Network Flow Approaches for Analyzing and Managing Disruptions to Interdependent Infrastructure Systems

Earl E. Lee, II, John E. Mitchell and William A. Wallace

Abstract

Modern society relies upon the complex interaction of the civil infrastructure systems, such as transportation, power, telecommunications and water. These systems are highly dependent on each other to provide service. The reliance on any of them on power is obvious. Failures in one system can have far-reaching effects. This paper will present an overview of research which explicitly models these systems and more importantly, their interconnectedness. The model and its associated decision support system, developed in this research, can be used by those responsible to responding to disruptions or for evaluating vulnerability with an ability to see across the boundaries of a single system and evaluate the system of systems.

Introduction

The American way of life relies on the operations and interactions of a complex set of infrastructure networks. These networks include transportation, electric power, gas and liquid fuels, telecommunications, wastewater facilities and water supplies. This set of civil infrastructures has also been included in the broader set of critical infrastructures defined by the USA Patriot Act of 2001 (2001). In the Patriot Act, critical infrastructures are those

> "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such would have a debilitating impact on security, national economic security, national public health or safety or any combination of these matters (2001)."

This research will focus on the interconnectedness of these networks.

Each of these infrastructure systems evolved independently. However as technology advanced, the systems became interconnected. The reliance of any of these systems on power is obvious. Failures, by whatever cause, within the communications networks in one locale may have far-reaching effects across many systems.

Infrastructure management systems did not allow a manager of one system to "see" the operations and conditions of another system. Therefore, emergency managers would fail to recognize this "interconnectedness" or interdependence of infrastructures in responding to an incident, a fact recognized by *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (The White House 2003). This research provides a "system of systems" view to better understand the interdependent nature of these systems with respect to mitigation and post-disruption response and recovery.

Background/ Past Work

The previous work relating to this research falls into one of three categories. There are the policy documents, the work on single system modeling and the work involving modeling system of systems. The policy documents include the U.S. Patriot Act (2001), *The 2002 National Strategy for Homeland Security* (Office of Homeland Security 2002), the 1997 report *Critical Foundations – Protecting America's Infrastructure* (President's Commission on Critical Infrastructure Protection 1997), The Clinton Administration's Policy on Critical Infrastructure Protection (The White House 1998), and *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (National Research Council 2002). General papers on the subject of interdependent infrastructures include (Robinson, Woodard et al. 1998; Heller 2001; Rinaldi, Peerenboom et al. 2001; Little 2002). Also, this discussion now extends globally, for example, *Thinking About the Unthinkable: Australian Vulnerabilities to High-Tech Risks* (Cobb 1998) and the November 2004 position paper, *Keeping Canadians Safe* (Office of Public Safety and Emergency Preparedness Canada 2004).

Many efforts over the years have focused on disruptions affecting single infrastructure systems. These efforts include the Complex Interactive Network Systems Initiative (CIN/SI), a joint endeavor between the Department of Defense, academia, and the Electric Power Research Institute (EPRI). The discussion of the CIN/SI program is found in (Hasse 2001) in the annual reports of the initiative consortia and in (Amin 2000; Amin

2000; Amin 2001; Amin 2002; Amin 2002). Salmeron et al. (2004) discussed analytic techniques to mitigate disruptions in electric power grids caused by terrorist attack, but only considered components in the power system and not systems they rely on. Haimes et al. (1998) looked at the issue of reducing vulnerability of water systems to willful acts and identified the need for further research in identifying critical points and quantitative methods focused on attack consequences, not likelihood of the disruptive event. Both of these needs are addressed in this research. The National Petroleum Council (2001) clearly identified the increased reliance of petroleum and gas systems on information technology and telecommunications. Their report also identified interdependency as one of the most difficult areas to understand. Kuhn (1997) provided a quantitative analysis of outages in the phone system and did include power system failure as a cause. Klincewicz (1998) looked at the integrated design of computer networks, but made no mention of considerations for the components reliance on power. Chamberland and Sanso (2001) discussed the design of multitechnology data networks, but failed to consider interconnectedness to other systems. Cremer et al. (2000) looked at issues relating to the physical construction of the Internet, focusing on issues of connectivity and degradation of service, but focused completely on only its system’s components. While not exhaustive, these papers and reports show the quantity and breadth of past and ongoing work.

