Vulnerability of Selfish Routing to Attacks: Game-theoretic Models and Initial Results

D. Genin, V. Marbukh, and A. Nakassis

Abstract—**This paper reports on work in progress on assessing and mitigating selfish routing vulnerability to strategic attacks. We explain mechanisms leading to this vulnerability, propose the corresponding game-theoretic model, solve this model for some particular case, and discuss implications of the vulnerability phenomenon. Our approach extends the well established research agenda on selfish routing by incorporating attacker(s) as separate agent(s) in the corresponding game. While each user makes its routing decision in attempt to minimize its transportation cost, the attacker(s) manipulate the link costs for the purpose of increasing the aggregate transportation cost to all or some users, e.g., by damaging the physical infrastructure or inserting malicious traffic as in Denial of Service (DoS) attack. Our initial results demonstrate that even "weak" attacker is capable of inflicting a serious damage measured by increase in the price of anarchy as compared to the case without attacker. Presence of attacker(s) can make Braess's paradox more pronounced. These initial results demonstrate importance of further research on the effect of the adversarial actions on selfish routing and a possibility of mitigating of this effect.**

***Index Terms*—Selfish routing, attacks, game-theoretic model, price of anarchy.**

I. INTRODUCTION

An emergent trend in networking attempts to resolve inefficiencies of network defined routing [1]-[2] by shifting responsibility for routing from the network to end users, e.g., by using source routing [3] or overlay routing [4]. Despite the fact that user-defined routing is much better than conventional network-defined routing in addressing specific user concerns, the downside may be the inherent selfish nature of user-centric routing, where each user attempts to optimize its own performance objective without concern for the overall network performance. This selfishness may lead to loss in overall network performance.

The comparative performance of these two routing schemes, network-defined and user-defined, is currently an active area of research. While performance limits of network-defined routing can be assessed by using optimization techniques, performance of selfish routing is typically identified with a Nash equilibrium in the corresponding non-cooperative game-theoretic model. Due to the typical multiplicity of Nash equilibria, loss in overall network performance resulting from user selfishness is defined by the price of anarchy: the worst-case ratio of the aggregate cost of selfish and socially optimal routing [5]. This definition assumes that network defined socially optimal routing minimizes the aggregate routing cost, and thus the price of anarchy always exceeds or equal one. Note that the route costs may represent actual payments for traffic delivery or they may instead characterize route quality with respect to delays, reliability, etc.

Theoretical and simulation results [6]-[7] suggest that despite the fact that the price of anarchy may be high and even unbounded, in practical situations performance deterioration due to user selfishness is within tolerable limits. Selfish user behavior can also lead to counterintuitive behavior known as the Braess paradox [8]: increasing the number of routing choices by adding more links to the network increases the aggregate transportation cost.

This paper attempts to gain an initial understanding of the effect of adversarial presence, e.g., attackers, on the performance of selfish routing. To this end we extend the conventional framework for performance evaluation of selfish routing by including the possibility of attacker(s) capable of manipulating the route costs in an attempt to maximize the aggregate transportation cost for all or some users, e.g., by damaging the physical infrastructure in transportation networks, inserting malicious traffic in a Denial of Service (DoS) attack on communication networks, or jamming in wireless networks. We propose an extended game-theoretic model, where strategic attacker(s) are modeled as separate agent(s) with limits on ability to manipulate route costs reflecting attacker power.

Quite surprisingly, our results indicate that even a weak attacker can inflict a significant damage on network performance. The reason for this disproportional effect is that an adversarial presence creates incentive for selfish users to avoid being attacked by making other users more appealing targets for attacker(s). This incentive may create a positive feedback eliminating the socially optimal equilibrium and driving selfish users to a very inefficient equilibrium.

The paper is organized as follows. Section II informally demonstrates how selfish user behavior in presence of even a weak adversary may lead to inefficient system equilibrium and Braess's paradox. Section III offers a game-theoretic performance model for selfish routing under attack, and introduces the corresponding generalized price of anarchy. Section IV solves this model in a particular case of several sources transmitting to a common destination either directly or via another source. Finally, Conclusion summarizes our results and outlines directions of future research.

Manuscript received March 5, 2010. This work was supported in part by the U.S. Department of Commerce under Cyber-security program.

