Promoting Resiliency in Emergency Communication Networks: A Network Interdiction Modeling Approach

Michael R. Bartolacci
Penn State University - Berks
mrb24@psu.edu

Stanko Dimitrov
University of Waterloo
sdimitrov@uwaterloo.edu

Larry J. LeBlanc
Vanderbilt University
larry.leblanc @owen.vanderbilt.edu

Abstract

Emergency communication networks provide the basis for preparing for, and responding to, manmade and natural disasters. With the increasing importance of information security, emergency network operators such as non-governmental organizations (NGOs), local and national governmental agencies, and traditional network operators must deal with the possibility of sabotage and hacking of such networks. A network interdiction modeling approach is proposed that can be utilized for planning purposes in order to identify and protect critical parts of the network infrastructure. These critical nodes or links represent opportunities where investment or "hardening" of such infrastructure may reduce or prevent reductions in network traffic flows created by nefarious actors prior, during, or after an emergency or disaster.

1. Introduction

Recent disasters such as Superstorm Sandy in the U.S. in 2012 and Typhoon Haiyan in the Philippines in 2013 represent just a few examples of events where an affected populace was in dire need of assistance from a variety of disaster relief organizations and emergency responders. Response and relief can come from a variety of sources including governmental organizations (GOs), non-governmental organizations (NGOs) such as the Red Cross, and the affected populace. All of these entities require a means to communicate and coordinate their activities in the affected region.

Most often wireless networks, whether they are operational parts of the existing mobile network (cell phone network) in the affected region, RF-based communication networks of local fire and police departments, or ad hoc networks set up specifically for disaster relief, are relied upon heavily to support emergency responders and the local populace. Wireless networks offer the obvious advantage of mobility for emergency responders as well as built-in rechargeable power sources for such devices during possible times of power outages.

This research's main contribution is the introduction of a network interdiction modeling approach in order to plan for and analyze possible disruptions in emergency communications created by the intentional, nefarious activities of would-be hackers or terrorists. These two groups, despite their motivation of profit, ideology, or other factors have the goal of disabling or disrupting emergency wireless communications thereby hampering emergency relief efforts and reducing the resiliency of the affected populace.

The application of a network interdiction approach, as opposed to a more traditional information security risk modeling and analysis approach, provides a game-theoretic view incorporating limitations of potential attackers. This modeling approach creates a scenario in which a potential attacker surveys a network's design and attempts to maximize damage subject to resource constraints. A would-be attacker's constraints could include limits on financial, manpower, and technical resources that are available for an attack. Our model essentially gives a network owner a rigorous model to aid in the decision of how and where to expend resources to "harden" a network in order to prevent an attack or mitigate damage from one.

2. Emergency communications and resiliency

The notion of resiliency in an affected population following a disaster is intimately tied to the ability of members of this entity to communicate with one another, emergency responders, and the "outside world" beyond the affected region. As has been learned in disaster such as the Japanese earthquake and tsunami of 2011 and Superstorm Sandy of 2012, traditional mobile network infrastructures may not be operable post-disaster or be overwhelmed with traffic and essentially rendered unusable. During Superstorm

URI: http://hdl.handle.net/10125/41459
ISBN: 978-0-9981331-0-2

(Hurricane) Sandy in the United States, an average of about 25% of the fixed mobile network base stations in the affected area lost service [1] and population in parts of this region were without wireless mobile access for days to follow. It should be obvious that emergency responders such as fire and police agencies, regional and national governmental agencies such as FEMA, and even major mobile network operators such as Verizon Wireless and AT&T in the U.S., would benefit from improved planning and deployment of their emergency management resources and portable infrastructure along with the portion of any fixed wireless network architecture that remains operational. The ability of a nefarious actor such as a terrorist or hacker to disable one or more key network components, must be planned for within the scope of an emergency communications scenario.

3. Emergency wireless communication network technologies

In order to understand how hackers or terrorists could disable a network used for emergency communications, one must examine the various technologies utilized in such networks. In particular, understanding that some networks are privately owned while others are operated by various governmental agencies is key to understanding their differences and their ability to survive a given disaster. It also helps to determine what type of traffic is granted priority on a heavily loaded wireless network following a disaster.