Past research has also studied vulnerability and reliability as they relate to interconnected systems. Haimes and Jiang (2001) present a Leontief-based input–output model called the inoperability input–output model (IIM) that enabled the accounting for interconnectedness among infrastructure systems. However, this approach worked at a macroscopic level, and while useful for vulnerability assessment, it would be difficult to extend this approach to restoration activities. In a more recent work (Haimes, Horowitz et al. 2005), they continue the development of the IIM and its ability to measure economic impact among various sectors in the economy by analyzing both the initial disruption and the ripple effects. Carullo and Nwankpa (2003) present experimental studies in electrical power systems with an embedded communication system for transmission of network conditions. However, their paper looks only at control issues due to communication system delay issues. Holmgren et al. (2001) also present issues in power control systems and the associated communication systems. Jha and Wing (2001) develop a constrained Markov decision process method to investigate survivability within infrastructures systems that rely on computers and computer networks. While the work refers to critical infrastructures and measuring impacts of disruptions, the work consists of computer network survivability analysis as those networks relate to a specific system, in this case, banking and finance.

Significant effort is being expended in the development of simulations of infrastructure interdependencies. The Department of Homeland Security's Information Analysis and Infrastructure Protection Division is sponsoring the National Infrastructure Simulation and Analysis Center. This program is a partnership between Sandia and Los Alamos National Laboratories and includes the Simulation Object Framework for Infrastructure Analysis, the Urban Infrastructure Suite, and the Interdependence Energy Infrastructure Simulation System projects. As simulations, they can improve the understanding of the system response to an event or scenario and can be useful in vulnerability studies. Additionally, the Infrastructure Assurance Center at Argonne National Laboratory is focused on identifying vulnerabilities to disruptions; assessing the impact of such disruptions on quality of life, economy, and national security; developing effective tools, methods, and technologies that address each phase of the infrastructure assurance cycle; and facilitating coordination efforts between involved parties. All of these efforts are noteworthy and work to improve understanding.

The Interdependent Layered Network Model

This research has developed a formal, mathematical representation of the set of civil infrastructure systems that explicitly incorporates the interdependencies among them and is called the Interdependent Layered Network model (ILN). The ILN is a mixed-integer, network-flow based model which has been implemented in software that enables the resulting model to be exercised. The mathematical formulation of the model can be found in (Lee, Mitchell et al. 2007) and (Lee 2006). The ILN is embedded in a prototype decision support system, the Multi-Network Interdependent Critical Infrastructure Program for Analysis of Lifelines (MUNICIPAL). MUNICIPAL consists of a geographic information system (GIS) interface for the user, a database with the attributes of the set of infrastructures, the ILN module, and a vulnerability and system design module.

MUNICIPAL provides the capability to understand how a disruptive event affects the interdependent set of civil infrastructures. This capability improves society's ability to withstand the impact of and respond to events that can disrupt the provision of services that are required for the health, safety and economic well being of its citizens. Managers of infrastructure systems will be able to assess the vulnerability of their own system due to its reliance on other systems. Organizations responsible for coordinating emergency response efforts will also be able to model different event scenarios and assess their impact across the full set of systems and the services they provide. With this broader perspective of impact, mitigation and preparedness strategies can be formulated and evaluated for their ability to reduce their effects on society.

The model is not based upon a unique configuration of infrastructures, but is generic and therefore, applicable to more than one location. It is also not specific to a particular type of event, such as an earthquake or hurricane. The only requirements are that the event is possible but unpredictable, the event is of sudden onset, and the event causes damage to the physical components of the infrastructure system.

