Towards a Metric for Communication Network Vulnerability to Attacks: A Game Theoretic Approach

Assane Gueye[1], Vladimir Marbukh[1], and Jean C. Walrand[2]

[1] National Institute of Standards and Technology, Gaithersburg, USA
[2] University of California, Berkeley, USA*

Abstract. In this paper, we propose a quantification of the vulnerability of a communication network where links are subject to failures due to the actions of a strategic adversary. We model the adversarial nature of the problem as a 2-player game between a network manager who chooses a spanning tree of the network as communication infrastructure and an attacker who is trying to disrupt the communication by attacking a link. We use previously proposed models for the value of a network to derive payoffs of the players and propose the network's expected *loss-in-value* as a metric for vulnerability. In the process, we generalize the notion of *betweenness* centrality: a metric largely used in Graph Theory to measure the relative *importance* of a link within a network. Furthermore, by computing and analyzing the Nash equilibria of the game, we determine the actions of both the attacker and the defender. The analysis reveals the existence of subsets of links that are more critical than the others. We characterize these critical subsets of links and compare them for the different network value models. The comparison shows that critical subsets depend both on the value model and on the connectivity of the network.

Keywords: Vulnerability Metric, Value of Communication Network, Spanning Tree, Betweenness Centrality, Critical Links, Nash Equilibrium.

1 Introduction

"...one cannot manage a problem if one cannot measure it..."

This study is an effort to derive a metric that quantifies the vulnerability of a communication network when the links are subject to failures due to the actions of a strategic attacker. Such a metric can serve as guidance when designing new networks in adversarial environments. Also, knowing such a value helps identify the most critical/vulnerable links and/or nodes of the network, which is an important step towards improving an existing network. We quantify the

* This material is based in part upon work supported by the NIST-ARRA Measurement Science and Engineering Fellowship Program award 70NANB10H026, through the University of Maryland.

V. Krishnamurthy et al. (Eds.): GameNets 2012, LNICST 105, pp. 259–274, 2012.

vulnerability as the *loss-in-value* of a network when links are attacked by an adversary. Naturally, the first question towards such quantification is: "what is the *value* of a communication network?"

The value of a network depends on several parameters including the number of agents who can communicate over it. It is widely accepted that the utility of a network increases as it adds more members: the more members a network has, the more valuable it is. But, there ends the consensus. There is no unanimity on how much this value increases when new members are added, and there is very little (if not zero) agreement on how important a given node or link is for a network. Experts also do not concur on how much value a given network has.

Attempts to assess the utility of a communication network as a function of the number of its members include the proposition by David Sarnoff [1] who viewed the value of a network as a linear function of its number of nodes $\mathcal{O}(n)$. Robert Metcalfe [7] has suggested that the value of a network grows as a function of the total number of possible connections ($\mathcal{O}(n^2)$). David Reed ([4], [16], [17]) has proposed an exponential ($\mathcal{O}(2^n)$) model for the utility of a network. For Briscoe *et. al.* ([13], [3]) a more reasonable approximation of the value of a network as a function of the number of nodes is $\mathcal{O}(nlog(n))$. Finally, the authors of the present paper have considered a power law model where the value of a network is estimated as $\mathcal{O}(n^{1+a}),\ a \leq 1$. The parameter a is a design parameter and needs to be specified. Details of these value models are discussed later in section 2.1.

Each of these very generic models is suitable for a particular network setting, as we will see later. However, they all have a number of limitations; two of which are particularly of interest to us: *They do not take into account the topology of the network nor do they consider the way in which traffic is being carried over the network.* In this paper, we build upon these models and use them in the process to quantify the vulnerability of a network. More precisely, we use the models as a proof of concept for defining the importance of network links *relative to spanning trees.* With this definition, we are implicitly considering networks where information flow over spanning trees. The topology is also taken into account because the set of spanning trees of the network has a one-to-one correspondence with its topology. We are particularly interested in an adversarial situation where links are the target of an attacker. We use a game theoretic approach to model the strategic interaction between the attacker and the defender[1].

Our focus on spanning trees is not a limitation as the techniques of the paper can be used to study other scenarios where the network manager chooses *some* subset of links (shortest path, Hamiltonian cycle, etc...) and the attacker is targeting more than one link as can be seen in Gueye [8, Chap. 4]. However, spanning trees have a number of desirable properties that have made them a central concept in communication networking. The Spanning-Tree Protocol (STP-802.1D 1998–[14] and [15]) is the standard link management protocol used in Ethernet networks.

[1] Throughout this paper the call the defender a "network manager". The defender can be a human or an automata that implements the game.

When communication is carried over a spanning tree, any node can reach any other node. In that sense, a spanning tree can be said to deliver the maximum *value* of the network (indeed this ignores the cost of communication). This value can be determined by using one of the models cited above. Now, assuming that information flows over a given spanning tree, two scenarios are possible when a link of the network fails.

If the link does not belong to the spanning tree, then its failure does not affect the communication. If, on the other hand, the link belongs to the spanning tree, then the spanning tree is separated into two subtrees, each of them being a connected subnetwork and also delivers some value. However, the sum of the values delivered by the two subnetworks is expected to be less than the value of the original network. We define the *importance* of the link, relative to the spanning tree, to be this *loss-in-value* (LIV) due to the failure of the link.

