Defending Link Flooding Attacks under Incomplete Information: A Bayesian Game Approach

Xu Chen*†, Wei Feng*†, Ning Ge*†, Xianbin Wang‡
*Department of Electronic Engineering, Tsinghua University, Beijing, China
†Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing, China
‡Department of Electrical and Computer Engineering, Western University, London, Canada
(e-mail: chenxu18@mails.tsinghua.edu.cn, fengwei@tsinghua.edu.cn, gening@tsinghua.edu.cn, xianbin.wang@uwo.ca)

***Abstract*—The link flooding attack (LFA) arises as a new class of Distributed Denial of Service (DDoS) attacks in recent years. By aggregating low-rate protocol-conforming traffic to congest selected links, LFAs can degrade the connectivity of target servers indirectly. Due to the fast proliferation of insecure Internet of Things (IoT) devices, the deployment of botnets is getting easier, which dramatically increases the risk of LFAs. Since the attacking traffic may not reach the victims directly and seems to be legitimate, LFAs are extremely difficult to detect and defend using traditional methods. In this work, we model the interaction between the LFA attacker and the defender as an extensive form game with incomplete information. By using action space compression and the divide and conquer method, we analyze the Nash equilibrium of the subgame on each link, which reveals the rational behaviors of attackers and the optimal strategies of defenders. Furthermore, we concretely expound how to adopt local optimal strategies in the Internet-wide scenario. Experimental results show the effectiveness and robustness of our proposed decision-making method in explicit LFA defending scenarios.**

***Index Terms*—Link flooding attack (LFA), distributed denial of service (DDoS), extensive form game, Bayesian Nash equilibrium (BNE).**

I. Introduction

Due to dramatically increased connectivity, securing communications over different networks becomes more and more critical. Many different methods have been developed to enhance network security, such as intrusion detection [1], malicious traffic mitigation [2], etc. However, as a major type of network security threats, botnet-enabled Distributed Denial of Service (DDoS) attacks are evolving quickly over time, many sophisticated and stealthy attacking mechanisms were developed in recent years. The emergence of link flooding attacks (LFAs) is such a typical case. In particular, *Crossfire* attacks [3] employ non-spoofed bots to iteratively flood links around targeted servers through sending legitimate traffic to nearby decoy servers, making their defense even harder.

To defend DDoS attacks, a mass of defense strategies, resource allocation policies and collaboration algorithms were developed to guide defenders [4]. However, most of these techniques, which aimed at addressing host-targeted DDoS attacks, are not suitable for LFAs. The targeted network-internal defenders are usually unaware of LFAs, the critical challenge to defend LFA is how to detect it effectively [5], [6].

Some researchers attempt to mitigate anomaly traffic without detecting it, by using smart TCP control [7], IP traffic differentiation [8], or BGP (Border Gateway Protocol) rerouting methods [9] instead. Such techniques often need an external network monitor to mediate different autonomous systems (ASes) to perform collaborative countermeasures. However global coordination between all the ASes seems unfeasible so far [10], [11]. An expectable solution to this issue resides in software defined network (SDN) technology [12], [13].

Based on these existing studies and observations, this work is motivated to develop a game theoretical approach for strategic decision making in LFA defending. Even though game theoretic approaches have been widely used in analyzing and addressing network security challenges [14], [15], including the strategy analysis in host-targeted DDoS defense, modeling an LFA game is still difficult. This is mainly because (i) the action space is extremely large. Any link in the network can be a victim, whereas targets of host-targeted DDoS are relatively clear. (ii) the LFA game is both imperfect and incomplete on the viewpoint of information availability to both players, which makes the analysis more complicated. So far as we know, there's no such model which has addressed both difficulties in literature. This work attempts to bridge this gap in an integrated framework.

Key contributions of this work are summarized below.

1) An *Extensive Form Game* model is proposed to formulate the interplay of players in LFAs.
2) Best strategies of both players are derived, and an integrated decision-making process is customized for defenders.
3) Evaluation of the proposed defending strategy is performed in terms of effectiveness and robustness.

The remainder of this paper is organized as follows. In section II, the LFA game is formulated. The pure strategy Bayesian Nash equilibriums on a single link are derived and analyzed in section III. In section IV, we compare our defending strategy with two typically adopted strategies. Section V shows the conclusion.

This work was supported in part by the National Key R&D Program of China (Grant No. 2018YFA0701601); the National Natural Science Foundation of China (Grant No. 61941104, 61922049, 61771286, 61701457); the Beijing Innovation Center for Future Chip, and the Peng Cheng Laboratory.

