INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS
VOL. 12, NO. 4, DECEMBER 2007, 307-316

How Resilient is the Internet against DDoS attacks? — A Game Theoretic Analysis of Signature-based Rate Limiting

Wanyu ZANG, Peng LIU, and Meng YU

***Abstract*— DDoS attack is a serious threat to the Internet. Although some DDoS attacks with clear signatures can be effectively countered by existing DDoS defense measures, most DDoS attacks without clear signatures (e.g., brute-force DDoS attacks) are very difficult to counter cost-effectively, since the defense system is not clear which packets are DDoS packets and which are not. Although several rate-limiting methods are proposed to counter the unclear signature DDoS attacks, each may drop good packets and their cost-effectiveness are not clearly understood. People would have a more urgent need to understand clearly the impact of the unclear signatures DDoS attacks on their network services. This paper presents a game theoretic analysis of the Internet's resilience against unclear signatures DDoS attacks when signature-based rate limiting is deployed, where (a) countering DDoS attacks is modeled as a Bayesian game, (b) a high volume of simulations is done to compute the Nash equilibria of the game, (c) a family of Nash equilibrium based resilience analyses are done, and (d) the *upper* bound of the defense system's resilience under unclear signatures DDoS attacks and which kinds of attacking strategies are more dangerous or more likely to be enforced by the attacker are given in the simulations. Our analysis may substantially improve people's understanding about the nature of (a) the DDoS threat and (b) the defense system's resilience against this threat.**

***Index Terms*— Game theory, Bayesian Game, DDoS attack.**

1. INTRODUCTION

In recent years, Internet Distributed Denial-of-service (DDoS) attacks [24] have increased in frequency, severity and sophistication and become a major security threat. A DDoS attack typically involves many zombies and a high volume of packets targeting the *victim*. To make sure that no host will ever send out such a DDoS packet is not a practical goal (due to the inherent vulnerability of computer systems), and most of the existing DDoS defense measures focus on how to exploit the attack-relevant information contained in a DDoS packet (and/or a router) to filter, rate-limit, detect, or trace back DDoS packet streams.

There are a variety types of DDoS attacks. Nevertheless, based on whether a DDoS packet stream has some unique features which can somehow "distinguish" itself from non-DDoS packets, DDoS attacks can be roughly classified into two classes: (A) DDoS attacks with clear *signatures*; and (B) DDoS attack with unclear signatures. The literature shows that Class A DDoS attacks may be effectively defended. For example, (1) SYN flooding attacks can be effectively detected [25] and countered (e.g., using SYN cookies) based on the signature (or feature) that SYN flooding packets only ask to but never really open a TCP connection; (2) Ingress filtering [7] can filter out the DDoS packets whose source addresses do not have a prefix matching the subnet of the sender. (3) Router-based packet filtering [20] can filter out the DDoS packets whose (spoofed) source addresses indicate that to reach the destination, they should never be forwarded by a specific router who is however forwarding them (during the attack).

However, Class B DDoS attacks are in general very difficult to counter cost-effectively. For one example, brute-force DDoS attacks (e.g., the Mstream DDoS attack) use authentic source addresses and do not exploit any security hole of TCP, ICMP, or UDP, but they can be very harmful and difficult to counter when a large number of zombies are sending DDoS packets while each one does not send a high volume of packets. Detecting class B DDoS attacks is difficult and time consuming since they do not have clear signatures. Although tracing-back is a technically easier job for Class B DDoS attacks, it is primarily a reactive technique; it can stop severe DDoS phenomena from continuing but cannot prevent them from happening.

Fortunately, several proactive Class B DDoS defense methods are recently developed and are promising. We call them *signature-based rate limiting* (SBRL) techniques since they are all based on the idea of making the routers be able to identify and rate-limit a specific set of packet streams (or aggregates) that are very possible to cause congestion or DoS. Each of the specific set of packet streams will match a specific *signature* which is associated with a unique feature of the packet stream. A representative SBRL technique is *pushback* [14]. Although the merit of SBRL is shown by some experiments, SBRL may drop good packets and its cost-effectiveness is not clearly understood due to several reasons. (1) Since Class B DDoS attacks do not have clear signatures, SBRL cannot guarantee that no good packets will be put into a rate-limited packet stream, and good packets can be dropped together with DDoS packets. (2) The effectiveness of defense measures such as SBRL is *relative* to a specific Class B DDoS attack. A SBRL technique may very effective to a Class B DDoS attack, but it may not still effective to another kind of Class B DDoS attack. On the other hand, a Class B DDoS attack that defeats a SBRL mechanism may be defeated by another SBRL mechanism. The relative nature indicates that Class B DDoS attack and SBRL have interdependent relationship.

Wanyu Zang and Meng Yu are with Western Illinois University, IL 61455, USA. Email: w-zang@wiu.edu, m-yu2@wiu.edu

Peng Liu is with Pennsylvania State University, University Park, PA 16802, USA. He was supported in part by DOE Early Career Principal Investigator Award. Email:pliu@ist.psu.edu

As Class A defense measures are more and more widely deployed, the attacker may be "forced" to enforce more Class B DDoS attacks which can surround these Class A defense measures and cause serious DDoS effects. As people are experienced with more Class B DDoS attacks, people would have a more urgent need to understand clearly the impact of Class B DDoS attacks on their network services, the overall resilience of the Internet's against Class B DDoS attacks, and the better defense strategies.