Link failures may occur because of random events (faults) such as human errors and/or machine failures: this is dealt with under the subject of *reliability* and *fault tolerance* [12]. They also can be the result of the action of a malicious attacker whose goal is to disrupt the communication. It is this type of failure that is the main concern of this paper. A network manager (defender) would like to avoid this disruption by choosing an appropriate communication infrastructure. We model this scenario as a 2-player game where the defender is choosing a spanning tree to carry the communication in anticipation of an intelligent attack by a malicious attacker who is trying to inflict the most damage. The adversary also plans in anticipation of the defense. We use the links' LIV discussed above to derive payoffs for both players.

Applying game theoretic models to the security problem is a natural process and it has recently attracted a lot of interest (see surveys [18], [11]). In this paper, we set up a game on the graph of a network and consider the Nash equilibrium concept. We propose the expected LIV of the game for the network manager as a metric for vulnerability. This value captures how much loss an adversary can inflict to the network manager by attacking links. By analyzing the Nash equilibria of the game, we determine the actions of both the attacker and the defender. The analysis reveals the existence of a set of links that are most critical for the network. We identify the critical links and compare them for the different network value models cited above. The comparison shows that the set of critical links depends on the value model and on the connectivity of the network.

In the process to quantifying the *importance* of a communication link, we propose a generalization of the notion of betweenness centrality which, in its standard form, is defined with respect to shortest paths ([6]). We consider networks where information flow over spanning trees, hence we use spanning trees in lieu of paths. Our generalization allows both the consideration of arbitrary (instead of binary) weights of the links as well as preference for spanning tree utilization.

The remainder of this paper is organized as follows. The next section 2.1 discusses the different network value models that we briefly introduced above. We use these models to compute the relative importance of the links with respect to spanning trees. This is shown in section 2.2, followed by our generalization of the notion of betweenness centrality in section 2.3. The strategic interaction between the network manager and the attacker is modeled as a 2-player game which is presented in section 3.1. The Nash equilibrium theorem of the game is stated in section 3.2 followed by a discussion and analysis of its implications in section 4. Section 4.1 discusses our choice of metric for the vulnerability of a network. In section 4.2 we compare the critical subsets of a network for the different value models cited above. Concluding remarks and future directions are presented in section 5. All our proofs are presented in the appendix of our online report [9].

2 On the Value of Communication Networks

The value of a network depends on several parameters including the number of nodes, the number of links, the topology, and the type of communication/information that is carried over the network. Assessing such value is a subjective topic and, to the knowledge of the authors, there is no systematic quantification of the value of a communication network. Next, we discuss some attempts that have been made to measure the utility of a network as a function of its number of nodes.

2.1 Network Value Models

Sarnoff's Law:
Sarnoff's law [1] states that *the value of a broadcast network is proportional to the number of users* ($\mathcal{O}(n)$). This law was mainly designed for radio/TV broadcast networks where the popularity of a program is measured by the number of listeners/viewers. The high advertising cost during prime time shows and other popular events can be explained by Sarnoff's law. Indeed as more viewers are expected to watch a program, a higher price is charged per second of advertising. Although Sarnoff's law has been widely accepted as a good model for broadcast network, many critics say that it underestimates the value of general communication networks such as the Internet.

Metcalfe's Law:
Metcalfe's law [5] was first formulated by George Gilder (1993) and attributed to Robert Metcalfe who used it mostly in the context of the Internet. The law states that *the value of a communication network is proportional to the square of the number of node.* Its foundation is the observation that in a general network with n nodes, each node can establish $n-1$ connections. As a consequence, the total number of undirected connections is equal to $n(n-1)/2 \sim \mathcal{O}(n^2)$. This observation is particularly true in Ethernet networks where everything is "logically" connected to everything else. Metcalfe's law, has long been held up along side with Moore's law as the foundation of Internet growth.

Walrand's Law:

Walrand's law generalizes the previous laws by introducing a parameter a. The intuition behind this law is as follows. Imagine a large tree of degree d that is rooted at you. Your direct children in the tree are your friends. The children of these children are the friends of your friends, and so on. Imagine that there are $L \geq 2$ levels. The total number of nodes is $n = d(d^L - 1)/(d - 1) + 1$. If d is large, this number can be roughly approximated by $n \approx d^L$. Assume that you only consider your direct friends i.e., about d people. Then the value of the network to you is $\mathcal{O}(d) = \mathcal{O}(n^a)$ where $a = 1/L$. If you care about your friends and their friends (i.e d^2 people) then your value of the network is $\mathcal{O}(n^{\frac{2}{L}})$. If all the nodes up to level $l \leq L$ are important to you (d^l nodes), then the network has a value of $\mathcal{O}(n^{\frac{l}{L}})$. Repeating the same reasoning for each user (node), the total value of the network is approximately equal to $\mathcal{O}(n * n^a) = \mathcal{O}(n^{1+a})$ with $0 < a \leq 1$. The parameter a is a characteristic of the network and needs to be determined. Notice that if all nodes value children at all levels, the total value of the network becomes n^2 which corresponds to the Metcalfe's law ($a = 2$). If on the other hand $a = 0$, we get back Sarnoff's model.

Reed's Law:

Reed's law, also called the Group-Forming law, was introduced by David Reed ([16],[4], [17]) to quantify the value of networks that support the construction of a communicating group. A group forming network resembles a network with smart nodes that, on-demand, form into such configurations. Indeed, the number *of possible groups that can be formed over a network of* n *nodes is* $\mathcal{O}(2^n)$. Reed's law has been used to explain many new social network phenomenons. Important messages posted on social networking platforms such as Twitter and Facebook have been witnessed to spread exponentially fast.