Private wireless networks that would be utilized in a disaster scenario would most likely be public cellular phone networks that allow for both voice and data communications. Base stations for such networks typically have a form of emergency power such as a generator or batteries that allow them to operate for some period of time in the event of a power failure. Unfortunately, the lifetime for generator or battery operations for a given base station is not more than a day or two. Such networks also suffer from the vulnerability of having their connections to the entire network cutoff through broken communication lines or disabled control stations that link several base stations together. An attacker could disable the backup power for a given network node (base station or controller station in a cellular network). Another possible way to affect the network would be to destroy or cut communication lines to/from network nodes.

Private networks do not necessarily need to give priority to the traffic of emergency responders, but generally do so thereby limiting the available capacity for network subscribers and others wishing to utilize them post-disaster. The ability of hackers to mimic such priority traffic, thereby reducing available capacity for true emergency traffic, represents one way such networks can be compromised. An analogy could be made that this type of attack would be the wireless equivalent of a traditional denial-of-service attack on a computer network. An attacker need not disable nodes or links on a network in order to disrupt emergency communications.

One method for ensuring that cellular wireless communications in a region affected by a disaster is available is to utilize portable mobile network base stations (BSs) that can be deployed when conditions are appropriate. Typically, cellular network providers maintain a cache of such devices that can be transported to a disaster-affected region and deployed in areas where the existing infrastructure has been destroyed or is overloaded with traffic. Having such devices available to first responders or an affected populace immediately following a disaster would be the ideal goal for a wireless cellular network operator. Unfortunately, this approach can be problematic from both a temporal and a logistical point of view. Often, such portable base stations must incur long transit times in order to be moved to an affected area. This is due to the fact that such devices are usually centrally stored to minimize inventory holding costs. Another potential problem is not having the required number of devices readily deployable to provide sufficient coverage for an affected area. This can hinder or delay relief efforts and create frustration among the affected populace that expects such networks to be continuously operable.

As wireless technologies advance, other options will become available for wireless network subscribers following a disaster. LTE-Direct (Long Term Evolution Direct) is an emerging standard that allows mobile network handsets to communicate with one another in addition to a fixed network base station. Such a standard would allow users to communicate through other users in order to reach an operable base station. The potential for hackers or terrorist to pose as a legitimate node in such a hybrid network architecture represents a potential threat. The application of technologies such as femto-cells, which utilize a fixed line broadband connection to act as a "mini" base station for mobile network handsets, represent other options that could be deployed post disaster by cellular network operators to facilitate emergency communications for an affected populace and emergency responders. The potential exists with these devices for hackers to offer their own “fake” connection points for collecting user traffic or to provide false traffic much the same way Wifi hotspots can be used for nefarious purposes.

Other technologies that might be utilized by governmental agencies or aid (disaster relief) organizations for emergency communication networks include VSAT (Very Small Aperture Terminal) networks that utilize satellite links for establishing local area networks in an affected region and HetNets (Heterogeneous Networks) which are a hybrid mix of wireless communication technologies deployed within a single framework. Such networks may fall under the general category of ad hoc networks in that their topological design is determined at the point of deployment. Such networks would represent a challenge for hackers or terrorists to disrupt due to this fact, but their ad hoc nature also creates less centralized control over network access.

Previous work in the literature addressing ad hoc network use for disaster recovery looks at technical details and not such issues as portable base station placement or required connectivity in an overall optimization framework. Unlike some of this previous work, we recognize that some fixed mobile network infrastructure existed prior to the disaster and may be optionally integrated into the model if still operating. A hacker or terrorist can add further damage to a surviving network and might even be able to disguise such damage as being a result of the disaster and not their sabotage. Wireless networks operated by governmental agencies would necessarily be designed to withstand natural disasters to a certain extent, but probably not the intentional damage or intervention by terrorists or hackers in a post-disaster scenario. In particular, the Radio-Frequency (RF)-based nodes (repeaters, central offices, etc.) of local wireless networks built for fire, emergency/rescue, and police with a city or county may withstand damage from disasters better than cellular network towers in public networks due to their original design considerations.

