Safety Science 51 (2013) 328–337

Contents lists available at SciVerse ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Vulnerability analysis of interdependent infrastructure systems under edge attack strategies

Shuliang Wang [a,b], Liu Hong [a,*], Min Ouyang [a], Jianhua Zhang [a], Xueguang Chen [a]

[a] Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, PR China
[b] Department of Information Science and Engineering, Chongqing Jiaotong University, Chongqing 400074, PR China

ARTICLE INFO

Article history:
Received 1 November 2011
Received in revised form 13 June 2012
Accepted 24 July 2012
Available online 8 September 2012

Keywords:
Interdependent infrastructure systems
Critical components
Vulnerability analysis
Edge attack strategies

ABSTRACT

Infrastructure systems construct the cornerstone of modern society, they become more and more interconnected and interdependent on multiple levels. Therefore protecting them from various disturbances become an active topic of research in safety science. This paper takes power and gas pipeline systems as example and focuses on the following problems: edge attack strategies and critical components. Applying network model the authors analyse interdependent responses under three types of edge disturbance strategies, and give a method for ranking critical components. Meanwhile, different interface design strategies are illustrated to minimize cascading failures. It has shown that the effects of different attacks on systems connectivity against cascading failures have close relations with the tolerate parameter. In addition, the results show interdependent systems with degree based interfaces provide good stability and good performance. Simultaneously it is represented that critical components for independent cases are those with high loads and connections. However, due to interdependency, critical components for interdependent cases have some differences compared to independent ones and can result in more performance losses, they should be protected with prior consideration. Provided by the results of the research, it is helpful to better shape an expansion of the systems, infrastructure owners could model different event scenarios and assess their impact on the systems.

1. Introduction

Critical infrastructure systems which are often called lifeline systems refer to the framework of systems comprising identifiable industries, institutions, and distribution capabilities (Presidential Decision Directive), they provide a reliable flow of products and services essential to the defense and economic security of the society. Infrastructure does not exist in isolation, but interconnect with each other. With the development of scientific technology and social economy, these infrastructure systems become more and more complicated and mutually dependent. Once the systems are disturbed by external or internal perturbations, the failures can spread very rapidly to other correlative infrastructure systems, sometimes they even return to the originated infrastructures which may cause the whole systems lose its function and collapse (Chang et al., 1996; O'Rourke, 2007; Adachi and Ellingwood, 2008). Increasing interconnectivities among critical infrastructure systems have made them more vulnerable than before.

Widespread losses of these systems can be very disruptive, they can cause great economic losses and physical disruptions, amplifying negative consequences and affecting unforeseeable and haphazard sets of users. An example of infrastructure disruptions is the major power blackout on August 14, 2003, the event lasted up to 4 days and led to 50 million people affected in at least ten northeastern states of the USA and one Canadian province, it caused traffic's congestion and affected many other critical infrastructures, the estimated direct costs were about $10 billion. Another example is the 2008 South-China snow storm disaster. Many infrastructure systems are badly affected by the advent of the snow storm. During that time, electricity, transportation, communication, houses and farmland had been seriously damaged. More seriously, apart from direct disruptions, economic losses and failures of services resulted from indirect influences due to interdependency were even greater. For example, the traffic which was influenced by the snow storm further threatened the electric power infrastructure which required coal transportation for its generation. subsequently, rescue was delayed due to inadequate power resources and bad traffic conditions.

These examples illustrate that disruptions may exceed the boundaries of a single infrastructure due to interdependency and cause significant damages. In purpose of protecting "the well-being of the population, functioning of government, and economic capabilities", risk and vulnerability analysis of interdependent infrastructure systems becomes a major concern, and an active topic of research. A lot of effort has been spent on analysing infrastructure

* Corresponding author. Tel./fax: +86027 87540084.
E-mail address: hongliu1978@mail.hust.edu.cn (L. Hong).

0925-7535/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ssci.2012.07.003

risk and vulnerabilities, and various methods have been proposed on this area.

As for the power system, taking into account historical data combined with statistical theory, vulnerability analysis under natural disasters has been developed (Davidson et al., 2003; Liu et al., 2005, 2009). On the other hand, with view to the intrinsic dynamics of the load of physical quantities, many important aspects of cascading failures have been considered and discussed, for instance, the performance of the network under cascade-based attacks (Motter et al., 2002; Wang and Rong, 2008; Wang et al., 2008), cascading failures in real networks (Albert et al., 2004), connectivity recovery (Zhang et al., 2011) and so on. However, these studies merely concentrate on cascading failures induced by the node overload breakdown, the edge failures are often overlooked, what's more, each of these systems has essentially evolved independently. While infrastructure systems have become more interconnected with each other, failures may propagate between different infrastructure systems, exceeding the boundaries of a single infrastructure, therefore risk and vulnerability analysis should not be studied in isolation.