Briscoe, Odlyzko, and Tilly (BOT)'s Law:

Briscoe, Odlyzko and Tilly ([3], [13]), have proposed an $\mathcal{O}(n \log(n))$ rule for the valuation of a network of size n. Their law is mostly inspired by Zipf's law that states that *if we order a large collection of items by size or popularity, the second element in the collection will be about half the measure of the first, the third element will be about 1/3 of the first, and the k-th element will measure about* $1/k$ *of the first.* Setting the measure of the first element (arbitrarily) to 1, the sequence looks like $(1, 1/2, 1/3, \ldots, 1/k, \ldots, 1/n)$. Now, assuming that each node in the network assigns value to the other nodes according to Zipf law, then the total value of the network to any given node will be proportional to the harmonic sum $\sum_{i=1}^{n-1} \frac{1}{i}$, which approaches $log(n)$. Summing over the nodes, we get the $nlog(n)$ rule. This growth rate is faster than the linear growth of Sarnoff's law and does not have the overestimating downside that is inherent to Reed and Metcalfe. It also has a diminishing return property that is missing in all the other models.

2.2 Assessing *Importance* of Links via Spanning Trees

Assuming that a model has been determined for the value of a network, we quantify the importance of a network link with respect to a spanning tree as the *loss-in-value* (LIV) when the link fails while communication is carried over the tree.

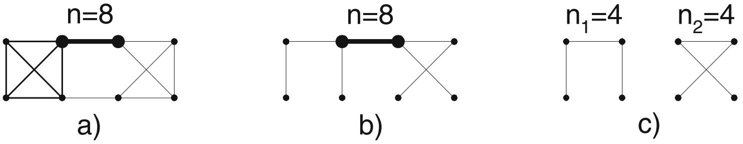

Fig. 1. Determining the loss-in-value (LIV) of a network link. a) Complete network of $n = 8$ nodes, with link 'e' of interest shown in bold. b)A particular spanning tree 'T' of the graph containing link e. c) When link e is removed network is disconnected in 2 connected components each with 4 nodes.

The LIV of a link e, relative to a given spanning tree T, is determined as follow (see Figure 1). Assume that communication is carried over T and delivers a value of $f(n) - \eta(T)$, where $\eta(T)$ is the cost of maintaining spanning tree T with $f(0) = 0$ if the network contains 0 node (i.e is empty). Now assume that link e of the network fails. If $e \in T$, then T is partitioned into 2 subtrees; each subtree T_i, $i \in \{1, 2\}$ represents a connected component with n_i nodes, where $n_1 + n_2 = n$. The net value of the resulting disconnected network is $f(n_1) + f(n_2) - \eta(T)$, where $f(n_i)$ is the value of the connected component i. When link e is removed, some exchanges that could be carried on the original network become impossible. As of such, it is reasonable to assume that $f(\cdot)$ is such that $f(n) \geq f(n_1) + f(n_2)$, which is the case for all the network value models cited above. We define the *importance* of link e, relative to spanning tree T, as this LIV $f(n) - (f(n_1) + f(n_2))$ when link e fails. If the link does not belong to the spanning tree, then removing it will leave the network connected, hence its LIV is equal to zero. More formally, the importance of link e relative to T is the (normalized) LIV $\boldsymbol{\lambda}(e, T)$:

$$\boldsymbol{\lambda}(T, e) = 1 - \frac{f(n_1) + f(n_2)}{f(n)}. \tag{1}$$

with the understanding that if $e \notin T$, $n_1 = n$ and $n_2 = 0$, giving $\boldsymbol{\lambda}(T, e) = 0$. Writing this expression for all spanning trees and all links of the network, we build the tree-link LIV matrix Λ defined by $\Lambda[T, e] = \boldsymbol{\lambda}(T, e)$.

Remark 1. With the definition in (1), the LIV of a link relative to any spanning tree is always equal to zero under Sarnoff's law (i.e $\boldsymbol{\lambda}(T, e) = 0$, $\forall e$ and T). As a consequence we drop Sarnoff's law in the analysis below. We consider the simple model (GWA) introduced in [10]. It gives the same normalized LIV of 1 if the link e belongs to the spanning tree and 0 otherwise (i.e. $\boldsymbol{\lambda}(T,e) = \mathbf{1}_{e\in T}$). The model basically assumes that whenever a link on the spanning tree is removed (i.e. successfully attacked and hence disconnecting the network), the network loses its entire value.

Table (1) shows the LIV of links for the different models presented above (Sarnoff replaced by GWA). It is assumed that removing link e divides spanning tree T into two subtrees with respective n_1 and n_2 nodes $(n_1 + n_2 = n)$

Table 1. Normalized LIV of link e relative to spanning tree T for the different laws. Removing link e from spanning tree T divides the network into two subnetworks with respective n_1 and n_2 nodes $(n_1 + n_2 = n)$.

Model	Normalized LIV
GWA	$1_{e\in T}$
Metcalfe	$1 - \frac{n_1^2+n_2^2}{n^2}$
Reed	$1 - 2^{-n_1} - 2^{-n_2}$
BOT	$1 - \frac{n_1 \log(n_1)+n_2 \log(n_2)}{n \log(n)}$
Walrand	$1 - \frac{n_1^{1+a}+n_2^{1+a}}{n^{1+a}}$

2.3 A Generalization of the betweenness Centrality Measure

The quantification we have described above for the significance of a link is relative to spanning trees: *there is a different value for each different tree.* In general, one would like to get a sense of the importance of a link for the overall communication process. Betweenness centrality is a measure that have long been used for that purpose. Next, we propose a quantification of the importance a link within a network that generalizes the notion of betweenness. We start by recalling the betweenness centrality measure as it was defined by Freeman [6].