978-1-7281-5089-5/20/$31.00 ©2020 IEEE

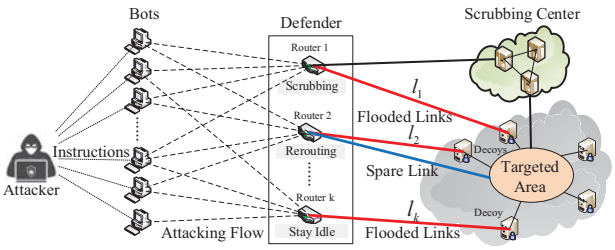

Fig. 1. The interplay between the attacker and defender in a typical LFA. The red links are under attack. The rectangle markes the control plane of the defender. To defend the occurrent LFA, the defender diverts traffic load on l_1 to scrubbing center, reroutes traffic load on l_2 to another spare link (the blue link), and stays idle to l_k.

II. Problem Formulation

A. Basic analysis and assumptions

Modelling network security problems as a game can be frequently seen in literatures. As a pioneering work, Chen et al. [14] establish an insightful non-cooperative game model on intrusion detection problem in heterogeneous networks. A Stackelberg game model is adopted and analyzed. The leader player of the game commits a randomized detecting strategy while the follower takes best response to it such that both sides maximize their payoffs. Stackelberg security game (SSG) has become a new branch of game theory. We follow these ideas in our LFA game model. In SSGs, the defender is usually assigned to be the leader [16], [17]. But this setup of roles is not suitable for modeling LFAs, because that SSGs are static games with complete information, while LFA game is a dynamic game with incomplete information. The defender can't deduce a Stackelberg strategy by using incomplete information. Besides, the late-mover can get some information advantages to benefit more. Therefore, in our LFA game the defender is set to be the follower.

Moreover, we make much efforts on extending the model assumptions of SSGs to make our model more applicable in practical network defense. We introduce a new parameter a_i, the volume of attacking traffic, to describe the attacking behavior more accurately. This is crucial for decision-making in LFA games. Likewise, we concretely take the defending actions such as "Rerouting" and "Scrubbing" into consideration, which makes the defending decisions more feasible. We will expound these extensions in the following subsections.

Two basic assumptions are made in our model. Firstly, we assume that there is a global network manager, who has the authority to flexibly schedule all the network resources. This is realizable in LANs, data center networks, or SDNs. Secondly, we assume that the bandwidth resources are sufficient to redirect traffic to scrubbing centers. The reason is twofold. On the one hand, comparing with traffic rerouting on the entrance node of the congested link, the defender has more choices to redirect the traffic to scrubbing centers, e.g., redirecting at upstream nodes. On the other hand, constraints on bandwidths exert a similar influence on the utility structures of both players as "Rerouting" does. So we make this assumption to feature "Scrubbing" as a different countermeasure from "Rerouting". One can release this assumption by slightly modifying the utility functions without challenging the main conclusions.

B. Elements of an LFA game

Consider a network $\mathcal{G}(N, L)$ where N is the set of nodes and L is the set of links. Assume that there are m links in $\mathcal{G}$. The interplay between the attacker and the network monitor, i.e., the defender of $\mathcal{G}(N, L)$ in an LFA is illustrated in Fig. 1. Let's denote the attacker to be *player 1* and the defender to be *player 2*. For $j \in \{1, 2\}$, a pure strategy s_j for player j is a function which assigns an action a_j for player j. Assume that player $-j$ (the opponent of player j) takes the strategy s_{-j}, then a best response of player j is a strategy $\bar{s}_j$ satisfies $u_j(\bar{s}_j, s_{-j}) \geq u_j(s'_j, s_{-j})$ for all $s'_j \in \mathcal{S}_j$, where $\mathcal{S}_j$ is the strategy space of player j. A strategy profile is a set of strategies in which each player has exactly one strategy. We say that a strategy profile (s^*_j, s^*_{-j}) is a Nash equilibrium (NE) if and only if for all $j \in \{1, 2\}$, all $s'_j \in \mathcal{S}_j$, $u_j(s^*_j, s^*_{-j}) \geq u_j(s'_j, s^*_{-j})$.

In LFAs, the network topology of $\mathcal{G}$ can be probed and analyzed by the attackers in order to get the routes and identify the target links within or around the target area. The maximum load capacity (i.e., link bandwidth) of each link in $\mathcal{G}$, and the possible utility structures of both players, are also easy to be known. We consider these information as *common knowledge*. Meanwhile, each player has his private information (i.e., his type) which is unknown to the other player. But based on priori and observed information, players can estimate the type of his opponent roughly, thus can further evaluate his expected payoff by Bayesian rule. Therefore, we formulate our game as an extensive form Bayesian game.

The elements of an LFA game are analyzed as follows.