This paper presents a game theoretic analysis of the Internet's resilience against Class B DDoS attacks when signature-based rate limiting is deployed, where (a) countering Class B DDoS attacks is modeled as a Bayesian game, (b) a high volume of simulations is done to compute an approximate solution of the game, and (c) a family of Nash equilibrium based resilience analyses are done. Our analysis shows that the Nash equilibria (of the game) and the associated payoffs indicate how resilient the defense system is. Our analysis not only estimates the *upper* bound of the defense system's resilience under Class B DDoS attacks, but also shows that the distribution of the Nash equilibria over the set of attack/defense strategy parameters indicates (1) which kinds of DDoS attacks are more likely to be enforced by the attacker and (2) which kinds of SBRL mechanisms are more effective in the simulation.

To out best knowledge, this study is the first game theoretic (optimization) analysis of DDoS attacks and defense. The relativity (or *strategy-interdependence*) nature of defending against Class B DDoS attacks implies the unique advantage of the game theoretic analysis performed in this paper. Our analysis may substantially improve people's understanding about the nature of (a) the DDoS threat and (b) the Internet's resilience against this threat. The insights gained through this study may motivate new breakthroughs in DDoS research.

The rest of the paper is organized as follows. We discuss the rationale of game theoretic analysis in Section 2. In Section 3, we propose our game model and analyze the solution. We present a simulation-based solution to the game, and perform the family of Nash equilibrium based resilience analyses in Section 4. In Section 5, we discuss the legitimate user aspect of the game and the impact of changes of network scenarios. We address the related work in Section 6 and conclude the paper in Section 7.

2. The fighting between Class B DDoS attacks and SBRL is a Bayesian game

The fundamental characteristics of the Class B DDoS attacks–SBRL relationship is interdependent. When fighting with Class B DDoS attacks, the effectiveness of SBRL depends on not only its strategy, but also the attacker' strategy. On the other hand, when fighting with SBRL, the effectiveness of the Class B DDoS attacks depends on not only attacker's strategy, but also the system's strategy. Besides, the legitimate users strategies also affect the strategies and payoffs of both the defense system and the attacker. Game theory is the primary tool to handle the strategic interdependence.

A Bayesian game [8] is an incomplete information game, which includes a set of player, a strategy spaces for each player, a type set for each player and payoff functions of players. In a game, the sets of players, the set of actions and the utility functions are known by all players while the type of the player is private. Each player knows the type of himself but none of others. A player knows the probability distribution of other players' types.

Similarly, between a Class B DDoS attacker and a SBRL defense system, the defense system and the attacker can learn the strategy space, the payoff functions of each other from public, such as websites or technical reports. Nevertheless, the defense system dose not know which traffic is really malicious or legitimate. When the defense system identifies a malicious traffic, it is possible that the defense system makes mistake. Only the attacker knows which traffic are his and legitimate users know which traffic are their. The information they have perfectly matches the definition of a Bayesian game. So we believe the game between the DDoS attacker and SBRL defense system is a Bayesian game.

Kodialam uses a *zero-sum* game [19] to model the detect of network intrusion and Lye uses a stochastic game to model the attacker and the administrator [13]. Both the zero-sum and stochastic games assume that the player knows other players very well. But in the Class B DDoS attacks, SBRL cannot distinguish the malicious user from legitimate users accurately. The zero-sum and stochastic games cannot handle the situation with incomplete information about the players' type, while a Bayesian game is perfect to model the game with this uncertainty. So, we believe that our Bayesian model is more suitable to model Class B DDoS attacks vs. SBRL defense system than the zero-sum and stochastic games.

3. Modeling defending DDoS attacks

3.1. Our model

We model the game between the Signature-based rate limiting defense system and users (the attacker and legitimate users) with a specific 2-player Bayesian game. Before we introduce the formal form of the game model, we define the set of players, the strategy space, the type set, the belief set and the payoff function for each player first.

There are two players in the game. One is the defense system d and the other is the user u (the attacker or the legitimate users, note that the defense system cannot identify the attacker clearly). The strategy space of the defense system is A_d, which consists of defending tasks.

We use communication task, e.g., visiting a web-sites, transferring file or a DDoS attacking, to construct the strategy space of the user (A_u). The task can be characterized by *the number of sources, the destination, the rate, the traffic pattern* and so on. Each task may involve more than one host. For example the attacker may have many zombies to launch an attack. The defense system has only one type, so its type set is $T_d = D$. The user has two types, say, attacker (A) and legitimate user(L), so the type set is T_u=$\{L, A\}$ and the user type is privately known by the user himself. The defense system has *belief* about the probability distribution of the user's type. The belief set of the defense system is $P_d = \{P_d(A|D), P_d(L|D)\}$. If $P_d(A|D)$=θ, which indicates that the

defense system believes that the possibility of a user being an attacker is θ, given its own type is D. Then $P_d(L|D)=1-\theta$. The belief set of the user is $P_u = \{P_u(D|L), P_u(D|A)\}$ and $P_u(D|L)=P_u(D|A)=1$. When the defense system and the attacker select their strategies, each of them gets some payoffs, which is determined by their payoff functions $\{U_u, U_d\}$.

