A Network Interdiction Perspective for Providing Emergency Communications: An Analysis for Promoting Resiliency Subject to Resource Constraints and Security Concerns

Michael Bartolacci
Pennsylvania State University - Berks
mrb24@psu.edu

Stanko Dimitrov
University of Waterloo
sdimitrov@uwaterloo.ca

ABSTRACT

Disasters, whether natural or manmade, and other types of emergencies create the need for immediate and secure communications between and among the affected populace, governmental agencies, non-governmental organizations (NGOs) and other types of emergency responders. It is through these communications that the affected populace is able to show resilient behavior, both psychologically and economically. A network interdiction model is proposed that can be utilized to create a more reliable design for such a communications network against the motives of would-be attackers whose aim it is to disrupt emergency communications and inflict damage on the affected populace. The contribution of this work is the application of the network interdiction modeling framework to an emergency communication scenario.

Keywords

Emergency Communications, Network Interdiction Model.

INTRODUCTION

The temporal aspect of all communications among the involved parties in a disaster scenario can play a major role in the reduction of both the physical and the psychological toll such events take on the people in an affected region. One might say that the ability to communicate with loved ones, neighbors, and emergency responders during, and immediately after, such tragedies allows for some mental solace amid the hardships, destruction, and even chaos that such events may bring. It is the responsibility of governmental agencies, existing telecommunications providers (both wired and wireless), and even NGOs (Non-Governmental Organization) in some cases, to provide the communications infrastructure and connectivity that is crucial for dealing with disasters and emergencies. There are a variety of specialized telecommunication technologies that can be utilized during disasters ranging from handheld and vehicular radios typically utilized by emergency personnel in more populated areas to VSAT (Very Small Aperture Terminal) equipment that requires satellite connectivity and is more suited to rural areas or areas where the existing telecommunications infrastructure has been rendered totally inoperative. Often there is a mix of companies and organizations responsible for providing whatever telecommunications can be brought to bear on an affected region. Many times some functioning portions of the existing mobile phone and landline networks remain that can also be utilized for providing critical communications capabilities post-disaster.

The notion of resilience in an affected population is intertwined with these various types of telecommunication systems available immediately before, during, and after a disaster or emergency. One of the definitions of resilience in the literature refers to the process, outcome or capacity of individuals and communities to resist, recover and return to baseline functioning after a misfortune, stress or external shock (Aldunce, et al., 2014). Planning within regions that are disaster-prone, which includes planning for the means of communications during and after a disaster, is stressed as part of the Hyogo Framework (Hyogo, 2005). A theme across the literature is that greater amounts of planning can lead to greater resilience in the wake of a disaster. This term "resilience" has a range of definitions in the literature, but we generally define it for the purposes of this work as the measure of how quickly an affected populace is able to return to both a stable economic, as well as a stable psychological, state. As previously described, the collective psychology of an affected population can be bolstered in a positive fashion with working and available communications technologies. Resiliency is often measured in economic terms with respect to the comparison of asset accumulation levels pre and post disasters. Hoddinott explains that the measurement of resilience involves levels of assets, but that return on assets is an important consideration as well in this process (Hoddinott, 2014).

If one includes a functioning and accessible telecommunications infrastructure as part of this economic measure of resiliency, then the provisioning and design of this infrastructure are key processes for its success. This brings us to the modeling focus of this work, the investment in telecommunications infrastructure and equipment made by various organizations prior to a disaster than can facilitate resiliency when a disaster or emergency does occur. Ideally, such an investment may deliver a return to a organization and the community in terms of lives saved, goodwill from the affected populace, and other tangible and intangible positive results. An organization such as a telecommunications provider may actually receive enough favorable publicity from the telecommunications services it provides during a disaster to ultimately result in greater revenue generation and profits. In providing such infrastructure to an affected region, an organization must ensure that it is reliable and secure. Network interdiction modeling has been successfully utilized in planning network recovery from various disasters as well as fortifying critical network components.

A NETWORK INTERDICTION MODEL

Network interdiction models tend to follow the process outlined by Smith (2010). In this process, the *interdictor* performs some interdiction actions on the network, such as removing nodes or links, subject to a budget constraint. The scenario of interest in this work involves a would-be attacker that takes advantage of the conditions following a natural disaster to inflict damage upon communication networks needed by emergency responders and the affected populace. Due to the fact that any nefarious organization attempting such an attack does not possess unlimited resources to carry out the attack, there exist restricting conditions on the attack. The *operator*, then responds by taking recourse actions on the network. This two stage process is similar to a Stackelberg game (Mas-Colell et al., 1995) 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.