- The action sets. An action $\mathcal{A}_1$ of the attacker is an assignment of attacking resources on the link set L, $\mathcal{A}_1 = (a_1, a_2, \cdots, a_m)$, where action a_i represents that he assigns an attacking traffic with volume a_i $(1 \leq i \leq m)$ to link l_i, and $a_i = 0$ stands for "**Not attack**" link l_i. An action of the defender is $\mathcal{A}_2 = (d_1, d_2, \cdots, d_m)$, where d_i $(1 \leq i \leq m)$ is a countermeasure selected from the action space $A_d = \{I, R, S\}$. Here "*I*" stands for "**Staying idle**", "*R*" means "**Rerouting**", which refers to balancing the load of the congested links to other detour links with free bandwidth, and "*S*" means "**Traffic Scrubbing**", which is one of the major DDoS countermeasures.
- The types. The attacker's type is the maximum volume of flooding traffic he can dispose. Let's denote it by F_a. The defender only knows the distribution of F_a (e.g., uniformly distributed on $[F_{min}, F_{max}]$). The attacker can use an arbitrary proportion of this volume, say $f_a = \alpha F_a (0 \leq \alpha \leq 1)$, while launching attacks. The defender's type is a vector $\phi = (\phi_1, \phi_2, \cdots, \phi_m)$, whose element ϕ_i is the benign traffic load on link l_i, $1 \leq i \leq m$. Intuitively, this is a time-varying stochastic process. We

assume that there is a stationary invariant distribution of this stochastic process. Likewise, the attacker only knows the distribution of ϕ_i.

- The strategies. A strategy of the attacker is a function $s_1 : \mathcal{F} \to \mathbb{R}^m$, which allocates the attacking resources f_a to the links in L, such that $f_a \leq F_a$. For ease of expression, we simply denote $s_1 = (a_1, a_2, \cdots, a_m)$, where $\sum_{i=1}^{m} a_i \leq F_a$. A strategy of the defender is a function $s_2 : \Phi \to A_d^m$, which assigns one countermeasure action to each link in defense based on his type ϕ. We denote it by $s_2 = (d_1, d_2, \cdots, d_m)$.

C. Utility function analysis

We next analyze the utility functions of the attacker and the defender. We consider the attacking and defending interplays towards one single link first. For any link $l_i \in L$, the average cost to flood link l_i with one unit of botnet traffic (e.g., per Gbps) is denoted by C_a. The utility of the attacker by obstructing one unit of benign network traffic is G_a. The profit that the defender can make from benign traffic load is G_d per unit of traffic. The cost to reroute one unit of network traffic is denoted by C_r, and the cost of scrubbing it (no matter it is benign or malicious) is C_s. Let b_i be the load capacity of l_i. These parameters are supposed to be known by both players.

We formulate the utility functions as $u_j(s_1, s_2, f_a, \phi)$ for $j = 1, 2$, where s_1 and s_2 are the strategies of the two players respectively, f_a is the total botnet traffic volume that the attacker imposed on all targeted links. For ease of expression, hereinafter we use a_i to represent the action profile with $a_i \neq 0$, while $a_s = 0$ for $s \neq i$, and use $d_i \in \{I, R, S\}$ to represent the corresponding defending action taken by the defender on link l_i. The utility function is thus denoted as $u_j(a_i, d_i),\ j = 1, 2$ accordingly.

If $a_i = 0$, the attacker doesn't attack l_i. The utility of the attacker will be 0 in any case, i.e., $u_1(0, d_i) = 0$ for any d_i. The utility functions of the defender are

$$\begin{aligned} u_2(a_i, I) &= \phi_i \cdot G_d, \\ u_2(a_i, R) &= \phi_i \cdot G_d, \\ u_2(a_i, S) &= \phi_i \cdot (G_d - C_s). \end{aligned} \tag{1}$$

If $a_i > 0$, we formulate the utility functions by enumerating the reactions of the defender.

1) $d_i = I$. If $a_i \leq b_i - \phi_i$, the link is not on full load, the attacker can't profit from the attack. Else, if $a_i > b_i - \phi_i$, the link congestion increases the packet loss rate, and the benign traffic load is proportionally obstructed. Since the legitimate package sources are usually distributed on the whole network, each contributes a very small amount of traffic flow, the effect of TCP congestion control is omitted here.

$$u_1(a_i, I) = \begin{cases} -a_i C_a, & a_i \leq b_i - \phi_i, \\ (1 - \frac{b_i}{a_i + \phi_i})\phi_i G_a - a_i C_a, & a_i > b_i - \phi_i. \end{cases} \tag{2}$$

$$u_2(a_i, I) = \begin{cases} \phi_i G_d, & a_i \leq b_i - \phi_i, \\ \frac{b_i}{a_i + \phi_i}\phi_i G_d, & a_i > b_i - \phi_i. \end{cases}$$

