Review of interdependent infrastructure systems vulnerability analysis

Shuliang Wang, Liu Hong, Xueguang Chen, Jianhua Zhang, Yongze Yan

Abstract—Critical infrastructures including, but not limited to power, natural gas, potable water are usually called the lifeline systems. They construct the cornerstone of modern society and are essential for the functioning of a society and its economy. As the development of the society they become more and more interconnected. The function of one infrastructure affects the function of the other infrastructures. Damages in one infrastructure often traverse to other correlative infrastructures and sometimes even back to the originated infrastructure making the infrastructure systems more fragile to various kinds of disturbances. Research on this area has become an important subject. This paper illustrates a review of vulnerability analysis for interdependent infrastructure systems and we conclude that there is no single ‘silver bullet solution’ to the problem of analyzing interdependent infrastructure risk and vulnerability. So a methodology framework of analysis is necessary and seems to be needed to effectively integrate the different methods in this area. At last we develop a framework for analyzing the problem of vulnerability in interdependent infrastructures.

Key Words—Interdependent infrastructure, Vulnerability analysis, Deliberate attack

I. INTRODUCTION

Critical infrastructure systems[1], which refer to systems comprising identifiable industries, institutions, and distribution capabilities providing a reliable flow of products and services essential to the defense and economic security of the society, are often called the lifeline systems. They include but are not limited to electric power system, telecommunications, water treatment and supply, natural gas supply, transportation systems etc. They construct the cornerstone of modern society. Infrastructure does not exist in isolation, but interconnected with each other. With the development of scientific technology and social economy these critical infrastructure systems become more and more complicated and mutually dependent, they need more and more resources and information to maintain day-to-day normal operation. The function of one infrastructure affects the function of the other infrastructures, once the systems are disturbed by external or internal perturbations and system failures are not isolated events, they can spread very rapidly to other correlative infrastructures and sometimes even back to the originated infrastructure which may cause the whole system lose its function and collapse [2–6], increasing interconnectivities among critical infrastructure systems have made them more vulnerable than before.

Widespread loss of these systems can be very disruptive. They can cause great economic, social, and physical disruption, amplify negative consequences and affect unforeseeable and haphazard sets of users. An example of infrastructure disruption is the 2003 North America power grid blackouts. The event leads to 50 million people affected in at least ten northeastern states and one Canadian province and about $10 billion U.S. dollars of losses. Because of interdependencies, most of the physical and organizational infrastructures are affected such as national security; health and welfare; communications; finance; transportation; food and water supply; heating and cooling; computers and electronics; commercial enterprises; and even entertainment. Another example is the 2008 South China snowstorms. The snowstorms disaster in South China caused many infrastructure disruptions. Road, rail, aviation, electricity, water, transport and other infrastructure systems in this area lose most of their functions and some even collapsed. More seriously, due to interdependency between different infrastructures, what happens to one infrastructure can affect other systems directly and indirectly, for example, the traffic which is influenced by the snow storm further threatens the electric power infrastructure which requires coal fuels for its generators, road and rail transportation to supply fuels to the generators. Subsequently, rescue is delayed due to lack of adequate power resources and bad traffic conditions worsening key segments of the vital human services network. The disaster lead to billions of dollars of losses, causing far-reaching security and reliability concerns. So these lifeline systems must be sufficiently reliable and governable to ensure people living and working in these areas have access to most utility services. However, because of different coupling modes and unique failure propagation patterns complex interdependent system responds distinctly to disruptions making it more difficult and important.

These examples illustrate that disrupting on one element of the systems may exceed the boundaries of a single infrastructure due to coupling and cause significant damages. In view of the importance of infrastructure systems on social development, the influence of infrastructure disruptions on social production and economics, interdependent infrastructure systems vulnerability analysis becomes
increasingly important. This article presents a review framework for addressing infrastructure interdependencies which would act as a basis for further understanding and research in this important area.

II. PERSPECTIVES ON VULNERABILITY AND INTERDEPENDENCY

Risk and vulnerability analysis are basic tools for critical infrastructure protection and risk management. They have very close interrelationship between each other and are related to attacks and disruptions. The meaning of the concepts varies considerably between different disciplines and even within a particular discipline [7]. Johansson illustrates two interpretations of the concept of vulnerability [8]. In the first interpretation vulnerability is seen as a global system property that expresses the extent of adverse effects caused by the occurrence of a specific hazardous event. In the second interpretation, vulnerability is used to describe a system component or an aspect of the system. Three aspects of vulnerability: Global vulnerability, critical components and critical geographical locations are analyzed. M. Ouyang introduces two types of vulnerability to analyze the vulnerability of interdependent infrastructures, structural vulnerability and functional vulnerability[9]. The infrastructures topologies are the only information for structural vulnerability. For functional vulnerability, operating regimes of different infrastructures should be considered.