Authors are with the National Institute of Standards and Technology, Gaithersburg, MD 80305 USA (corresponding author V. Marbukh: 301-975-2235; fax: 301-975-3553; e-mail: marbukh@nist.gov).

D. Genin and A. Nakassis are with the Advanced Networking Division (e-mails: dgenin@nist.gov and nakassis@nist.gov). V. Marbukh is with the Mathematics and Computer Science Division.

ISBN: 978-988-17012-9-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

II. Motivation: Informal Case Study

Figure 1 shows a simple network with two sources s_1 and s_2 sending traffic at rates λ_1 and λ_2 respectively to the common destination s_0.

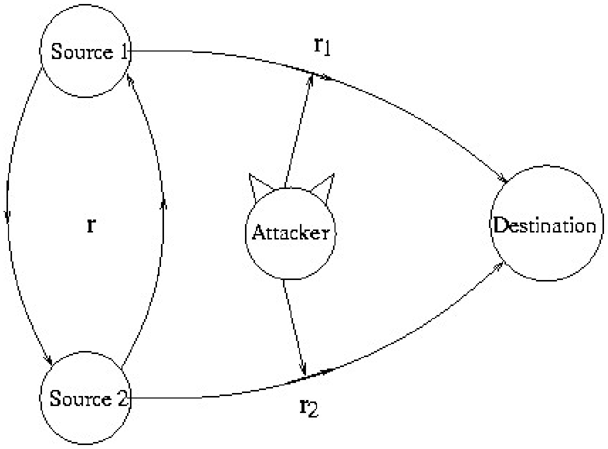

Figure 1. Motivational example

Sending traffic over a direct route $r_i, i = 1,2$ connecting source s_i to the destination is associated with cost $c_i \geq 0$ per unit of rate. Sending traffic over the bi-directional route r connecting sources s_1 and s_2 is associated with cost $d \geq 0$ per unit of rate. The transmission cost over a route is additive with respect to all the links comprising the route. We assume that an attacker can disrupt a certain portion ξ of traffic on either direct route r_1 or r_2, resulting in a certain penalty for the sources affected by the disruption, e.g., due to disrupted traffic.

Consider two scenarios. In the first scenario sources s_1 and s_2 are not directly connected. i.e., route r does not exist. In this scenario each source s_i can send traffic to the common destination s_0 only over a single direct route r_i, $i = 1,2$. A weak attacker can destroy a small portion ξ of this direct traffic, but the negative effect on the network performance, which is proportional to ξ, will be small. In the second scenario, sources s_1 and s_2 are directly connected by a bi-directional route r and have a choice to split their traffic between direct route r_i and the bypass route (r, r_{3-i}), $i = 1,2$. In the rest of this Section we informally demonstrate that this ability to choose increases the routing cost, which is reminiscent of the Braess paradox.

For simplicity we demonstrate this possibility in a symmetric case when sources s_i transmit at the same rate: $\lambda_i = \lambda$, both direct routes $r_i, i = 1,2$ have the same costs: $c_{i0} = c_0$, $i = 1,2$, and a strategic attacker disrupts a certain portion ξ of traffic on either direct route r_1 or r_2 where route selection is intended to maximize the total amount of affected traffic before reaching the destination. Since transit routes are "more expensive" than direct routes for both sources, the socially optimal routing for both sources s_i is to send the entire traffic over the direct links r_i and do not use link r at all regardless of attacker presence. In this case each source s_1 and s_2 incurs transportation cost of $c\lambda$ while having portion $(\xi/2)\lambda$ of its traffic disrupted due to symmetry.

However, selfishness will drive sources away from this social optimum as follows. Source s_1 can improve its position by shifting a very small portion $\varepsilon \to 0$ of its traffic from the direct route r_1 to bypass route (r, r_2) and thus making route r_2 more appealing target for attack than route r_1. Indeed after this shift, route r_2 will be carrying load $(1+\varepsilon)\lambda$ while route r_1 will be carrying load $(1-\varepsilon)\lambda$. As a result of this shift, source s_1 reduces the portion of its disrupted traffic by a finite amount $(1-\varepsilon)(\xi/2) = O(1)$ at the cost of very small increase $\varepsilon\lambda c$ in the transportation cost as $\varepsilon \to 0$. By symmetry, source s_2 has incentive to shift a very small portion $\varepsilon \to 0$ of its traffic from the direct route r_2 to bypass route (r, r_1). As both selfish sources s_1 and s_2 attempt to improve their positions by shifting portions of their traffic from direct to bypass routes, they will likely to move away from socially optimal equilibrium towards competitive equilibrium where both sources split their traffic equally between direct and bypass routes.