For link e, and nodes i and j, let $g_{i,j}$ be the number of shortest paths between i and j and let $g_{ij}(e)$ the numbers of those paths that contain e. The partial betweenness measure of e with respect to i and j is defined as $\vartheta_{ij}(e) = \frac{g_{ij}(e)}{g_{ij}}$ and the betweenness of e is defined as $\vartheta(e) = \sum_{i<j} \vartheta_{ij}(e)$. Freeman [6] made the observation that in the definition of betweenness, $g_{ij}(e)$ can be seen as a weight given to e for a communication between i and j, and $\frac{1}{g_{ij}}$ can be seen as a probability (uniform here) of choosing among the several alternative geodesics that can carry communication between i and j.

Using this observation and using spanning trees (in lieu of shortest paths), we can easily generalize the betweenness centrality to quantify the importance of a link as

$$\vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha}) = \sum_{T} \boldsymbol{\alpha}_T \boldsymbol{\lambda}(T, e), \tag{2}$$

where the summation is now over spanning trees. The parameter $\boldsymbol{\lambda}(T,e)$ is the weight of link e for spanning tree T, and $\boldsymbol{\alpha}(T)$ is the probabilities (preference) of using T as communication infrastructure.

In general, $\boldsymbol{\lambda}$ and $\boldsymbol{\alpha}$ can be determined by considering relevant aspects of the communication network (e.g. cost of utilizing the links, overall communication delay, vulnerability of links). In this paper, the parameters $\boldsymbol{\lambda}$ are chosen to be equal to the LIV of the links relative to spanning trees, and $\boldsymbol{\alpha}$ is chosen to be the mixed strategy Nash equilibrium in a game between a network manager and an attacker. Details of the game are presented next.

3 Game Theoretic Approach

3.1 Game Model

The game is over the links of the network with a topology given by a connected undirected graph $G = (\mathcal{V}, \mathcal{E})$ with $|\mathcal{E}| = m$ links and $|\mathcal{V}| = n$ nodes. The set of spanning trees is denoted $\mathcal{T}$; we let $N = |\mathcal{T}|$.

To get all nodes connected in a cycle-free way, the network manager chooses a spanning tree $T \in \mathcal{T}$ of the graph. Running the communication on spanning tree T requires a maintenance cost of $\eta(T)$ to the network manager. If link e is attacked, the total cost to the manager is $\boldsymbol{\eta}(T)+\boldsymbol{\lambda}(T,e)$, where $\boldsymbol{\lambda}(T,e)$ is the LIV introduced in (1). The attacker simultaneously selects an edge $e \in \mathcal{E}$ to attack. Each edge $e \in \mathcal{E}$ is associated with some cost $\boldsymbol{\mu}(e)$ that an attacker needs to spend to launch a successful attack on e, and gives an attack reward of $\boldsymbol{\lambda}$(T,e). Hence, the net attack reward is equal to $\boldsymbol{\lambda}(T,e) - \boldsymbol{\mu}(e)$ for the attacker. It is assumed that the attacker has the option $e_\emptyset$ of not attacking, with $\boldsymbol{\lambda}(T, e_\emptyset) = 0$, $\forall$ T, and $\boldsymbol{\mu}(e_\emptyset) = 0$.

We are mainly interested in analyzing mixed strategy Nash equilibria of the game where the defender chooses $\boldsymbol{\alpha}$ over $\mathcal{T}$ to minimize the expected net communication cost $L(\boldsymbol{\alpha},\boldsymbol{\beta})$ while the attacker is choosing $\boldsymbol{\beta}$ over $\mathcal{E} \cup \{e_\emptyset\}$ to maximize the expected net reward $R(\alpha,\beta)$.

$$L(\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{T\in\mathcal{T}} \boldsymbol{\alpha}_T \left(\boldsymbol{\eta}(T) + \sum_{e\in T} \boldsymbol{\beta}_e \boldsymbol{\lambda}(T,e)\right), \tag{3}$$

$$\tag{4}$$

$$R(\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{e\in\mathcal{E}} \boldsymbol{\beta}_e \left(\sum_{T\ni e} \boldsymbol{\alpha}_T \boldsymbol{\lambda}(T,e) - \boldsymbol{\mu}(e)\right). \tag{5}$$

In this paper, we have focused on the case where $\boldsymbol{\eta}(T) = \eta$ is constant; hence not relevant to the optimization of $L(\boldsymbol{\alpha},\boldsymbol{\beta})$, which now becomes the minimization of $\sum_{T\in\mathcal{T}} \boldsymbol{\alpha}_T \sum_{e\in T} \boldsymbol{\beta}_e \boldsymbol{\lambda}(T,e)$. As a consequence, we ignore $\boldsymbol{\eta}(T)$ for the rest of this paper. The general case of $\boldsymbol{\eta}(T)$ will be considered in subsequent studies.

3.2 Nash Equilibrium Theorem

To state the NE theorem of the game, we need to make a certain number of definitions.

For each subset of edges $E \subseteq \mathcal{E}$, we let Λ_E be the matrix Λ where columns corresponding to links not in E are set to zero. Matrix Λ is defined in section 2.2 and its entries are given in (1).