The formal form of the game is denoted by DDoSGM=$\{A_u, A_d, T_u, T_d, P_u, P_d, U_u, U_d\}$, where $A_u=\{T_1,\cdots T_i,\ldots,T_n\}$ is the strategy space of users. T_i is a communication task. $A_d=\{D_1,\cdots, D_i,\cdots,D_m\}$ is the strategy space of the defense system. D_i is a defense task. T_u and T_d are type spaces of the user and the defense system respectively. P_d is the belief set of the defense system, P_u is the belief set of the user.

$U_u(D_i,T_i;L)= U_l = B_{lo}/B_{lw}$ and $U_a(D_i,T_i;A)=U_a=\alpha B_{ao}/B_t + (1-\alpha)(1-B_{lo}/B_{lw})$ are the payoff functions for the legitimate user and the attacker respectively, where B_{lo} is the network bandwidth occupied by the legitimate user, B_{lw} is the bandwidth that legitimate users want to occupy, B_{ao} is the bandwidth occupied by the attacker and B_t is the target network bandwidth that the attacker tries to attack, α is the weight and less than 1.

$U_d = (1-\theta)U_d^L(D_i,T_i;L) + \theta U_d^A(D_i,T_i;A)$, $U_d^L(D_i,T_i;L) = B_{lo}/B_{lw}$ and $U_d^a(D_i,T_i;A) = -B_{ao}/B_t$, is the payoff function of the defense system, where $U_d^L(D_i,T_i;L)$ and $U_d^A(D_i,T_i;A)$ are payoffs of the system given the users type is L(legitimate) and A(Attacker) respectively.

The payoff functions represent interests. For the legitimate users, they mainly concern whether they can obtain the network bandwidth that they need. U_l represents the obtained service ratio of legitimate user. For the attacker, he wants to consume as more resources as possible to prevent the legitimate users from getting service. U_a represents the attacking capacity of the attacker. The attacker has two interests, occupied malicious bandwidth ratio B_{ao}/B_t and legitimate users' service loss ratio $1-B_{lo}/B_{lw}$. The occupied malicious bandwidth ratio determines the upper bound of the available bandwidth for legitimate users and it is also an very important goal in *degrading DDoS attack* [17]. For example when the legitimate traffic rate is only 5 percent of bandwidth and $B_{ao}/B_t = 0.9$, although the legitimate users' service loss ratio is zero, attacker knows the available bandwidth for legitimates users at most 10 percent of the bandwidth. α weights the interest of the attacker and its value is between 0 and 1. If the attacker is more interested in occupying the network bandwidth, then he can increase the α. For the defense system, it would like to supply all the resources to legitimate users and do not give resources to bad ones. U_d represents the resilient capacity of a defense system against the DDoS attacks. Each of the maximum obtained service ratio of legitimate users, the maximum attacking capacity of the attacker and the maximum resilient capacity of the defense system is 1.

All of the legitimate users, the attacker and the defense system want to find the Nash equilibria strategies (T^{l*}, T^{a*}, D^*) from their strategies space A_u, A_d to maximize their payoffs,

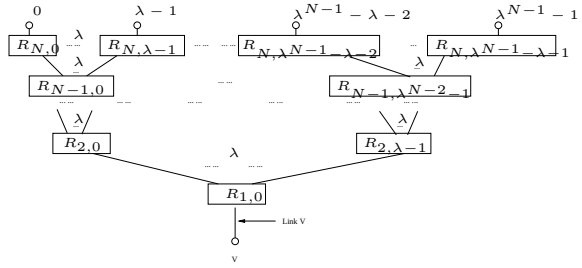


Fig. 1. An example of DDoS attacks scenario

where (T^{l*}, T^{a*}, D^*) must satisfy:

$$U_u(D^*, T^{l*}; L) \geq U_u(D^*, T_i^l; L) \quad (1)$$

$$U_u(D^*, T^{a*}; A) \geq U_u(D^*, T_i^a; A) \quad (2)$$

$$(1-\theta)U_d^L(D^*, T^{l*}; L) + \theta U_d^A(D^*, T^{a*}; A) \geq (1-\theta)U_d^L(D_i, T^{l*}; L) + \theta U_d^A(D_i, T^{a*}; A) \quad (3)$$

where $T_i^l \in A_u \wedge T^{l*} \neq T_i^l$, $T_i^a \in A_u \wedge T^{a*} \neq T_i^a$ and $D_i \in A_d \wedge D^* \neq D_i$.

In the paper we mainly consider strategies and payoffs of the attacker and the defense system since they are the most active players who monitor the payoffs all the time and change their strategies. We discuss the legitimate users strategies and payoffs in session 5.

3.2. Analytic solution

In this section, we give the analytic solution considering relative restrict assumptions. To solve (T^{l*}, T^{a*}, D^*), we need to calculate payoffs first. consider the network in Figure 1. In the Figure, the attacker launch Class B DDoS attacks to consume the bandwidth of link V. The circles are hosts, and the rectangles are routers. Except for the router at the highest level, each router has a fan-in of λ. The bandwidth of link V is B. The routers have N levels and there are totally $M = \lambda^{N-1}$ hosts. Each host connects to a router at level N. The router j at level i is denoted as $R_{i,j}$. We assume that there are M_A zombies and M_L legitimate users. Each zombie sends packets to V at rate r_a and each legitimate user sends packets to V at rate r_l. The signatures of malicious traffic and legitimate traffic are s_a and s_l respectively, which are related to the source address, destination address, flow id, aggregate and other properties of the traffic. We assume that there is a SBRL defense system consists of the routers along the path from zombie to the victim. For simplicity, we do not consider the legitimate traffics that go through the routers and are not sent to V although they may be affected by the defense system. For each router $R_{i,j}$, we denote the malicious and legitimate traffic incoming rate to $R_{i,j}$ by $R_{i,j,Ain}$ and $R_{i,j,Lin}$ respectively. We denote the malicious and legitimate traffic outgoing rate from $R_{i,j}$ by $R_{i,j,Aout}$ and $R_{i,j,Lout}$ respectively.