The intended use of MUNICIPAL was for response and restoration efforts following a disruptive event and as a training tool for personnel who would be guiding response and restoration efforts. As the research progressed, MUNICIPAL was found to be useful in supporting system design, in assessing the vulnerability of a system, in measuring the benefits of pre-staging resources or installing backup power systems and even changing the physical design of the existing systems. This research has developed a network flow formulation of interdependent networks which clearly identifies effects of a disruptive event across the set of infrastructure systems. The next section discusses the five types of interdependence included in the ILN and how each of these possible interdependencies was modeled.

Types of Interdependence

Rinaldi et al. (2001) formalized the definitions of interdependence within this ongoing discussion of critical infrastructure and defined four classes of interdependency. Due to the number of different types of dependencies and interdependencies, these authors classified the entire family of interrelationships among systems as interdependencies, an approach retained in this paper.

This research identified five types of interrelationships between infrastructure systems – input, mutual, shared, exclusive-or and co-located. A discussion of these is provided below. The mathematical details of each can be found in (Lee 2006) and (Lee, Mitchell et al. 2007).

Input

An infrastructure is input interdependent when it requires as input one or more services from another infrastructure in order to provide some other service. As an example, in the case of a telephone switching station, the switching station itself is a transshipment node within the telecommunications network. However, this same switching station from the perspective of the electrical network is seen as a demand node since it needs an adequate source of electricity to operate. If insufficient pwer is available for the switching center, then it will be unable to operate and this change of capacity will affect the telecommunications system. The effect on any set of systems can be analyzed in a similar manner. Note that some interdependent infrastructure system failures may result in reducing capacity to some value other than zero. For example, loss of supervisory control systems in a subway system may result in operators exercising greater care and slowing trains. So the post-disruption capacity may be lower than normal.

Mutual

A collection of infrastructures is said to be mutually interdependent if at least one of the activities of one infrastructure system is dependent upon any other infrastructure system and at least one of the activities of this other infrastructure system is dependent upon the first infrastructure system. Consider a natural gas system pump and a gas-fired electric power generator. From the perspective of the natural gas system, the pump is a transshipment node and the generator is a demand node. From the perspective of the electrical network, the generator is a supply node and the pump is a demand node. The generator needs gas to produce electricity; the pump needs electric power to deliver gas through the system to the generator. Failure of one component causes its corresponding binary variable to be set to zero, thus reducing the effective capacity of the other component to zero. In other words, if the pump were to fail, supply of gas to the generator would be inadequate. If the capacity of the generator is set to zero (since its effective and because the generator is a supply node, all flows on the arcs (i.e., the power lines) leaving the generator would now be zero, by flow conservation. Alternately, a lack of power at the pump demand node in the electrical generating network causes its capacity to be set to zero. To correct his situation, either an alternate source of gas must be found for the generator or an alternate source of power must be found for the pump.

Shared

Shared interdependence occurs when some physical components and/or activities of the infrastructure used in providing the services are shared. Phone lines could be considered in the shared interdependency. Each phone line carries two types of calls, incoming and outgoing. Therefore, if a cable section contains 50 lines, they could be 50 incoming calls or 50 outgoing calls or some combination totaling 50. This type of interdependence is common in modeling of multicommodity systems. This is modeled mathematically by limiting the sum of the flows of the various commodities across the component to not exceed the total capacity.

Exclusive-or

Exclusive-or interdependence occurs when multiple services share infrastructure component(s), but the component can only be used by one service at a time,. In the first few days following the WTC attacks, streets (i.e., shared components) could not be used by both the emergency response personnel and financial district workers. This conflict had to be resolved prior to reopening the New York Stock Exchange (Lohr 2001).

Exclusive-or interdependencies are modeled by selecting additional constraints to restrict flow to one commodity or the other.