From a game-theoretic point of view, if a network operator is interested in deploying a minimum cost telecommunications network in 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 the 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 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 bring down 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 communication networks can be pieced together from varying technologies post-disaster. As such, knowing that at most k nodes may be removed, the operator may choose a telecommunication network composition that is resilient to k node failures. For example, sole reliance on an ad-

hoc network post-disaster may not be a wise design choice because the removal of any one node in the network may result in complete network failure if one or more nodes in the network use the removed node as an intermediate node which may disconnect segments of the network. However, not utilizing ad-hoc networks may increase network deployment costs. As such, balancing the telecommunications-technology portfolio in order to respond in a resilient fashion to a post-disaster attack on the infrastructure being used is of interest to network planners and post-disaster implementers. A network-interdiction model will enable the provisioning of a network that is resilient to such attacks at the lowest cost.

We conclude this section by formulating a generic interdiction model 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 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.

CURRENT WORK ON MODEL DEVELOPMENT

In order to better ascertain the usefulness of an interdiction model, we are currently developing a case study of a region in order to develop an 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. This region has some unique features with respect to its emergency response organizations, its vulnerability to hurricanes and severe weather, and its population density/dispersion. The area we intend to focus on covers four counties from Palm Beach County in the north to Monroe County in the south. The majority of the population of these counties is concentrated along the coastline. The cities, towns, and other municipalities of these four counties form a chain of population centers that stretch from northeast to southwest as Florida's coastline curves towards, and into, the Gulf of Mexico. Included in this area of study is Monroe County, a mostly rural county that includes the island chain known as the Florida Keys and a large portion of the Everglades. A diversity of municipalities exists in this chain of counties, but the approximate center of it geographically is the Miami metropolitan area. Population density drops off very significantly as one travels southwest from the city of Miami (which resides in Miami-Dade County) into Monroe County. Moving northeast from Miami sees a much more gradual drop-off in population density as one eventually enters Palm Beach County after having moved through Broward County. Current work is focusing on collecting demographic data on major population centers in each county in order to develop an approximation of the demand for emergency communications for links and nodes on the multi-tiered network infrastructure in the region. The eventual development of the network interdiction model for the region will require both the network designer and the network attacker to know which nodes and links in the overall network are the most "valuable" in terms of the amount of utilization or traffic flow that would be found during an emergency such as a hurricane.

Each of the four counties has its own emergency management organization in addition to the emergency management organizations within specific cities, towns and municipalities in each county. Therefore, a three tier system exists for emergency communications: local, county-wide, and inter-county. One might picture the emergency network topology of a given city or town to be a full mesh design (where all nodes can communicate with each other directly) with a centralized super node (emergency management control center for the city or town) that is part of the county-wide network. A county-wide network can also be viewed as a full mesh topology with each city or town's emergency management control center being a node on the network. Again, a centralized super node exists on the county-wide network which would be part of the inter-county network topology. The telecommunication technologies involved in the connections of these intra-county nodes might be different from the ones used within a given city or town. Finally, each of the county emergency management centers would be connected to the inter-county network. This network can also be considered to have a full mesh logical network design such that each county emergency management center can directly contact each of the other ones in the region being studied. Much like the intra-county network, the telecommunication technologies utilized can also be different from the lower level networks. This multi-tier network architecture will represent a unique application of the network interdiction model which traditionally focuses on a single layer topology.

EXPECTED BENEFITS OF THE MODEL USAGE

The importance of telecommunications during and after an emergency or disaster can be magnified when considering its potential impact on the ability of an affected populace to withstand, and recover from, the hardships endured. Planning for a reliable telecommunications infrastructure than can be utilized in the face of potential attacks by hackers and/or terrorists is an important process that can benefit from a network interdiction modeling approach. Even the implementation process for a given telecommunications architecture that is created post-disaster can reap the benefits of taking security considerations and network vulnerability into account.

REFERENCES

1. Aldunce, P., Beilin, R., Handmer, J., and Howden, M. (2014) Framing disaster resilience: The implications of the diverse conceptualisations of "bouncing back". *Disaster Prevention and Management*, *23*(3), 252-270.
2. Hoddinott, J. (2014) Understanding Resilience For Food and Nutrition Security", *Proceedings of the Conference on Building Resilience for Food and Nutrition Security*.
3. Hyogo Framework for Action 2005 - 2015: Building the Resilience of Nations and Communities to Disasters. (2005), *World Conference on Disaster Reduction*.
4. Mas-Colell, A., Whinston, M. D., Green, J. R., Jun. (1995) Microeconomic Theory. Oxford University Press, USA.
5. Smith, J. C. (2010) Basic Interdiction Models. John Wiley & Sons, Inc., Hoboken, NJ, USA.