The SBRL mechanism cannot identify the malicious signature accurately. The routers may drop some legitimate packets and let some malicious packets pass. We define that the false positive dropping ratio (FPDR) and the false negative dropping ratio (FNDR) for $R_{i,j}$ are $FP_{i,j}$ and $FN_{i,j}$. $FP_{i,j}$ is given by the number of packets dropped by $R_{i,j}$ as attack packets

that are in fact legitimate, divided by the total number of legitimate packets. $FN_{i,j}$ is given by the number of malicious packets that pass $R_{i,j}$ as legitimate packets, divided by the total number of malicious packets. In fact, some routers may not drop packets since they did not detect any congestion or receive any requests to control the traffic. We consider that these routers are also part of the defense system and their FPDR is 0 and FNDR is 1. We assume that the routers in the defense system have same configurations, which is denoted by C. We also assume the router based on the incoming traffic and its configurations to identify and control the traffic. Then, we have $FP_{i,j} = f(R_{i,j,Ain}, R_{i,j,Lin}, s_a, s_l, C)$ and $FN_{i,j} = g(R_{i,j,Ain}, R_{i,j,Lin}, s_a, s_l, C)$

We assume that the zombies and legitimate users are unified distributed among the hosts. For each router k at the level N, The $R_{N,k,Ain} = \frac{r_a M_A}{\lambda^{N-1}}$, $R_{N,k,Lin} = \frac{r_l M_L}{\lambda^{N-1}}$. For each router at level N, the incoming traffic is same, so does the outgoing traffic. Similarly, for each router at the same level, the incoming traffic is same. Then, the FPDR and FNDR are same. Therefore, for the routers at level j $FP_{j,1} = FP_{j,2} = \cdots = FP_{j,\lambda^{i-1}} = FP_j$ and $FN_{j,1} = FN_{j,2} = \cdots = FN_{j,\lambda^{i-1}} = FN_j$.

In the example, the attacker's strategy is determined by $\langle M_A, r_a, s_a \rangle$; the legitimate users' strategy is determined by $\langle M_L, r_l, s_l \rangle$; and the defense system's strategy is determined by $\langle C \rangle$. We set $\alpha = 0.5$. The payoff of each player is

$$U_l = R_{1,Lout} = \prod_{j=1}^{N}(1 - FP_j)$$

$$U_a = R_{1,Aout} = \frac{r_a M_a \prod_{j=1}^{N} FN_j}{2B} + \frac{(1 - \prod_{j=1}^{N}(1 - FP_j))}{2}$$

$$U_d = (1-\theta)\prod_{j=1}^{N}(1 - FP_j) - \theta\frac{r_a M_a \prod_{j=1}^{N} FN_j}{2B}$$

The Nash equilibria strategies $\{\langle M_L^*, r_l^*, s_L^* \rangle, \langle M_A^*, r_a^*, N^*, s_a^* \rangle, \langle C^* \rangle\}$ are described by the following equations. The Nash equilibria strategies satisfy Equation 1, 2 and 3. We have

$$\prod_{j=1}^{N}(1 - FP_j^*)) \geq \prod_{j=1}^{N}(1 - FP^{li})) \tag{4}$$

$$\frac{r_a^* M_A^* \prod_{j=1}^{N} FN_j^*}{2B} + \frac{1 - \prod_{j=1}^{N}(1 - FP_j^*)}{2} \geq \frac{r_a^i M_A^i \prod_{j=1}^{N} FN_j^{ai}}{2B} + \frac{1 - \prod_{j=1}^{N}(1 - FP_j^*)}{2} \tag{5}$$

$$(1-\theta)\prod_{j=1}^{N}(1 - FP_j^*) - \theta\frac{r_a^* M_A^* \prod_{j=1}^{N} FN_j^*}{2B} \geq (1-\theta)\prod_{j=1}^{N}(1 - FP_j^{di}) - \theta\frac{r_a^* M_A^* \prod_{j=1}^{N} FN_j^{di}}{2B} \tag{6}$$

$$FP_j^* = f(R_{j,Ain}^*, R_{j,Lin}^*, s_a^*, s_l^*, C^*) \tag{7}$$

$$FN_j^* = g(R_{j,Ain}^*, R_{j,Lin}^*, s_a^*, s_l^*, C^*) \tag{8}$$

$$FP_j^{li} = f(R_{j,Ain}^*, R_{j,Lin}^i, s_a^*, s_l^i, C^*) \tag{9}$$

$$FN_j^{ai} = g(R_{j,Ain}^i, R_{j,Lin}^*, s_a^i, s_l^*, C^*) \tag{10}$$

$$FP_j^{di} = f(R_{j,Ain}^*, R_{j,Lin}^*, s_a^*, s_l^*, C^i) \tag{11}$$

$$FN_j^{di} = g(R_{j,Ain}^*, R_{j,Lin}^*, s_a^*, s_l^*, C^i) \tag{12}$$

In Equations, $M_L^i, r_l^i, s_L^i \in A_u \wedge i \neq *$ is a strategy in the attacker' strategies spaces , $M_A^i, r_a^i, N^i, s_a^i \in A_u \wedge i \neq *$ is a strategy in the legitimate users' strategies spaces, and $C^i \in A_d \wedge C^i \neq C^*$ is a strategy in the defense system's strategies spaces.