Definition 1. *For any subset of links $E \subseteq \mathcal{E}$, we define the function $\kappa(E)$*

$$\begin{aligned} \kappa \;:\; & 2^{\mathcal{E}} \longrightarrow \mathbb{R}_+ \\ & E \longmapsto \kappa(E) = \min\left\{\mathbf{1}'\mathbf{y},\ \mathbf{y} \in \left\{\tilde{\mathbf{y}} \in \mathbb{R}_+^m \mid \Lambda_E \tilde{\mathbf{y}} \geq \mathbf{1}\right\}\right\}. \end{aligned} \tag{6}$$

$\kappa(E)$ is the value of a linear program (LP) that might be infeasible (e.g. when a row of Λ_E is all zeros). However, its dual is always feasible (see [9, App.E]), and when the dual LP is bounded, the primal is necessarily feasible [2]. Let $\mathbf{y}_E$ be a solution of the primal program whenever the dual LP is bounded. If this dual is unbounded for some subset E, we let $\mathbf{y}_E = K\mathbf{1}_m$, for an arbitrary large constant K, where $m = |\mathcal{E}|$, and $\mathbf{1}_m$ is the all-ones vector of length m. With this "fix", $\kappa(E) = m * K$ when the dual LP is unbounded. Hence, we can define the following quantities.

Definition 2. *The probability distribution induced by E is defined as $\boldsymbol{\beta}_E = \mathbf{y}_E/\kappa(E)$.*
The induced expected net reward $\theta(E)$ and the maximum induced expected net reward θ^* are defined by

$$\theta(E) := \frac{1}{\kappa(E)} - \sum_{e \in E} \boldsymbol{\beta}_E(e)\boldsymbol{\mu}(e), \quad \textit{and} \quad \theta^* := \max_E \left(\theta(E)\right). \tag{7}$$

We call a subset E critical *if $\theta(E) = \theta^*$ and we let $\mathcal{C}$ be the set of all critical subsets.*

Remark 2.
- In our online report [9, App.E], we argue that a critical subset E is such that $0 < \kappa(E) < \infty$, hence its corresponding $\mathbf{y}_E$ and $\boldsymbol{\beta}_E$ are always well-defined.
- With the definition of $\kappa(\cdot)$, if $\boldsymbol{\mu} = \mathbf{0}$, a subset E of links is critical, than any subset $F \supseteq E$ is critical. In this case, the *most critical* subset is the critical subset with the minimum size. More details about this can be found in [9].

Theorem 1. *For the game defined above, the following always hold.*

1. *If $\theta^* \leq 0$, then "No Attack" (i.e. $\boldsymbol{\beta}(e_\emptyset) = 1$) is always an optimal strategy for the attacker. In this case, the equilibrium strategy $(\boldsymbol{\alpha}_T,\ T \in \mathcal{T})$ for the defender is such that*

$$\vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha}) = \sum_{T \in \mathcal{T}} \boldsymbol{\alpha}_T \boldsymbol{\lambda}(T, e) \leq \boldsymbol{\mu}(e), \quad \forall e \in \mathcal{E}. \tag{8}$$

   The corresponding payoff is 0 for both players.

2. *If $\theta^* \geq 0$, then for every probability distribution $(\gamma_E, E \in \mathcal{C})$ on the set of critical subsets, the attacker's strategy $(\boldsymbol{\beta}(e), e \in \mathcal{E})$ defined by $\boldsymbol{\beta}(e) := \sum_{E \in \mathcal{E}} \gamma_E \boldsymbol{\beta}_E(e)$ is in Nash equilibrium with any strategy $(\boldsymbol{\alpha}_T, T \in \mathcal{T})$ of the defender that satisfies the following properties:*

$$\begin{cases} \vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha}) - \boldsymbol{\mu}(e) = \theta^* & \textit{for all} \;\; e \in \mathcal{E} \;\; \textit{such that} \;\; \boldsymbol{\beta}(e) > 0. \\ \vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha}) - \boldsymbol{\mu}(e) \leq \theta^* & \textit{for all} \;\; e \in \mathcal{E}. \end{cases} \tag{9}$$

Furthermore, there exists at least one such strategy $\boldsymbol{\alpha}$.
The corresponding payoffs are θ^* for the attacker, and $r(\gamma) := \sum_{E \in \mathcal{C}} \frac{\gamma_E}{\kappa(E)}$ for the defender.
3. *If $\boldsymbol{\mu} = 0$, then every Nash equilibrium pair of strategies for the game has the form described above.*

4 Discussion and Analysis

The NE theorem has three parts. If the quantity θ^* is negative then the attacker has no incentive to attack. For such choice to hold in an equilibrium, the defender has to choose his strategy $\boldsymbol{\alpha}$ as given in (8). Such $\boldsymbol{\alpha}$ always exists. When $\theta^* \geq 0$ there exists an equilibrium under which the attacker launches an attack that focuses only on edges of critical subsets. The attack strategies (probability of attack of the links) are given by convex combinations of the induced distributions of critical subsets. The corresponding defender's strategies are given by (9). When there is no attack cost, the attacker always launches an attack ($\theta^* > 0$) and the theorem states that all Nash equilibria of the game have the structure in 9.

4.1 Vulnerability Metric and the Importance of Links

For simplicity, let's first assume that there is no attack cost i.e $\boldsymbol{\mu} = \mathbf{0}$. In this case, $\theta(E) = \frac{1}{\kappa(E)}$ and $\theta^* > 0$. Also, a subset of link E is critical if and only if $\kappa(E)$ is minimal. Since in this case the game is zero-sum, the defender's expected loss is also $\theta^* = (min_E \kappa(E))$. θ^* depends only on the graph and the network value model $(f(n))$. It measures the worst case loss/risk that the network manager is expecting in the presence of any (strategic) attacker. Notice that in our setting, a powerful attacker is one who does not have a cost of attack (i.e. $\boldsymbol{\mu} = \mathbf{0}$). When θ^* is high, the potential loss in connectivity is high. When it is low, an attacker has very little incentive, hence the risk from an attack is low. Hence, θ^* can be used as a measure of the *risk of disconnectivity* in the presence of a strategic attacker. A graph with a high θ^* is a very *vulnerable* one.

