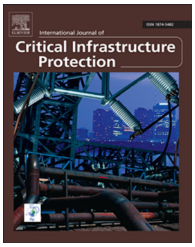
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Risk mitigation strategies for critical infrastructures based on graph centrality analysis

George Stergiopoulos[a], *Panayiotis Kotzanikolaou*[b], *Marianthi Theocharidou*[c,*], *Dimitris Gritzalis*[a]

[a]*Information Security and Critical Infrastructure Protection Laboratory, Department of Informatics, Athens University of Economics and Business, 76 Patission Avenue, GR-10434 Athens, Greece*

[b]*Department of Informatics, University of Piraeus, 85 Karaoli and Dimitriou, GR-18534 Piraeus, Greece*

[c]*Security Technology Assessment Unit, Institute for the Protection and the Security of the Citizen, European Commission Joint Research Centre, via E. Fermi 2749, I-21027 Ispra, Italy*

ARTICLE INFO

Article history:
Received 8 January 2015
Received in revised form
4 May 2015
Accepted 13 May 2015

Keywords:
Critical infrastructures
Dependency risk graphs
Graph centrality
Cascading failure
Information gain
Feature selection
Mitigation

ABSTRACT

Dependency risk graphs have been proposed as a tool for analyzing cascading failures due to critical infrastructure dependency chains. However, dependency chain analysis is not by itself adequate to develop an efficient risk mitigation strategy – one that specifies which critical infrastructures should have high priority for applying mitigation controls in order to achieve an optimal reduction in the overall risk. This paper extends previous dependency risk analysis research to implement efficient risk mitigation. This is accomplished by exploring the relation between dependency risk paths and graph centrality characteristics. Graph centrality metrics are applied to design and evaluate the effectiveness of alternative risk mitigation strategies. The experimental evaluations are based on random graphs that simulate common critical infrastructure dependency characteristics as identified by recent empirical studies. The experimental results are used to specify an algorithm that prioritizes critical infrastructure nodes for applying controls in order to achieve efficient risk mitigation.

1. Introduction

(Inter)dependencies between critical infrastructures are a key factor in critical infrastructure protection because they may allow a failure that is seemingly isolated in one critical infrastructure to cascade to multiple critical infrastructures. One way to analyze critical infrastructure dependencies is to use dependency risk graphs whose nodes represent critical infrastructures or components and directed edges represent the potential risk that the destination node may suffer due to its dependency on the source node in the event of a source node failure.

Kotzanikolaou et al. [7–9,14,15] have proposed a risk based methodology for assessing the cumulative risk of dependency risk paths – chains of critical infrastructure nodes that are (inter)connected due to their (inter)dependencies. The methodology uses as input existing risk assessment results from critical infrastructure operators and, based on the first-order dependencies between critical infrastructures, assesses the potential risk values of all the n^{th}-order dependency risk

*Corresponding author.
E-mail address: marianthi.theocharidou@jrc.ec.europa.eu (M. Theocharidou).

http://dx.doi.org/10.1016/j.ijcip.2015.05.003

chains. By computing and sorting all the dependency risk paths, a risk assessor may identify the most critical dependency chains by examining all potential dependency risk paths with cumulative risk above a predefined threshold.

Although the identification of the most important dependency chains is a key step towards efficient risk mitigation, certain open problems exist. A simple mitigation strategy is to apply security controls at the root node of each critical dependency chain. However, this may not always be a cost effective strategy because the effects on some nodes may not be measured properly. For example, consider the case where a small subset of nodes (not necessarily the roots of critical chains) affect a large number of critical dependency paths. Decreasing the probability of failure of these nodes by selectively applying security controls to them may result in a greater overall risk reduction. Another example is when nodes of high importance exist outside the most critical dependency paths (such as nodes that simultaneously affect many other nodes that belong to the set of most critical paths, or nodes that affect the overall dependency risk of the entire structure/graph).

Most current risk mitigation methodologies are empirical in nature and typically focus on critical infrastructures that initiate cascading failures (e.g., energy and information and communications infrastructures). By studying actual large-scale failures, it is clear that the two sectors often initiate serious cascading effects in interdependent critical infrastructures (e.g., the famous California blackouts of 2000 and 2001, and the Northeast Blackout of 2003). Nevertheless, focusing on some sectors and on potential initiators may not be suitable in every case. Therefore, the impact of each dependency should be considered along with the position of each critical infrastructure within the network of interdependent critical infrastructures.