4. SIMULATIONS

In this section we evaluate the Nash equilibria strategies by simulation. we start from the network configuration, then we describe how the attacker and system strategies affect the capacity of the attacker and the defense system. After that we analyze the Nash equilibria (optimal) strategies, the upper bound of the resilient capacity of the defense system and attacking capacity of the attacker. Finally we discuss which kinds of strategy are more likely to be enforced by the attacker and the defense.

4.1. Network configuration

Our simulation system is based on ns-2 [1]. In our simulation, we select Pushback as the defense mechanism. Pushback is a kind of signature-based defense scheme. Unlike other defense systems that usually identify the signature based on the flow, source or destination address, Pushback uses *aggregate* (a collection of packets from one or more flows that have some property in common) to construct the *congestion signature*. The defense system can choose various aggregate properties according to the different attack scenarios to identify the congestion signature more accurately, which makes pushback more flexible, comprehensive and effective against the DDoS attacks.

Pushback has two Aggregate-based Congestion Control (ACC) mechanisms. The first is Local ACC and the second is Pushback. Local ACC consists of an agent to identify the congestion signature based on the given aggregate property

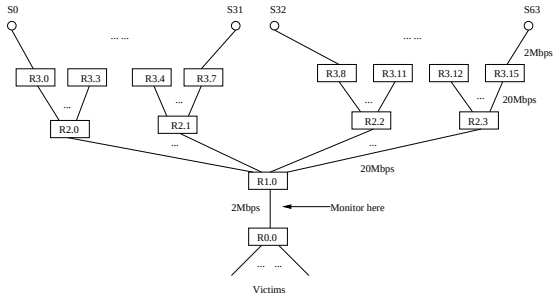


Fig. 2. Network topology

and a rate limiter before the output queue to control the corresponding aggregates to a reasonable level. When the router detects a congestion, it will request adjacent upstream routers to rate-limit the corresponding aggregates by sending pushback message. The message includes the malicious aggregate signature and the threshold of rate limit. There are good users, poor users and attackers in Pushback. The poor users and good users are both legitimate users. The packets sent by poor users have the same aggregates as the bad users, so they may be considered as bad ones by the defense system.

Figure 2 is the network topology of our experiment, which is similar with Figure 1 and is the same as the experimental topology of Pushback [14]. In the figure, the circles represent the source hosts, we randomly select zombies of attacker and legitimate users from these hosts. Zombies launch the Class B DDoS attack by flooding packets. The rectangles represent the routers. Except for the router at the lowest level, each router has a fan-in of 4. Every router has a Pushback agent to detect and control the traffic. The link bandwidths are shown in the Figure, and have been allocated such that congestion is limited to the access links at the top and bottom. We set $\alpha = 0.5$ and $\theta = 0.99$ when we calculate the payoffs.

4.2. Strategies for the defense system and the attacker

The system's strategies have many parameters, such as the number of routers, the topology, the configuration of each router and so on. In our experiments, for the given topology we mainly concern some specific parameters in each router. Let $A_d = \langle$*aggregate property, congestion checking time, cycle time, target drop rate, free time, rate limit time, maximum session*$\rangle$. The default value of the the parameters are $\langle$*destination address prefix, 2s, 5s, 0.05, 20s, 30s, 3*$\rangle$, which are explained as follows.

In pushback, agents identify the malicious traffic based on the aggregate property. The aggregate property usually includes the destination address prefix, source address prefix, the protocol layer, the flow id or their combinations. *Congestion checking time* is the interval time that the router checks congestion. When serious congestion is detected, the Local ACC will identify the aggregate(s) responsible for the congestion. *Cycle time* is the interval time that the agent reviews the limit imposed on the aggregates and sends refresh to the adjacent upstream routers to update the rate limit. The *target drop rate* is the upper bound of drop rate of the output queue. In order to achieve the given *target drop rate*, the rate limiter should let the rates sending to the output queue be less than $B/(1-tdr)$, where B is the bandwidth of the output link and tdr is the target drop rate. *Free time* of the limited session is the earliest time to release an limited aggregate after it goes below the limit imposed on it. *Rate limit time* determines the period that the rate limiter controls for each identified aggregate, After the period, the agent will check whether the aggregate is still needed to be rate limited. *Maximum session* determines the maximum sessions (aggregate) the rate limiter can control.