This competitive equilibrium is less efficient than the socially optimal equilibrium with both sources using only direct routes. Indeed, due to the symmetry, the portion of disrupted traffic for each source $\xi/2$ is the same in both equilibria. However, while the socially optimal transportation cost is $2c\lambda$, the competitive equilibrium has higher transportation cost of $(2c+d)\lambda$. Thus, a surprising conclusion is that even a very "weak", meaning $\xi \to 0$, adversary can significantly reduce performance of selfish routing.

It is instructive to look at this phenomenon as an increase in the transportation cost with increase in the number routing choices for selfish users. When only direct routes $r_i, i = 1,2$ are available, an adversarial presence does not affect the routing cost. However, adding more routing possibilities for traffic delivery by adding route r directly connecting sources s_1 and s_2, results in an increase the transportation cost from $2c\lambda$ to $(2c+d)\lambda$. This phenomenon is very similar to the Braess paradox [8]. However, since in our simple network without adversary the transportation cost is not affected by the presence of route r, the inefficiency of selfish routing is entirely due to adversarial presence. The purpose of this paper is to propose a formal framework for addressing these issues for general topology networks.

III. Minimum-Cost Routing

This Section formally describes minimum cost routing, identifies possible exogenous reasons for link cost uncertainty, and discusses possible approaches to minimum cost route selection under uncertain link costs.

A. Known Link Costs

Consider a network with set of nodes N and set of links L. Users (s,n) attempt to send traffic from node $s \in N$ to node $n \in N \setminus s$ at fixed rate λ_{sn} by splitting its traffic into flows of rates λ_r over feasible routes $r \in R_{sn}$:

$$\lambda_{sn} = \sum_{r \in R_{sn}} \lambda_r \tag{1}$$

The link l aggregate load is the sum of rates of all flows traversing this link:

$$\mu_l = \sum_{r: l \in r} \lambda_r \tag{2}$$

Each user sending traffic over link l at rate λ incurs cost $\lambda c_l(\mu_l)$, and the cost of transmission over a route is the sum of the costs of transmissions over all links comprising this route.

Thus, the transmission cost for user (s,n) over route $r \in R_{sn}$ is

$$f_r(\lambda) = \lambda_r \sum_{l \in r} c_l \left(\sum_{r': l \in r'} \lambda_{r'} \right) \tag{3}$$

and the total cost to user (s,n) is

$$F_{sn}(\lambda) = \sum_{r \in R_{sn}} \lambda_r \sum_{l \in r} c_l \left(\sum_{r': l \in r'} \lambda_{r'} \right) \tag{4}$$

where the vector $\lambda = (\lambda_r)$ characterizes flow rates on all feasible routes r in the network. We assume link cost $c_l(\mu_l)$ to be increasing and either linear or convex in link load $\mu_l \geq 0$ for all links $l \in L$.

Socially optimal load allocation minimizes the aggregate cost for all users:

$$F^{\min} = F(\lambda^{opt}) = \min_{(\lambda_r \geq 0)} F(\lambda) \tag{5}$$

where the aggregate cost is

$$F(\lambda) = \sum_{(s,n)} \sum_{r \in R_{sn}} \lambda_r \sum_{l \in r} c_l \left(\sum_{r': l \in r'} \lambda_{r'} \right) \tag{6}$$

and minimization is subject to constraints (1). Due to our assumptions, optimization problem (1), (5)-(6) is convex, and thus has unique computationally tractable solution.

