Reliability Engineering and System Safety 119 (2013) 11–17

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

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

Evaluating the damage associated with intentional supply deprivation in multi-commodity network

G. Levitin [a,b,*], I. Gertsbakh [c], Y. Shpungin [d]

[a] Collaborative Autonomic Computing Laboratory, School of Computer Science, University of Electronic Science and Technology of China, China
[b] The Israel Electric Corp., PO Box 10, Haifa 31000, Israel
[c] Department of Mathematics, Ben Gurion University, Beersheva, Israel
[d] Department of Software Engineering, Sami Shamoon College of Engineering, Beersheva, Israel

ARTICLE INFO

Article history:
Received 9 August 2011
Received in revised form
18 October 2012
Accepted 5 May 2013
Available online 11 May 2013

Keywords:
Network
Multi-commodity supply
Supply deprivation
Attack
Defense
Link failure
Damage

ABSTRACT

This paper presents a method for evaluating an expected damage associated with nodes deprivation of supply of commodities in multi-commodity networks with a given topology as a result of intentional attack on randomly chosen network links. The method is based on a Monte Carlo simulation approach for evaluating the expected number of nodes deprived of all possible subsets of commodities. It also uses the contest success function that evaluates destruction probability of individual links as a function of per-link attack and defense efforts. It is assumed that the defender has no information about the attacker's actions and the attacker has no information about the network structure. The method allows the analysts to compare different solutions of expected damage reduction under conditions of uncertainty. Illustrative examples are presented.

1. Introduction

Defense against external impacts, and especially against intentional external impacts, becomes increasingly important due to the increasing threats of malicious attacks [1–7]. The defender's objective for a system is that it survives and functions reliably under all circumstances. In order to evaluate the efficiency of defensive measures the defender should evaluate the effect of these measures on the expected damage that can be caused by attacks. The main difference between the unintentional impacts (caused by natural disasters or accidents) and intentional impacts (caused by attacker's malicious actions) is in resource distribution. If the attacker attacks several objects, it has to distribute its limited resources among these objects. In contrast, the magnitude of the impact of an accident/disaster on any given object does not depend on the number of objects exposed to the impacts.

Most critical infrastructures that are vital to the economic and societal well-being can be described as delivery or service networks. Research in network reliability and risk analysis must help us to understand how to prevent or mitigate the damage caused by intentional attacks on the networks. An area of research that concentrates on understanding how attacks on network components affect the entire network performance is the area of network interdiction [8–16]. It is usually assumed that an interdictor (attacker) is interested in reducing the flow through the network by interdicting (destroying) network elements, usually the links. Moreover, it is assumed that the interdictor has limited resources to interdict network elements and as such it faces a resource allocation problem, where the objective is to maximize the damage inflicted to the network (i.e. minimize the source-sink flow in the network or maximize the probability that this flow lowers below a required level). In [17] the case when the network provides connection among different terminal nodes corresponding to users or critical facilities is considered and a tool that evaluates the probability of network disintegration into disconnected sub-networks and estimates the associated damage is suggested.

In [18,19] the multi-commodity networks survivability is considered. It is assumed that different commodities must be supplied through network links and node-to-node demands must be routed across the network subject to link capacity restrictions. The robust network design must build enough capacity and diverse routing paths through the network to ensure that feasible multi-commodity flows continue to exist, even when some components of the network are destroyed by attacks.

This paper also deals with multi-commodity networks and assumes that each network node needs supply of all types of commodities. The sources of commodities are located at different nodes (the same commodity can be supplied from different

* Corresponding author at: The Israel Electric Corp., PO Box 10, Haifa 31000, Israel.
E-mail address: levitin@iec.co.il (G. Levitin).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.05.002

Nomenclature

$\boldsymbol{E}$	set of links in the network
L	number of links in the network $L=\|\boldsymbol{E}\|$
$\boldsymbol{H}$	set of nodes in the network
h	number of nodes in the network $h=\|\boldsymbol{H}\|$
k	number of attacked links
R	entire attacker's resource
y	attacker's impact effort per attacked link
z	defender's protection effort per link
$v(y,z)$	link vulnerability as a function of attacker's and defender's efforts
$q_j(k)$	probability that exactly j links are destroyed after attack on k links
$\boldsymbol{\Phi}$	set of supplied commodities
$\boldsymbol{T}_s$	set of terminals that supply commodity s
G	number of terminals in the network
N	$\|\boldsymbol{\Phi}\|$, number of supplied commodities
$\boldsymbol{\phi}_f$	fth subset of supplied commodities
$d(f)$	per-node damage associated with losing the supply of subset f of commodities
$n(j,f)$	average number of the network nodes that lose supply of subset of commodities $\boldsymbol{\phi_f}$ as a result of destruction of j randomly chosen links
$\varepsilon(i)$	probability that i links are attacked
$^{\triangle}R$	expected damage under assumption that the attacker chooses random number of attacked links
$^{\triangle}W$	expected damage under assumption that the attacker chooses the most harmful number of attacked links
m	contest intensity

