# Chapter 48
# Promoting Resiliency in Emergency Communication Networks:
## A Network Interdiction Stylized Initial Case Study Model of a Miami-Dade County Network

**Michael R. Bartolacci**
*Pennsylvania State University – Berks, USA*

**Stanko Dimitrov**
*University of Waterloo, 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. In this article, Michael R. Bartolacci and Stanko Dimitrov 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. They develop a case study for wireless networks utilized by the sheriff's department of Miami-Dade County in Florida in the United States. Finally, the authors' 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.*

## 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

DOI: 10.4018/978-1-5225-6195-8.ch048

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