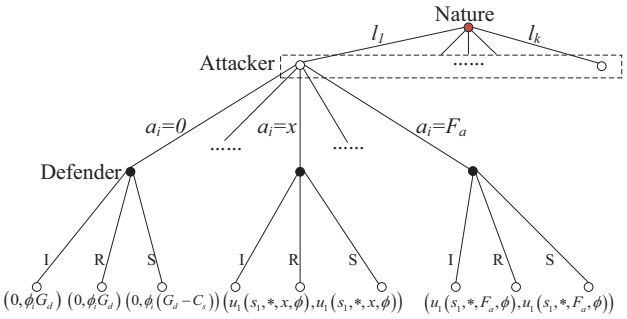

Fig. 2. Extensive form representation of an LFA game. Here we take l_1 as an example to elucidate the interplay. The dashed rectangle marked an action profile of the attacker. Formulas at the leaf nodes are the corresponding outcomes.

2) $d_i = R$. Let's denote the defender's rerouting ability towards link l_i by W_i and suppose that it is also known by the attacker. If the overflowed traffic load exceeds this capacity, the targeted link would be congested. Then we have

$$u_1(a_i, R) = \begin{cases} -a_i C_a, & a_i \leq b_i - \phi_i + W_i, \\ (1 - \frac{b_i + Wi}{a_i + \phi_i}) \cdot \phi_i G_a - a_i C_a, & a_i > b_i - \phi_i + W_i. \end{cases}$$

$$u_2(a_i, R) = \begin{cases} \phi_i G_d, \ a_i \leq b_i - \phi_i, \\ \phi_i G_d - (a_i + \phi_i - b_i) C_r, \\ \qquad b_i - \phi_i < a_i \leq b_i - \phi_i + W_i; \\ \frac{b_i + Wi}{a_i + \phi_i}\phi_i G_d - W_i C_r, \\ \qquad a_i > b_i - \phi_i + W_i. \end{cases} \tag{3}$$

3) $d_i = S$. The utility functions will be

$$\begin{aligned} u_1(a_i, S) &= -a_i C_a, \\ u_2(a_i, S) &= \phi_i G_d - (\phi_i + a_i) C_s. \end{aligned} \tag{4}$$

The game tree of LFA game is illustrated in Fig. 2. Based on the formulation of single-link utility functions, the global utility functions of both players are

$$\begin{aligned} u_1(s_1, s_2, f_a, \phi) &= \sum_{l_i \in L} u_1(a_i, d_i), \\ u_2(s_1, s_2, f_a, \phi) &= \sum_{i_i \in L} u_2(a_i, d_i). \end{aligned} \tag{5}$$

Given the types ϕ and f_a, both players can distinguish their optimal action profiles on link set L according to their strategies, which maximize the global utilities in Eq. (5), respectively.

III. Optimal strategy derivation and integration

A. Action space compression

Before solving the game, we simplify the problem by compressing the action spaces of the players to a manageable range by eliminating most of dominated strategies. For cost reasons, a target-link selection procedure is usually performed firstly by the attacker, aiming at constructing a minimal cutset between

the target area and Internet [3], using some "bottleneck" links of Internet route paths. Since the target areas are usually unclear to the defender, it is usually complicated for him to identify the potential targeted links.

Under a game theoretical perspective, action space compression problem becomes much simpler. The value of link l_i can be measured by $v_i = G_d\phi_i$. The greater v_i is, the higher priority to attack/protect l_i. So the defender can sort all the links in a descending order and protect the top k links, or determine a threshold $\bar{v}$ and protect links satisfying $v_i \geq \bar{v}$ if he want to deploy some monitor modules or probes beforehand. While the attacker can estimate ϕ_i by priori knowledge, to get an estimation $\hat{\phi}_i$, then estimate v_i based on $\hat{\phi}_i$, and implement the same link selection method as the defender does. Suppose that k critical links are selected by the attacker. We denote them by $L_t = \{l_1, l_2, \cdots, l_k\}$, then L_t can be considered as the action space for both players.

B. Optimal strategy derivation

We solve this game by firstly deducing the best strategy of the attacker, then let the defender best response to him. By a preliminary analysis of the utility functions, we get the following lemma.