In the simulation, for the attacker's strategies, we mainly concern the $\langle$*number of zombies, ratio, traffic pattern, attacking traffic aggregates*$\rangle$. We set the number of zombies as 12 (FEWBAD) or 32 (MANYBAD). If the total rate of attacking traffic is stable, then each zombie has lower sending rates under MANYBAD. We got three typical traffic from http://ita.ee.lbl.gov/html/traces.html. They are RATE1 = 67.1kbps(the rates to a web-site at the rush hour), RATE2 = 290kbps (the average rates from an Intranet to Internet) and RATE3 = 532kbps (the rates from an Intranet to Internet at the rush hour). In this paper, we use the three rates to set up three typical scenarios. We set the total poor rate as the RATE1, RATE2 and RATE3 since the poor traffic is sent to the same destination as the bad traffic. The *ratio* is given by the total rate of the attacking traffic, divided by the total rate of the poor traffic. We set the *ratio* as 30, 35, 40, 35 and 50(in RATE3, the ratio is 30,35 and 40). For example, when the poor rates is 67.1kbps, the total attacking traffic rate is 2013kbps, 2348.5kbps, 2684kbps, 3019kbps and 3355kbps respectively, which is larger than the bandwidth of the target link. There are 4 kinds of traffic patterns for attackers, Constant bits rate(CBR), Exponential(EXP), ICMP and Mixed (half CBR and half ICMP). According to the different aggregate properties, the attacking traffic can be divided into several aggregates. For example, when the aggregate property is destination address prefix and zombies send packets to one victim, then the attacking traffic belongs to one aggregate. If zombies send packets to with three destination prefix address, attacking traffic has three aggregates.

Legitimate users' strategies also affect the payoffs of system and attacker. Regarding the legitimate users' strategies, the good traffic is always sent to different destinations from the victims and its aggregate differs from the attack aggregate. We set number of poor users as 2 (FEWPOOR) or 4 (MANYPOOR) and number of good users as 5 (FEWPOOR) or 10 (MANYPOOR). For simplicity, we just set the sending rate from each good user is same as that of the poor user. So when the poor rate goes up, the legitimate rate goes up also. Legitimate traffic only use CBR pattern.

Figure 3 and Figure 4 show how the system and attacker strategies affect the attacking capacities of attacker and system resilience respectively. Axis X is for the attacker's strategies. Attacker has 40(24) strategies in RATE1 and RATE2 (RATE3). In the first 20 (12) strategies, the number of zombies is FEWBAD, followed by 20 (12) strategies with the number as MANYBAD. For each 5 (3) strategies in each 20 (12) strategies, attacking traffic patterns are ordered as CBR, Ex-

ponential, ICMP and Mixed. In each 5 (3) strategies, the data is ordered according to the ratio, which is 30,35,40,45 and 50 (30,35 and 40).

In the first three subfigures in each figure, the aggregate property is DEST (destination address prefix). Then followed by three figures with DESTPATT (destination address prefix plus traffic pattern) aggregate property. We let the zombies and poor users send packets to one destination address. Since the attacking traffic has three type of traffic pattern (the defense system regards the Mixed traffic as CBR and ICMP), the attacking traffic has three aggregates. The poor traffic is CBR and shares one aggregates with the attacking traffic. In the following three figures, the aggregate property is DESTPORT (destination address prefix plus port number). We let the zombies send packets to one victim but four different port number, so the attacking traffic has four aggregates. We let the poor users send packets to the same victim but different port number. For the last three figures, the aggregate property is SOUR (source address). The defense system uses the source address as the aggregation property. Attacking traffic has 12(FEWBAD) or 32(MANYBAD) aggregates in this strategy. In the simulator, we set the maximum session larger than the number of attacking traffic aggregates. So the routers can control all attacking traffic.

Axis Y is for system's strategies, which are ordered as *congestion checking time (4s), cycle time(10s), drop rate (0.03), drop rate (0.07), free time (10), free time (30), default configuration, rate limit time (15), rate limit time (50),maximum session(5)* when the aggregate property is DEST. In the first 9 strategies, we let the attacker sends packets to one victim, so the attacking traffic belongs to one aggregate. In the last strategy, in order to observe what will happen when the attacking traffic has multiple aggregates, we let the attacker send packets to 4 subnet, so the attacking traffic has 4 aggregates. When the aggregate property is DESTPATT, DESTPORT or SOUR, there is no maximum session (5) strategy, since all the attacking traffic has multiple aggregate.

4.3. The defense capacity vs. DDoS attack capacity

Figure 3 and Figure 4 show the capacity of the defense system and the attacker. We consider four parameters for attacker in our observations. The influence of attacker strategies is as follows.

Number of zombies When the number of zombie is MANYBAD, the system earns lower resilient capacity and the attacker earns higher attacking capacity. When the aggregate property is SOUR, the number of zombie affects the system and attacker's results greatly.

Ratio The ratio affects the attacker's attacking capacity only when the poor rate is 67.1kbps, the traffic pattern includes ICMP (ICMP or Mixed) and the number of zombie is Many. In this situation, attacker gets higher attacking capacity when the ratio goes up. In other strategies, the ratio does not affect the attacker's attacking capacity much.