Other types of wireless network architectures beyond public cellular and those utilized by fire/emergency/police exist. One of the relevant works on wireless network design that addresses disaster recovery is by Lu and coauthors [2]. They outline hybrid ad hoc network designs for disaster recovery using Wi-Fi, WiMax, and geostationary satellite technologies. It should be obvious from the mention of both WiMax and satellite technologies that the network architectures they propose assume no existing mobile network connectivity (functioning fixed BS's) to link to and require specialized WiMax and satellite equipment. Their work looked at 2 tier (Wi-Fi linked to Satellite) and 3 tier (Wi-Fi linked to WiMax linked to Satellite) architectures and merely proposed such hybrid network designs for disaster recovery without any notion of optimization. More recent work by Tsai and collaborators [3] provided an architecture design for applications utilized for emergency management.

A technological example of a wireless emergency infrastructure in the U.S. would be low cost handsets that use unlicensed frequencies. They represent an inexpensive way for an affected populace to communicate during and after a disaster. These point-to-point handsets are readily available in the U.S. at retail department stores in most cities and towns. FRS (Family Radio Service) handsets, which are essentially half duplex "walkie talkie" units that are sold for family and recreational use and have a useful range of a few hundred feet, are an example of this type of technology. A small rural community that encourages the purchase of such devices by its residents could be considered a public investment in an emergency communications infrastructure. Unfortunately, sole reliance on these inexpensive point-to-point mobile handsets for localized communications among volunteers acting as emergency response personnel post-disaster may not be a wise design choice. This is due to the possibility that the removal of any one node in the network may result in complete network failure if such a node acts as the sole intermediate node for relaying important information to other parts of the network. RF jamming or the sabotage of a handset's battery power source by a nefarious actor (interdictor) could seriously hinder such an ad hoc network architecture as well. However, not utilizing such an inexpensive ad hoc wireless technology may increase emergency network deployment costs significantly. The purchase of a more sophisticated trunked radio system for a small community could cost tens of thousands of dollars or more.

One can therefore see that the investment in emergency communications is a balancing between available resources, the needs of emergency responders, and the requirements of the affected populace during and post-disaster. It is the intentional disruption of a network that we will model. In particular we look at the cost tradeoffs of investment in “hardening” wireless communication network given a level of cost that a nefarious actor (terrorist or hacker) is willing to spend in order to inflict damage on a given network.

4. Network interdiction modeling

A network interdiction modeling approach was chosen to model the intentional sabotage of emergency wireless networks prior to or during a crisis or disaster. Such a modeling approach tends to follow the process outlined by Smith [4]. In this process, the *interdictor* performs some interdiction actions on the network, such as removing nodes or links, subject to one or more budget constraints which represent scarce resources such as monetary funds, time, or manpower.

It is assumed that any nefarious organization or individual does not possess unlimited resources to carry out an attack. The scenario of interest in this work involves a would-be attacker that takes advantage of the conditions just prior to, during, or immediately following a natural disaster to inflict damage upon communication networks needed by emergency responders and the affected populace. For example, one can imagine a perpetrator lurking behind during the chaotic conditions of a pre-hurricane evacuation of a coastal area in order to disrupt power sources for mobile base stations or cut cabling to antennae for repeaters used by EDACS (Enhanced Digital Access Communication System) systems for fire, police and emergency responders.

After an interdictor takes some course of action in order to disrupt the wireless network(s), the *operator*, then responds by taking recourse actions on the network. This two stage process is similar to a Stackelberg game [4] and 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. This objective function is the normal throughput and operation of the wireless network when needed by emergency responders. From a game-theoretic point of view, if a network operator is interested in deploying a minimum cost wireless network to support emergency responders in an area that is prone to disasters (such as coastal areas subject to hurricanes, floods, and tsunamis), then the interdictor will look to maximize the minimum cost of the resulting network. This perspective results in the interdictor playing a maximin strategy while the operator playing a minimax strategy. Similarly, 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.