Lemma 1. *If $a_i \leq b_i - \phi_i$, "Attack" is strictly dominated by "Not attack" for the attacker. Thus the attacker's strategy to a single link is either "Not attack" ($a_i = 0$) or "saturated attack" ($a_i > b_i - \phi_i$).*

Proof. Let $0 < a_i \leq b_i - \phi_i$, it suffices to show that $u_1(a_i, d_i) < 0 = u_1(0, d_i)$. This conclusion is obvious by (2), (3) and (4). □

Theorem 1. *For any $a_i > b_i - \phi_i$, $u_1(a_i, I)$ has a unique maximum point $\bar{a}_i^I = \sqrt{\frac{b_i\phi_i G_a}{C_a}} - \phi_i$, $u_1(a_i, R)$ has a unique maximum point $\bar{a}_i^R = \sqrt{\frac{(b_i+W_i)\phi_i G_a}{C_a}} - \phi_i$. For any $a_i \geq 0$, $u_1(a_i, S)$ has a unique maximum point $\bar{a}_i^S = 0$, for any $1 \leq i \leq k$.*

Proof. We take the derivatives of $u_1(a_i, I)$ with respect to a_i for $a_i > b_i - \phi_i$,

$$\frac{\partial u_1}{\partial a_i} = \frac{b_i}{(a_i + \phi_i)^2} \cdot \phi_i G_a - C_a. \tag{6}$$

By Eq. (6) we have $\frac{\partial^2 u_1}{\partial a_i^2} < 0$, i.e., $u_1(a_i, I)$ is convex with respect to a_i while $a_i > b_i - \phi_i$. We can get the unique point by letting $\frac{\partial u_1}{\partial a_i} = 0$. The same conclusion still holds for $u_1(a_i, R)$ by simply substituting b_i in Eq. (6) with $b_i + W_i$. For $u_1(a_i, S) = -a_i C_a$, $\frac{\partial u_1}{\partial a_i} < 0$, thus it is a monotone decreasing function with respect to a_i. So the unique maximum point is $a_i = 0$. Therefore the theorem holds. □

By Theorem 1, if attacking resources are sufficient, $\hat{a}_i \in \{0, \bar{a}_i^I, \bar{a}_i^R\}$ will be the optimal strategy set to l_i. The specific decision depends on his belief about the action that the defender may take after being attacked.

Now we come to the strategy analysis of the defender. In general, the defender will always take the action which maximizes his utility after observed the attacking traffic volume a_i, that is

$$d_i^*(a_i) = arg\max\{u_2(a_i, I), u_2(a_i, R), u_2(a_i, S)\}. \tag{7}$$

To make this clearer, we pairwise compare the three alternative choices of actions "*I*", "*R*" and "*S*".

- For "*I*" and "*R*"

$$u_2(a_i, R) - u_2(a_i, I) = \begin{cases} 0, & a_i \leq b_i - \phi_i, \\ (\frac{\phi_i G_d}{a_i + \phi_i} - C_r)(a_i + \phi_i - b_i), & \\ \quad b_i - \phi_i < a_i \leq b_i - \phi_i + W_i, & \\ (\frac{\phi_i G_d}{a_i + \phi_i} - C_r)W_i, & \\ \quad a_i > b_i - \phi_i + W_i. \end{cases} \tag{8}$$

- For "*R*" and "*S*", we have

$$u_2(a_i, R) - u_2(a_i, S) = \begin{cases} (a_i + \phi_i)C_s, & a_i \leq b_i - \phi_i, \\ (a_i + \phi_i)(C_s - C_r) + b_i C_r, & \\ \quad b_i - \phi_i < a_i \leq b_i - \phi_i + W_i, & \\ (\frac{b_i + W_i}{a_i + \phi_i} - 1)\phi_i G_d + (a_i + \phi_i)C_s - W_i C_r, & \\ \quad a_i > b_i - \phi_i + W_i. \end{cases} \tag{9}$$

- For "*I*" and "*S*", we have

$$u_2(a_i, I) - u_2(a_i, S) = \begin{cases} (a_i + \phi_i)C_s, & a_i \leq b_i - \phi_i, \\ (\frac{b_i}{a_i + \phi_i} - 1)\phi_i G_d + (a_i + \phi_i)C_s, & \\ \quad a_i > b_i - \phi_i. \end{cases} \tag{10}$$

Based on analysis of (8)-(10), we get the following theorem.

Theorem 2. *The defender's optimal strategy in response to the attack action a_i on link l_i complies with the following principles:*

1) *If $a_i \leq b_i - \phi_i$, then $d_i^* = I$ (or $d_i^* = R$ since they are indifferent in such situation).*
2) *If $b_i - \phi_i < a_i \leq b_i - \phi_i + W_i$, then*

$$d_i^* = \begin{cases} R, & g_{RI} \geq 0, \\ I, & g_{RI} < 0. \end{cases} \tag{11}$$

where $g_{RI} = \frac{\phi_i G_d}{a_i + \phi_i} - C_r$.

