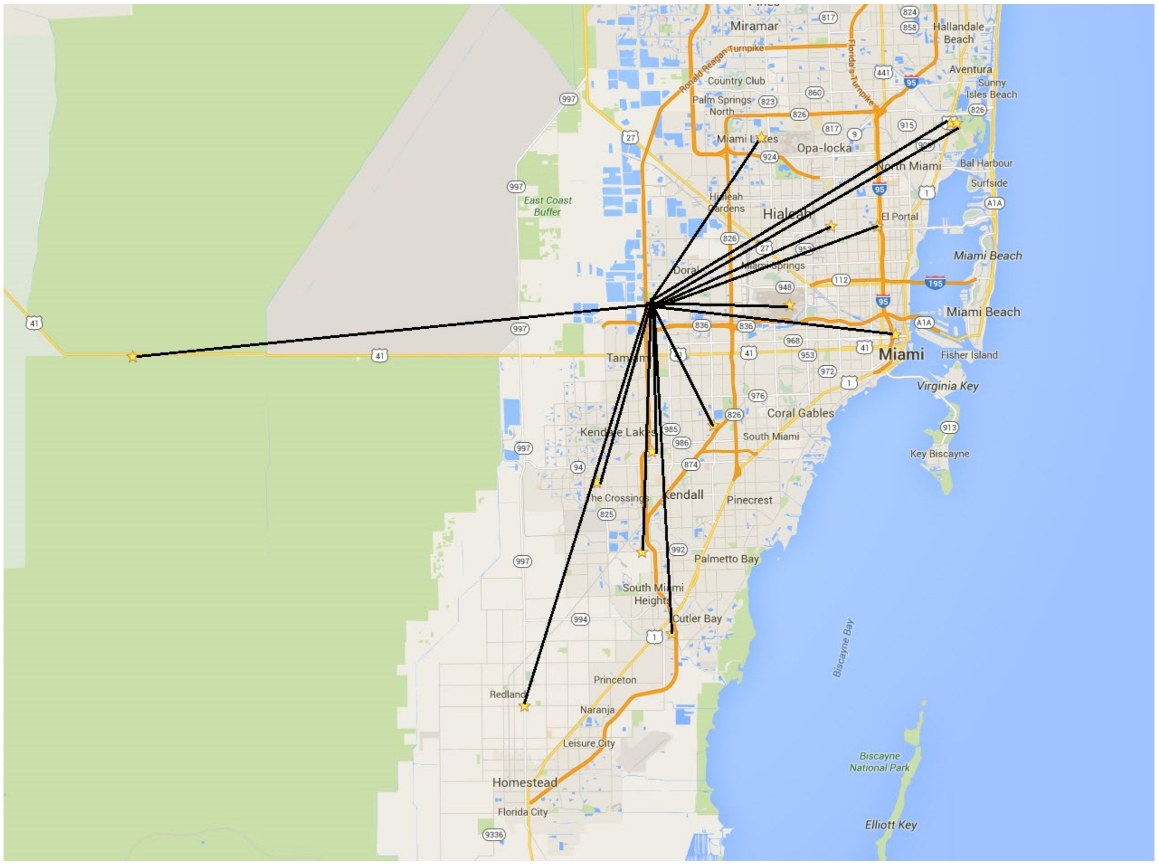

Figure 1 – Topology of the Miami-Dade Sheriff's Department wireless network.

Due to the assumption that every node on the network serves a given geographic region, one can draw a service area radius around each node based on an assumed maximum power level for a given node and the height of its antenna (which is known and published by county) using standard telecommunication engineering theory. After establishing this radius for each node, we then used demographic population data to estimate the population for each node’s service area. In order to account for overlaps in coverage areas between nodes, we subsequently decremented the total nodal population-served number for a given node by an estimate of the population in the overlap areas it shares with other nodes. It was through the use of these assumptions that traffic flows for each link on the network could be estimated, thus establishing the hierarchy of utilization for the links across the entire theoretical network topology.

Once the traffic flows were established, costs to disable each type of node were estimated based on information found through online searches and other assumptions. Once can imagine that the base control unit connected to an outdoor antenna could be disabled in one of several possible ways. The use of firearms, small explosives, and relatively inexpensive electro-magnetic jamming devices are just three of the many potential ways a terrorist or hacker could disable such a node on the network. A typical repeater antenna node that would not be located at a sheriff’s station node was assumed to have a cost range of $650 in order to disable it. The cost for a base station node located at a sheriff’s station was assumed to have a cost range of $2000. In addition, it was assumed that if the central node on the network was disabled, a cost of $10,000 would be incurred in order to switch main network management operations to another sheriff’s station-based network node. Once these cost estimates were utilized in the network interdiction mathematical programming model, along with possible budgets for both the attacker (hacker or terrorist) and the defender (sheriff’s department), the model was solved with an online solver based on the procedure outlines by McLay (2015).