For the concept of infrastructure interdependency we know infrastructure does not exist in isolation. Especially with the development of scientific technology and social economy, many infrastructure systems in our life become more and more interconnected and interdependent. First we must address the issue of characterizing interdependencies for modeling critical infrastructure systems. There are different explanations of interdependence in the literatures by different standards. Rinaldi et al. [10] consider the concept of interdependency as a bidirectional relationship between two infrastructures and categorizes four general types of interdependencies: physical interdependency, cyber interdependency, geographic interdependency and logic interdependency. six dimensions(i.e. Infrastructure Characteristics, Type of Failure, Coupling and Response Behavior, Environment, Types of Interdependencies, State of Operation) are considered for analyzing critical infrastructures interdependency. However, Mc Daniels consider it as unidirectional relationship between systems [11]. Earl et al. [12] have concluded five types of interrelationship between infrastructure systems namely, input dependence, mutual dependence, shared dependence, exclusive-or dependence and co-located dependence. The term geographic interdependency is used by Restrepo et al.[13] to denote power outages that spread across several US states. For Kjell Hausken[14], relations between infrastructures can be in parallel, series, combined series-parallel, complex, k-out-of-n redundancy, independent, interdependent, and dependent. Alessandro indicates that infrastructures show a large number of interdependencies of differing types[15]: physical interdependency when energy, material or people flow from one infrastructure to another, cyber interdependency when information is transmitted or exchanged, geographical interdependency such as the close spatial proximity of the elements of the infrastructure, logical interdependency such as financial dependence, political coordination and so on.

III. RESEARCH ON INTERDEPENDENT INFRASTRUCTURE SYSTEMS VULNERABILITY

National security, economic prosperity, and the quality of life of today's societies depend on the continuous and reliable operation of critical infrastructures. Models have been developed to capture the performance and operation of these systems to support planning, maintenance, and retrofit decision making from multiple view points.

For a single infrastructure, many researchers studied the reliability and vulnerability of infrastructure and the impact of random disturbance - deliberate attack and natural disasters on it. When there is little information about the operation of the infrastructure being analyzed, probabilistic risk analysis (PRA) methods have been developed for estimating and managing infrastructure risk[16-18]. Then historical data combined with statistical learning theory has been developed by scholars to analyze and predict natural disasters on infrastructure performance[19]. Haibin Liu et al.[20-21] analyze two types of faults may occur during natural disasters and a sophisticated statistical framework is employed to develop a model for predicting outages in future hurricanes. However neither PRA nor statistical regression models has taken into account the network topology and the impact of infrastructure layout on network performance cannot be studied.

Approaches based on graph and network theory modelling infrastructure through abstract graphs made of nodes and arcs representative of links between components in an infrastructure are then developed. Scientists have discovered complex network in the last two decades then gave in-depth research, got a lot of valuable conclusions, thus forming a complex network theory. The theory has been applied to many research areas such as equipment weapons systems, environmental protection, industrial production, network and communications, control systems, fiscal and financial, computer engineering and artificial intelligence, infrastructure systems, etc. For infrastructure systems graph and network theory have been widely used to characterize their topology, performance, and uncertainty taking advantage of closed form expressions and numerical simulations, analysis of network topology is used extensively to identify layout features linked to infrastructure reliability. [22-23] Assesses structural vulnerability against earthquakes and quantifies uncertainty in seismic risk assessment. Jian-Wei Wang and Li-Li Rong[24] investigate cascading failures induced by the intentional edge attacks in the power grid of the western United States based on load model of cascade. Water distribution systems are regarded as large sparse planar graphs with complex network characteristics.
Alireza Yazdan[25] studied water distribution network robustness and vulnerability and proposed indicators to quantify redundancy. James Winkler etc combine power network topology and component fragility damage model to study how network topology affects the reliability of the power system under natural disasters[26]. Graham Booker estimates cellular network performance when subjected to hurricane events[27]. Pertinent topological properties of electrical and other infrastructure networks are analyzed [28-30]. Risk and vulnerability of a single infrastructure is illustrated above using graph and network theory. However with the increasingly interlinked, failures may propagate between different infrastructure systems, exceeding the boundaries of a single infrastructure. Therefore, risk and vulnerability analysis cannot be studied in isolation. Relevance of the infrastructure must be considered for a perspective of global analysis.

