3-2003

An Analysis of Multiple Layered Networks

Kevin T. Kennedy

AN ANALYSIS OF MULTIPLE LAYERED NETWORKS

THESIS

Kevin T. Kennedy, Captain, USAF

AFIT/GOR/ENS/03-14

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GOR/ENS/03-14

AN ANALYSIS OF MULTIPLE LAYERED NETWORKS

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Kevin T. Kennedy, BS

Captain, USAF

March 2003

AFIT/GOR/ENS/03-14

AN ANALYSIS OF MULTIPLE LAYERED NETWORKS

Kevin T. Kennedy, BS
Captain, USAF

Approved:

Richard F. Deckro, DBA (Co-Advisor)	date
Victor D. Wiley, PhD (Co-Advisor)	date
James W. Chrissis, PhD (Reader)	date

Acknowledgements

I would like to give my sincere appreciation to my faculty advisors Dr. Deckro and Maj. Wiley, and to my reader Dr. Chrissis. I would also like to thank my sponsor for their support and latitude provided for this research effort. In addition, I want to express sincere love and admiration to my wife and children. They have provided the foundation to allow me to make it though the difficulties along the way.

Kevin T. Kennedy

Table of Contents

Page

List of Figures

Page

List of Tables

Page

Abstract

Current infrastructure network models of single functionality do not typically account for the interdependent nature of infrastructure networks. Infrastructure networks are generally modeled individually, as an isolated network or with minimal recognition of interactions. This research develops a methodology to model the individual infrastructure network types while explicitly modeling their interconnected effects. The result is a formulation built with two sets of variables (the original set to model infrastructure characteristics and an additional set representing cuts of interdependent elements). This formulation is decomposed by variable type using Benders' Partitioning and solved to optimality using a Benders' Partitioning algorithm.

I. Introduction

1.1 *Background*

The President's Commission on Critical Infrastructure Protection (PCCIP) defines infrastructures as

> [A] network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services (President's Commission on Critical Infrastructure Protection, 1997: 3).

In addition to the national infrastructures necessary for the public good, the Department of Defense also utilizes multiple interrelated infrastructures. While many of these networks are synonymous with those already listed in PCCIP, others are uniquely military. A comparison of perspectives developed by Tom Bozek (2002:3), Office of the Secretary Defense, is provided in Figure 1.

U.S. Federal Perspective		**U.S. DoD Perspective**
• Telecommunications	⟷	• Global Information Grid
• Energy	⟷	• Public Works
• Water systems	⟷	• Public Works
• Transportation	⟷	• Transportation
• Banking and Finance	⟷	• Financial Services
• Emergency Services	⟷	• Emergency Services
• Government Operations	⟷	• Command, Control & Communications
		• Intelligence, Surveillance, & Reconnaissance
		• Personnel
		• Space
		• Logistics
		• Health

Figure 1. United States Infrastructures

Just as the United States depends on infrastructure networks for survival, potential adversaries of the United States also depend on their infrastructure networks. Because of these dependencies, infrastructure networks have been studied extensively to identify and locate vulnerabilities, bottlenecks, and other problem areas. Once identified, measures can be taken to mitigate vulnerabilities in our own infrastructures, while building doctrine, methodologies, and techniques to exploit vulnerabilities in our foe's networks. In an increasingly interconnected and complex world, these vulnerabilities may span several infrastructures, possibly located in multiple countries.

Because of the size and complexity of individual infrastructures, these networks are typically modeled individually. History shows, however, that interdependent and cascading effects can potentially have unexpected results completely outside any predicted (and sometimes desired) consequence. In a study conducted by Hauer (1999) for the Department of Energy, eleven major cascading power failures were analyzed - most were traced back to a single trigger. For example, the 1965 blackout throughout the northeast was caused by a single relay switch in Ontario (Hauer, 1999: 5). Ideally, such effects would be captured in any model of these interrelated networks, and captured without having a significant impact on usability or running time of the model.

1.2 *Problem Statement*

Current infrastructure network models of single functionality do not typically account for the interdependent nature of infrastructure networks. Infrastructure networks are generally modeled individually, as an isolated network or with minimal recognition of interactions. In part, this is because one large model of all infrastructure networks, even

if it existed, would be too complex to effectively manipulate and analyze in most operational time frames. No model currently exists in the open literature to include effects from individual infrastructure network types while accounting for interdependent effects across network types. This research develops a methodology to model the individual infrastructure network types while explicitly modeling their interconnected effects.

1.3 *Problem Approach*

Inadequate modeling of interdependent networks results in unforeseen events which can cost lives and weaponry in military applications. To model the individual networks along with their interdependencies, an additional set of variables is added to the infrastructure network models. These binary variables represent whether or not a set of interdependent network elements are removed from the network. The result is a formulation built with two sets of variables (the original set to model infrastructure characteristics and an additional set representing cuts of interdependent elements). This formulation is decomposed by variable type using Benders' Partitioning and solved to optimality using a Benders' Partitioning algorithm.

The approach is based on large scale optimization methods. The overall problem of modeling infrastructure networks and their interdependencies is decomposed into the individual network types, while overlapping effects are isolated in a separate problem. This approach leverages information and techniques that have been developed for modeling individual infrastructure networks, while accounting for coupling effects.

1.4 *Assumptions*

The overriding assumption of the proposed model is that either a cost or benefit is defined for each element (*i.e.* nodes and arcs in a graph) in the model. These numbers are dependent on the use, mission, and desired output of the model. Developing effective multicriteria measures of performance for infrastructure networks is a major research effort in and of itself. While such an effort is outside the scope of this thesis, the modeling approach utilized here can be adapted to *any* additive resource that conforms to the assumptions of linear programming. This area has been extensively researched at the Air Force Institute of Technology (see Pinkstaff (2001), Leinhart (1998), Renfro (2001), among others).

1.5 *Summary*

Current infrastructure network models do not typically account for the interdependent nature of such networks. Infrastructure networks are generally modeled individually in isolation. The size and complexity of these models prohibit modeling all infrastructures as a single network.

This approach is demonstrated on a set of four notional networks. The networks presented are small so the methodology can be easily followed, but as stated previously, the intended applications of this approach are very large networks for which other approaches are neither practical nor desirable. Chapter two provides a review of the literature to form the foundation for the work done in this area. Chapter three discusses the proposed methodology and procedure which is then demonstrated in Chapter four.

The last chapter presents a set of improvements and extensions that can be made to this methodology.

II. Literature Review

This chapter defines terms and concepts relevant to this research effort. Key concepts and ideas from the literature are presented. Finally, background information on the systems under analysis is presented.

2.1 *Infrastructures*

> Our national defense, economic prosperity, and quality of life has long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence (PCCIP, 1997, ix).

To select targets of a physical infrastructure, first a general understanding of how each infrastructure functions is required. Therefore, a brief description of infrastructure layers is provided.

2.1.1 Information and Communications

The "information and communications infrastructure [consists] of the Public Telecommunications Network (PTN), the Internet, and the many millions of computers in home, commercial, academic, and government use" (PCCIP, 1997: 4).

2.1.1.1 Telephone

To provide an understanding of telephone networks, the following is a summary of detailed explanations taken from http://www.howstuffworks.com. Telephones use copper wires to transmit signals to/from the telephone itself directly to a local telephone switch or to a digitizer. Digitizers convert incoming analog signals to digital signals so

they can be combined and sent to the local switch with a much smaller subset of wires (copper, fiber optic or coaxial cable). Local switches connect local calls to the destination and connect long distance calls to the appropriate long distance switch.

To determine the appropriate long distance switch for a given signal, computers at the local switch find the incoming signal's phone number in a database and determine the selected long distance provider. Long distance switches route calls though a series of long distance switches connected by fiber-optic lines, satellite, microwave towers, and undersea cables, and finally to the local switch in the area of the destination of the call which then completes the call to the selected number.

Cellular communications work in much the same way. The main difference is that signals are sent though the air to the closest tower which connects to a Mobile Telephone Switching Office (MTSO). The MTSO acts as a local coordinator between the cellular towers and connects to a local switch as necessary.

Both traditional phone systems and cellular phones are vulnerable to attack. "When exploiting a telecommunications system, the campaign planner must choose one of three attack methods—physical, jamming, or spoofing" (Hurst, 1993: 23). The first method is physical attack where "system redundancy, centralization of key nodes, and hardness and location of those nodes will determine the resources required to obtain the desired system degradation from physical attack" (Hurst, 1993: 24). Depending on the desired effect, physical destruction presents a broad range of options. On one end, a Special Forces unit can use wire clippers to cut the phone line into a building. On the other end of the spectrum, physical destruction can be bombing local/long distance switches covering the area desired.

Although not physically destroying links or nodes, jamming also "focuses resources on particular links, messages, or time periods in order to have increased effectiveness in disrupting the network as a whole" (Hurst, 1993: 30). Wireless communications such as satellite communications, microwave transmissions, and even cell phone calls are exceptionally vulnerable to jamming.

Spoofing injects false information directly into a network. Spoofing changes the information that the infrastructure relies on. Both traditional and cell phones can be spoofed, as they rely on databases to carry out their functions. For example, if the cell phone database for particular cell(s) were accessible, the attacker could locate what cell phones are inside particular cells, and then corrupt the database making the cell phone(s) unusable (Hurst, 1993: 30).

In addition, areas outside the telecommunications system could be targeted to affect communications service. For example, every element of the telecommunications infrastructure requires electricity to function. Some components, such as local switches, have battery or generator backups; however, they can only function for a limited time and are themselves dependent on other infrastructures functioning correctly.

2.1.1.2 Internet

In simple terms, the Internet is a network of computer networks. There are several high-level networks connecting to each other through Network Access Points (NAPs). Computers connect to an internet service provider (ISP) and become part of the networks. Routers join networks together at these NAPs, passing information from one network to the other, as necessary. Routers also protect the networks from one another,

preventing the traffic on one from unnecessarily spilling over to the other (http://www.howstuffworks.com/internet-infrastructure.htm).

Every machine on the Internet has a unique identifying number, called an internet protocol address, or IP Address. Every time a domain name is used, the Internet's domain name system (DNS) server translates the human-readable domain name into the machine-readable IP address. Routers need this information to pass requests and information. There are multiple DNS servers at every level to serve as backups as systems fail.

Much like telecommunications, the Internet is subject to physical attack, jamming, and spoofing. Certainly, routers and backbones can be physically attacked. Denial of Service attacks effectively "jam" targeted IP addresses. Finally, since Internet routers do not verify accuracy of information passed to them, they can be spoofed to direct traffic in a desired direction. "Most vulnerable are the interconnection points between major ISPs, where there are no grounds at all for rejecting route advertisements" (Schneider, 1998: 20).

The dependency of the Internet on other infrastructures is clear. Every component requires electricity, and at times, the internet and telecommunications are inseparable. Both dial-up and DSL internet connections use telephone components for their connection. In addition, telephones can use internet components during the completion of a call.

2.1.2 Energy

"The electrical power infrastructure consists of generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of our economy"(PCCIP, 1997: 4). The following is a summary based on http://www.howstuffworks.com. This site explores how the electrical infrastructure works from a non-technical point of view.

Electricity is produced by power plants using spinning electrical generators. In hydroelectric dams, a water wheel spins the generator. However, most power plants use steam produced by burning coal, oil, natural gas, or nuclear reactors to turn the generator.

Electricity leaves the generator and enters a transmission substation at the power plant. There, transformers convert the generator's voltage into much higher voltages for transmission on the transmission grid. Transmission lines are long distance transmission lines which are interconnected permitting the interchange of electricity between utilities.