In a particular case of load-independent link costs $c_l(\mu_l) = c_l$ the socially optimal routing can be identified explicitly: the optimal route for user (s,n) is

$$r_{sn}^* = \arg\min_{r \in R_{sn}} \sum_{l \in r} c_l \tag{7}$$

the corresponding minimal user (s,n) cost is

$$F_{sn}^{\min} = \lambda_{sn} \min_{r \in R_{sn}} \sum_{l \in r} c_l \tag{8}$$

and the total cost for all users is

$$F^{\min} = \sum_{(s,n)} \lambda_{sn} \min_{r \in R_{sn}} \sum_{l \in r} c_l \tag{9}$$

A. Unknown Link Costs

Cost based strategies naturally arise as a result of optimization of the network performance [9] or incorporating Quality of Service (QoS) requirements into admission and routing processes [10]. In the case of QoS routing, the cost of a route r reflects the expected level of the QoS provided to a request carried on this route. For example, c_l may represent the expected delay, packet loss or available bandwidth on link l. Typically, link costs depend not only on the user routing decisions affecting link loads (2), but also on some exogenous parameter(s), which are often not known precisely.

Uncertainty in the exogenous parameters creates uncertainty in the link costs making minimum cost route selection dependent on the nature of uncertainty. In the case of statistical uncertainty it is natural to minimize the average route cost. In this paper we are concerned with adversarial uncertainty created by attacker(s). In this case it is natural to base route selection on a worst-case route cost minimization. In the rest of this Subsection we consider some examples leading to link $l \in L$ cost of the form

$$f_l(\mu_l | \xi_l) = c_l(\mu_l) + b_l(\mu_l)\xi_l \tag{10}$$

where μ_l is link l aggregate load, $\xi_l \geq 0$ is an exogenous parameter, functions $c_l(\mu_l)$ and $b_l(\mu_l)$ are increasing and convex in $\mu_l \geq 0$. Further in the paper we consider a particular case of link costs (10) with $c_l(\mu_l) = c_l$ and $b_l(\mu_l) = b_l$ being link load independent. In this case link costs (10) take the following form

$$f_l(\mu_l | \eta_l) = c_l + \eta_l \tag{11}$$

where $\eta_l = b_l \xi_l \geq 0$ is an exogenous parameter.

In the case when a small portion ξ_l of traffic traversing link l can be disrupted, user (s,n)'s aggregate cost (4) takes the following form:

$$F_{sn}(\lambda | \xi) = \sum_{r \in R_{sn}} \lambda_r \sum_{l \in r} \left[b_{sn}\xi_l + c_l \left(\sum_{r': l \in r'} \lambda_{r'} \right) \right] \tag{12}$$

where parameter b_{sn} quantifies user (s,n) sensitivity to traffic disruption. In the case when all users have the same sensitivity to the traffic disruption, e.g., parameters $b_{sn} = b$ do not depend on (s,n), aggregate user (s,n) cost (12) can be rewritten as follows:

$$F_{sn}(\lambda | \xi) = \sum_{r \in R_{sn}} \lambda_r \sum_{l \in r} f_l \left(\sum_{r': l \in r'} \lambda_{r'} | \xi \right) \tag{13}$$

where link l cost is

$$f_l(\mu_l | \xi_l) = c_l(\mu_l) + b\xi_l \tag{14}$$

User cost (13) has the same form as cost (4), but with modified link l costs (14), which now depend on the exogenous parameters ξ_l. In another example link costs are associated with delays, and a Denial of Service (DoS) attacker inserts malicious load ξ_l on link l. In this case the modified link l cost becomes

$$f_l(\mu_l|\gamma_l) = c_l(\mu_l) + b_l(\mu_l)\xi_l \tag{15}$$

where $b_l(\mu_l) = [dc_l(\mu)/d\mu]_{\mu=\mu_l}$.

Further in the paper we assume link costs (15), aggregate user cost (13), and the aggregate cost for all users

$$F(\lambda|\xi) = \sum_{(s,n)}\sum_{r\in R_{sn}} \lambda_r \sum_{l\in r} f_l\left(\sum_{r':l\in r'}\lambda_{r'}|\xi\right) \tag{16}$$

IV. Routing under Adversarial Uncertainty

This Section proposes game-theoretic models for socially optimal and selfish load allocation under attack, which is interpreted as adversarial uncertainty. In a general case of load-dependent link costs, considered in Subsection A, the agents have continuous sets of strategies and agent's best responses are discontinuous. Subsection B considers the simpler case of load-independent link costs, when the corresponding games have finite sets of strategies.