Interdependent infrastructure is a relatively new area of research, although the United States proposed the concept of infrastructure as early as 1997, but it did not appear in the literature on the description of interdependent infrastructure until 2001, prominently in this research area includes three U.S. National Laboratories (Sandia, Argonne, Los Alamos) and a research center (National Infrastructure Simulation and Analysis Center, NISAC). Researchers begin employing network theory and other methods to model infrastructure interdependencies and take advantage of closed form expressions and numerical simulations to characterize their topology, performance, and uncertainty. Using network theory and system reliability, Dueñas-Osorio et al[31-32] present a novel approach to model the interdependent response of infrastructure networks to natural hazards and deliberate attacks. They make use of spatial proximity and logical interactions to establish the density and degree of coupling between power and water systems in their model. Svendsen et al[33-34] develop a similar graph theoretic approach for modeling interdependent infrastructure systems by enduing network nodes and arcs functional attributes. Vulnerability and flow analyses, failure propagation and crises evolution simulations have also been studied by the joint use of topological signatures and structural fragility[9,35]. Network theory provides an alternative to other modeling methods by being more physical component detailed. However, the approach alone lacks the ability to capture uncertain characteristics of an infrastructure and is unable to model event-driven links such as an instant command sent from SCADA to SUC in case of an emergency[36].

IV. OTHER MODELING TECHNIQUES

Research and implementation studies have attempted to address interdependence modeling through various techniques, such as graph theory introduced above and modeling approaches including: Object-Oriented Modeling, Agent Based simulation, Input-Output Inoperability, System Dynamics Model etc.

Object-Oriented Modeling is another approach characterizing and analyzing dynamic behaviors of infrastructure systems. In this model, behavior at individual level, and global behavior emerging as a result of many individuals are defined following its own behavior rules, living together in some environment and communicating with each other[36-37]. This model has been widely used in critical infrastructures interdependency study[38-39]. However, this approach needs a better computer configuration in order to ensure a faster simulation speed and it increases the complexity of simulation platform due to large number of parameters.

Agent Based simulation[40-41] was a methodology emerged in the early phase for modeling infrastructure interdependencies which was used to analyze the behavior of infrastructure network and its associated economic entity. In agent based simulations, infrastructures are modeled as complex adaptive systems composed of agents representing different aspects in an infrastructure system. An agent is a singular piece of code with a specific physical location, function, and memory of past interactions and behaviors. Different agents can be modeled at varying degrees of granularity based on the intended level of resolution modeling.

Another methodology for modeling infrastructure interdependencies is the Input-Output model[42-44]. In 1973 Wassily Leontief proposed the Input-Output model and got the Noble Prize. Later this model was used to establish the relationships between economic sectors and quantify the correlation between various infrastructure networks. However, the interconnectedness is still modeled among infrastructure sectors without dealing with elements of each infrastructure.

System Dynamics Model makes use of attributes in System Dynamics to characterize the functions of infrastructure systems such as production, transmission and consumption. Services and quantities of products flowing between infrastructures are used to describe infrastructures interdependencies. System dynamics based model can give a good description of functions and processes and depict dynamics features of interdependent infrastructure.

HLA[36,45], another model for interdependent infrastructure systems vulnerability analysis is a comprehensive method, a hybrid approach combining various modeling/simulation techniques in a distributed simulation environment. It was developed originally by the US Department of National Defense, aiming at incorporating interoperability, modularity into long-term simulation objectives.

Each of the modeling techniques can be used for interdependency studies although each of them has its own advantages and limitations. When selecting the appropriate approach, several factors should be considered such as task framing and information of the infrastructure, goal of the simulation, the complexity of the model/simulation and evaluated scope etc.
V. A FRAMEWORK FOR THE VULNERABILITY ANALYSIS OF INFRASTRUCTURES

As the complexity of critical infrastructure systems structure, risk analysis becomes more interdisciplinary, risk management becomes more cross-institutional. In practice, there is no ‘silver bullet solution’ to the problem of analyzing vulnerability of critical infrastructure systems. Absolutely comprehensive, integrative approach to these issues becomes too difficult. So a framework of analysis is necessary and seems to be needed to effectively integrate the different methods in this area. The proposed methodical framework for the vulnerability analysis of critical infrastructures is described in table 1.