Co-located

The co-located interdependency occurs when any of the physical components or activities of the civil infrastructure systems are situated within a prescribed geographical region. It was previously noted that managers of individual infrastructure systems would identify the components of their respective system at or near the site of the incident which may have been affected by the event. Based on further investigation, the status of these components will be adjusted. However, since only those emergency response agencies who are responsible for coordinating activities across multiple agencies maintain the complete view of all civil infrastructure systems, it is ultimately their responsibility to ensure that all co-located interdependencies have been considered and the models of the affected infrastructures revised as appropriate.

The Components of MUNICIPAL

The user interface

A geographic information system (GIS) was selected as the user interface as this seemed to be the most natural method of displaying systems and determining affected areas. The interface allows the operator to update the conditions of the components of the set of systems modeled, to add temporary systems during restoration and the display areas affected by inabilities to meet demands.

The Database

The database contains the component attributes such as a name, their capacity and their priority, as well as spatial attributes, such as location and length. These spatial characteristics are generated automatically by the GIS software, ESRI's ArcGIS (ESRI 2004) in this case. The remaining attributes are added by the modeler. Changes to attributes due to disruption can easily be made.

The Manhattan Dataset

In Manhattan, the goal was to develop highly detailed models in the area south of 60th Street of the power, telecommunications and subway systems, three major infrastructure systems impacted by the September 11 attacks. While unable to obtain details on specific components and their locations, Consolidated Edison, Verizon and the Metropolitan Transit Authority were very open in discussing the general construction and operation of their respective systems and have provided feedback during the model's construction. The subway system includes 115 stations and 338 local and express track sections. The phone system includes 18 switching centers and their associated service areas, 72 controlled environmental vaults where distribution cables are joined into larger feeder cables and the all the associated wiring. Below Canal St., approximately 500 blocks of phone service were modeled in detail. The power system as modeled includes 16 substations and 32 service areas. Each substation distributes power along 8-24 feeders to 18 phone switching centers, 178 AC/DC rectifiers for the subways and service to all residences and businesses in the area.

The Los Angeles Area Dataset

The ILN and the Manhattan data set demonstrate the model's usefulness to emergency response organization managers when facing disruptions among interdependent infrastructures. Although the demand for service is dense and complex, the geographic area of Lower Manhattan is about ten square miles. The purpose of developing the Los Angeles dataset was to demonstrate the applicability of the ILN to a geographic area with approximately the same demands for service, but with these demands being dispersed, over a much larger geographic area, approximately 800 square miles. The Los Angeles data set included the power, telecommunications, gas, water systems and MUNICIPAL was changed to provide new management capabilities.

The management of disruptive events can be viewed as existing on three levels. First is a regional view. This would be the perspective for a county or multi-county disruptive event. (Statewide or national events are not considered here, since emergency management operations are conducted at regional and local levels; state and federal response is one of support to the local agencies.) When looked at from a regional view, infrastructure managers focus on the major components that provide service. In a power system, this would be the supplies of power from outside the region, the generators inside the region, and the transmission system throughout the region down to the substations delivering power to their respective service areas. Water system managers focused on major supplies, treatment facilities and the major pipelines delivering water to service zones. This view is a broad perspective and solving the ILN at this level would indicate inabilities to deliver service to entire service zones and not provide much detail. The next level of management would be at the service area. At this level, the substations which were viewed as demand nodes at the regional view now become the supplies for service areas. Their feeder system delivers the power across the service area to the residential and commercial customers. The level of detail would be that considered most appropriate by the individual managers of infrastructure systems. The final level is that most familiar to one other group that must be considered in managing disruptions, that of the local government. Civic leaders will want to know how the event is affecting their community and will want input on setting priority for restoration. Communities will likely be served by several service areas of a single infrastructure system, and service area boundaries among infrastructure systems usually do not coincide. Therefore, city government needs an integrated view of the status of systems within their municipal boundaries, not some confusing overlay of service areas. This view will aid local government in getting the proper information to its citizens. As important, local governments officials can participate in the priority setting process. However, the emergency manager can view all the service areas and all of the services affected. Details of how this multi-level modeling was accomplished can be found in (Lee 2006).