If we move away from network deployment costs and instead consider the ability of a wireless network to perform during and after a disaster or emergency, then the following example may provide some additional insight. Consider the same nefarious organization as the interdictor that is interested in disrupting post-disaster telecommunications which only adds to the difficulties encountered by emergency responders and the affected populace. Given a network architecture, the nefarious organization or individual will have a budget that places an upper limit on the number of network components it may destroy or disable. For example, the attackers may disable or destroy at most k of n nodes due to this restriction. Also, it should noted that the model allows for nodes to vary in their nature and cost of removal, much the same way wireless communication networks can be pieced together in an ad hoc fashion from varying technologies post-disaster. As such, knowing that at most k nodes may be removed, the operator may choose a wireless telecommunications network composition that is resilient to k node failures by investing in additional network infrastructure or redundancy for nodes or links.

The example provided above deals with network sabotage, but could just as easily apply to network hacking. An interdictor may pose as an emergency responder and relay false information to other responders. Another possibility is that the hacker utilizes location information being relayed to inflict damage on the populace, infrastructure, or property. To build upon the previous example, if unlicensed FRS units were utilized, an interdictor could pose as a volunteer emergency responder for very little cost or preparation.

5. Specific network interdiction modeling

We begin this section by formulating a generic interdiction optimization model to determine the minimum cost network deployment strategy for a network owner or operator with three different communication technologies $T = (A, B, C)$ that can be implemented in L locations for n nodes and the interdictor has a budget of k to remove nodes with a cost of k_i to remove a node of type i.

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

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

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

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

$$connectivity\ constraints$$

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, $x_{i,j} = 1$ if the node at location j using technology i is removed by the interdictor. The connectivity constraints are technology-specific, and as such, must be added for a given network architecture. An example of a constraint might be the maximum number of users a node using a particular technology can provide service for in a specific location.

Unlike a fixed line infrastructure that could support large amounts of broadband traffic, if operational,

during and after a disaster, a wireless network would necessarily first support voice communications for emergency responders. Data traffic would be considered secondary for those same responders and possibly the affected populace. The network interdiction model's ability to deal with the varying technologies provides an advantage to this modeling approach. One only has to deal with the costs of creating and maintaining connectivity from the operator's viewpoint and the limitations on resources from the interdictor's viewpoint.

We have further developed this basic network interdiction model to allow for optimization utilizing the approach in [5]. A bi-level formulation of this model then requires the dual of the inner minimization to be taken and solved.

Notation for the Model Formulation

- Parameters:
  - d_i:The demand for node i
  - K_i: The amount of cost required to bring down node i
  - CO: The set of all central office locations
  - I: The set of all repeaters and sheriff locations
  - B: The budget of the attacker
  - s_i: The cost to the defender for repairing a CO
  - C: The budget of the defender
- Decision variables:
  - x_i: The investment decision of the attacker, how much is put to attack node i
  - y_i: The investment decision of the defender, how much is put to defend node i
  - f_i: The remaining capacity of node i

In order to properly bound this maximization during solving by standard optimization software, the notion of a budget for the defender (network operator or owner) had to be incorporated. Thus the model included budgets for both the network interdictor (attacker) and network defender (owner or operator). The resulting optimization for the derived network interdiction model yields very useful information encompassed in the decision variables of the inner dual formulation. The information resulting from the optimization identifies which network components

Bilevel Formulation of the Network Interdiction Model

$$\max_{y} \min_{x,f} \quad \sum_{i\in I\cup CO} d_i \frac{f_i}{K_i} + (|CO| - \sum_{i\in CO} f_i/K_i) \cdot \sum_{i\in I} d_i$$

$$\begin{aligned}
s.t. \quad & f_i = K_i - x_i + y_i && \forall i \in I \cup CO \\
& f_i \le K_i && \forall i \in I \cup CO \\
& \sum_{i\in I\cup CO} x_i \le B \\
& x_i \le y_i + K_i && \forall i \in CO \\
& \sum_{i\in I\cup CO} y_i + \sum_{i\in CO} \frac{f_i}{K_i} s_i \le C \\
& \sum_{i\in I\cup CO} y_i \le C \\
& \frac{f_i}{K_i} \ge \frac{f_{i-1}}{K_{i-1}} && \forall i \in CO\backslash\{1\} \\
& y, x, f \in \Re^+
\end{aligned}$$