These transmission lines also connect to power substations which step-down the voltage to "distribution" voltages. These distribution lines carry electricity to drum transformers immediately before entering homes and businesses. Power substations typically include safeguards which allow for the disconnection of the substation from the transmission grid, or separate distribution lines if necessary to help prevent cascading electrical failures.

Control centers offer an additional measure to monitor and control power distribution. Control centers collect data from remote terminal units (RTUs) which, in turn, collect data from field instruments and equipment. Control centers monitor and control these units and the power grid itself though Supervisory Control and Data

Acquisition (SCADA) systems. SCADA systems collect electric system data from the field, initiate alarms, and issue control commands to the field as directed by the applications in the control center system (The President's National Security Telecommunications Advisory Committee (PNSTAC), 1997: 6).

Although much emphasis has been placed on the vulnerabilities of the electric infrastructure to non-kinetic means of attack, "physical destruction is still the greatest threat facing the electric power infrastructure," (PNSTAC, 1997: 6).

> Attacking the generation portion of an electrical system is attractive for several reasons. First, it eliminates the power at the source, spreading the impact of electrical outages to a large number of users. Second, the generators and turbines are vulnerable to damage by bombing and are not easily replaced (Griffith, 1994: 6).

These generating plants are large, easy to find, and expensive and time consuming to fix. Of particular concern are nuclear power plants. An attack on a nuclear facility could potentially disperse radioactive material throughout the local atmosphere and ground water supply.

Step-up transformers are also vulnerable to physical attack. These transformers are generally in open areas, easily identifiable, and not well guarded. The advantage to attacking transformers is that they are each unique, specifically designed for the varying voltages and physical arrangements. Consequently, the transformers are often custom made, and there is not usually a large number of spares available (Griffith, 1994: 7).

In addition, although not traditionally vulnerable, the power lines themselves can be targets. According to Aviation Week & Space Technology, the US Air Force has used CBU-94 bombs that eject spools of specially-treated carbon-graphite wire which unravel into a web shape as they near the ground. The scattered reels drape over power lines

shorting them out, causing flash fires, and large explosions. This results in power surges which open power plant circuit breakers, and shut off the distribution of electricity. Alternatively, the shells can be filled with small fibers which float down and engulf a target, disabling everything electronic. "The fibers, measured in thousandths of an inch, are even pulled through cooling fans into the interior of electronic equipment where they cause arcing and shorting." In addition, because of their small size, they are virtually impossible to completely clean out (Fulghum, 1999: 34-35).

Electromagnetic pulse (EMP) weapons can also be used to physically attack the electric infrastructure. EMPs cause a large spike in voltage which destroys all electrical components, including those in a generator and/or transformer. Even areas not affected by the initial pulse could collapse from the "late-time EMP effect." The late-time EMP effect occurs about 15 minutes after detonation: EMP surges through electrical systems create localized magnetic fields. When these magnetic fields collapse, electricity surges through the power and telecommunication infrastructure. Therefore, heavily guarded sites, such as telephone switching centers and electronic funds-transfer exchanges, could be attacked through their electric and telecommunication connections (Wilson, 2001: 1).

Substations are also vulnerable to electronic attack. Both digital breakers and RTUs can be dialed into from any telephone connection.

> By dialing into a port on a digital breaker, a utility engineer can reset the device or select any of six levels of protection. An electronic intruder who could identify the telephone line serving such a device could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected by the breaker can withstand. By doing this, it would be possible to physically destroy a given piece of equipment within a substation. The intruder could also set the device to be more sensitive than conditions for normal operations and cause the system to shut down for self-protection (PNSTAC, 1997: 6).

The communication systems the electric utilities rely on are also vulnerable to electronic attack.

> "Utilities rely on a mix of private microwave radio, private fiber, and public networks for communications among control systems elements. Any one of these mediums could be exploited in an electronic attack. In most cases, an attack on the communications infrastructure alone would constitute a nuisance attack," (PNSTAC, 1997: 6).

Clearly, there are a number of ways to attack the electrical infrastructure of a nation.

2.1.3 Vital Human Services

2.1.3.1 Water Supply

"The water supply infrastructure assures a steady flow of water for agriculture, industry (including various manufacturing processes, power generation and cooling), business, firefighting, and our homes," (PCCIP, 1997: 4). In many cases, water supplies not used for drinking (*i.e.* agriculture and industry) come from outside the public water supply system; being drawn by the users directly from surface or ground sources," (Ryan, 1998: 14-15).

Drinking water itself comes from a variety of sources: rivers, lakes, reservoirs, or pumped from aquifers. Depending on the community and source of the water supply, the water is subject to some or all of the following to remove contaminants: filtration, flocculation and sedimentation, and disinfection. Filtration involves a series of filters used to remove suspended particles such as clay, silts, organic matter, and precipitants from other treatment processes. Flocculation and sedimentation combine the smaller particles which settle out as sediment. Finally, the water is disinfected before it is

distributed. Disinfection is typically done by treating the water with chlorine, chloramines, or chlorine dioxides (EPA, 2002: 1).

Once the water is treated, it is sent to a community via a distribution network of buried pipes. Most communities make use of water towers which store water at higher elevations than the community it serves. From there, gravity maintains a constant pressure on the water network as the main pumping force. Smaller pipes, called house service lines, are attached to the distribution water lines to bring water from the distribution network into homes and businesses (EPA, 2002: 2).

Once the water is used, it is collected and sent to a wastewater treatment facility. Usually these plants are located in low-lying areas to allow gravity to bring the water to the facility. Pipes from each building flow to a sewer main. The sewer main consists of a series of pipes which get progressively larger until the treatment plant is reached. In areas where gravity alone cannot force the flow toward the treatment plant, grinder-pumps or lift stations are used to move the sewage along (http://www.howstuffworks.com).

Once the water reaches the wastewater treatment plant, it usually goes through three stages of treatment. The first stage, known as "primary treatment," allows solids to settle out of the water and the scum to rise. All the solid material is collected and disposed. The second stage, known as "secondary treatment," removes organic materials and nutrients. Water flows to large, aerated tanks where bacteria consume additional waste. The wastewater then flows to settling tanks where the bacteria settle out. The third stage, known as "tertiary treatment," uses chemicals to remove phosphorous and nitrogen from the water, and may also include filter beds and other types of treatment.

Lastly, chlorine is added to the water to kill any remaining bacteria before it is discharged into a river, ocean, or other body of water. (http://www.howstuffworks.com)

Supply interruptions can be caused by numerous acts, including physical destruction. For instance, "one city has six giant pumps, and they're all in one building. If you crashed an airplane into that building or blew it up, it would cause half a million people to lose their water supply almost instantly. Pumps of this size must be custom-built and can take as long as 18 months to replace," (Isenberg, 2001: 1).

Water towers also make large, vulnerable targets. They tend to serve smaller areas which may be important if the desired goal is to isolate a small subset of a population or strike at a particular military, governmental, or industrial complex. Simple loss of pressure can aggravate an ongoing emergency such as a fire or decontamination operations.

Supply interruptions can also occur as an indirect result of contamination. Although not a tactic (weapon) used by western governments, it is typical of terrorist organizations/states. For that reason, it is included here for completeness. In his recent report, Deininger listed five potential sites for contamination (Deininger, 2000: 16). Each of these sites has an associated probability of success (*i.e.* not diluted or killed by chlorine). In addition, each potential contaminate has its own associated "benefits" and risks. All of these factors must be weighed along with the associated desired effect to determine how an attacker plans to disrupt water supply.

The first potential site for contamination is upstream from the intake of a water supply system. A second option is to insert contaminants near the intake of the treatment plant. Third, a contaminant can be placed in service reservoirs. Service reservoirs are

usually accessible by manholes and ventilation ducts. A fourth possibility is to insert the contaminant at some point in the distribution system. For example, a water truck can hook up to a fire hydrant, overcome the pressure, and inject the contents of the tank; thereby easily contaminating an entire street or subdivision. The last point of insertion considered by Deininger was at individual house connections (Deininger, 2000: 16-20). Water flow can be reversed using simple devices such as vacuum cleaners or bicycle pumps. The resulting backflow would push the contaminant into the local water distribution system (Isenberg, 2002, 1-2). If these were done in several places nearly simultaneously, it could create the appearance of a large scale attack (Deininger, 2000: 18).

In addition to physical attacks, supply can also be interrupted as a result of interruption of SCADA systems. These systems monitor and control water pressure, flow, and dam operations. Again, depending on the desired effect, SCADA systems could potentially be used to achieve the desired goals. For an extensive discussion explaining SCADAs in water systems, see Ezell (1998) and Ezell *et al* (2001). In addition to the SCADA dependence on the telecommunications infrastructure, water systems also need energy to power pumps and treatment facilities.

2.1.3.2 Government Services

The purpose and scope of government is a hotly debated item. However, according to our values, a key mission of governments is to provide the necessary functions outlined in the Preamble to the Constitution such as establishing justice, ensuring domestic tranquility, providing for the common defense, promoting the general welfare, and securing the blessings of liberty (Ryan, 1998: 15). To disrupt these

functions, the leadership can be targeted, directly, through physical attack, or indirectly. Indirect targeting can include isolating leadership communications such that the leaders are unable to send messages/orders. In addition, government records (such as the Social Security or Medicare systems) could be attacked potentially affecting millions, spoofing the public and causing panic.

2.1.3.3 Emergency Services

"This infrastructure includes firefighting, police, rescue, and emergency medical services. Its objectives are to contain and deal with emergencies in order to save lives and preserve property," (Ryan, 1998: 15). These areas are rarely targeted directly; however, they typically become crippled due to attacks on other infrastructures on which they depend. For example, downed transportation bridges, jammed telecommunications, or power outages critical to operations make emergency services' functions difficult to maintain. Secondary explosions timed to attack first responders are a direct attack. The disruption of governmental or emergency services can spread panic. These services depend on communication and logistics and a continual disruption can cause widespread problems.

2.1.4 Physical Distribution

> Transportation makes it possible for materials to be moved to processing centers, for finished products to be moved to market, for commodities essential to transportation and to production and marketing to be distributed as necessary, and for the population to move to and from work and other commercial activities. Transportation also supports the activities of the Department of Defense and other governmental functions (PCCIP, 1997: 2).

This infrastructure supports both passenger and freight transportation. Physical distribution includes highways, pipelines, railroads, ports and waterways, civil aviation, mass transit, and "vehicles" that use these facilities.

In addition to the roads themselves, highways include tunnels, bridges, and trucked hazardous materials. Pipelines include control systems, pumping stations, above-ground pipes, river crossings, control centers, and storage facilities. Railroads include train control systems, rails, switches, bridges, trestles, rail hazardous material, intercity passenger, and control centers. Ports and waterways include locks, dams, cargo vessels, passenger vessels, and terminals. Civil aviation includes planes, airports, and air traffic control components. Finally, mass transit includes tunnels, stations, trains and buses, train control system, and control centers.

Disruption to critical links in the transportation system provides an opportunity to cause serious economic harm. Therefore, transportation facilities may be targets of terrorists intending to harm the economy (Polzin, 2002: 2). "Terrorists may be motivated to cause personal injury to concentrations of people. Transportation facilities often provide anonymous gathering places for large numbers of individuals (Polzin, 2002: 2).

To study attacks on the transportation infrastructure, the US Department of Transportation conducted a vulnerability assessment. Included in this study were potential targets grouped by types of weapons used. The target and weapon used will depend on the desired effect. The table is reproduced as a summary of potential target/weapon combinations.