Using MUNICIPAL During System Disruptions

When an event occurs which disrupts any of the infrastructure systems included in MUNICIPAL, the operators would first to use the GIS interface to identify components in and around the area of the disruption that may have been affected. Crews could then be dispatched to determine actual conditions of these possibly affected components. Outage reports from customers could also be entered in a separate database and linked to the GIS. On-scene reports would ascertain the actual conditions of these components and the GIS would be used to update the component database. In general, these updates would be to capacity of links and nodes or to available supplies at components like generators, etc.

With the direct impact of the disruption entered, MUNICIPAL can be run to determine where demands for service are not being met. These outages would be due to failures of components in a system and its customers needs as well as outages caused by failure in among interdependent systems.

With the full extent of the disruption modeled, the operators can use MUNICIPAL to begin restoration planning. Priorities can be set for each customer outage and plans can be developed in a collaborative environment. A complete example of the use of MUNICIPAL for a disruption is found in (Lee 2006) and (Lee, Mitchell et al. 2007). When a restoration plan is decided upon, MUNICIPAL can then develop work schedules based upon available resources, cost and priorities.

Using MUNICIPAL for Vulnerability Analysis

System managers are limited in their ability to evaluate the resilience of the systems they control because they cannot take into account the interdependencies of their systems with other infrastructures. In Lee et al (2004) and in (Lee 2006) , a procedure was introduced to evaluate the vulnerability of current or proposed designs of infrastructures that considers their interdependence to other systems. This procedure allows a system engineer to evaluate existing paths which a considered to provide redundancy. For example, two existing paths in a telecommunications network between two important government or corporate offices. Since these two paths do not share any telecommunications components, they would appear to be redundant. However, using MUNICIPAL and its interconnected system model, the system engineer can conduct a backward trace into each system that telecommunications relies on. If these backward traces find single components in other systems whose failure causes both telecommunications paths to fail, then redundancy is not truly being provided. Examples could include single points in a power system that could lead to failure of redundant paths in telecommunications or single components in a gas system which provide fuel to both the normal and backup generators for a facility or region.

MUNICIPAL can also aid in designing redundant paths. By conducting its backward trace along any path considered vital into all systems the path relies on, MUNICIPAL can be used to determine if a new, redundant path can be provided, utilizing the components not used by the current path and new connections or components, when appropriate.

Conclusions

This paper has provided an overview of the ILN and MUNICIPAL and the capabilities of each. Our work continues and includes alternative formulations and solvers, extension of the work from the civil infrastructure systems to service systems, like supply chains and public safety. There is also an intent to improve the method by which priorities are established during system restoration, based upon methods found in the social sciences and economic impacts. Future work will also include the improvement of the decision support system and user interfaces.

Acknowledgements

The authors wish to acknowledge the valuable assistance of the Manhattan offices of Consolidated Edison and Verizon, as well as the New York City Office of Emergency Management and the New York State Emergency Management Office. This work was supported by the National Science Foundation under Grant CMS 0139306, Impact of the World Trade Center Attack on Critical Infrastructure Interdependencies; Grant DMII 0228402, Disruptions in Interdependent Infrastructures: A Network Flows Approach; and Grant CMS 0301661, Decision Technologies for Managing Critical Infrastructure Interdependencies.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 , Public Law 107-56, October 26, 2001.

Amin, M. (2000). Modeling and Control of Complex Interactive Networks. IEEE Control Systems Magazine**:** 20-24.

Amin, M. (2000). Toward Self-Healing Infrastructure systems. Computer. **33**.

Amin, M. (2001). Toward Self-Healing Energy Infrastructure Systems. IEEE Computer Applications in Power. **14:** 20-28.

Amin, M. (2002). Modeling and Control of Complex Interactive Networks. IEEE Control Systems Magazine**:** 22-27.

Amin, M. (2002). "Toward Secure and Resilient Interdependent Infrastructures." Journal of Infrastructure Systems **8**(3).

Carullo, S. P. and C. O. Nwankpa (2003). Experimental Studies and Modeling of an Information Embedded Power System. 36th Hawaii International Conference on System Sciences, Hawaii, IEEE.