This vulnerability metric also corresponds to a quantification of the *importance* of the most critical links. This is captured by the inequalities in (9), which, when $\boldsymbol{\mu} = \mathbf{0}$, become

$$\vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha}) \leq \theta^* \;\; \text{for all} \;\; e \in \mathcal{E}, \tag{10}$$

with equality whenever link e is targeted with positive probability ($\boldsymbol{\beta}(e) > 0$) at equilibrium. From (9) we see that $\boldsymbol{\beta}(e) > 0$ only if edge e belongs to a critical subset, and hence is critical. Thus, the attacker focuses its attack only on critical links, which inflict the maximum loss to the defender.

For the defender, since the game is zero-sum, the Nash equilibrium strategy corresponds to the *min-max* strategy. In other words, his choice of $\boldsymbol{\alpha}$ minimizes the maximum expected loss. Hence, the defender's equilibrium strategy $\boldsymbol{\alpha}$ can be interpreted as the best way (in the min-max sense) to choose a spanning tree in the presence of a strategic adversary. Using this interpretation with our generalization of betweenness centrality in (2), we get a way to quantify the *importance* of the links to the overall communication process. The inequalities in (10) above say that the links that are the most important to the defender (i.e. with maximum $\vartheta(e, \boldsymbol{\lambda}, \boldsymbol{\alpha})$) are the ones that are targeted by the attacker (the most critical). *This unifies the* positive *view of* importance *of links when it comes to participation to the communication process to the* negative *view of* criticality *when it comes to being the target of a strategic adversary.* This is not surprising because since the attacker's goal is to cause the maximum damage to the network, it makes sense that she targets the most important links.

When the cost of attack is not zero ($\boldsymbol{\mu} \neq \mathbf{0}$), our vulnerability metric θ^* takes it into account. For instance, if the attacker has to spend too much effort to successfully launch an attack, to the point where (the expected net reward) θ^* is negative, the theorem tells that, unsurprisingly, the attacker will choose to not launch an attack. To "force" the attacker to hold to such choice (i.e to maintain the equilibrium), the defender has to randomly pick a spanning tree according to (8). With this choice, the relative value of any link is less than the amount of effort needed to attack it (which means that any attack will result to a negative net-payoff to the attacker). When $\boldsymbol{\mu}$ is known, *such choice of $\boldsymbol{\alpha}$ can be seen as a deterrence tactic for the defender.*

If the vulnerability θ^* is greater than zero, than there exists an attack strategy that only targets critical links. To counter such attack, the defender has to draw a spanning tree according to the distribution $\boldsymbol{\alpha}$ in (9). For such choice of a tree, the relative importance of any critical link, offset by the cost of attacking the link, is equal to θ^*. For any other link, this difference is less than θ^*. In this case, the criticality of a link is determined not only by how much importance it has for the network, but also how much it would take for the adversary to successfully attack it. Hence,*when $\boldsymbol{\mu} \geq \mathbf{0}$, θ^* is a measure of the willingness of an attacker to launch an attack.* It includes the loss-in-value for the defender as well as the cost of attack for the attacker.

Observe that when $\boldsymbol{\mu} \geq \mathbf{0}$ the theorem does not say anything about the existence of other Nash equilibria. It is our conjecture (verified in all simulations) that even if there were other equilibria, θ^* is still the maximum payoff that the attacker could ever receive. Hence, it measures the worst case scenario for the defender.

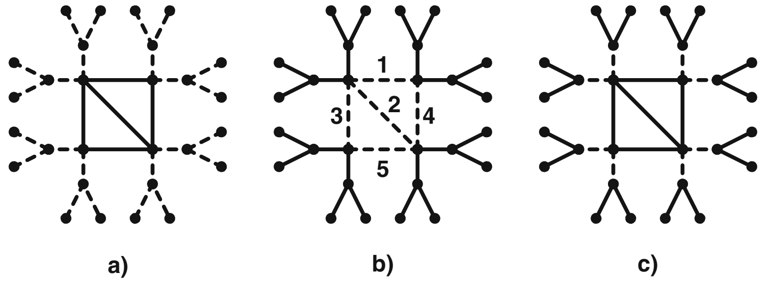

Fig. 2. Example of critical subsets for different value models. a) GWA model b) BOT, Walrand, and Metcalfe's models. c) Reed's model.

4.2 Critical Subsets and Network Value Models

In this section we discuss how the critical subsets depend on the model used for the value of the network. Figure 2 shows an example of network with the critical subsets for the different value models discussed earlier. The example shows a "core" network (i.e the inner links) and a set of bridges connecting it to peripheral nodes. A bridge is a single link the removal of which disconnects the network. In all figures, the critical subset of links is shown the dashed lines. In this discussion we mainly assume that the attack cost $\boldsymbol{\mu}$ is equal to zero.