TABLE 1: SCENARIOS CONSIDERED IN THE U.S. DOT VULNERABILITY ASSESSMENT

Physical Attacks	
• Car bomb at bridge approach • Series of small explosives on highway bridge • Single small explosive on highway bridge • Single small explosive in highway tunnel • Car bomb in highway tunnel • Series of car bombs on adjacent bridges or tunnels • Bomb(s) detonated at pipeline compressor stations • Bomb detonated at pipeline storage facility • Bomb detonated on pipeline segment • Simultaneous attacks on ports • Terrorist bombing of waterfront pavilion • Container vessel fire at marine terminal • Ramming of railroad bridge by maritime vessel	• Attack on passenger vessel in port • Shooting in rail station • Vehicle bomb adjacent to rail station • Bombing of airport transit station • Bombing of underwater transit tunnel • Bus bombing • Deliberate blocking of highway-rail grade crossing • Terrorist bombing of rail tunnel • Bomb detonated on train in rail station • Vandalism of track structure and signal system • Terrorist bombing of rail bridge • Explosives attack on multiple rail bridges • Explosive in cargo of passenger aircraft
Biological Attacks	
• Biological release in multiple subway stations • Anthrax release from freight ship	• Anthrax release in transit station • Anthrax release on passenger train
Chemical Attacks	
• Sarin release in multiple subway stations	• Physical attack on railcar carrying toxics
Cyber and C3 Attacks	
• Cyber attack on highway traffic control system • Cyber attack on pipeline control system • Attack on port power/telecommunications	• Sabotage of train control system • Tampering with rail signals • Cyber attack on train control center

Source: National Research Council, *Improving Surface Transportation Security, A Research and Development Strategy*, Washington D.C: National Academy Press, 1999.

Figure 2. Transportation Attacks

Many types of attacks on the transportation sector would not cause a significant disruption on a national scale, serious economic harm, or public danger. However, the wide variety of possible attacks could be symbolic and frighten people from traveling, especially using mass transit. Although not a direct national threat, the combination of vulnerability and symbolism of local attacks make the transportation sector a likely target.

2.1.5 Banking and Finance

"The banking and finance infrastructure was defined by the Commission as composed of five principal sectors: banks, financial service companies, payment systems, investment companies, and securities and commodities exchanges," (Ryan, 1998: 14).

Often attacked for financial gain, the financial sector has the most advanced defenses of all industry sectors. However, they are not invulnerable. High visibility targets in this sector could be physically attacked for symbolic/psychological reasons. Financial markets are sensitive to these events. For example, an attack in Manhattan could potentially cause a crash in the stock market, causing cascading effects into other sectors. The terrorist attacks on the US on September 11, 2001, closed Wall Street for days, bringing most trading to a stop on those exchanges. Once the markets did open, they immediately plummeted. Psychological operations could also be used against a target population to create instability in the targeted area. Consider the national dependence on ATMs. An attack that crippled these systems would not only inconvenience millions, it would affect economic vitality and consumer confidence.

Other vulnerabilities include the economic dependence on electronic transfers. Western economies are not set up to smoothly function on a cash basis. Disruption of electronic transfer would disrupt the entire economy. Another potentially crippling effect would be a large scale identity theft. The economy is built on trust that identity can be verified by some means. These examples are only the tip of the iceberg for the havoc that could result from an attack on the financial sector.

2.2 Infrastructure Interdependencies

As mentioned previously, each infrastructure is dependent on some or all of the others in order to function properly. A thorough study into these interdependencies was conducted by Rinaldi, Peerenboom, and Kelly (2001).

There are four types of interdependencies: physical, cyber, geographic, and logical. An infrastructure is physically dependant on another infrastructure if it requires material produced by another. For example, most power plants rely on the transportation sector for delivery of its fuel. Without transportation into the power plant, no electricity can be produced. Cyber dependency occurs when the state of an infrastructure is dependent on information sent though the information infrastructure. Both energy and water (vital human services) infrastructures depend heavily on the use of SCADA systems. Infrastructures are geographically interdependent if their immediate environment is the same. For example, if energy and telecommunications lines are attached to a bridge, both would be affected if the bridge is destroyed. Lastly, logical dependencies are those relationships between infrastructures not included in the other categories (Rinaldi, 2001: 14-16).

When targeting an infrastructure component, the decision must be made as to the level of damage necessary to obtain the desired end effect. This is referred to as the "state of operation." "Conceptually, the state of operation of an infrastructure can range from optimal design operation to complete failure" (Rinaldi, 2001: 21). Typically, the desired effect of targeting an infrastructure is to disrupt, degrade, or destroy the targeted components.

If complete failure is the desired effect, this can be accomplished via a variety of means. Multiple infrastructure failures can interact via cascades, escalations, or common causes. Cascading failures are failures in one infrastructure that cause failures in a second infrastructure. Escalating disruptions are the result of a disruption in one infrastructure which intensifies an independent disruption of a second infrastructure. A common cause disruption is one in which two or more infrastructures are disrupted at the same time because of a common cause (Rinaldi, 2001: 22). While cascading or escalation effects are desirable in some settings, they have the potential to cause undesired collateral damage in other settings.

To predict the effects of targeting an infrastructural component, one must be able to determine the impact across all infrastructures. This will depend on the degree of coupling, type of coupling, and adaptability to change of multiple infrastructures. Tightly coupled systems have little slack in their connecting links, whereas loosely coupled systems can often accommodate failures by adapting. "Numerous factors contribute to adaptability, including the availability and number of substitutes for critical processes or products, workarounds and contingency plans, backup systems, training and educational programs for operational personnel, and even human ingenuity in the face of disasters," (Rinaldi, 2001: 20). The type of coupling refers to either a linear coupling or more complex coupling. Linear coupling can be visualized as an assembly-line effect, where each effect has a preceding cause. Complex couplings are more subtle and often involve effects not easily explained or understood.

2.3 Targeting

Air Force doctrine describes two broad approaches to target analysis: target system analysis and critical node analysis. Target system analysis looks at individual targets to determine their vulnerabilities and how these vulnerabilities can be exploited. It compares the effects of attacking the system through various means to determine which method will most likely achieve the desired effect on the targeted system. This requires a thorough knowledge of how the targeted system works - its capabilities, limitations, and interactions. Combined with knowledge of various weapon effects, targeteers decide the best method to neutralize the target based on the needs of the mission (AF Pamphlet 14-210, 1998: 41).

Critical node analysis considers interdependent relationships among multiple target systems. This analysis considers potential cascading effects as well as effects across multiple systems of an adversary. In other words, critical node analysis looks at a network of target systems (along with potentially non-targeted systems). "The objective is to determine the most effective way to influence or affect enemy systems" (AF Pamphlet 14-210, 1998: 42).

AF Pamphlet 14-210 also covers specific characteristics of targets which should be taken into account when selecting targets. These elements are summarized in Table 1.

Table 1. Target Selection (AF Pamphlet 14-210, 1998: 48-51)

Importance and Significance
Depth
Reserves
Cushion
--Process and equipment substitutes
--Product or service substitutes
--Availability of substitute supplies and services
Capacity
Product or Service Economic Value
Vulnerability
Reconstitution or Recuperability
--Type of Installation
--Availability of Repair Materials
--Similarity and Interchangeability of parts
--Importance and significance to the enemy
Geographic Location -Target Location
Concentration or Dispersal
--Mobility
Countermeasures

The relative importance of each characteristic depends on the nature of the mission and objectives. Selecting targets based on these characteristics is a function of experience, values, and to the extent possible, quantifiable objectives. Of course, some of these characteristics are more quantifiable than others.

For example, suppose planners wish to evaluate the desirability of bombing a power plant. Obviously electricity is vital to modern society and military applications. Power plants are clearly vulnerability to physical attack because of their size and inability to relocate. Most have only minimal stockpiles of fuel to guard against supply interruptions, and there are few alternatives to users when electricity is interrupted.

However, the transmission grid protects against small-scale attacks by redirecting power from unaffected plants. Due to the uniqueness of each power plant, repair times for individual plants cause long term shortages from which the grid may have difficulty recovering.

In addition to target characteristics, the effects of candidate weapons against targeted systems must also be considered. The following effects are taken from the research paper co-authored by 23 students at the Air Command and Staff College at Maxwell AFB, AL., "Information Warfare: An Opportunity For Modern Warfare."

Table 2. Weapon Effects

Corruption	Changing the content of information.
Deception	Changing information to portray a situation different from reality.
Delay	Slowing the flow, acquisition, and dissemination of knowledge.
Denial	Prevention of the flow, acquisition, and dissemination of knowledge.
Disruption	The reduction of the capacity to provide and/or process information.
Degradation	The permanent reduction in the capacity to provide and/or process information.
Destruction	The destruction of information before it can be transmitted.

To illustrate, suppose a telephone switch is the potential target to be evaluated. Obviously, physical destruction of the building is still an option. However, if an information attack is considered, the characteristics in the table "Weapon Effects" describe the attack. For example, the database of long distance carriers can be corrupted, causing telephone calls rerouted to incorrect destinations. The switch could be flooded with false traffic, preventing or reducing the flow of calls through the switch.

Lastly, attributes of using a particular weapon against a particular target must also be considered. Table 3 is a list of potential attributes:

Table 3. Weapon Attributes (AF Pamphlet 14-210, 1998: 88-89)

Persistency	Length of time weapon will affect the target.
Speed	Length of time necessary to achieve desired weapon effect.
Latency	Ability to lie dormant until needed.
Reversibility	Ability of weapon effects to be reversed.
Fratricide	Adverse affects on friendly weapon systems.
Collateral Damage	Undesired affects possible though use of weapon against target.
Stealth	Ability to stay hidden from enemy.
Mutual Interference	Interference of using weapons on other weapons/goals.

Target characteristics, effects, and attributes are combined to select potential targets and evaluate weapons to be applied to these candidate targets. Referring to the previous telephone switch example, these characteristics allow the comparison of options such as physical destruction or information attack. Physical attacks are fast, long lasting, and irreversible. Other factors such as collateral damage and fratricide are highly dependent on local environments and factors. An information attack relies on stealth, can remain dormant until activated, and generally have low chances of collateral damage. However, these weapons are generally untested which may (or may not) lead to unforeseen effects.

2.4 Effects Based Operations

Until recently, operations were planned and executed in multiple stages with little or no overlap between the specialized areas. Target classes were chosen by decision makers, specific targets were selected by targeteers, weaponeers optimized weapons against the targets, and mission planners planned the execution of bombs on target. However, a process is taking hold which is referred to as "effects based operations (EBO)."

In their October 2001 White Paper, the J9 Concepts Department defined EBO as, "a process for obtaining a desired strategic outcome or 'effect' on the enemy through the synergistic and cumulative application of the full range of military and non-military capabilities at all levels of conflict." The stove-piped specializations are replaced by a continuous five stage process as shown in Figure 3.