Due to the fact that the focus of this paper is to show the benefits of a network interdiction modeling approach for providing useful information to wireless network operators and planners for hardening such networks, we will not detail the complete optimization procedure. The automated approach afforded to us by the use of the online mathematical programming solver allowed for a range of inputs to be tested and optimized, thus giving a clearer picture of what nodes may be more vulnerable to attackers and the costs to harden such nodes

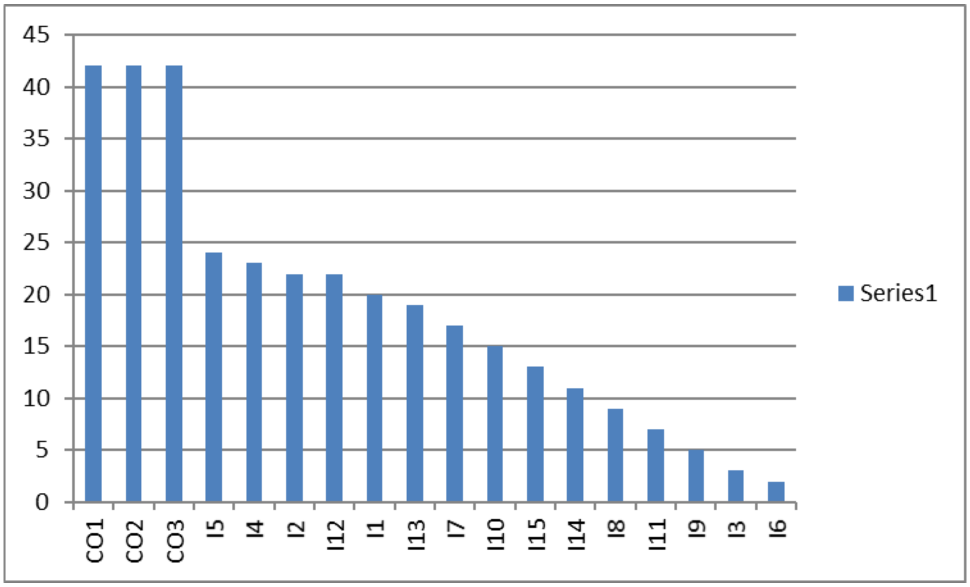

Figure 2 – Histogram of the number of times a given node was disabled

An example of the information resulting from multiple runs of the optimized model can be seen in Figure 2 above which displays a histogram of the number of times a given node was disabled. This chart clearly shows that the central office was the number one target of attackers across the multiple optimization budget scenarios. Figure 3 clearly shows another piece of information that would be very useful for the network operator (sheriff's department). This graph shows the effect of the defender's budget, representing the ability to harden network nodes, on the overall damage received by the network in terms of the number of nodes disabled for a given level of the attacker's budget. If this level of an attacker's budget is assumed to be realistic and most likely, then the graph clearly shows that not more than $25,000 should be budgeted for "hardening" network nodes since any amount beyond that does not reduce the number of nodes disabled. It also shows that three nodes the network operator should expect at least 3 nodes to be disabled despite any prevention measures taken for this given level of an attacker's budget.