3) *If $a_i \geq b_i - \phi_i + W_i$, then*

$$d_i^* = \begin{cases} R, & g_{RI} \geq 0 \text{ and } g_{RS} \geq 0, \\ S, & g_{RS} < 0 \text{ and } g_{IS} < 0, \\ I, & g_{RI} < 0 \text{ and } g_{IS} \geq 0. \end{cases} \tag{12}$$

where $g_{RS} = (\frac{b_i + W_i}{a_i + \phi_i} - 1)\phi_i G_d + (a_i + \phi_i)C_s - W_i C_r$, $g_{IS} = (\frac{b_i}{a_i + \phi_i} - 1)\phi_i G_d + (a_i + \phi_i)C_s$.

Proof. It is obvious that 1) holds by checking the corresponding formulas. We only prove 2) and 3). By Eq. (8) we find that if $C_r > \frac{\phi_i G_d}{a_i + \phi_i}$ for $a_i > b_i - \phi_i$, "*R*" is strictly dominated by "*I*". It indicates that if the costs of rerouting is too expensive or the attacking traffic volume is too heavy,

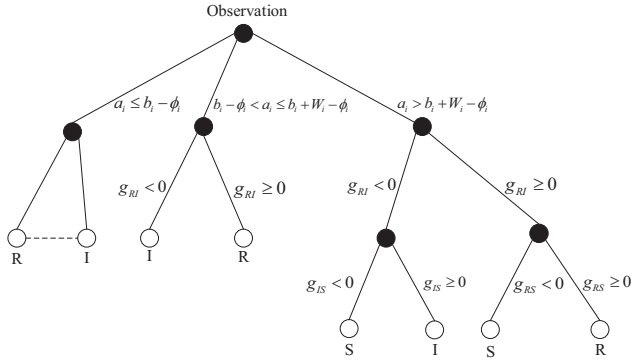

Fig. 3. The decision tree of the defender condition on observed a_i. The dashed line means that the connected two strategies are indifferent.

the defender would rather stay idle while being attacked. Note that $g_{RI} = \frac{\phi_i G_d}{a_i + \phi_i} - C_r$, then action "*R*" dominates "*I*" if and only if $g_{RI} \ge 0$, i.e., $a_i \le \frac{(G_d - C_r)\phi_i}{C_r}$.

Note that $C_s > C_r$ always holds since "Rerouting" is the first necessary step to implement traffic scrubbing. By Eq. (9) we know that "*S*" is dominated by "*R*" if and only if $g_{RS}(a_i, \phi_i) \ge 0$ when $a_i > b_i - \phi_i + W_i$.

Similarly, by Eq. (10) we have "*S*" is dominated by "*I*" if and only if $g_{IS}(a_i, \phi_i) \ge 0$ when $a_i > b_i - \phi_i$. By synthesizing the discussions above, Theorem 2 follows. □

Note that $g_{RS} = g_{IS} + W_i g_{RI}$, Theorem 2 covers all the decision cases the defender may confront. The integrated decision process is illustrated in Fig. 3. Since the utility structure is actually determined by the action of the defender, a rational attacker would deduce the possible reactions of the defender adequately before making up his mind. Based on Theorem 1 and 2, the attacker can determine his optimal strategy on each link by implementing the following steps.

1) Estimating ϕ_i by priori knowledge. If the estimation $\hat{\phi}_i \le \frac{b_i C_a}{G_a}$, then $a_i^* = 0$. Else, turn to step 2).
2) Calculating his alternative strategies using Theorem 1, $\hat{a}_i^I$ and $\hat{a}_i^R$.
3) Implementing the strategy in Theorem 2 by substituting $\hat{\phi}_i$ and $\hat{a}_i^I$ for ϕ_i and a_i, predicting the possible response action $\hat{d}_i$ of the defender. If $\hat{d}_i = I$ and $u_1(\hat{a}_i^I, I) > 0$, then $a_i^* = \hat{a}_i^I$. Else, turn to step 4).
4) Predicting d_i similarly using $\hat{\phi}_i$ and $\hat{a}_i^R$. If the prediction $\hat{d}_i = R$ and the corresponding utility $u_1(\hat{a}_i^R, R) > 0$, then $a_i^* = \hat{a}_i^R$. Else, turn to step 5).
5) If the strategy hasn't been determined by the steps above, then let $a_i^* = 0$.

Note that the attacker would prefer $\hat{a}_i^I$ to $\hat{a}_i^R$ because the latter requires more attacking resources while generates equal profit. It's obvious that (a_i^*, d_i^*) is an *Bayesian Nash Equilibrium* (BNE) of the LFA game on link l_i since neither of the players has a motivation to deviate form it.

C. Strategy Integration

In order to obtain an integrated strategy profile of the game on the whole network, we aggregate the BNE derivating methods on each link to a global strategy. If the attacking/defending resources are sufficient, the local optimal strategy is already global optimal one. However, this may not be true in practice. A problem that both players encounter is how to optimally allocate their limited resources.