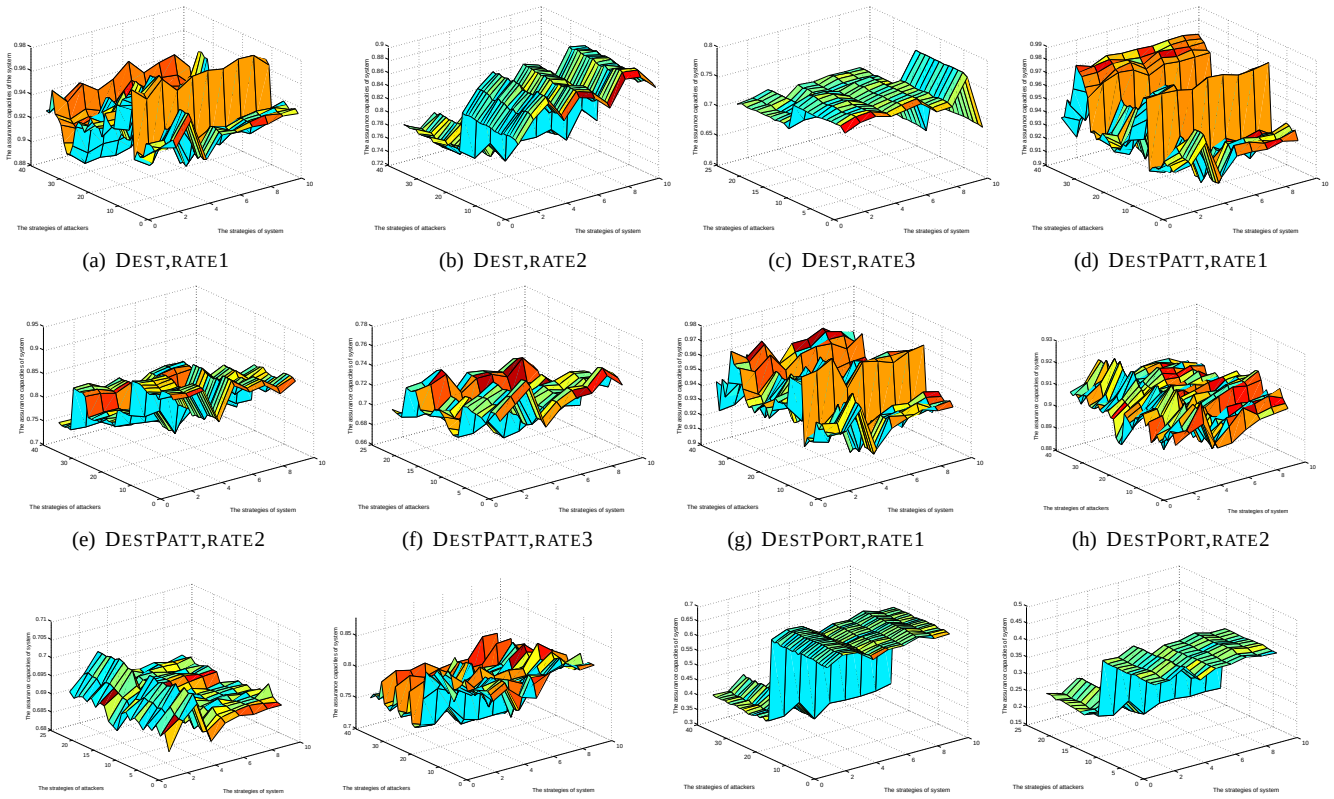
Pattern When the poor rate is low, the system earns high resilient capacity and the attacker earns low attacking capacity if the attacker sends ICMP packets. When the poor rate increases, the traffic pattern does not affect the capacity of the attacker and defense system whatever the aggregate property is DEST, DESTPORT or SOUR. In DESTPATT, the traffic pattern affects the payoffs because the router constructs the signature based on the destination address prefix and traffic pattern. When the poor rate is RATE2 or RATE3, attacker earns high attacking capacity when the attacking traffic is Mixed.

The number of aggregates We simulate how the number of traffic aggregates affects the results only in DEST. The system gets low assurance capacities when the attacking traffic has multiple aggregates, which is shown in Figure 3(a), Figure 3(b) and Figure 3(c). The attacker gets high attacking capacity when its traffic has multiple aggregates, which is shown in Figure 4(a), Figure 4(b) and Figure 4(c),

The influence of system's strategies is as follows. **(1)** The cycle time, drop rate, rate limit time and aggregate property affect payoffs, other system strategies do not affect the results much. **(2)**The system always gets high resilient capacity when the drop rate is 0.03 and gets low resilient capacity when the drop rate is 0.07. The system sometimes also gets high resilient capacity under cycle time (10s) and rate limit time (50s) strategies. **(3)** The destination address based aggregate property is better than the source address based aggregate property for the system. The system gets the lowest resilient capacity when the aggregate property is SOUR. In SOUR strategy, attacking traffic has 12 (32) aggregates. So the rate difference between each attack aggregate and each legitimate aggregate is less than that in other strategies. It is more difficult for the router to identify the malicious traffic and more legitimate packets may dropped. The accurate congestion responsible aggregate property the system can identify, the high resilient capacity the system can obtain. For example, using DESTPATT or DESTPORT is better than using DEST only for the defense system.

4.4. Optimal attack and defense strategies

The Nash equilibria of the game specify the expected-utility maximizing best-response of one player to every other player. Hence the Nash equilibria strategies are the optimal strategies for attacker and defense system. We know that aggregate property determines how defense system identities the attacking traffic, so it is a very important parameter for the defense system. We calculate the optimal strategies for each aggregate property and network scenario (different rate) from the payoff vectors (totally 16224) we got. We set the relative error as 0.005 for the payoffs of the attacker and the defense system and get 100 Nash equilibria. In other words, if the difference between two payoffs of one player is less than the relative error, we treat them as the same one. Due to the limit space, we list only 16 detail descriptions of the Nash equilibria strategies, system's resilient capacities and attacker's attacking capacities in Table I, where the attacker's strategies are list in the sequence of ⟨*number of zombies, ratio, traffic pattern, number of aggregate*⟩.