The systematic identification of the most important nodes and the prioritization of nodes for applying security controls can be complex tasks. The need for a high-level and efficient risk mitigation technique that considers multiple characteristics of interdependent critical infrastructures is clear [3]. An optimal risk mitigation methodology would help identify the smallest subset of critical infrastructures that yields the highest overall risk reduction in a risk graph, although the candidate nodes may not initiate critical paths or may not even belong to the most critical paths.

This paper explores the use of graph centrality metrics in dependency risk graphs in order to prioritize critical infrastructures when applying risk mitigation controls. Alternative risk mitigation strategies are implemented algorithmically and subsequently evaluated empirically using simulations. The ultimate goal is to identify the minimum subset of critical infrastructure nodes in a dependency risk graph whose risk treatment (application of security controls) would result in the maximum risk reduction in the entire graph of interdependent critical infrastructures. The approach incorporates three key extensions: (i) data mining techniques to identify correlations between centrality metrics and high impact critical infrastructure nodes in a dependency risk graph; (ii) optimum centrality metrics to develop and test various risk mitigation strategies that maximize risk reduction; and (iii) analysis of nodes with high numbers of inbound (sinkholes) and outbound connections and the comparison of their risk reduction results.

Experiments were conducted on hundreds of random graphs with randomly selected dependencies in order to validate the proposed mitigation strategies. The random graphs were created to satisfy the constraints encountered in real-world interconnected critical infrastructures. The experimental results demonstrate the efficiency of the proposed risk mitigation strategies. The mitigation strategies can be used proactively to analyze interconnections in large-scale interdependent infrastructures and pinpoint underestimated or ignored infrastructures that are, in fact, critical to reducing the overall risk.

2. Building blocks

The proposed methodology has three building blocks: (i) dependency risk graphs and a multi-risk dependency analysis methodology for modeling cascading failures; (ii) graph centrality metric based analysis of dependency risk graphs; and (iii) feature selection techniques that help evaluate the effects of centrality metrics on risk mitigation. This section briefly describes the three building blocks.

2.1. *Multi-risk dependency analysis methodology*

A dependency is defined as “the one-directional reliance of an asset, system, network or collection thereof – within or across sectors – on an input, interaction or other requirement from other sources in order to function properly” [17]. The methodology described in this paper extends the dependency risk methodology of Kotzanikolaou et al. [7,8], which was developed to analyze multi-order cascading failures.

2.1.1. *First-order dependency risk*

Kotzanikolaou et al. [7,8] initially consider first-order dependencies between critical infrastructures and go on to model n^{th}-order dependencies. Each dependency from a node CI_i to a node CI_j is assigned an impact value $I_{i,j}$ and likelihood value $L_{i,j}$ of a disruption. Note that the impact and likelihood values are assumed to be obtained from organization-level risk assessments performed by critical infrastructure operators. The product of $I_{i,j}$ and $L_{i,j}$ is the dependency risk $R_{i,j}$ of infrastructure CI_j due to its dependency on CI_i. Dependencies are visualized in a graph $G=(N,E)$ where N is the set of nodes (or infrastructures or components) and E is the set of edges (or dependencies). The graph is directional and a destination critical infrastructure receives a risk from a source critical infrastructure as a result of its dependence on the source infrastructure.

2.1.2. *Extension to n^{th}-order dependency risk*

Let $\mathbb{CI}=(CI_1,\ldots,CI_m)$ be the set of all the considered critical infrastructures. An algorithm proposed by Kotzanikolaou et al. [7,8] examines each critical infrastructure as a potential root node of a cascading effect. Let CI_{Y_0} denote a critical infrastructure that is the root of a dependency chain and $CI_{Y_0}\rightarrow CI_{Y_1}\rightarrow\ldots\rightarrow CI_{Y_n}$ denote the corresponding chain of length n. Then, the algorithm computes the cumulative

Please cite this article as: G. Stergiopoulos, et al., Risk mitigation strategies for critical infrastructures based on graph centrality analysis, International Journal of Critical Infrastructure Protection (2015), http://dx.doi.org/10.1016/j.ijcip.2015.05.003