For the attacker, the upper bound of attacking traffic volume is F_a. He may need to solve a linear programming (LP) problem to maximize his utility function $u_1(s_1, *, f_a, \hat{\phi})$ subject to $f_a \le F_a$. Yet in our LFA game this problem can be approximately solved by simply considering $a_i \in \{0, \bar{a}_i^I, \bar{a}_i^R\}$ and $d_i \in \{I, R, S\}$ using method of exhaustion since k is usually small. We ignore the details.

For the defender, defending resources are sufficient seemingly, but because of cost considerations, he may want to employ defending resources as less as possible. It suffices for him to protect the links with top k values. Alternatively, he can predict the attacking behaviors by adversary modeling. The defender may form a belief on the maximum attacking capacity F_a of the attacker based on his priori and predict the actions of the attacker by solving a similar LP problem as above. By doing so, a global strategy profile under cost minimization can be obtained.

IV. Performance Evaluation

To verify the effectiveness and robustness of our proposed defending strategy, we simulate the interplay process in explicit network communication scenarios. Since the aggregated defending profit on the whole network is the summation of which on every single link, we only consider the defending profit on one link l. The LFA defending methods mentioned in section I mitigate attacking traffic without cost and benefit considerations, thus they are not suitable to compare with our method. The strategies for comparison are two of most typically used in industry, we name them by "Simply Rerouting" and "On-condition Scrubbing", respectively. "Simply Rerouting" is the strategy that once congestion is detected, rerouting the redundant traffic load immediately to spare paths. "On-condition Scrubbing" is the strategy that if packet loss probability exceeds some intolerable threshold, then diverting the relevant traffic to a scrubbing center. We take this threshold as 50% in our experiments.

The link capacity of l is set to be $b_l = 10$ Gbps. The average value of benign traffic, G_d, is supposed to be 1000 per Gigabit, the cost to reroute network traffic is supposed to be $C_r = 10$ per Gigabit, and the cost of scrubbing it is $C_s = 40$ per Gigabit. The rerouting ability towards link l is $W_i = 20$ Gbps. The volume of attacking traffic rises from 0 Gbps to 100 Gbps and persists for one second in every iteration. The volume of benign traffic on link l, denoted by ϕ_l, is drawn from a uniform distribution on $[0, b_l]$. We average the outputs of 1000 experiments, the final result is illustrated in Fig. 4. The performances of our strategy and "Simply rerouting" are very close when the volume of attacking traffic is less than 25

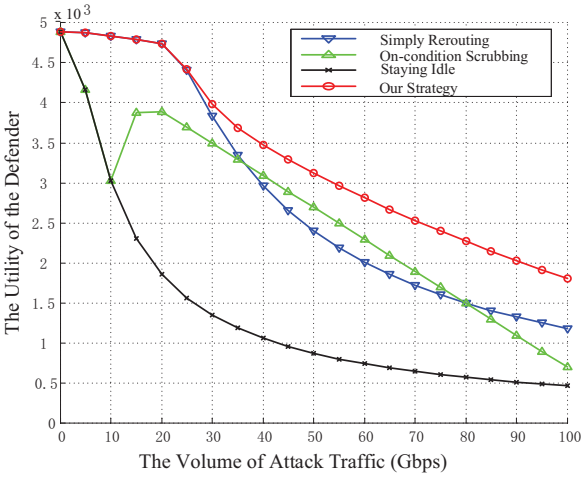

Fig. 4. The effectiveness comparison of different defending strategies. The abscissa axis refers to the volume of attacking traffic, while the ordinate axis represents the utility of the defender. The performance of "Staying idle" is also plotted as supplement for comparison.

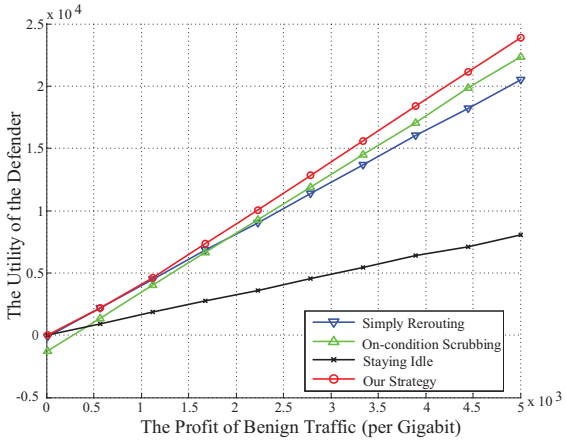

Fig. 5. The robustness comparison of different defending strategies. The abscissa axis refers to the profit of benign traffic, while the ordinate axis represents the utility of the defender. The performance of "Staying idle" is also plotted as supplement for comparison.