Primal of the Inner Minimization

Note that we added a term to the first constraint to ensure that the mathematical program is feasible.

$$\min_{x,f,w} \quad \sum_{i\in I\cup CO} d_i \frac{f_i}{K_i} + (|CO| - \sum_{i\in CO} f_i/K_i) \cdot \sum_{i\in I} d_i + \sum_{i\in I\cup CO} w_i M$$

$$\begin{aligned}
s.t. \ (\alpha) \quad & f_i + w_i = K_i - x_i + y_i && \forall i \in I \cup CO \\
(\delta) \quad & f_i \le K_i && \forall i \in I \cup CO \\
(\gamma) \quad & \sum_{i\in I\cup CO} x_i \le B \\
(\beta) \quad & x_i \le y_i + K_i && \forall i \in CO \\
(\sigma) \quad & \sum_{i\in I\cup CO} y_i + \sum_{i\in CO} \frac{f_i}{K_i} s_i \le C \\
(\rho) \quad & \frac{f_i}{K_i} \ge \frac{f_{i-1}}{K_{i-1}} && \forall i \in CO\backslash\{1\} \\
& y, x, f \in \Re^+
\end{aligned}$$

Dual of the Inner Minimization

$$\max_{\alpha,\beta,\gamma,\delta,\sigma,\rho} \quad \sum_{i\in I\cup CO} \alpha_i(K_i + y_i) + \sum_{i\in I\cup CO} \delta_i K_i + \sum_{i\in CO} \beta_i(y_i + K_i) + \gamma \cdot B + \sigma\left(C - \sum_{i\in I\cup CO} y_i\right)$$

$$\begin{aligned}
s.t. \quad & \alpha_i + \delta_i \le d_i/K_i && \forall i \in I \\
& \alpha_i + \delta_i - \frac{\rho_i}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} && i = 1 \,\&\, i \in CO \\
& \alpha_i + \delta_i - \frac{\rho_i}{K_i} + \frac{\rho_{i-1}}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} && i \ne 1, |CO| \,\&\, i \in CO \\
& \alpha_i + \delta_i + \frac{\rho_{i-1}}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} && i = |CO| \,\&\, i \in CO \\
& \alpha_i + \gamma \le 0 && \forall i \in I \\
& \alpha_i + \gamma + \beta_i \le 0 && \forall i \in CO \\
& \alpha \in \Re;\ \delta, \beta, \gamma, \sigma \in \Re^-;\ \rho \in \Re^+
\end{aligned}$$

were successfully attacked by the network interdictor (in that some traffic flow reduction was accomplished) with its budgeted resources and which network

components were successfully defended (no reduction in traffic flows) by the defender given its budgeted resources. This information provides useful insight for network planners/operators and would allow for a more insightful investment in network redundancy or "hardening" to prevent network disruption through sabotage or hacking during a disaster and its aftermath.

Including the Budget for the Defender

$$\max_{i,\gamma,\delta,\sigma,\rho} \quad \sum_{i\in I\cup Co} \alpha_i(K_i + y_i) + \sum_{i\in I\cup Co} \delta_i K_i + \sum_{i\in Co} \beta_i(y_i + K_i) + \gamma \cdot B + \sigma\left(C - \sum_{i\in I\cup Co} y_i\right)$$

$$\text{s.t.}$$

$$\alpha_i + \delta_i \le d_i/K_i \qquad \forall i \in I$$

$$\alpha_i + \delta_i - \frac{\rho_i}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} \qquad i = 1 \,\&\, i \in CO$$