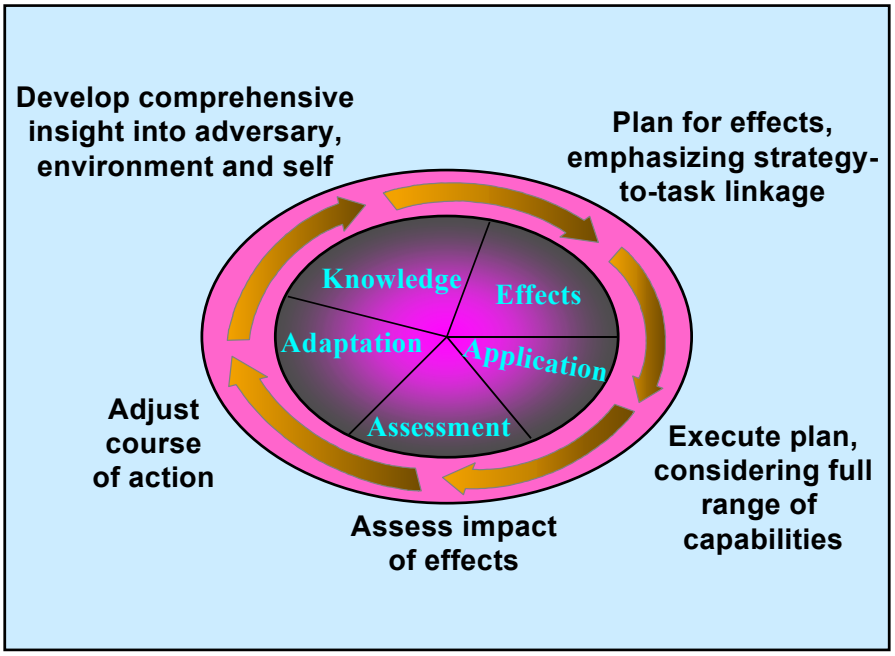

Figure 3: Effects Based Operations (Uchida, 2002: 2)

The first step is to gain an understanding of capabilities, objectives, the adversary (or potential adversary), and the environment. With this knowledge, an informed decision about desired effects and means to achieve them are planned. When ordered, the plan is executed, and information is collected and analyzed to determine the success or failure of the mission. This information is then rolled into adjustments needed for the adaptation and assessment of future planning and missions (Uchida, 2002: 2). EBO is

becoming a key element in targeting. To properly exploit EBOs use, interrelated effects must be considered.

To demonstrate this philosophy, the example of the telephone switch developed in Section 2.3 can be expanded. Previously, specific telephone switches would be selected as targets based on specified criteria, weaponeers would then decide the best way to attack the target. Effects based operations first approaches the problem by asking what the desired outcome of an attack is. If the goal is to disrupt telephone service to a local community for an extended period of time, then the method to achieve this goal will be significantly different than if the goal is to block one building from receiving calls for a short amount of time. The best solution to the first problem is probably putting bombs on target. The second problem offers different options, such as those available by information attack.

2.5 Network Flow

Network flow modeling, a subset of linear programming, have special structures which allow larger problems to be solved in less time than more general linear programming would allow. Exploiting this network structure allows problems to be analyzed that often could not otherwise be solved in a reasonable amount of time via other mathematical programming methods. Since many real world systems can be modeled as networks, a great deal of work has gone into developing analytical techniques in dealing with networks.

Most network analysis is based on flow through the system. Examples of analytical techniques include finding the maximum flow of a commodity through a

network and minimizing the cost of the flow through a network subject to demands. Other techniques, investigate the structure of the network itself. For example, algorithms can identify the shortest path through a network or a minimum spanning tree of a network.

Infrastructure analysis uses many of these ideas and algorithms. In the completion of a telephone call, the switch calculates a shortest path from the caller to the called. If that path is blocked or busy, the next shortest path is calculated. This process is carried out until a path is completed. Water and electric power flow can be viewed as a form of minimum cost flow. This thesis research is based on disrupting these networks. Specifically, a network analysis technique called s-t cut sets is used. Ideally, the disruption of these networks would be done at minimum cost. For more information on network theory, algorithms, and applications, see Ahuja, Magnanti, and Orlin (1993).

2.6 Isolation Sets

In the network isolation algorithm, the goal is to partition a network into *r* sets of distinguished nodes at minimum cost. These *r* sets of nodes are those to be isolated from one another (Bellmore, 1970: 461-469).

The algorithm described here takes advantage of node partitioning properties to find the set *J*. Therefore, the formulation is modified slightly. Here, a cost is assigned to inter-network arcs with nodes in separate partitions. To develop this formulation, distinguished nodes are first assigned to their separate partitions as follows:

$$\pi_{i,j}(x_i) = \begin{cases} 1 \text{ if } x_i \in \text{ partition } j \text{ of network } i \\ 0 \text{ otherwise} \end{cases}$$

All nodes must be assigned to a partition, so the sum across all partitions of a network for each node must be equal to 1.

$$\sum_{j=1}^{r} \pi_{i,j}(x_i) = 1 \text{ for } i=1 \text{ to } k$$

If costs are to be assigned to arcs which span multiple networks, there must be a way to determine when this occurs. This is done via the following equation:

$$\pi_{i,j}(x) - \pi_{i,j}(y) + \gamma_{i,j}(x,y) - \delta_{i,j}(x,y) = 0$$

where $\pi_{i,j}(x)$ $\gamma_{i,j}(x,y)$ $\delta_{i,j}(x,y)$ are 0-1 variables

the $\gamma_{i,j}(x,y)$ and $\delta_{i,j}(x,y)$ are variables used to ensure the balance. For more information, see Bellmore (1970)

The *j*th subproblem is

Minimize $\quad W = -\sum_{x \in N} \sigma(x)\pi_j(x) + \sum_{(x,y)\in E} c(x,y)[\gamma_j(x,y) + \delta_j(x,y)],$

Subject to

$$f(x,y): \quad \pi_{i,j}(x) - \pi_{i,j}(y) + \gamma_{i,j}(x,y) - \delta_{i,j}(x,y) = 0, \qquad (x,y) \in E,$$

$$p(x): \quad -\pi_j(x) \begin{cases} = -1, & x \in R_j, \\ = 0, & x \in R_i,\ i \neq j, \\ \geq -1, & x \in N - \bigcup_{i=1}^{r} R_i, \end{cases}$$

$$\pi_j(x),\ \gamma_j(x,y),\ \delta_j(x,y) \geq 0$$

where $\sigma(x)$ is the simplex multiplier corresponding to each constraint in the master problem for the free nodes (*i.e.*, $x \notin R_i$, i=1, 2, . . ., *r*), and $\sigma(x)$ =0 for the fixed nodes (*i.e.*, $x \in \bigcup_{i=1}^{r} R_i$). (Bellmore, 1970: 461-469) (Bennington, 1969)

2.7 Decomposition Methods

One method for dealing with "large" problems is to decompose them into smaller more manageable parts. These subproblems are managed by a "master problem" which combines the subproblem solutions to find an optimal solution to the overall problem. Ideally, the large problem decomposes into subproblems which have structure which can be exploited to quickly generate solutions.

Dantzig and Wolfe in their 1961 paper developed a technique which exploits block angular structures of continuous linear programs (Dantzig, 1961). Baumol and Fabian demonstrated how the steps of the Dantzig-Wolfe algorithm can be interpreted as an economic model for managing a distributed decision making system (Baumol, 1964). In addition, Sweeney and Murphy developed a similar method to solve large scale integer problems (Sweeney, 1979).

Benders in his 1962 paper Partitioning Procedures for Solving Mixed-Variables Programming Problems presented a procedure for solving mixed-variable programs. Benders takes a problem of the form

$$\max\{c^T x + f(y) \mid Ax + F(y) \le b, x \in R_p, y \in S\}$$

and partitions it into two mutually exclusive subsets which are solved separately. One set consists only of the continuous variables (i.e. the x's) with all the other variables fixed at some value. Either this problem is solved directly, or the dual is solved, and the dual variable values are passed to the "master" problem. This master problem then solves for the new *y*'s which are again fixed for the other partition(s). This technique has also been extended to solve nonlinear problems (Geoffrion, 1972: 237).

Chapter 2 has reviewed the background relevant to approaching the multilayered network analysis. This background serves as the basis for the methodology outlined in Chapter 3 and illustrated in Chapter 4.

III. *Methodology*

This chapter develops the methodology used in this research. It provides a step in modeling and analyzing effects between infrastructure networks. The information in this chapter should allow the reader to duplicate and modify this research to model multilayered networks with interdependent elements.

3.1 Modeling Approach

The intended use of the methodology presented here is on multiple infrastructure networks which have overlapping or common components. Although developed for infrastructure networks, this approach is general enough to be appropriate for any set of multiple network models with common elements.

The approach developed here is robust enough to work with a variety of different objectives. Chapter Two introduced several types of analysis appropriate for network models. Any of these types of network analysis could be utilized with the methodology presented here for layered networks. For example, network algorithms such as those for finding maximum flow, minimum cost flow, minimum cost disconnecting sets, isolation set, or any other applications across a *single* network can be used in conjunction with the partition approach outlined provided commonalities can be defined. The method in this thesis extends these and other applications across layered networks.

Additional elements required for implementation depend on the purpose(s) of analyzing the networks. If flow across the networks is a consideration, then at a minimum, upper and lower capacities of each arc of the networks must be specified. In

addition, if cost and/or benefits are considered in the objective, then these must also be specified.

While the goal of the methodology presented here is to extend network algorithms across multiple interdependent layers, the approach leverages the valuable information gained from implementing algorithms across a single layer. To build on the foundation of these algorithms, the majority of conventions and notations developed here mimic the single layered case as much as possible.

3.2 Model Description

Each network is modeled as a directed graph G=[N, A] where N is the set of nodes and A is the set of arcs creating the network topology.

$$\text{G=[N, A] where A} \subseteq \{(i, j) : i, j \in \text{N}\}$$

The requirement that the networks be directed is nonrestrictive, as any undirected arc can be replaced with two directed arcs with opposite orientations. It is noted, however, that such an approach does increase the problem size. Without loss of generality, each network contains a source node, which supplies flow, and a sink node, which requests flow.

In general, a cost or benefit is associated with each arc. For applications which do not consider cost or benefit, this requirement can be ignored. Depending on the mission, a benefit (target values, for example) may be substituted for cost. Although only arcs have a cost or benefit by assumption, this is not a restrictive assumption. Variations that allow for both nodes and edges to be considered could be implemented in a straightforward way: every node represented is replaced with two nodes, say u and v, in

which there is an arc (u, v) and an arc (v, u); removal of either of these arcs is equivalent to removing the corresponding node. However, this increases the size of the network as the number of nodes is doubled and the same number of arcs is added to the model. Of course, codes which deal with nodes directly can also be utilized.

The variable x_{ij} is defined as the flow across an arc from node i to node j. There is some upper limit on the capacity of individual arcs, denoted u_{ij},

$$x_{ij} \leq \mu_{ij} \; for \; each \; (i, j) \in A \, .$$

Lower capacities are assumed to be zero. Again, this is not a restrictive assumption, as any nonnegative lower bound can be substituted out:

$$x_{ij} \geq 0 \; for \; each \; (i, j) \in A \, .$$

In addition, flow into each node must equal the flow out of each node, except for the source and sink nodes:

$$\sum_{j:(i,j)\in A} x_{ij} - \sum_{j:(j,i)\in A} x_{ji} = 0 \text{ for all } i \in N - \{s \; and \; t\}$$

The objective function for each network will depend on the mission. This notation and formulation works well for single layered networks. In fact, if the node labeling is unique across all networks, then the above notation will also work for multiple networks. Alternatively, a subscript could be added to each variable to indicate what network to which it belongs, x_{ijk}.

However, nothing in the single layered network formulation specially accounts for commonalities from other networks. These "commonalities" may be a shared corridor or effect. For example, a bridge might support road/rail traffic as well as power and telecommunications. This common corridor would be modeled as an arc in ***each***

individual network. A kinetic attack that destroys the bridge would sever the arc in each of the respective networks. On the other hand, an EMP attack may only affect the power and telecommunication networks, thus effecting some, but not all of the elements in the common corridor. Finally, a specific attack by the SOF team on only the road and rail lines without significant collateral damage would only affect those networks. Alternatively, an attack on one link of a network may have desired effects in another network. The effect would impact multiple networks, and hence should be modeled affecting the appropriate networks.