Chamberland, S. and B. Sanso (2001). "On the Design of Multitechnology Networks." INFORMS Journal on Computing **13**(3): 245-256.

Cobb, A. (1998, September 27,2001). "Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks."   Retrieved April 10, 2006, from http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm.

Cremer, J., P. Rey, et al. (2000). "Connectivity in the Commercial Internet." The Journal of Industrial Economics **48**(4): 433-472.

ESRI (2004). ArcGIS. Redlands, CA, ESRI.

Haimes, Y. and P. Jiang (2001). "Leontief-based Model of Risk in Complex Interconnected Infrastructures." Journal of Infrastructure Systems **7**(1): 1-12.

Haimes, Y. Y., B. M. Horowitz, et al. (2005). "Inoperability Input-Output Model for Interdependent Infrastructure Sectors." Journal of Infrastructure Systems **11**(2): 67-79.

Haimes, Y. Y., N. C. Matalas, et al. (1998). "Reducing Vulnerability of Water Supply Systems to Attack." Journal of Infrastructure Systems **4**(4): 164-177.

Hasse, P. (2001). Of Horseshoe Nails and Kingdoms:. EPRI Journal.

Heller, M. (2001). "Interdependencies in Civil Infrastructure Systems." The Bridge **31**(4): 9-15.

Holmgren, Å., S. Molin, et al. (2001). Vulnerability of Complex Infrastructure. The 5th International Conference on Technology, Policy and Innovation, Delft, The Netherlands.

Jha, S. and J. M. Wing (2001). "Survivability analysis of networked systems." Proceedings - International Conference on Software Engineering: 307-317.

Klincewicz, J. G. (1998). "Hub Location in backbone/tributary network design: a review." Location Science **6**(1): 307-355.

Kuhn, D. R. (1997). Sources of Failure in the Public Switched telephone Network. Computer**:** 31-36.

Lee, E. E. (2006). Assessing Vulnerability and Managing Disruptions to Interdependent Infrastructure Systems: A Network Flows Approach. Decison Sciences and Engineering Systems. Troy, NY, Rensselaer Polytechnic Institute. **Ph. D.**

Lee, E. E., J. E. Mitchell, et al. (2004). Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems. 37th Hawaii International Conference on System Science., Hawaii.

Lee, E. E., J. E. Mitchell, et al. (2007). "Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach." IEEE Transactions on Systems, Man and Cybernetics, Part C Applications and Reviews **37**(6): 1303-1317.

Little, R. (2002). "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures." Journal of Urban Technology **9**(1): 109-123.

Lohr, S. (2001). Financial District Vows to Rise From the Ashes. New York Times. New York, NY**:** A-6.

National Petroleum Council Committee on Critical Infrastructure Protection (2001). Securing Oil and Natural Gas Infrastructures in the New Economy. Washington, DC.

National Research Council (2002). Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C., The National Academy Press.

Office of Homeland Security (2002). The National Strategy for Homeland Security. Washington, DC.

Office of Public Safety and Emergency Preparedness Canada. (2004, February 3, 2006). "National Critical Infrastructure Assurance Program."   Retrieved 2006, April 10, from http://www.psepc-sppcc.gc.ca/prg/em/nciap/position_paper-en.asp.

President's Commission on Critical Infrastructure Protection. (1997, October). "Critical Foundations - Protecting America's Infrastructures." from www.ciao.gov.

Rinaldi, S. M., J. P. Peerenboom, et al. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. **21:** 11-25.

Robinson, C. P., J. B. Woodard, et al. (1998). Critical Infrastructure: Interlinked and Vulnerable. Issues in Science and Technology. **15**.

Salmeron, J., K. Wood, et al. (2004). "Analysis of Electric Grid Security Under Terrorist Threat." IEEE Transactions on Power Systems **19**(2): 905-912.

The White House (1998). The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Washington, DC.

The White House (2003). The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington, DC.