A. Load-dependent Link Costs

Consider an adversarial uncertainty when vector $\xi \in \Xi$ is controlled by an adversary who attempts to maximize the total cost for all users ( ):

$$\xi^*(\lambda) = \arg\max_{\xi\in\Xi} F(\lambda|\xi) \tag{17}$$

Vector $\xi^*(\lambda)$ represents the best attacker response to load allocation λ. We consider two scenarios for load allocation against adversarial uncertainty: socially optimal and competitive.

In a socially optimal scenario, given attacker strategy $\xi \in \Xi$, the social planner allocates all user loads in an attempt to minimize the aggregate cost to all users:

$$\lambda^*(\xi) = \arg\min_{\lambda} F(\lambda|\xi) \tag{18}$$

where minimization is subject to constraints (1) and $\lambda_r \geq 0$. Load allocation (18) represents the best response by a social planner to attacker strategy $\xi \in \Xi$. It is natural to view (17)-(18) as best responses in a two-player: social planner and attacker, zero-sum game, where the social planner selects load allocation (18) in an attempt to minimize the aggregate routing cost while the attacker selects "attack vector" (17) in an attempt to maximize this cost. The value of this game $F_{\min}^{\max}$ quantifies the equilibrium aggregate cost when both players act to the best of their abilities.

In a competitive scenario each selfish user (s,n) allocates its own load $\lambda_{(sn)} = \{\lambda_r : \sum \lambda_r = \lambda_{ns},\ \lambda_r \geq 0,\ r \in R_{sn}\}$ in an attempt to minimize its cost in adversarial environment (17):

$$\lambda^*_{(sn)}(\lambda_{-(sn)}) = \arg\min_{\lambda_{(sn)}} F_{sn}[\lambda|\xi^*(\lambda)] \tag{19}$$

where vector $\lambda_{-(sn)}$ characterizes load allocations by all users except user (s,n). User (s,n)'s load allocation (19) represents the best user (s,n) response to other user load allocations $\lambda_{-(sn)}$ in the Stackelberg game with non-cooperative selfish users being leaders as they simultaneously allocate their loads in attempt to minimize their routing cost and an attacker being a follower who manipulates link costs in an attempt to maximize the aggregate routing cost to all users. Generally, this game may have multiple Nash equilibria with different aggregate routing costs.

Let $\hat{F}_*^*$ be the maximum aggregate cost over all Nash equilibria in this game. The price of anarchy [5]-[6]

$$\gamma = \hat{F}_*^* / F_{\min}^{\max} \tag{20}$$

characterizes loss in the aggregate performance due to user selfishness. It is easy to see that $\gamma \geq 1$ since coordinated user strategy can better counteract an adversarial action. The novelty of our approach is its ability to quantify the loss in the aggregate performance due to user selfishness under attack as a function of the attacker "power" represented by the set of feasible attacker strategies Ξ:

$$\gamma = \gamma(\Xi) \tag{21}$$

Note that the typical discontinuity of the best responses (17)-(19) makes conventional results about existence and uniqueness of the game equilibrium non-applicable for games proposed in this Subsection for socially optimal and selfish load allocations under adversarial uncertainty. Consider, as an example, a case of load-unaware link costs (11) and assume that set of feasible adversarial actions $\gamma = \gamma(\Xi)$ is

$$\Xi = \left\{\xi_l : \sum_l a_l \xi_l \leq \eta, \xi_l \geq 0, l \in L\right\} \tag{22}$$

with some $a_l > 0$. In this case the optimal adversarial response (17) is to concentrate "the attack":

$$\xi_l^*(\lambda) = \begin{cases} \eta/a_l & if \quad l = l^* \\ 0 & otherwise \end{cases} \tag{23}$$

on a link:

$$l^*(\lambda) = \arg\max_{l\in L}(b_l/a_l)\sum_{r:l\in r}\lambda_r \tag{24}$$

where the impact is maximal. In a situation of several such "highest impact" links, the attacker is indifferent with respect to distributing its efforts among these links.