terminals located at different nodes). The deprivation of any node from supply of any commodity is associated with certain damage. The damage at each node depends on the set of commodities the node is deprived from. The total damage caused by the attack depends on the amount of nodes deprived from different sets of commodities. The novelty of the suggested approach is threefold:

- unlike the previous research dealing with the reduction to source-sink flows for different commodities, it considers the damages associated with nodes deprivation from any possible subsets of commodities;
- it assumes that different commodities can be supplied from arbitrary sets of terminal nodes, which allows to evaluate the effect of addition of terminals on the system survivability;
- it takes into account the optimal attack resource distribution by assuming that the link destruction probability depends on the per-link attack effort and the attacker can choose the number of links to attack.

Using the proposed method analysts can evaluate the effect of such defense measures as link protection enhancement, network structure changes and commodity source relocation on the expected damage that can be caused by intentional attack. By comparing the effect of different combinations of the defense measures one can choose the most effective defense strategy. To the best of our knowledge, such practical tools for evaluating efficiency of different defense strategies for multi-commodity networks with multiple sources did not exist previously.

In this paper we consider a network which has a node set $\boldsymbol{H}$, edge (link) set $\boldsymbol{E}$ and a subsets $\boldsymbol{T}_s \subseteq \boldsymbol{H}$ of special nodes called terminals. All terminals belonging to T_s supply commodity s. The total number of terminals in the network is $G=\sum_{s=1}^{N}|\boldsymbol{T}_s|$. All nodes are considered as absolutely reliable ones while the edges are subject to failure as a result of the attacker action. Edge (link) failure means its elimination from the network. The nodes represent customers, important infrastructure centers, etc. The links represent the road segments, communications and supply channels, etc. It is assumed that any node gets supply of commodity s if a path exists between this node and at least one terminal node belonging to set $\boldsymbol{T}_s$.

Observe that the assumption of full nodes reliability does not prevent the possibility to model the influence of the nodes destruction on system connectivity and damage associated with the attacks. Indeed, the destruction of any node can be easily modeled by simultaneous elimination of all incident links corresponding to this node.

The attacker strikes the network links trying to cause damage by depriving the network nodes from supply of as many commodities as possible. The extent of the damage depends on the number of nodes suffering from this deprivation. It is assumed that both the attacker and the defender have limited and fixed resources. The attacker does not know the network structure, and attacks a randomly chosen subset of links distributing its attack resources evenly among these links. However, the attacker can choose the number of links to attack, determining, thereby, the per-link attack effort. The defender has no information about the subset of links chosen for the attack. All links are equally protected (we consider the case when the defender has no organizational or technological possibility to protect the links differently).

The model presented in this paper is based on a Monte Carlo simulation algorithm. This algorithm is based on a so-called disjoint set structure (DSS) presentation of the network on each stage of its destruction as a collection of isolated connected components (clusters). It allows obtaining, for each number of failed links, an accurate estimate of the average number of nodes deprived of supply of any set of commodities.

2. Problem formulation

We consider a network with a given topology. The network contains L protected links. Each link is protected with effort z. The attacker strikes k randomly chosen links. The attacker has resource R and distributes it evenly among the attacked edges (links), so that the per-link attack effort is $y=R/k$. We assume that the vulnerability of attacked link is determined by a contest between the defender and the attacker. The contest is expressed by a contest success function modeled with the common ratio form [20,21] as

$$v=\frac{y^m}{y^m+z^m}. \tag{1}$$

The contest success function was initially used in rent seeking literature and expresses the success of agents in securing a rent dependent on efforts exerted [20,21]. Higher effort gives higher success, but is also costly. There are several different forms of the contest success function. The common ratio form (1) is the most simple, flexible and analytically tractable [22]. Recently this form has been used in several models of optimal system defense [6,7,14]. Skaperdas [20] offered three axioms for contest success functions that make them suitable for representing the object vulnerability as a function on the attacker's efforts. First, $1\geq v\geq 0$ and the contest success for the defender and attacker sum to one