Let I be a node or arc(s) with common interdependencies across *k* networks. I has common elements in all layers of the K networks of interest, or in some subset of the layers. Let W_1 be the set of all effects options, *w*, which can be applied to the elements in I. The option *w* may affect all the elements in I or it may affect a subset of I. Consider the example above, I=1 is the bridge carrying road, rail, power and telecommunication lines. There different options were outlined, so $W_1=\{1, 2, 3\}$.

For the set W_1:

w=1 Effects-based option 1 affects all networks
w=2 Effects-based option 2 affects only power and telecommunications
w=3 Effects-based option 3 affects only road and rail

where *w*=1 was the kinetic attack, *w*=2 is the EMP weapon and *w*=3 was a SOF team attack on the road and rail.

Associated with each option against a particular interdependent element is the actual effect. For a given I and $w \in W_I$, let δ_{i_k} be the change (effect) on node *i* of network *k* given the selection of $w \in W_I$. In addition, define δ_{ijk} to be the change (effect)

on arc (*i,j*) of network *k* given the selection of $w \in W_I$. If there is no actual effect, δ_{i_k} or δ_{ijk} would be zero for the particular combination. On the other hand, affecting a node could also affect a number of arcs. In general, for some $w \in W_I$

$$\underline{\delta}_{w \in W_I} = \begin{bmatrix} \delta_{i_1} \\ \vdots \\ \delta_{i_k} \\ \cdots \\ \delta_{ij_1} \\ \vdots \\ \delta_{ij_k} \end{bmatrix} \quad \begin{bmatrix} \text{Nodes} \\ \cdots \\ \text{Arcs} \end{bmatrix}$$

Finally, for a given $w \in W_I$, assume y_w=1 if option *w* is selected and zero otherwise. It is assumed that one would not wish to double strike a target (at least in planning) so, at most, one of the common attack options *w* is selected. Therefore, the regularity constraints

$$\sum_{w \in W_I} y_w \leq 1 \quad \text{for all } I \in C$$

where *C* is the set of all commonalities I, would generally apply.

Consider the following development, based on the minimum cost flow problem to illustrate the modeling. Given an A matrix of network flow, with right-hand sides b, flow over arcs, x, is limited by the capacity, μ. For a single network

$$\begin{aligned} &\text{Min } \partial^{\mathrm{T}}\mathbf{x} \\ &\text{s.t. } A\mathbf{x}=\mathbf{b} \\ &\quad \mathbf{x} \leq \boldsymbol{\mu} \end{aligned}$$

which may be rewritten as

$$\text{Min } \partial^{\mathrm{T}}\mathbf{x}$$

$$\text{s.t. } \begin{bmatrix} \mathrm{A} \\ \cdots \\ \mathrm{I} \end{bmatrix}\mathbf{x} \begin{matrix} = \\ \\ \leq \end{matrix} \begin{bmatrix} \mathbf{b} \\ \cdots \\ \boldsymbol{\mu} \end{bmatrix}$$

If there are K multiple layered networks, each individual network $k \in K$ may be written with the subscript identifying the network.

$$\text{Min } \partial_k{}^{\mathrm{T}}\mathbf{x}_k \qquad \text{k Networks Model}$$

$$\text{s.t. } \begin{bmatrix} \mathrm{A}_{\mathrm{k}} \\ \cdots \\ \mathrm{I}_{\mathrm{k}} \end{bmatrix}\mathbf{x}_k \begin{matrix} = \\ \\ \leq \end{matrix} \begin{bmatrix} \mathbf{b}_k \\ \cdots \\ \boldsymbol{\mu}_k \end{bmatrix}$$

To incorporate the interdependent effects and their costs, the vector of costs associated with the interdependent costs $w \in W_I$, e_w, of some option for all I is defined as

$$\mathbb{C} = [e_1, e_2, \cdots, e_m]$$

and with the costs associated with the individual networks defined by

$$\boldsymbol{\mathcal{C}}^T = [\partial_1{}^T, \partial_2{}^T, \cdots, \partial_K{}^T]$$

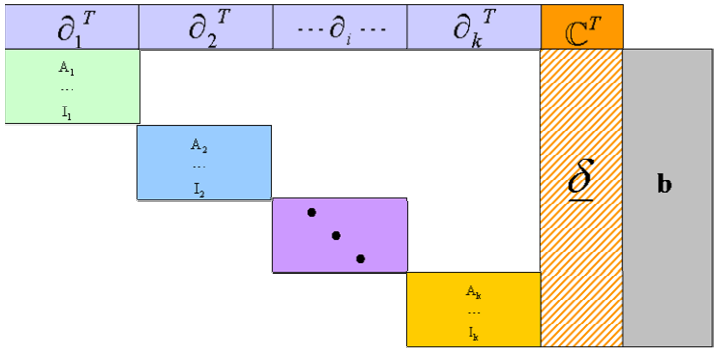

Figure 4. Commonalities Model

Now, the formulation across multiple layers is

$$\min \ \mathbf{c}^{\mathbf{T}}\mathbf{x} + \mathbf{C}^{\mathbf{T}}\mathbf{y} \qquad \text{Commonalities Model}$$

$$\begin{bmatrix} A_1 & & & & \\ \cdots & & & & \\ I_1 & & & & \\ & A_2 & & & \\ & \cdots & & & \\ & I_2 & & & \\ & & \ddots & & \\ & & & A_K & \\ & & & \cdots & \\ & & & I_K & \end{bmatrix} \mathbf{x} + \boldsymbol{\delta}\mathbf{y} \begin{matrix} = \\ \leq \end{matrix} \begin{bmatrix} \underline{\mathbf{b}} \\ \underline{\boldsymbol{\mu}} \end{bmatrix}$$

If Benders' partitioning is applied to this problem, the ***x*** variables break into independent subproblem networks given a fixed vector, $\bar{\mathbf{y}}$. The *y* variables problem can be expressed as a minimization of the original objective function coefficients, $\mathbf{C}^{\mathbf{T}}$, and the maximum of the extreme points associated with the feasible regions of the duals, ν^l, of each of the subproblem networks at iteration *l*.

$$\begin{aligned} \min \quad & C^T y + \max_{\nu^l} \left\{ \nu^l (b - \partial y) \right\} \\ s.t. \quad & \\ & \nu^l \geq 0, \quad l = 1, \ldots, L \\ & \mathbf{y} \geq 0 \end{aligned}$$

where $(\nu^l) = [(\nu_1^{\,l}), (\nu_2^{\,l}), \cdots, (\nu_k^{\,l})]$ which gives the master problem

$$\min \ z \qquad \text{SP}$$

$$\text{s.t.} \quad z \geq \mathbb{C}^T y + \nu^l (b - \boldsymbol{\delta} y) = \nu^l b + (\mathbb{C} - \nu^l \boldsymbol{\delta}) y \ \text{ for } l = 1, 2, \ldots, r$$

$$1 \ \leq \ \mathrm{r} \ \leq \ \mathrm{L}$$

Normally, Benders' decomposition would then be applied to the independent networks and the Benders' subproblem, SP (See Taha (1975) for a detailed description of Benders' approach). Depending on the network model used, this could be carried out in a

straight forward fashion. However, the structure present in the commonality model can be exploited. At each iteration l of the Benders' algorithm, a Benders' cut of the form

$$z \geq \nu^l \mathbf{b} + (\mathbb{C} - \nu^l \boldsymbol{\delta})\mathbf{y}$$

is added. It has also been assumed the regularity conditions

$$\sum_{w \in W_I} y_w \leq 1 \quad \text{for all } I \in C$$

which could be added to SP. Instead of taking the traditional Benders' cut model for the minimum cost flow commonality problem, we formulate the multiple dimensional knapsack problem SP* with the current Benders' cut as the objective and the optimal selection constraints (which are special ordered sets) defined over a feasible region. This creates SP*, given as

$$\begin{aligned} \min \quad & \nu^l \mathbf{b} + (\mathbb{C}^T - \nu^l \delta)\mathbf{y} && \text{SP*} \\ \text{s.t.} \quad & \sum_{I \in C} \sum_{w \in I} y_w \leq 1 \\ & y_w \in [0,1] \end{aligned}$$

Note for any iteration l, ν^l yields the term $\nu^l b$ which is a constant, and therefore does not affect the optimization with respect to $\boldsymbol{y}$ (but is necessary for the test of optimality). In addition, since this is a minimization problem, any objective function coefficients $(\mathbb{C} - \mathbf{v}^l \boldsymbol{\delta})$ that are positive will not contribute to the solution. Therefore, the associated y_w can be fixed at zero and what remains is a relatively smaller multi-dimensional knapsack problem (Martello and Toth, 1990). The process continues by iterating between Benders' problems—the independent layers with fixed y and SP* until the Benders' optimality condition is met.

IV. Methodology Demonstration and Analysis Results

4.1 Introduction

In this chapter, the methodology developed in Chapter 3 is applied to a set of notional, layered networks with interdependent arcs. The following steps are followed in this implementation:

Step 1: The objective of the analysis is decided. (In this case, minimum cost cut sets)
Step 2: Notional networks are presented
Step 3: Interdependencies are identified
Step 4: Master and subproblem(s) are generated
Step 5: The iterative procedure outlined in Chapter 3 is applied
Step 6: Solution and analysis is presented

4.2 Objective

Current models in the open literature generally treat infrastructure networks in isolation. However, as infrastructures become more linked and inseparable, the need has arisen to incorporate common effects across multiple infrastructures. In this thesis, given layered networks with interdependent arcs, the objective is to minimize the cost of the combined *s*-*t* cuts across all networks with individual and shared elements in the overall cut set as driven by model objective. An *s*-*t* cut set is defined as a partition of the node set into two parts, with a node defined as *s* in one part, and a node defined as *t* in the other. Each cut defines a set of arcs with one node in one partition, and the other node in the other partition. A cost is associated with each of these arcs, and the goal to find the minimum cost set of arcs which determines this partition (Orlin, 27-28).

For example, suppose the desired effect is to prevent military transportation and electricity flow to a specified island. Further assume that only one bridge connects to the island, and all power lines are tied beneath the bridge. One obvious solution is to bomb the bridge severing both the bridge itself and the power lines. However, if the costs are too high (*i.e.* civilian casualties resulting from an inability to exit the island or decision to use the bridge in the future), then another form of attack would be more appropriate. Perhaps a less costly attack would be to hit the bridge with an EMP bomb, severing power, and physically bombing the military transportation hub on the island. Currently, these two objectives are considered in isolation, but this method incorporates both.

Consider π_{i_k}, the dual variable associated with the conservation of flow equation for node *i* of network *k*. Let ν_{ijk} be the dual variable associated with the capacity constraint of arc(i,j) of network *k*. A minimum cut formulation for each of the *k* networks would be

$$\begin{aligned} &\min \sum_{(i,j)\in A_k} c_{ijk}\nu_{ijk} \\ s.t. \quad &\pi_{i_k} - \pi_{j_k} + \nu_{ijk} \geq 0 \text{ for all (i,j)} \in \mathrm{A_k} \\ &\pi_{t_k} - \pi_{s_k} \geq 0 \text{ for all s,t} \in \mathrm{N_k} \end{aligned}$$

where c_{ijk} is the flow capacity along arc(i,j) of network *k*. Therefore, the objective function, $\sum c_{ijk}\nu_{ijk}$, is the relative cost of cutting the flow of goods in network *k*.