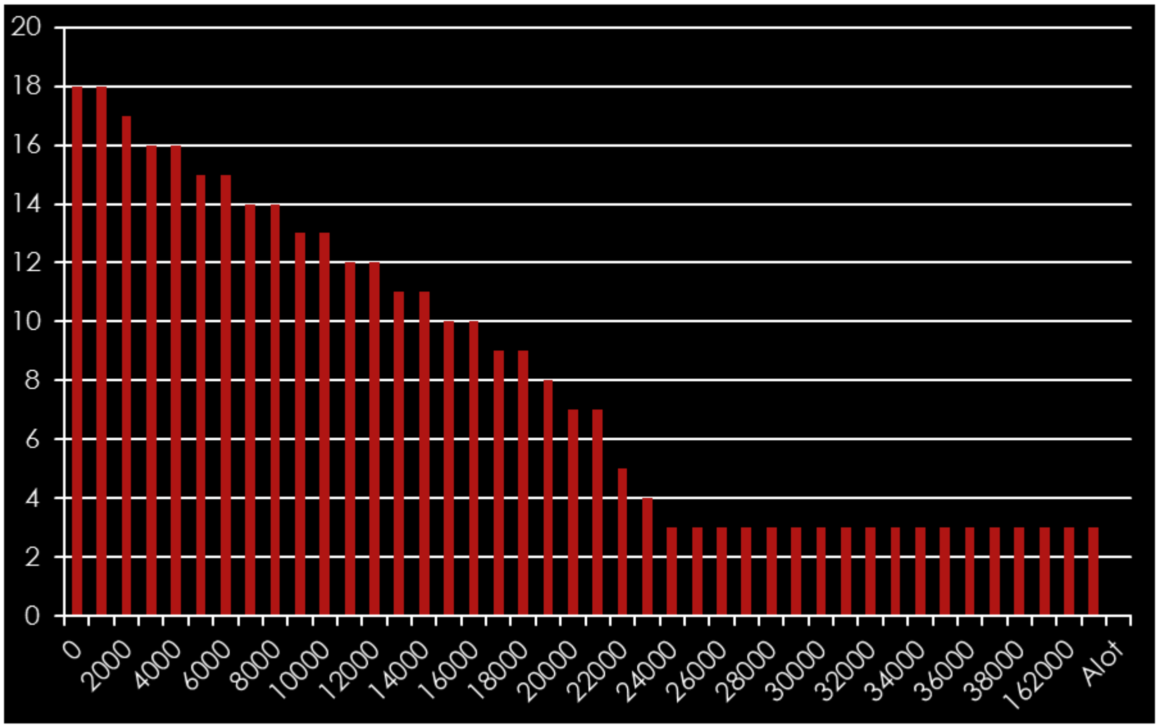

Figure 3 – Number of nodes disabled versus the budget of the defender

The two charts above are just the "tip of the iceberg" with respect to information that could be gleaned from the results of our network interdiction modeling case study for the Miami-Dade County sheriff's department network.

CONCLUSIONS

The utilization of a network interdiction model for the analysis of where to invest in the "hardening process" for wireless network nodes was conducted in this work. A focus on a real world wireless network utilized by the Miami-Dade County sheriff's department was undertaken. In particular, the network structure and an estimate of traffic flows were defined through the gathering of publicly available information. This information was then used as input to a network interdiction modeling that also utilized estimates of budgets for the network defender, the network attacker, and the costs to disable each of the network nodes. The results of the optimizations from this modeling approach show how many nodes would be disabled given certain budgets for the both the attacker and the network defender (operator). Additionally, it provided information on how much the cost would be to "harden" the network in order to reduce damage to a certain level. The real contribution of this case study was to show that with relatively little input information (network structure, costs to disable nodes, assumed budgets, and estimated traffic flows), useful information could be generated to pinpoint network node vulnerabilities and to provide guidance on budgeting for their "hardening" of nodes.

REFERENCES

Bartolacci, M. R., Mihovska, A., & Ozceylan, D. (2013). Optimization modeling and decision support for wireless infrastructure deployment in disaster planning and management. In ISCRAM *2013 Conference Proceedings - 10th International Conference on Information Systems for Crisis Response and Management*.

Dimitrov, N.B. & David P. Morton, D.P (2013). Interdiction Models and Applications. In Springer *Handbook of Operations Research for Homeland Security*, International Series in Operations Research & Management Science (Vol. 183, pp. 73-103).

Mas-Colell, A., Whinston, M. D., & Green, J. R. (1995). Microeconomic theory. *The Canadian Journal of Economics*. http://doi.org/10.2307/135312

Matisziw, T. C., & Murray, A. T. (2009). Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure. *Computers and Operations Research*, 36(1), 16–26.

McLay, L.A. (2015). Discrete Optimization Models for Homeland Security and Disaster Management, In *INFORMS Tutorials in Operations Research* (Oct. 26, 2015). http://dx.doi.org/10.1287/educ.2015.0136

McMasters, A. W., & Mustin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly*, 17(3), 261–268.

Miami-Dade County Government Website, http://www.miamidade.gov/police/contacts-communications.asp, accessed on January 15, 2017.

Murray, A. T., Matisziw, T. C., & Grubesic, T. H. (2007). Critical network infrastructure analysis: Interdiction and system flow. *Journal of Geographical Systems*, 9(2), 103–117.

Ozceylan, D., & Bartolacci, M. R. (2012). The impact and opportunities for wireless communications in chinese disaster planning and management. In *ISCRAM 2012 Conference Proceedings - 9th International Conference on Information Systems for Crisis Response and Management*.

Smith, J. C. (2010) *Basic Interdiction Models*, John Wiley and Sons, Inc., Hoboken, NJ, USA.

Smith, J. C., & Lim, C. (2008). Algorithms for network interdiction and fortification games. In Springer *Optimization and Its Applications*, (Vol. 17, pp. 609–644).

Vose, D. (2008). Risk Analysis: A Quantitative Guide. Wiley.

Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling*, 17(2), 1–18.