Figure 2.a shows the critical subset corresponding to the GWA link cost model introduced in [10] for which $\boldsymbol{\lambda}_{T,e} = \mathbf{1}_{e \in T}$. With this model, the defender loses everything (i.e. 1) whenever the attacked link belongs to the chosen spanning tree. Since a bridge is contained in any spanning tree, attacking a bridge gives the maximum outcome to the attacker. As a consequence, the critical subsets correspond to the set of bridges as can be observed in the figure. In fact, with the GWA value model and Definition 1 of [10], on can easily show that that $\kappa(E) = \frac{|E|}{\mathcal{M}(E)}$, where $\mathcal{M}(E) = \min_T (|T \cap E|)$. Notice that if E is a disconnecting set (i.e. removing the edges in E divides the graph into 2 or more connected components), $\mathcal{M}(E) \geq 1$. Now, if e is a bridge, $|T \cap \{e\}| = 1$ for all spanning trees T, implying that $\mathcal{M}(\{e\}) = 1$ and $\theta(\{e\}) = \kappa(\{e\}) = 1$, which is the maximum possible value of θ^*. As a consequence, each bridge is a critical subset and any convex combination over the bridges yields an optimal attack.

Figure 2.b depicts the critical subsets with the Metcalfe, BOT, and Walrand ($a = 0.6$) models. For all these models (as well as for Reed's model), the function $f(x) - (f(x_1) + f(x_2))$, where $x_1 + x_2 = x$, is maximized when $x_1 = x_2 = x/2$. This suggests that attacks targeting links that evenly divide (most) spanning trees are optimal. This *conjecture* "*seems*" to be confirmed by the examples shown in the figure. The most critical links are the *innermost* or *core* links of the network for all three models. The Nash equilibrium attack distributions are slightly different for the 3 models. The distribution on links $(1, 2, 3, 4, 5)$ is given in Table 2 for Metcalfe, BOT, and Walrand($a = 0.6$) models. Notice that for all models, the middle link (2) is attacked with a higher probability.

Table 2. Attack probabilities on links $(1, 2, 3, 4, 5)$ for Metcalfe, BOT, and Walrand models

Model	Attack probability
Metcalfe	$(0.1875, 0.2500, 0.1875, 0.1875, 0.1875)$
BOT	$(0.1911, 0.2356, 0.1911, 0.1911, 0.1911)$
Walrand$(a = 0.6)$	$(0.1884, 0.2465, 0.1884, 0.1884, 0.1884)$

Although Reed's (exponential) model also has the same property discussed in the previous paragraph, the critical subset with Reed is different, as can be seen in figure 2.c. While Metcalfe, BOT, and Walrand models lead to the core network being critical, with Reed's model, the critical links are the links giving access to the core network. Each of the links is attacked with the same probability. This might be a little surprising because it contradicts the conjecture that innermost links tend to be more critical. However, observing the attack's reward function $\left(1 - \frac{f(n_1)+f(n-n_1)}{f(n)}\right)$ as shown in figure 3, Reed's model coincides with the GWA model in a wide range of n_1. This means that any link that separates (most of the spanning) into subtrees of n_1 and $n - n_1$ nodes gives the maximum reward to the attacker, for most values of n_1. Also, notice that since the core network is "well connected", the defender has many options for choosing a spanning tree. This means that in the core, the attacker has less chances of disrupting the communication. Links accessing the core, on the other hand, deliver high gain and better chances of disrupting the communication. Hence, the best strategy for the attacker is, in this case, to target access to the core. Notice that Metcalfe, BOT, and Walrand $(a \leq 1)$ models do not have this optimal *tradeoff choice*.

By choosing the parameter a to be sufficiently large in the Walrand model, we have (experimentally) observed that the critical subset moves from being the core, to corresponding to the one in GWA model (the bridges) for very large values of a. In fact, with all network topologies we have considered (more than 50), we could always choose the parameter of the Walrand so that the critical subset matches the one in GWA model. This implies that as the model loss function $\left(1 - \frac{f(n_1)+f(n-n_1)}{f(n)}\right)$ gets closer to the GWA function $\mathbf{1}_{e \in T}$, the critical subset moves away from the inner links to the outer links.

These observations indicate that the critical subsets of a graph depend on the value model used to setup the game. The value model is however not the only factor that characterizes the critical subset(s) of a graph. Figure 4 shows the same network as in the previous example with one additional (core) link. With this link, the connectivity of the network is enhanced. The critical subset does not change for the GWA models. However, for all other 4 models, the critical subset is now the access to the core. This suggests that *connectivity* is another factor that characterizes the critical subset(s).

As was observed (with simulations) in the previous example, in this case also, when the parameter a of Walrand's model is chosen sufficiently large, the critical subsets become the same as the GWA critical subsets.

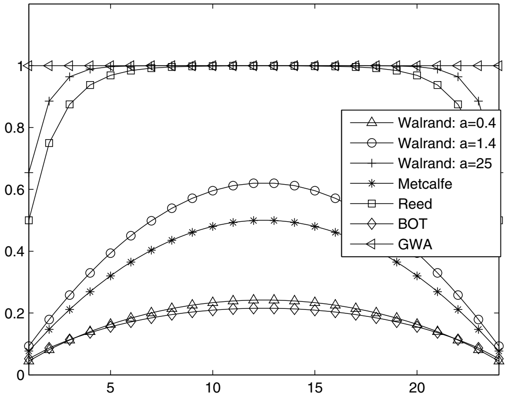

Fig. 3. Comparison of the loss functions $1 - \frac{f(n_1)+f(n-n_1)}{f(n)}$ when a link belonging to the chosen spanning tree is cut, dividing it into 2 subtrees of n_1 and $n - n_1$ nodes. (**x-axis** n_1, **y-axis** $1 - \frac{f(n_1)+f(n-n_1)}{f(n)}$). For GWA, since $\boldsymbol{\lambda}_{Te} = \mathbf{1}_{e\in T}$, the loss is always 1. The models GWA, Reed, and Walrand (for large values of a), overlap in a wide region of values of n_1.