In the preparatory phase, we aim at reaching a clear understanding of the objective purpose and goal to be researched. Critical infrastructure systems such as telecommunications, power, transportation, and water constitute the so-called lifeline systems which suffer constant threat from malicious attacks and natural disasters should be understood. These threats include failures induced by natural disasters such as earthquakes, hurricanes, storms, ice and those induced by random failure, such as operation errors, aging, animals, vandalism, etc and those induced by intentional disruption: Terrorist attacks, etc.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Evaluated Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method For Vulnerability Analysis</td>
<td>Network theory, Dynamic, Agent-based, Monte Carlo simulation Statistical Methods,</td>
</tr>
<tr>
<td>Type of Interdependency</td>
<td>Physical, Geographic, Cyber, Economic, Geographic, Logical</td>
</tr>
<tr>
<td>Task framing and Information of the Infrastructure</td>
<td>Operational state, Complexity, Type of fault propagation</td>
</tr>
<tr>
<td>Evaluated Scope</td>
<td>- Structural and Functional Dimensions - Risk, Robust, reliability</td>
</tr>
<tr>
<td>Types of effects may confer vulnerability on a system</td>
<td>1. Direct infrastructure effects 2. Indirect infrastructure effects. 3. Exploitation of infrastructure.</td>
</tr>
<tr>
<td>Development of adequate system understanding</td>
<td>Functioning, Dependencies, Interconnectedness, type of disaster spread etc</td>
</tr>
<tr>
<td>Evaluation of statistical data</td>
<td>bottlenecks, deficits in design, operation, maintenance, emergency procedures</td>
</tr>
<tr>
<td>Topology-driven analysis of vulnerabilities</td>
<td>Severity of consequence etc.</td>
</tr>
<tr>
<td>Provision of Modeling techniques</td>
<td>Component based modeling System performance modeling and simulation techniques Modeling and simulation between coupling infrastructure</td>
</tr>
<tr>
<td>System Improvement</td>
<td>Infrastructure Protection Infrastructure repair Research agenda To determine mitigation strategies helpful for design or improvement of the performance of systems To establish a framework for addressing additional research questions</td>
</tr>
<tr>
<td>Identification Of Result</td>
<td>Satisfied or not Yes: next phase No: return</td>
</tr>
<tr>
<td>Decision Supporting</td>
<td>Suggestions for system owner and operator</td>
</tr>
</tbody>
</table>

Tab.1: A framework for the vulnerability analysis of critical infrastructures
common objectives are risk and vulnerability analysis, risk mitigation measures and infrastructure protection, failure propagation prediction, and interdependence modeling and simulation. Risk, function and operating mechanisms and other definition of the terms should be understood for further analysis. There are many ways for the vulnerability analysis of infrastructures such as Network theory, Dynamic, Agent-based, Monte Carlo simulation Statistical Methods and so on. Here network theory based approaches are illustrated in this paper as an example.

After we get a fundamental understanding about the task framing and related information, information of the infrastructure should be collected and Network characterization should be done. Statistical parameters need to be investigated for description of network topology and performance metrics will be developed for quantifying generic network function. Evaluated scope includes structural level and functional level. To build adequate performance analysis the analysis on structural level will be helpful to design or improve the infrastructures in the long run while the discussion on functional level will be useful in the short period. Modeling critical Infrastructures is a key problem in basic research of complex systems and for the technological activities aimed at analyzing and controlling large infrastructures. The models presented in the literature have various objectives such as network theory, dynamic, agent-based, Monte Carlo simulation and statistical Methods. Network theory modeling approaches adopted in this paper are used for the performance analysis of electricity network because of unique network characteristics of the power systems. For purposes of broad comparative analysis, other modeling techniques can be used. In the part of network improvement, depending on the obtained results and related feedbacks we need to identify infrastructure protection, and then select or prioritize the options that would best improve infrastructure mitigation strategies need to be determined that ensure continuous functionality of systems especially when resources are limited and a research agenda needs to be established for addressing additional research questions revealed by the analysis. The final decision about actually implementing the proposals of improvement is left to the system owner and operator, works done in this paper can provide a decision support for decision-making departments.

REFERENCES