$$\alpha_i + \delta_i - \frac{\rho_i}{K_i} + \frac{\rho_{i-1}}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} \qquad i \ne 1, |CO| \,\&\, i \in CO$$

$$\alpha_i + \delta_i + \frac{\rho_{i-1}}{K_i} + \frac{s_i}{K_i}\sigma \le \frac{d_i}{K_i} + \sum_{i\in I} \frac{d_i}{K_i} \qquad i = |CO| \,\&\, i \in CO$$

$$\alpha_i + \gamma \le 0 \qquad \forall i \in I$$

$$\alpha_i + \gamma + \beta_i \le 0 \qquad \forall i \in CO$$

$$\sum_{i\in I\cup Co} y_i \le C$$

$$\alpha \in \Re; \quad \delta, \beta, \gamma, \sigma \in \Re^-; \quad y, \rho \in \Re^+$$

6. A case study region

In order to better ascertain the usefulness of the interdiction model we developed, we are currently creating a case study of a region in order to apply the interdiction model for its emergency communication networks. The region we have chosen is the Southeast coast of the state of Florida in the United States and in particular, Miami-Dade County within this region. The region has some unique features with respect to its emergency response organizations, its vulnerability to hurricanes and severe weather, and its population density/dispersion. Although our original intent was to cover the four counties from Palm Beach County in the north to Monroe County in the south of this region, we have chosen to focus on one specific emergency management network which operates at the county-wide level. In particular, Miami-Dade County within this region has the busiest 911 (centralized emergency management network/dispatch) in the Southeastern United States. The county also possesses the unique characteristic that most of the county's land area is patrolled/governed by its sheriff department. Only a handful of cities and municipalities in the county have their own police departments. Thus the emergency network we are using in our case study is the primary one for the entire country as opposed to a patchwork of many smaller networks for each city, town and municipality.

The county's emergency network is utilized by the sheriff's department, but also serves both the fire and the emergency/rescue departments within the county's public services framework. Again, in order to create a working test case network interdiction model, we have chosen to narrow the focus to the network infrastructure serving the Miami-Dade Sheriff Department. The topology of this network is fairly simplistic, but it is representative of such networks for other counties, cities, and municipalities. It includes the central node of the 911 dispatch center located in Doral, Florida and 14 other nodes that are logically connected to it. This includes 8 sheriff stations spread across throughout the county and repeaters/antennas which extend the transmission range of the overall network. The network's logical topology can be seen in Figure 1. Figure 2 displays the locations of sheriff's offices and repeaters without the logical links. It can be seen from both figures that certain areas of Miami-Dade County have no sheriff stations and limited network coverage. These include cities and municipalities such as Hialeah, Miami Beach and Miami that have their own police forces and fire and emergency management services. Although there exist overlapping communication channels between these other cities' departments and the county network, we do not consider such channels in our network interdiction modeling analysis.

Figure 1 - Logical Network Topology – Central 911 Dispatch Node at Doral

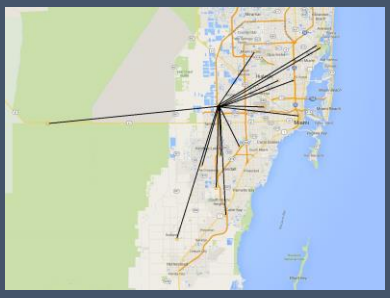
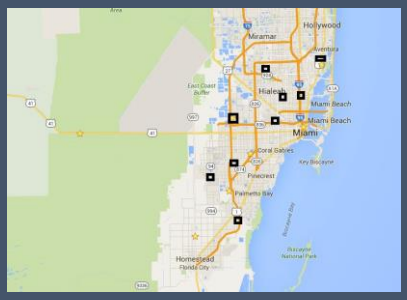


Figure 2 - Repeater Locations (yellow stars) and Sheriff/Central Dispatch Locations (black boxes)