In recent years, researchers have focused on modeling interdependent infrastructure systems. First, the concept of interdependency is investigated. There are different explanations of interdependency in the literatures by different standards. Rinaldi et al. (2001) consider the concept of interdependency as a bidirectional relationship between two infrastructures and categorize four general types of interdependency: physical interdependency, cyber interdependency, geographic interdependency and logic interdependency. However, McDaniels et al. (2007) consider it as unidirectional relationship between systems. Earl et al. (2007) have concluded five types of interrelationship between infrastructure systems. Namely, input dependence, mutual dependence, shared dependence, exclusive-or dependence and co-located dependence. For Hausken (2010), relations between infrastructures can be inparallel, series, combined series–parallel, complex, k-out-of-n redundancy, independent, interdependent, and dependent. Vespignani (2010) indicates that infrastructures show a large number of inter-dependencies of differing types. Then different methods such as complex network theory, agent-based method, input–output method, and other hybrid approaches have been developed for interdependency studies. Complex network theory is an approach that graphically represents the coupling phenomenon between different infrastructures as a set of nodes linking to a set of edges, it has been widely used to characterize infrastructures topologies and layout features by taking advantage of closed form expressions and numerical simulations (Koutsourelakis, 2010; Ellingwood and Kinali, 2009). Agent Based Modeling (ABM) method (Borshchev and Filippov, 2004; Tolk and Uhrmacher, 2009) is another methodology that can be used for modeling infrastructure interdependency. In agent based simulations, infrastructures are modeled as complex adaptive systems composed of agents representing different aspects in infrastructure systems, an agent is a singular piece of code with a specific physical location, function and memory of past interactions and behaviors. Meanwhile, input–output model (Leung et al., 2007; Haimes et al., 2005) is used to establish the relationships between economic sectors and quantify the correlation between various infrastructure networks. High Level Architecture (HLA) (Nan and Eusgeld, 2011; Eusgeld and Nan, 2011) is a general architecture for modeling and simulating complex distributed systems, combining HLA and various modeling/simulation techniques in a distributed simulation environment, a hybrid approach is constructed for vulnerability analysis. However, studies mainly consider infrastructure systems with fixed interdependent topologies or relationships, different interface design strategies based on infrastructure topological properties have attracted little attention (Ouyang and Duenãs-Osorio, 2011). We believe that analyzing interdependent infrastructure systems with different interface design criterias are essential for network security, meanwhile cascading failures on edges are as important for vulnerability analysis as those on nodes. Motivated by these opinions, this paper takes power and gas pipeline systems as example, and focused on vulnerability analysis of interdependent infrastructure systems under edge attack strategies with different interface design criteria.

The rest of this article is structured as follows: Firstly, a methodological framework to analyze interdependent infrastructure systems vulnerability is introduced in Section 2. Modeling techniques and disturbance strategies are presented, perspectives on vulnerability and interdependency as well as interface topologies design strategies will be also introduced in this section. Section 3 further analyzes the results, and a detailed vulnerability analysis of the interdependent systems are illustrated, additionally, critical components of the power network for both independent and interdependent cases will be researched in this section. Then in Section 4 implications of the study to infrastructure improvement and decision making are discussed. Finally, conclusions and a discussion of future research consideration are presented in Section 5.

2. Methodology for interdependent infrastructure systems vulnerability analysis

In this section, a methodological framework (Fig. 1) for analysing the vulnerability of interdependent infrastructure systems is introduced. Firstly, we aim at reaching a clear definition of the terms and getting a mutual understanding of the systems researched, environment and state of operation will also be described to better comprehend the systems. Then the topology of each infrastructure researched need to be extracted. Using complex network theory, infrastructure systems such as power and gas can be described as networks composed by nodes and edges, topology characteristics to each of the infrastructure systems can be extracted. Next, based on operation mechanism, function characteristic to each of the infrastructure systems is abstracted. With regard to the power grid cascading failures based on load redistribution of edges are analysed. As for the gas pipeline system, a generalized betweenness centrality model is applied to analyse the function property. Meanwhile infrastructure systems often suffer various threats, which include failures induced by natural disasters, random failure and those induced by malicious attacks. These threats to infrastructure systems can cause great losses and amplify negative consequences, types of threats need to be identified for vulnerability analysis. At the same time, modeling of interdependency are processed, due to interdependency between different infrastructure systems, the functions of infrastructure systems are mutually affected. Once the systems are disturbed by external or internal perturbations, disruptions of components from one system may cause components in the other systems to fail, too. When some initial failures of components arise, they may trigger are cursive process of cascading failures that can damage the systems seriously. So a good understanding of interdependency across infrastructure systems is necessary. Aspects such as interdependent type, interdependent strength, and interdependent effect need to be identified. On the other hand, in addition to vulnerability analysis of interdependent infrastructure systems with fixed interdependent topologies, analyzing interdependent infrastructure systems with different interface design criteria is essential for network security, they play a key role in operation and failure propagation. Different interface design strategies based on topological properties are proposed to find the optimum design under edge attack strategies.