To incorporate the interdependencies described in Chapter 3, let

$$y_w = \begin{cases} 1, \text{ if } w \in W_I \text{ chosen to cut commonality I} \\ 0, \text{ otherwise} \end{cases}$$

The "cost," $\mathbb{C}_w$, then represent the relative cost of cutting the independent arcs associated with commonality I using option *w*. The Commonality Model then becomes

$$\min \sum_{k \in K} \sum_{(i,j) \in A_k} c_{ijk} v_{ijk} + \sum_{I \in C} \sum_{w \in W_I} \mathbb{C}_w y_w$$

$$s.t. \quad \pi_{i_k} - \pi_{j_k} + v_{ijk} + \delta_{ijkw} y_w \geq 0 \text{ for all (i,j)} \in \mathrm{A_k} \text{ and } k \in K$$

$$\pi_{t_k} - \pi_{s_k} \geq 1 \text{ for all s,t} \in \mathrm{N_k} \text{and } k \in K$$

$$\sum_{I \in C} \sum_{w \in W_I} y_w \leq 1$$

where

$$\delta_{ijkw} = \begin{cases} 1 \text{ if arc}(i,j) \text{ of network } k \text{ is part of commonality I affected by option } w \in W_I \\ 0 \text{ otherwise} \end{cases}$$

Note, however, this formulation does not need to be solved directly. Since valuable information is gained from the dual variables of the Benders' subproblem, when the y variables have been fixed, the dual of Benders subproblem is solved instead. This dual is a maximum flow formulation given as

$$\max \quad \sum_{k} \sum_{(i,j) \in A_k} x_{t_k s_k} + \sum_{i \in C} \sum_{w \in W_I} \mathbb{C}_w^{\mathrm{T}} y_w \qquad \text{Subproblem (dual)}$$

$$\text{s.t.} \quad \sum_{j:(i,j) \in A_k} x_{ijk} - \sum_{j:(j,i) \in A_k} x_{jik} = 0 \text{ for all } k \in K$$

$$x_{ijk} \leq c_{ijk} - c_{ijk} * \delta_{ijkw} \bar{y}_w, \text{ for all (i,j)} \in \mathrm{A_k},\ k \in K,\ w \in W_I,\ I \in C$$

$$x_{ijk} \geq 0 \ \textit{for each} \ (i,j) \in A, k \in K$$

4.3 Notional Networks

Figures 5-8 are graphical representations of four notional networks. They may be power, communication, fuel and road ways, for example. Nodes are numbered arbitrarily, but uniquely to avoid confusion. Each network has an identified source (*s*)

and sink (t). In addition, each arc has an associated cost of removal as illustrated in the following pictorial representations:

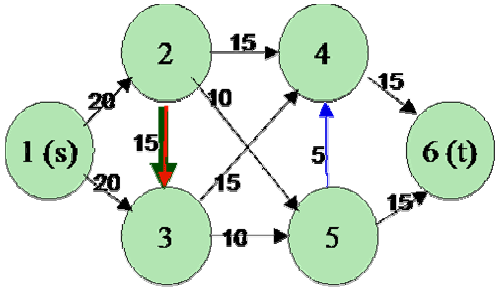

Figure 5. Network 1

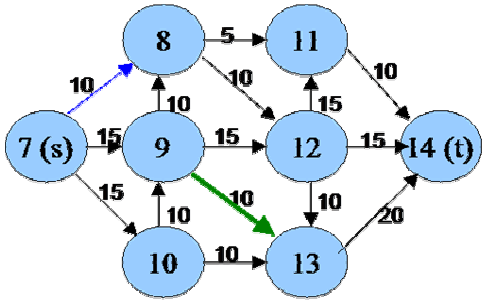

Figure 6. Network 2

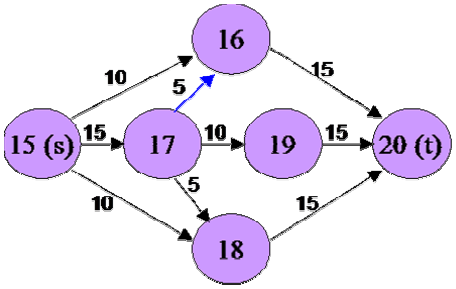

Figure 7. Network 3

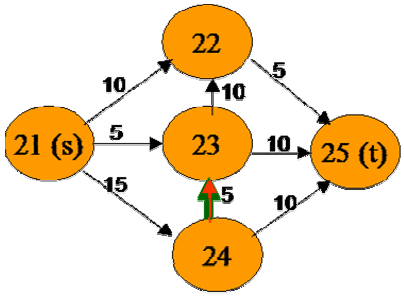

Figure 8. Network 4

4.4 Interdependencies

In this notional example, there are three sets of interdependent arcs. The first set, y_1, consists of the arcs $x_{2,3,1}$, $x_{9,13,2}$, and $x_{24,23,4}$. If cut as a set, the combined cost is 18. The second set, y_2, set is $x_{2,3,1}$ and $x_{24,23,4}$. The combined cost if cut in whole is 3. Finally, the third, y_3, consists of the arcs $x_{5,4,1}$, $x_{7,8,2}$, $x_{17,16,3}$. This cut set has a combined cost cut of 5. Note that y_1 and y_2 represent two options against the same set of targets; y_1 represent removing all three elements, while y_3 represents only removing two of the three. For example, the three elements could be a highway, a power line, and a telephone

line, across a bridge. A physical attack would sever all three links (y_1), whereas another form of attack (as represented by y_2), such as an EMP bomb, would only remove two of the three elements.

Table 4. Summary of Interdependencies.

Element	Associated Arcs	Cost of Removal
I=1	{(2,3),(9,13), (24,23)}	
w=1	{(2,3),(9,13), (24,23)}	18
w=2	{(2,3), (24,23)}	3
I=2	{(5,4),(7,8),(17,16)}	
w=1	{(5,4),(7,8),(17,16)}	5

Note that $W_1=(w_1,w_2)$ and $W_2=(w_1)$.

4.5 Benders Reformulation

Solving this problem via Benders requires the original minimum cost cut formulation (Base Model) to be reformulated into a "master" problem along with subproblems. The master problem will only be a function of the binary variables which represent the interdependent arcs.

$$\min \quad z \qquad \text{Master Problem}$$

$$s.t. \quad z \geq \sum_{i\in C}\sum_{w\in W_I} \mathbb{C}_w^{\mathrm{T}} - ((\sum_{k\in K}\sum_{(i,j)\in A_k} x_{ijk}^{\,l}\delta_{ijkw})y_w)+\sum_{k\in K}\sum_{(i,j)\in A_k} c_{ijk}x_{ijk}^{\,l}$$

$$\sum_{I\in C}\sum_{w\in W_I} y_w \leq 1$$

$$1 \leq r \leq L$$

To solve the master problem, the only information needed from the subproblems is the dual vector associated with each constraint. This presents two options for solving the subproblems. First, the minimum cut can be determined for each network directly, then the dual values can be calculated and passed to the master problem. The second option is to take the dual of the minimum cost cut network, solve the dual problem, and

pass the values directly back to the master problem. The advantage of the second approach is that the dual of the minimum cost cut problem is the maximum flow problem. Although either method is equally correct, maximum flow codes are generally faster and more flexible. Orlin discusses seven of the most common algorithms for solving maximum flow, along with their speed and flexibility (Orlin, 1993: 240). For these reasons, the subproblems in this example have been solved as maximum flow problems, and flow over each arc is passed to the master problem. Each subproblem will have the general form

$$\max \quad \sum_{(i,j)\in A_k} c_{ijk}x_{ijk} + \sum_{w} C^T{}_w \bar{y}_w \qquad \text{Subproblem k}$$

$$\text{s.t.} \quad \sum_{j:(i,j)\in A} x_{ijk} - \sum_{j:(j,i)\in A_k} x_{jik} = 0$$

$$x_{ijk} \le c_{ijk} - c_{ijk} * \delta_{ijkw} \bar{y}_w$$

$$x_{ij} \ge 0 \ \ for\ each\ (i,j) \in A$$

$$y_w \in \{0,1\}$$

Specifically, there are four subproblems (one for each network).

For each network, an artificial arc is added which connects the sink and the source. The links connecting this node to the source and sink are assigned an arbitrary high value so they will not be a limiting factor in the algorithm. This formulation makes it easier to express the maximum flow though the network, by maximizing the flow though one of the artificial arcs.

4.6 Algorithm

As the first pass, assume that none of the interdependent sets are selected. A closer look at the networks might reveal a better starting solution, but any starting point may be used so long as it is feasible. If none of the interdependent arcs are cut as a

group, then the subproblems are maximum flow problems with unchanged capacities (*i.e.*, the original network viewed independently). The flow across an arc (of the dual problem) is the value needed to be passed to the master problem. These problems are small enough that they were programmed and solved using Microsoft Excel 2002 with its built in solver. For larger problems, a more robust network code would be more efficient. If the notional problems are solved independently then the following solutions are obtained:

Table 5: Subproblem Solution

Network	Cutset	Common
1	(4,6), (5,6)	
2	(7,8),(7,9),(7,10)	
3	(15,16)(15,17)(15,18)	
4	(21,23)(22,25)(24,23)(24,25)	

These values are passed to the master problem defined earlier.

The master problem also needs the values associated with each of the interdependent arcs given in Table 4. With these values, the following linear program results:

$$\begin{aligned} & \min \ z \\ s.t. \quad & z \geq 13y_1 - 2y_2 - 90y_3 \\ & y_1 + y_2 \leq 1 \\ & y_3 \leq 1 \\ & y_j \in (0,1) \end{aligned}$$

This problem, solved for the *y*'s yields the following optimal solution:

Table 6: Master Problem Solution

y_1	y_2	y_3
0	1	1

Since y_2 and y_3 are equal to 1, then the interdependent arcs represented by these variables are "cut." These arcs are removed indirectly by setting their upper bound capacity to 0,

effectively removing any possible flow across those arcs. The subproblems are again solved with the flow capacities altered by the interdependent arcs represent by y_2 and y_3. With y_2 and y_3 equal to 1, the arcs corresponding to these have an upper bound capacity of 0. In other words, with no capacity they have been effectively cut. To illustrate, the arcs dependent on y_1 and y_2 have been deleted from the pictorial representation.