B. Load-independent Link Costs

Consider the case of load-independent link costs (11), and assume that each user (s,n) chooses a single feasible route $r \in R_{sn}$ for transmitting its entire flow of rate λ_{sn}, while the attacker chooses a single link $l \in L$ to attack by raising its cost from c_l to $c_l + h$, where $h > 0$. It is convenient to characterize feasible pure strategies of the attacker by the binary variables: $\delta_l = 1$ if link l is attacked, and $\delta_l = 0$ otherwise. Thus, user (s,n)'s transportation cost is

$$\Phi_{sn}(r|\delta) = \lambda_{r_{sn}} \sum_{l\in r_{sn}}(c_l + h\delta_l) \sum_{(ij):l\in r_{ij}}\lambda_{ij} \tag{25}$$

and the total transportation cost for all users is

$$\Phi(r|\delta) = \sum_{(s,n)} \Phi_{sn}(r|\delta) \tag{26}$$

where vector $r = (r_{sn})$ characterizes route selections by all users, and vector $\delta = (\delta_l)$ characterizes attacker strategy.

Again, we consider two scenarios for load allocation in an adversarial environment: socially optimal and competitive. In both scenarios, given route selections by all users $r = (r_{sn})$, the attacker selects a link to attack in an attempt to maximize the aggregate cost (26):

$$\delta^*(r) = \arg\max_{\delta} \Phi(r|\delta) \tag{27}$$

The socially optimal scenario [11]-[13] is modeled as a zero-sum game of social planner and attacker, where for a given attacker strategy δ the social planner assigns routes to all users $r = (r_{sn})$ in attempt to minimize the aggregate cost for all users:

$$r^*(\delta) = \arg\min_{r} \Phi(r|\delta) \tag{28}$$

The competitive scenario is modeled as a Stackelberg game with non-cooperative users being the leaders and the attacker being the follower. All users (s,n) simultaneously select their routes r_{sn}^* in attempts to minimize their own costs (25):

$$r_{sn}^*(r_{-(sn)}) = \arg\min_{r_{sn}} \Phi_{sn}[r|\delta^*(r)], \tag{29}$$

assuming attacker strategy (27), where $r_{-(sn)} = \{r_{km} : (k,m) \neq (s,n)\}$.

Since both scenarios are modeled as games with finite sets of strategies, each of these games always has at least one Nash equilibrium. These equilibria may be either pure, e.g., specify a feasible route for each source and a link to attack, or mixed, e.g., a probability distribution on sets of feasible routes and links to attack. It is natural to view a mixed routing strategy as the corresponding load split among feasible routes, and a mixed attacker strategy as the corresponding splitting of the attacker efforts among different links. This interpretation provides a link between the game-theoretic formulation with finite set of strategies in this Subsection and the game-theoretic formulation with continuous sets of strategies in the previous Subsection.

The price of anarchy consistent with definition (20) is

$$\gamma = \hat{\Phi}_*^* / \Phi_{\min}^{\max} \geq 1, \tag{30}$$

where $\Phi_{\min}^{\max}$ is the total user cost in the unique socially optimal equilibrium, and $\hat{\Phi}_*^*$ is the total user cost in the worst-case competitive equilibrium. Note that performance of a mixed Nash equilibrium is characterized by the corresponding average cost.

Consider price of anarchy (30) as a function of the power of attacker $h \geq 0$: $\gamma = \gamma(h)$. Apparently, in absence of an attacker the price of anarchy $\gamma(h)\big|_{h=0} = 1$, i.e., there is no loss in performance due to user selfishness, since selfish users will choose socially optimal minimum cost routes. The Braess paradox refers to a counterintuitive situation when providing more choices to the selfish users by adding links to the network increases the total transportation cost. Apparently, in absence of an attacker: $h = 0$, the Braess paradox cannot occur. Informal arguments of Section II confirmed by formal analysis in the next Section of the paper demonstrate that the presence of an attacker, i.e., $h > 0$ may lead to loss in routing performance, i.e., $\gamma(h) > 1$, and occurrence of the Braess paradox even in a case of load-independent link costs.

V. Example

Subsection A describes the example network and discusses the corresponding equilibria, price of anarchy and Braess paradox. Subsection B briefly outlines the derivation of the Nash equilibria for the example network.