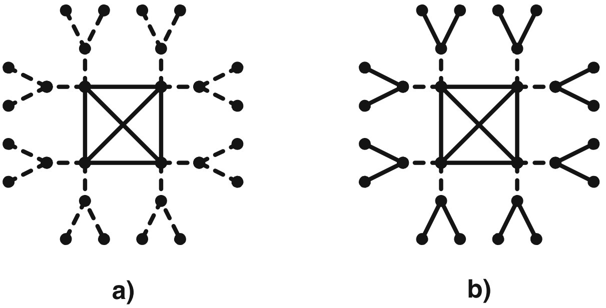

Fig. 4. Example of critical subsets for different value models. a) GWA model b) BOT, Walrand, Metcalfe and Reed's models.

5 Conclusion and Future Work

In this study, we quantify the vulnerability of a communication network where links are subject to failures due to the actions of a strategic attacker. Such a metric can serve as guidance when designing new communication networks and determining it is an important step towards improving existing networks.

We build upon previously proposed models for the value of a network, to quantify the *importance* of a link, relative to a spanning tree, as the *loss-in-value* when communication is carried over the tree and the link is failed by a strategic attacker. We use these values to setup a 2-player game where the defender (network manager) chooses a spanning tree of the network as communication infrastructure and the attacker tries to disrupt the communication by attacking one link. We propose the equilibrium's expected *loss-in-value* as a metric for the vulnerability of the network. We analyze the set of Nash equilibria of the game and discuss its implications. The analysis shows the existence of subsets of links that are more critical than the others. We characterize these sets of critical subsets and, using examples, we show that such critical subsets depend on the network value model as well as the connectivity of the graph. The nature of this dependency is an interesting question that we are planning to investigate in future studies. Finally, we propose a generalization of the notion of betweenness centrality that allows different weights for the links as well as preference among the graph structures that carry the communication (e.g. spanning trees for this paper).

Several future directions are being considered as a followup to this paper. First, in here, we have discussed the critical subsets using illustrative examples. To get a better intuition about the relationship between the value function and the critical subset of the network, a more rigorous analysis of the game value function ($\kappa(E)$) is needed. With such an analysis we will be able to integrate and understand more realistic (and potentially more complicated) network value models. Also, in this paper, we use spanning trees to define the relative importance of links. This implicitly considers only networks in which information flows over spanning trees. However, our result is general and can be used to study games on other type of networks. One interesting extension is the situation where the network manager chooses $p \geq 1$ spanning trees (example $p = 2$ is the situation where the manager chooses a communication tree and a backup one), and the attacker has a budget to attack $k \geq 1$ links. Also, we have assumed, in this paper, that the cost of communicating over any spanning tree is the same. In the future, we will study versions of the problem where some spanning trees might be more costly then others. Finally, this study has focused on the failure of links in a network. Nodes also are subject failures: whether random or strategic. A more thorough study should consider both links and nodes.

References

1. USN Admiral James Stavridis. Channeling David Sarnoff (September 2006), http://www.aco.nato.int/saceur/channeling-david-sarnoff.aspx
2. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press (March 2004)
3. Briscoe, B., Odlyzko, A., Tilly, B.: Metcalfe's Law is Wrong. IEEE Spectrum, 26–31 (July 2006)
4. Marketing Conversation. Reeds Law States that Social Networks Scale Exponentially (August 2007), http://marketingconversation.com/2007/08/28/reeds-law/
5. Marketing Conversation. A Short discussion on Metcalfe's Law for Social Networks (May 2008), http://marketingconversation.com/2007/08/28/reeds-law/
6. Freeman, L.: Centrality in Social Networks Conceptual Clarification. Social Networks 1(3), 215–239 (1979)

7. Gilder, G.: Metcale's Law And Legacy (November 1995), http://www.seas.upenn.edu/~gaj1/metgg.html
8. Gueye, A.: A Game Theoretical Approach to Communication Security. PhD dissertation, University of California, Berkeley, Electrical Engineering and Computer Sciences (March 2011)
9. Gueye, A., Marbukh, V., Walrand, J.C.: Towards a Quantification of Communication Network Vulnerability to Attacks: A Game Theoretic Approach. Technical report, National Institute of Standards and Technology (December 2011), http://www.nist.gov/itl/math/cctg/assane.cfm
10. Gueye, A., Walrand, J.C., Anantharam, V.: Design of Network Topology in an Adversarial Environment. In: Alpcan, T., Buttyán, L., Baras, J.S. (eds.) GameSec 2010. LNCS, vol. 6442, pp. 1–20. Springer, Heidelberg (2010)
11. Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T., Hubaux, J.-P.: Game Theory Meets Network Security and Privacy. Technical report, EPFL, Lausanne (2010)
12. Medhi, D.: Network Reliability and Fault-Tolerance. John Wiley & Sons, Inc. (2007)
13. Odlyzko, A., Tilly, B.: A refutation of Metcalfe's Law and a better estimate for the value of networks and network interconnections
14. Cisco Press. Spanning Tree Protocol: Introduction (August 2006), http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html
15. Cisco Press. Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches (August 2006), http://www.cisco.com/en/US/tech/tk389/tk621/technologies_configuration_example09186a008009467c.shtml
16. Reed, D.P.: That Sneaky Exponential: Beyond Metcalfe's Law to the Power of Community Building (Spring 1999), http://www.reed.com/dpr/locus/gfn/reedslaw.html
17. Reed, D.P.: Weapon of Math Destruction (February 2003), http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GENREF/C030200D.pdf
18. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A Survey of Game Theory as Applied to Network Security. In: Hawaii International Conference on System Sciences, pp. 1–10 (2010)