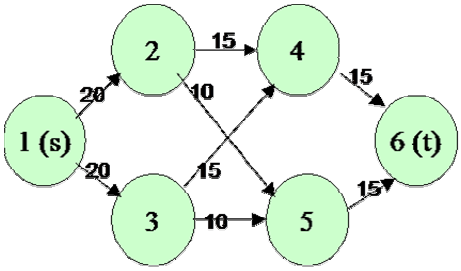

Figure 9. Network 1 Modified

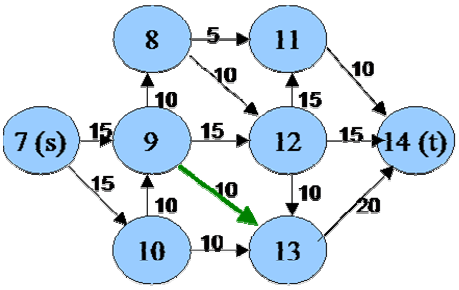

Figure 10. Network 2 Modified

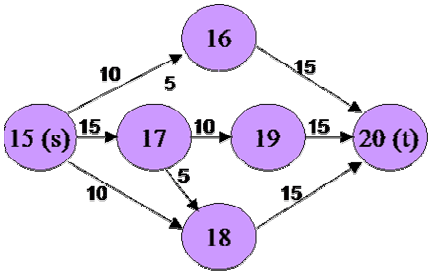

Figure 11. Network 3 Modified

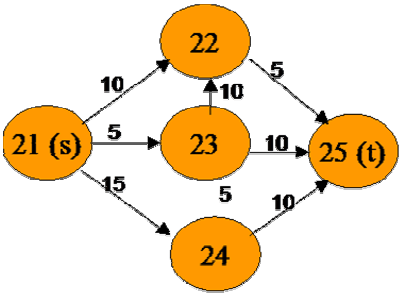

Figure 12. Network 4 Modified

With the new upper bound capacities on arc flow, the maximum flow subproblems are again solved. The new solutions are as follows:

Table 7: Problem Solution

Network	Cutset	Common
1	(4,6), (5,6)	
2	**(7,8)**,(7,9),(7,10)	y_3
3	(15,16)(15,18),**(17,16)**,(17,19),(17,18)	y_3
4	(21,23)(22,25)**(24,23)**(24,25)	y_2

To calculate the lower bound on the optimal solution, the following equation from Benders' approach is used:

$$z_l = \sum_{i \in C} \sum_{w \in W_l} \mathbb{C}_w^{\mathrm{T}} - ((\sum_{k \in K} \sum_{(i,j) \in A_k} x_{ijk} \delta_{ijkw}) y_w) + \sum_{k \in K} \sum_{(i,j) \in A_k} c_{ijk} x_{ijk}$$

When the incumbent solutions are used, the lower bound is calculated to be 13. The upper bound is found when the master problem is solved. The master problem again results in the solution y_1=0, y_2=1, y_3=1 with an upper bound of 13. Following Benders' approach, when the upper bound equals the lower bound, optimality conditions have been met. Therefore, the solution with y_1=0, y_2=1, y_3=1 is the optimal cut of the interdependent arcs. With these values fixed, the problem simply becomes finding the minimum cost cut set for the four independent networks where the capacities of dependent arcs are modified by solution in Table 6. This can either be found directly though a minimum cost cut algorithm, or by once again solving the maximum flow problem and finding the reduced costs. Since the reduced costs represent the value of the primal variable, the arcs with a reduced cost of 1 are the arcs in the original formulation to be cut.

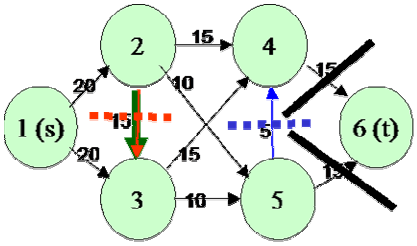

Figure 13. Network 1 Cut

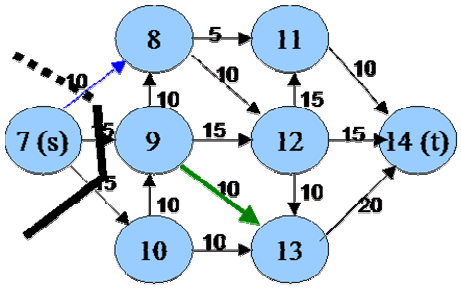

Figure 14. Network 2 Cut

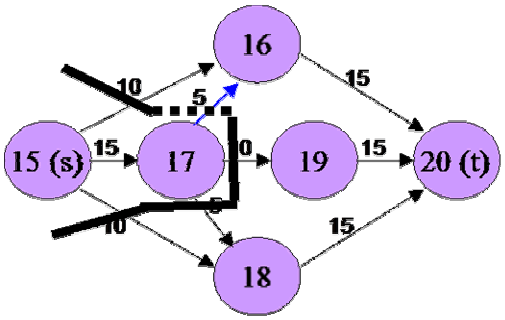

Figure 15. Network 3 Cut

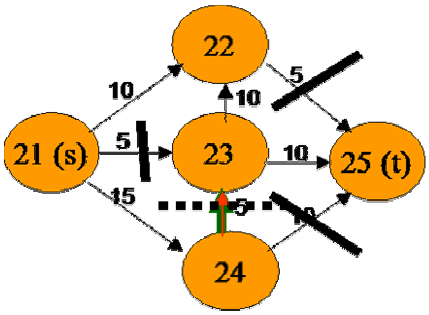

Figure 16. Network 4 Cut

To calculate the costs of the combined cuts, the cost (c_{ikj} and $\mathbb{C}_w$)are summed over each arc which is removed. If the sum of each individually cut arc is added to the sum of the two interdependent arcs cut, the sum cost is 123.

4.7 Results and Analysis

It is interesting to note that the optimal solution includes y_2 and not y_1 although y_1 includes more arcs; y_2 is actually a subset of y_1. Because of the costs (desired effects), it is more efficient to cut two of the three arcs with a single interdependent arc instead of all three arcs with another interdependent arc. This clearly illustrates potential options in selecting ways to interdict an arc (either individually or as a member of some interdependent set).

For this small problem, the general formulation could have been easily been solved directly without the need for partitioning. However, the power of the methodology lies in very large or complex networks with interdependent arcs. A potentially large mixed integer program can be transformed into independent network problems and a pure 0-1 problem. The special structure of these subproblems means solutions can be found efficiently. Initial experiments indicate that the Benders'

algorithm converges to optimality very quickly. If the interdependent effects can be specified, this methodology provides a framework for solving layered network problems.

The methodology presented here fills a gap in the open literature about dealing with layered networks such as infrastructure networks. The simple example could be scaled to solve much larger network problems. It can also be applied to different types of network flow models. For the minimum cost cut set problem presented, this approach shows a way to find the cut set across all networks simultaneously, not just across one layer of it. In addition, this approach has many potential areas for improvement as discussed in the next chapter.

V. Conclusion

5.1 Overview

This thesis developed and demonstrated a methodology to model multiple networks with interdependent arcs and decompose them into easily solved partitions. This methodology is demonstrated on four small notional networks, but the concept applies to networks regardless of size. Therefore, even networks as large as infrastructure models can be analyzed. Depending on the objective underlying network analysis, methods other than a cut-set approach can be used to take advantage of the structure of the network models. For example, Out-of-Kilter algorithms can be used to take advantage of structure of the partitioned networks which only change in the upper limit in interdependent arcs.

5.2 Research Results

This study showed that Benders' decomposition can be used to partition multiple interdependent networks into independent networks with their interdependencies modeled separately. Of course the power of this methodology is in its application to large, complex, layered networks. Small networks such as those modeled here can be solved as a single problem. However, infrastructure networks on a national level are very large and complex requiring one or more models for each layer of the infrastructure. Infrastructure models have vastly different structures, methodologies, and requirements. Combining or interfacing these models together is a daunting task. This method does not replace those

tools, but provides a framework for modeling the crossover effects not explicitly modeled within the individual network models themselves.

5.3 Recommendations for Future Research

5.3.1 Benders' Cuts

Close inspection of the cuts generated by the Benders' algorithm reveal potential to take advantage of special structures in the binary problem. Every sample problem solved was solved with a single Benders' cut. The reason seems clear when all binary variables are mutually exclusive; *i.e.* all binary variables could be chosen simultaneously. In this case, an interdependent cut is chosen if its cost is less than the sum of the costs for all arcs it cuts. Otherwise, if the interdependencies are not mutually exclusive, the Bender's cut create a special ordered set from which those cuts are chosen which have the highest reduced cost. In his textbook, William refers to this type of problem as a special ordered set (SOS), and he talks about the computational advantage of having these types of constraints (William, 1992: 179).

5.3.2 Cascading effects

One commonly cited example of cascading effects is in the power sector. In a study conducted for the Department of Energy, eleven major cascading power failures were analyzed, most traced back to a single trigger. For example, the 1965 blackout throughout the northeast was caused by a single relay switch in Ontario (Hauer, 1999: 5). Another study, conducted by Carreras, developed the flow chart in Figure 17 to show the formulation of the progression of blackouts.

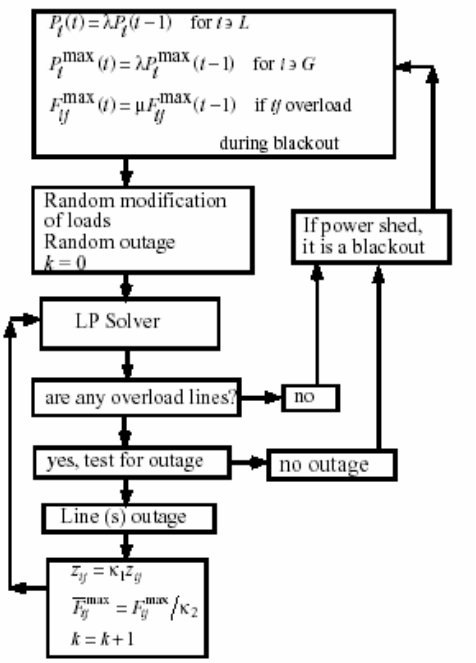

Figure 17. Cascade Flowchart (Carreras, 2001: 2)

The main cause of blackouts cannot be written into equations of a predictive code. Therefore, to understand the global dynamics of power system blackouts, the random character of the events that trigger them and the overall response of the system to such events need to be modeled. If the system operates close to a "critical" point, some aspects of the response of the system to random perturbation may have a universal character (Carreras, 2002: 9).

Cascading links contain four properties: link direction, link type, definition of the origin vulnerability, definition of the repercussion function, and definition of the destination vulnerability (Robert, 2002: 3). The link direction defines the direction a cascade may continue. The link type is either direct or indirect. Direct are either physical connections or predictable cause and effect relationships between components.

Indirect links are complex interactions not characterized by direct cause and effect relationships (Robert, 2002: 3).

The vulnerability of the origin component is defined as "the possible consequences of failure as shown by the impacts on the operation of the component or on its ability to perform the role for which it is designed (Robert, 2002: 20)." The vulnerability repercussion function defines how consequences connected to the origin component are propagated, modified, or transformed before reaching the destination component. Lastly, the destination vulnerability consequences resulting from the origin component and then propagated are now considered and studied as direct causes that affect the vulnerability of the destination component.

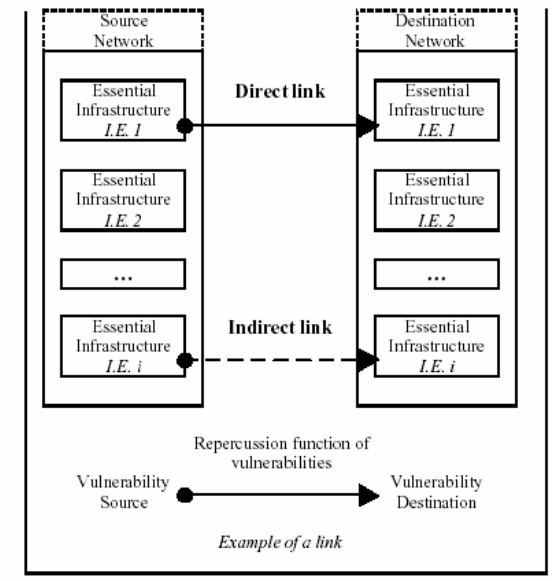

Figure 18. Cascade links (Robert, 2002: 20)

A subset of cascading effects is time-dynamics. Discussed in the paper Motter (2002) as "slow timescale evolution" and "fast timescale evolution."

We have also considered the electrical power grid of the western United States. The degree distribution in this network is consistent with an exponential and is thus relatively homogeneous. The distribution of loads, however, is more skewed than that displayed by semi-random networks with the same distribution of links, indicating that the power grid has structures that are not captured by these models. As a result, global cascades can be triggered by load-based intentional attacks but not by random or degree-based removal of nodes, as shown in Fig. 4. We see that the attack on a single node with large load reduces the largest connected component to less than a half of its initial size, even when the network is highly tolerant (Motter, 2002: 3).