A. Price of Anarchy and Braess Paradox

Consider a network comprised of sources $s \in \{1,..,S\}$ transporting traffic to a common destination at rate λ_s. Each source $s \in \{1,..,S\}$ can either use a direct route to the destination r_s at cost of $c_s > 0$ per unit of rate, or use any route r_{sn} to the destination via any one other source $n \in \{1,..,S\} \setminus s$ at the cost of $d_{sn} + c_n$ per unit rate, where $d_{sn} > 0$ is a transportation cost from source s to source n. In this paper, due to space limitations, we consider the symmetric case when all users $s \in \{1,..,S\}$ have the same transmission rates $\lambda_s = \lambda$ and direct transportation costs: $c_s = c$. We assume that transportation costs between any two sources and $n \in \{1,..,S\} \setminus s$ are the same: $d_{sn} = d$. We also assume that attacker can raise transportation cost on one of S direct routes r_s from c to $c + h$.

Due to the symmetry, the socially optimal routing transports all traffic over direct links while the attacker attacks direct links equiprobably. The corresponding total aggregate transportation cost is

$$\Phi_{\min}^{\max}(h) = (Sc + h)\lambda \tag{31}$$

For simplicity we only consider the game-theoretic model introduced in Subsection IVB with a finite set of strategies. One can verify that while in socially optimal equilibrium users transport their traffic over direct routes, for $h > 0$ the competitive equilibrium exists, where each selfish user equally splits its traffic among all S feasible routes, which include one direct route and $S - 1$ bypass routes via other users. Formal arguments supporting this statement are briefly outlined in the next Subsection. In the rest of this Subsection we discuss the corresponding price of anarchy and a Braess paradox as links directly connecting different sources are added.

In is easy to verify that the total transportation cost in the described above competitive equilibrium is

$$\Phi_*^* = \begin{cases} [Sc + (S-1)d + h]\lambda & if \quad h > 0 \\ Sc\lambda & if \quad h = 0 \end{cases} \tag{32}$$

and the corresponding price of anarchy, shown in Figure 2, is

$$\gamma^*(h) = \begin{cases} 1 + \dfrac{(S-1)d}{Sc+h} & if \quad h > 0 \\ 1 & if \quad h = 0 \end{cases} \tag{33}$$

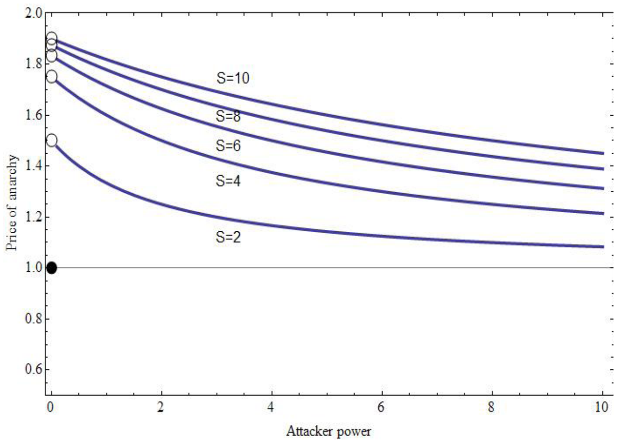

Figure 2. Price of anarchy γ vs. attacker power h.

The price of anarchy γ jumps from 1 for $h = 0$ to

$$\gamma^{\max} = 1 + \left(1 - \frac{1}{S}\right)\frac{d}{c} \tag{34}$$

as h becomes positive. Then, as h increases, the price of anarchy monotonically decreases approaching 1 due to ability of a powerful attacker to overwhelm any defense. The price of anarchy (33) also quantifies the severity of the Braess paradox as the network in question is expanded from one with only direct routes to include links directly connecting different sources.

B. Outline of Nash Equilibrium Derivation

Let us assume that some source, say source $s = 1$, chooses direct route r_1 with probability $\alpha \in [0,1]$ and each of $S-1$ transit routes with probabilities $(1-\alpha)/(S-1)$. Sources $s = 2,..,S$ choose direct route with probability $\beta \geq 0$ and each of $S-1$ transit routes with probabilities $(1-\beta)/(S-1)$. The cost per unit of rate for the source depends on either $\alpha > \beta$, $\alpha < \beta$, or $\alpha = \beta$. In the case $\alpha > \beta$ route r_1 carries more load than other direct routes $r_s, s \in \{2,..,S\}$. Thus, route r_1 will be attacked making the source $s = 1$ transportation cost