Gbps since they take the same actions. While as the attacking traffic gets heavier, our proposed strategy overwhelms others in utility performance.

Since the business value of network traffic may vary in different kind of applications, we implement another experiment to verify the robustness of our strategy. The value of benign traffic, G_d is set to be ranged from 10 to 5000. The volume of benign traffic ϕ_l is set to be 5 Gbps. The volume of attacking traffic is drawn from a uniform distribution on $[10, 50]$ Gbps. Other parameters remain as above. We also average the results for 1000 experiments, as illustrated in Fig. 5. Our strategy outperforms all other strategies in every value levels while G_d is greater than about 1000, and performs as good as "Simply Rerouting" Strategy while G_d is less than 1000 since they take identical actions. This verifies the robustness of our strategy with regard to the variation of business application.

V. Conclusion

In this work, we have modeled the interplay of LFAs as a two-person extensive form Bayesian game. We have analyzed and solved the LFA game using the divide and conquer method, deduced the local optimal strategies for both players link by link. Then we have discussed how to integrate the local optimal strategies to a global one under resource constraints. Moreover, we have verified the effectiveness as well as the robustness of our proposed strategy, which has further confirmed that the model and methods proposed in this work are available for practical cybersecurity confrontation.

References

[1] T. Alpcan and T. Başar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proc. IEEE Int. Conf. Decis. Control*, Maui, HI, USA, 2003, pp. 2595–2600.

[2] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: an architecture for mitigating DDoS attacks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 1, pp. 176–188, Jan. 2004.

[3] M. S. Kang, S. B. Lee, and V. D. Gligor, "The crossfire attack," in *Proc. IEEE Symp. Secur. Priv.*, Berkeley, CA, USA, 2013, pp. 127–141.

[4] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, Feb. 2013.

[5] C. Liaskos, V. Kotronis, and X. Dimitropoulos, "A novel framework for modeling and mitigating distributed link flooding attacks," in *Proc. IEEE INFOCOM*, San Francisco, CA, USA, 2016.

[6] C. Liaskos and S. Ioannidis, "Network topology effects on the detectability of crossfire attacks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1682–1695, Jul. 2018.

[7] G. Yang, H. Hosseini, D. Sahabandu, A. Clark, J. ao Hespanha, and R. Poovendran, "Modeling and mitigating the coremelt attack," in *Proc. Annu. Amer. Control Conf.*, Milwaukee, WI, USA, 2018, pp. 3410–3416.

[8] A. Furfaro, P. Pace, and A. Parise, "Facing DDoS bandwidth flooding attacks," *Simul. Model. Pract. Theory*, vol. 98, no. 101984, pp. 1–12, Sep. 2019.

[9] J. M. Smith and M. Schuchard, "Routing around congestion: Defeating DDoS attacks and adverse network conditions via reactive BGP routing," in *Proc. IEEE Symp. Secur. Priv.*, San Francisco, CA, USA, 2018, pp. 599–617.

[10] M. Tran, M. S. Kang, H.-C. Hsiao, W.-H. Chiang, S.-P. Tung, and Y.-S. Wang, "On the feasibility of rerouting-based DDoS defenses," in *Proc. IEEE Symp. Secur. Priv.*, San Francisco, CA, USA, 2019, pp. 1169–1184.

[11] X. Ma, J. Li, Y. Tang, B. An, and X. Guan, "Protecting internet infrastructure against link flooding attacks: a techno-economic perspective," *Inf. Sci.*, vol. 479, pp. 486–502, Apr. 2019.

[12] J. Wang, W. Ru, J. Li, Y. Fei, and F. Yu, "Detecting and mitigating target link-flooding attacks using SDN," *IEEE Trans. Dependable Secure Comput.*, vol. PP, no. 99, pp. 1–13, 2018.

[13] L. Wang, Q. Li, Y. Jiang, X. Jia, and J. Wu, "Woodpecker: Detecting and mitigating link flooding attacks via SDN," *Comput. Netw.*, vol. 147, pp. 1–13, Sep. 2018.

[14] L. Chen and J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," *IEEE Trans.Inf. Forensics Security*, vol. 4, no. 2, pp. 165–178, Jun. 2009.

[15] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Attacker-centric view of a detection game against advanced persistent threats," *IEEE Trans. Mobile Comput.*, vol. 17, no. 11, pp. 2512–2523, 2018.

[16] X. Ma, B. An, M. Zhao, X. Luo, L. Xue, Z. Li, T. T. Liu, and X. Guan, "Randomized security patrolling for link flooding attack detection," *IEEE Trans. Dependable Secure Comput.*, Jan. 2019.

[17] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games: Looking beyond a decade of success," in *Proc. Int. Joint Conf. Artif. Intell.*, Stockholm, Sweden, 2018, pp. 5494–5501.