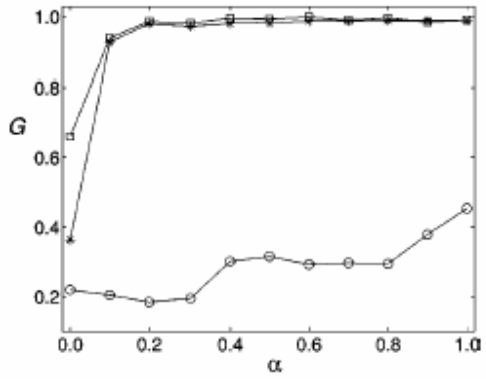

FIG. 4. Cascading failure in the western U.S. power transmission grid [31], which has $N = 4941$ and $\langle k \rangle \simeq 2.67$. The average is obtained via 5 triggers for attacks and 50 for random breakdown. The legends are the same as in Fig. 1.

Figure 19. Cascading Failures (Motter, 2002: 3)

This type of data could be used to model the cumulative effects of attacking multiple targets. For example, the synergy in this case is triggered with five specific targets are hit resulting in cascading power failures across thousands of points. This would appear to be a critical area for future analysis. In this thesis, interdependencies were modeled as binary variables affecting multiple arcs simultaneously. However, nothing in the method requires simultaneity, and logic could be included to model the resulting effects when a threshold is met, triggering the cascade.

5.3.3 Weaponeering

The approach presented here assumed interactions and "cuts" had binary values. For example, if a binary variable assumed a value of one, then several arcs were effectively removed from its associated network. One interpretation of this approach is that the binary variable represents a weapon capable of removing the identified set of arcs.

This approach could be modified slightly to directly include weaponeering, in addition to its targeting interpretation. First, a probability of kill (p_k) could be assigned to each variable associated with a weapon. Second, the objective function could be modified to include maximizing the probability of kill subject to the other objectives (such as minimum cost cut set). The result would be an algorithm for identifying both targets and weapons to attack these targets; two things which are currently done separately. This is similar to the two stage stochastic programs looked at in the telecommunications industry (Lisser, 1999). However, instead of stochastic demand, the probability of kill will be stochastic.

5.3.4 Advanced Starting Basis

The proposed methodology involves solving a pure network flow problem or problems repeatedly. As the binary values change, the upper capacities of interdependent arcs are the only change in the networks from iteration to iteration. For very large networks, re-solving the network problems may become computationally expensive, so we would like to take advantage of the fact that only the upper capacities of some of the arcs are changing.

Donohue and Birge (1995) consider a two-stage problem. Similar to the methodology here, the second stage problems are pure minimum cost network flow problems where only the arc upper capacities change. An approximation is made on the objective function in repeated iterations by finding an upper bound for the expected value of the network objective function.

The method reformulates the objective function as a function of the upper capacities on the arcs and shows they are a non-increasing convex function with a property called convex marginal return functions. These properties are then used to find an effective upper bound on the expected value of the network objective function. This often significantly decreases the function evaluations needed, while still finding an effective bound. (Donohue and Birge, 1995)

5.4 Conclusion

The methodology presented in this research effort demonstrates a promising methodology for solving multiple layered networks with interdependencies. This approach also has many promising areas of extension including weaponeering and cascading effects. The potential computational savings of applying this methodology over solving the formulation directly as one large program is significant. Given that the general methodology is applicable to any of the network models and structures, it has broad applications. It should serve as the foundation for an array of interdependency analysis.

Bibliography

Air Force Pamphlet 14-210. *USAF Intelligence Targeting Guide* (U). 1 February 1998.

Baumol, W. J. and T. Fabian, "Decomposition, pricing for decentralization and external economies,' *Management Science,* Volume 11, Issue 1 (Sep. 1964), 1–32.

Bellmore, M, G Bennington, and S Lubor. "A Network Isolation Algorithm." Naval Research Logistics Quarterly, 17 (1970): 461-469.

Benders, J. F. "Partitioning Procedures for Solving Mixed-Variables Programming Problems." Numerische Mathematik, 4 (1962): 238-252.

Bennington, Gerald E. "Multi-Commodity Disconnecting Sets in Undirected Graphs by Node Partitioning." Diss. Johns Hopkins U, 1969.

Bozek, Tom. *DoD Critical Infrastructure Protection* 18th NDIA Security Division Symposium & Exhibition, 25-27 June 2002. http://www.dtic.mil/ndia/2002security/bozek.pdf

Carreras, B. A., Lynch, V. E., Dobson, I., Newman, D. E.. Critical points and transitions in an electric power transmission model for cascading failure blackouts. *Chaos*, 12, 985 - 994, (2002).

Carreras, B. A., Lynch, V. E., Dobson, I. & Newman, D. E. and Sachtjen, M. *Modeling Blackout Dynamics in Power Transmission Networks with Simple* Structure 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Volume 2, 25-27 Maui HI 03-06 January 2001.

Christian, Shelley (Maj), and others. *Information Warfare: An Opportunity For Modern Warfare*. ACSC Research Paper, ACSC/DEC/020/95-05, Air Command and Staff College, Maxwell AFB AL. 1 May 1995.

Dantzig, G. B. and P. Wolfe, The decomposition algorithm for linear programs, *Econometrica,* Volume 29, Issue 4 (Oct. 1961), 767–778.

Deininger, R.A. 2000. Constituents of Concern. The Threat of Chemical and Biological Agents to Public Water Supply Systems. Appendix F in Pipeline Net User's Guide, SAIC. McLean VA.

Donohue, C.J., Birge, J. R. "An Upper Bound on the Network Recourse Function," Technical Report 95-5, Department of Industrial and Operations Engineering, University of Michigan, March 1995.

Ezell, Barry C. Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply. Diss. U of Virginia, 1998. 01 Mar. 2003 <http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html>.

Ezell B. C., Y.Y. Haimes, and J. L. Lambert. "Risks of Cyber Attack to Water Utility Supervisory Control and Data Acquisition Systems," Military Operations Research Society, 6 (2), 2001.

Fulghum, David A. "Electronic Bombs Darken Belgrade." Aviation Week & Space Technology 10 May 1999: 34-35.

Geoffrion, A. M. "Generalized Benders Decomposition." Journal of Optimization Theory and Applications 10 (1972): 237-260.

Griffith, Thomas E. Strategic Attack of National Electrical Systems. Diss. Air U, 1994. 01 Mar. 2003 <http://www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/Griffith/griffith.pdf>.

Hauer, J. F., Dagel, J. E. *Consortium for electric reliability technology solutions, grid of the future: White paper on review of recent reliability issues and system events*. U.S. Dept. of Energy. (1999). http://certs.lbl.gov/pdf/CERTS-Reliability.pdf

Hurst, G.R. *Taking Down Telecommunications.* Maxwell AFB AL: Air University Press, September 1994.

Isenberg , David. Securing U.S. Water Supplies. 19 July 2002. 01 Mar. 2003 <http://www.cdi.org/terrorism/water.cfm>.

Lai, Ying-Cheng, and Adilson E. Motter. "Cascade-Based Attacks on Complex Networks." Physical Review E 66 (2002).

Lisser A., Ouorou A., Vial J.-Ph. and Gondzio J., "Capacity planning under uncertain demand in telecommunications networks," Logilab Technical Report, Department of Management Studies, University of Geneva, Switzerland, October, 1999.

Martello, Silvano, Toth. *Knapsack Problems*, John Wiley & Sans, New York, 1990.

National Security Telecommunications Advisory Committee (NSTAC), Information Assurance Task Force (IATF). Electric Power Information Assurance Risk Assessment. March 1997.

President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America'sInfrastructures,* Robert T. Marsh, Chairman (Washington, D.C.: GPO, October 1997), 01 March 2003. <http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf >

Polzin, Steven. "Security Considerations in Transportation Planning: A White Paper." Center for Urban Transportation Research for the Southeastern Transporation Center. 1 Mar. 2003 <http://www.cutr.eng.usf.edu/pubs/Security%20paper%200402.doc>.

Kelly, Terrence K., James P. Peerenboom, and Steven M. Rinaldi. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." IEEE Control Systems Magazine, Dec. 2001: 11-25.

Robert, Benoît. 2001a. *A Method for the Study of Cascading Effects Within Lifeline Networks.* Workshop on Mitigating the Vulnerability of Critical Infrastructure to Catastrophic Failures, Alexandria VA (USA), September 10-11. http://www.ari.vt.edu/workshop/

Robert, Benoît, Sabourin, Jean-Pierre, Glaus, Mathias, Petit, Frédéric, and Senay, Marie-Hélène**.** *A New Structural Approach for the Study of Domino Effects Between Life Support Networks*. The Future of Disaster Risk: Building Safer Cities, December 2002, http://www.proventionconsortium.org/files/conference_papers/robert.pdf

Ryan, Julie. The Infrastructure of the Protection of the Critical Infrastructure (1998). 01 March 2003. <http://www.julieryan.com/Infrastructure/IPdoc.html>.

Sweeney, Dennis J., Murphy, Richard, A. "A Method of Decomposition for Integer Programs," Operations Research, 27: 1128-1141 (1979).

Taha, Hamdy A. *Integer Programming: Theory, Applications, and Computations,* New York NY: Academic Press, 1975.

Uchida, Ted T. Analysis of Effects-Based Operations – The Road Ahead to Doing Business Differently.

Where Does My Drinking Water Come From? 26 Nov. 2002. Environmental Protection Agency. 01 Mar. 2003 <http://www.epa.gov/OGWDW/wot/wheredoes.html>.

William, H.P. *Model Solving in Mathematical Programming*. Wiley, Chichester, (1992).

Wilson, Jim. "E-Bomb." Popular Mechanics Sept. 2001. 1 Mar. 2003 <http://popularmechanics.com/science/military/2001/9/e-bomb/print.phtml>.

Vita

Captain Kevin Kennedy entered undergraduate studies at the University of Kentucky in Lexington, Kentucky where he graduated with a Bachelor of Science degree in Mathematics and a Bachelor of Arts degree in Chemistry in May 1998. He graduated with honors, Phi Beta Kappa, Tau Beta Pi, and Cum Laude. He was commissioned through the Detachment 290 AFROTC at the University of Kentucky.

His first assignment was at Kirtland AFB where he served as Lethality Section Chief for the Joint Air-to-Surface Standoff Missile. In August 2001, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to the Air Force Logistics Management Agency at Gunter-Annex, Maxwell AFB, Alabama.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
14-03-03	**Master's Thesis**	Sep 02 - Mar 03

4. TITLE AND SUBTITLE
AN ANALYSIS OF MULTIPLE LAYERED NETWORKS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Kennedy, Kevin, T, Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Street, Building 642, WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GOR/ENS/03-14

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Current infrastructure network models of single functionality do not typically account for the interdependent nature of infrastructure networks. Infrastructure networks are generally modeled individually, as an isolated network or with minimal recognition of interactions. This research develops a methodology to model the individual infrastructure network types while explicitly modeling their interconnected effects. The result is a formulation built with two sets of variables (the original set to model infrastructure characteristics and an additional set representing cuts of interdependent elements). This formulation is decomposed by variable type using Benders' Partitioning and solved to optimality using a Benders' Partitioning algorithm.

15. SUBJECT TERMS
Large Scale Optimization, Layered Networks, Network Interdiction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**Dr. Richard F. Deckro**
U	**U**	**U**	**UU**	73	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565 x4325 (Richard.Deckro@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18