$$\phi_1(\alpha|\beta) = (c+h)\alpha + (c+d)(1-\alpha). \tag{35}$$

In a case $\alpha < \beta$ route r_1 carries less load than other direct routes $r_s, s \in \{2,..,S\}$. Thus, the attacker will attack each of other direct routes $r_s, s \in \{2,..,S\}$ with probability $1/(S-1)$ raising its cost by $h/(S-1)$ on average. The average transportation cost for source $s = 1$ in this case is

$$\phi_1(\alpha|\beta) = c\alpha + \left(c + d + \frac{h}{S-1}\right)(1-\alpha) \tag{36}$$

In the case $\alpha = \beta$ route r_1 carries the same load as other direct routes $r_s, s \in \{2,..,S\}$. Thus, the attacker will split its efforts among all direct routes $r_s, s \in \{1,..,S\}$ with probability $1/S$ raising the average cost of each direct route by h/S. The average transportation cost for source $s = 1$ in this case is

$$\phi_1(\alpha|\beta) = c\alpha + \left(c + d + \frac{h}{S-1}\right)(1-\alpha) \tag{37}$$

Since source $s = 1$ will attempt to minimize its cost (37) over $\alpha \in [0,1]$, it is natural to identify Nash equilibria of the corresponding game with solution to equation

$$\beta = \arg\min_{\alpha \in [0,1]} \phi_1(\alpha, \beta) \tag{38}$$

VI. Conclusion

This paper proposes a research agenda on the effect of adversarial presence measured by the price of anarchy. Initial models and results suggest practical importance as well as theoretical challenges of this research. For example, a possibility of reducing of the price of anarchy while preserving the distributed nature of resource allocation is an important question to answer.

Acknowledgment

Authors thank Dr. R. Boisvert for careful reading of the paper and numerous useful suggestions.

References

[1] S. Savage, T. Anderson, A. Aggarwal, D. Becker, N. Cardwell, A. Collins, E. Hoffman, J. Snell, A. Vahdat, G. Voelker, and J. Zahorjan, “Detour: a case for informed Internet routing and transport,” In *IEEE Micro*, volume 19(1), pages 50–59, Jan. 1999.

[2] H. Tangmunarunkit, R. Govindan, S. Shenker, and D. Estrin, “The impact of routing policy on Internet paths,” In *Proceedings of IEEE INFOCOM ’01*, Anchorage, AK, Apr. 2001.

[3] I. Castineyra, N. Chiappa, and M. Steenstrup, “*The Nimrod Routing Architecture,” RFC 1992*, Aug. 1996.

[4] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, “Resilient overlay networks,” In *Proceedings of SOSP ’01*, Banff, Canada, Oct. 2001.

[5] C.H. Papadimitriou, “Algorithms, games, and the Internet,” In *Proceedings of STOC ’01*, Hersonossos, Crete, Greece, July 2001.

[6] T. Roughgarden and E. Tardos, “How bad is selfish routing?” *Journal of ACM*, 49(2):236–259, 2002.

[7] L. Qiu, Y.R. Yang, Y. Zhang, and S. Shenker, “On selfish routing in Internet-like environments,” In *Proceedings of SIGCOMM ’03.*

[8] T. Roughgarden. "The Price of Anarchy." MIT Press, Cambridge, MA, 2005.

[9] F.P. Kelly, "Routing in Circuit-Switched Networks: Optimization, Shadow Prices and Decentralization," *Adv. Appl. Prob*., 20 (1988) 112-144.

[10] R.A. Guerin and A. Orda, "QoS Routing in Networks with Inaccurate Information: Theory and Algorithms," *IEEE/ACM Trans. on Networking*, 7 (1999) 350-364.

[11] V. Marbukh, “On Shortest Random Walks under Adversarial Uncertainty”, *Fortieth Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, 2002.

[12] V. Marbukh, "Minimum Cost Routing under Adversarial Uncertainty: Robustness through Randomization," *Int. Symp. on Information Theory (ISIT2002)*, Lausanne, Switzewland, 2002.

[13] V. Marbukh, "QoS Routing under Adversarial Binary Uncertainty: Solution for a Symmetric Case," *Int. Conf. on Communications (ICC2002),* New York, 2002.