7. Current work

We are currently testing various budget scenarios (both attacker and defender) for our network interdiction test model for the Miami-Dade Sheriff Department. We are utilizing published information on voice traffic on the Miami-Dade network that supports the sheriff department and have been able to segment the traffic into sheriff, fire, and EMS categories. We have estimated costs for network interference/sabotage from various information security websites on the Internet. For instance, an "off the shelf" 300 Megawatt EMP (electromagnetic pulse) device that is capable of jamming signals for a mobile network base station can be purchased for a few thousand dollars. A network interdictor might even resort to an unsophisticated and low cost methodology such as using a firearm or common explosive materials to disable antenna cables or power sources for repeaters or base stations. The notion of hacking a network is similar in nature. A hacker or hacking organization would have to invest in equipment or specific intelligence about the network and its physical and electronic security mechanisms in order to gain access to network components for hacking purposes.

Recent optimization runs utilizing these realistic costs and budgets for the Miami-Dade County sheriff's network point to a diminishing return on investment for the defender (network owner or operator) and a theoretical limit as to how much a defender should spend in order to prevent network sabotage or hacking. The results of one set of optimization experiments where the defender's (Miami-Dade network) budget is incrementally increased, while holding the network interdictor's budget constant at a reasonable total, is shown in Figure 3 below. It can be seen from this graphic that despite the increasing budget for the defender, the ability to reduce further damage to nodes (which equates to a reduction in traffic flows at those nodes) in the network is exhausted at about $24,000. The practical interpretation of these optimization results are that the network owner should invest up to this amount of money to harden or prevent network attacks. Spending greater than this amount, given the assumed budget for the network interdictor, does not bring any additional protection or benefit. Such a model and its resource expenditure guidelines would be useful for network planners and government officials.

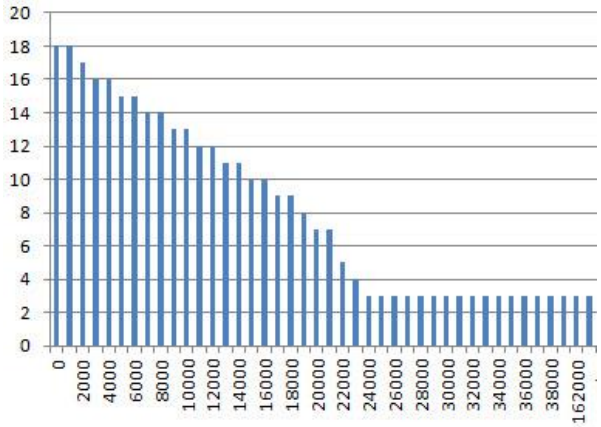


Figure 3 - Nodes affected by the attacker on Y axis versus budget of the defender on X axis (Miami-Dade Sheriff)

We are currently running a series of experiments for the Miami-Dade sheriff department's portion of the county emergency communications network and will expand the scope for the county and region. We plan to utilize the modeling approach for fire and EMS network traffic for the county and eventually expand the geographical scope to include neighboring county networks in Southeast Florida in order to get a more regional planning viewpoint.

8. References

[1] A. Kwasinski, "Lessons from Field Damage Assessments about Communication Networks, Power Supply and Infrastructure Performance during Natural Disasters with a Focus on Hurricane Sandy", FCC Workshop on Network Resiliency 2013, Brooklyn, N.Y., USA.

[2] W. Lu, W. Seah, E. Peh, and Y.Ge, "Communications Support for Disaster Recovery Operations using Hybrid Mobile Ad-Hoc Networks", Proceedings of the 32nd IEEE Conference on Local Computer Networks, 2007, pp. 763 - 770.

[3] M. Tsai, R. Chen, J. Sung, E. Wu, E. Wei, Z. Wu, and J. Liang, " Efficient and Flexible Emergency Communications in Next Generation Mobile Network", Proceedings of the

2011 IEEE Conference on e-Business Engineering, 2011, pp. 96-101.

[4] J.C. Smith, Basic Interdiction Models, John Wiley and Sons, Inc., Hoboken, NJ, USA, 2010.

[5] L.A. McLay, "Discrete Optimization Models for Homeland Security and Disaster Management", Tutorials in Operations Research", October 26, 2015, http://dx.doi.org/10.1287/educ2015.0136