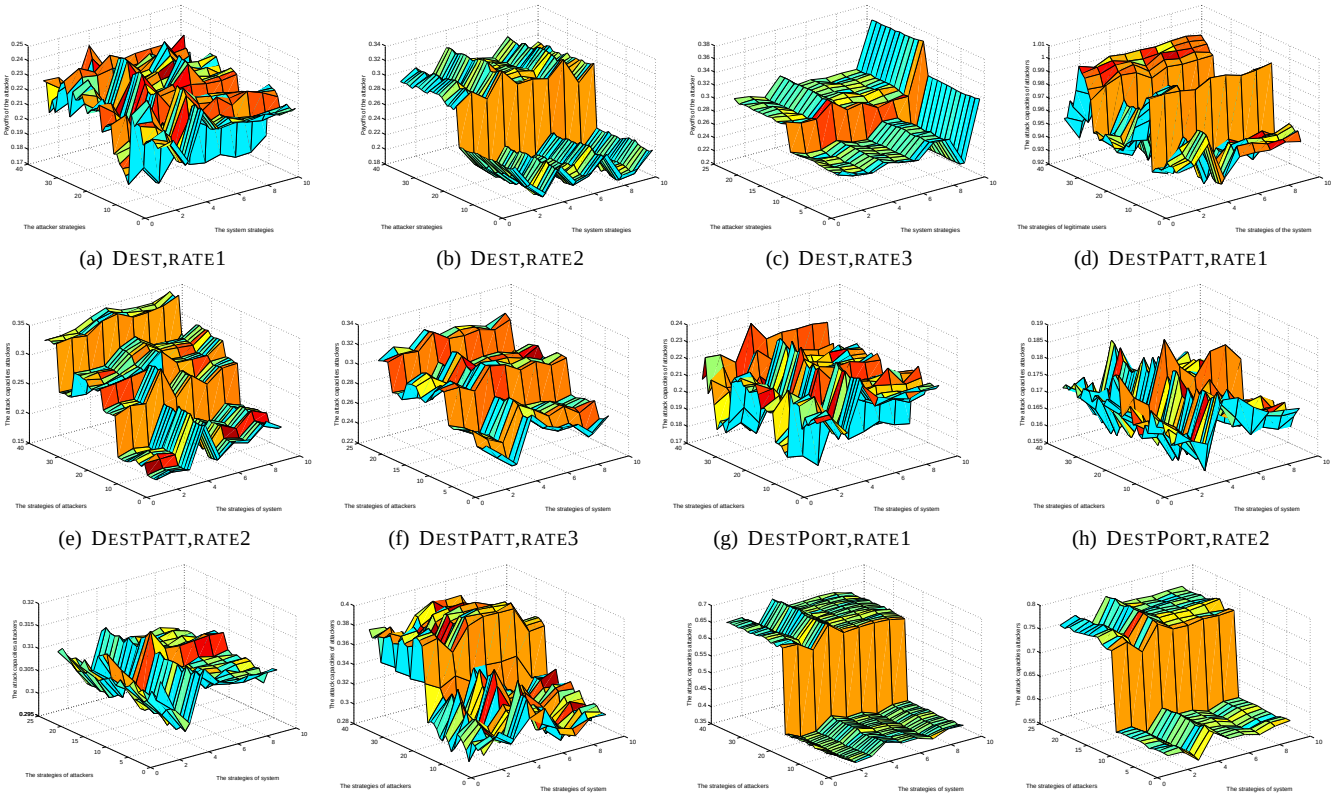


(a) DEST,RATE1 (b) DEST,RATE2 (c) DEST,RATE3 (d) DESTPATT,RATE1

(e) DESTPATT,RATE2 (f) DESTPATT,RATE3 (g) DESTPORT,RATE1 (h) DESTPORT,RATE2

(i) DESTPORT,RATE3 (j) SOUR,RATE1 (k) SOUR,RATE2 (l) SOUR,RATE3

Fig. 3. The resilient capacity of the system under different system and attacker's strategies



(a) DEST,RATE1 (b) DEST,RATE2 (c) DEST,RATE3 (d) DESTPATT,RATE1

(e) DESTPATT,RATE2 (f) DESTPATT,RATE3 (g) DESTPORT,RATE1 (h) DESTPORT,RATE2

(i) DESTPORT,RATE3 (j) SOUR,RATE1 (k) SOUR,RATE2 (l) SOUR,RATE3

Fig. 4. The attacking capacity of the attacker under different system and attacker's strategies

TABLE I

THE OPTIMAL STRATEGIES AND CAPACITIES [A]

system strategy	attacker strategy	AttC	RC
DEST,dr0.03	MB, 45, CBR, OA	0.459	0.9495
DEST,dr0.03	MB, 50, CBR, OA	0.459	0.9495
DEST,sess5	FB, 50, EXP, MA	0.489	0.9218
DEST,sess5	MB, 45, CBR, MA	0.472	0.9267
DESTPATT,dr0.03	FB, 30, CBR, MA	0.458	0.9495
DESTPATT,dr0.03	MB, 45, EXP, MA	0.456	0.9436
DESTPATT,dr0.03	MB, 30, CBR, MA	0.462	0.9435
DESTPORT,dr0.03	MB, 30, CBR, MA	0.458	0.9505
DESTPORT,dr0.03	MB, 35, CBR, MA	0.456	0.9525
DESTPORT,dr0.03	MB, 45, CBR, MA	0.455	0.9554
DESTPORT,dr0.03	MB, 30, CBR, MA	0.298	0.9145

[a] $dr0.03$ - target drop ratio (0.03). $sess5$ - maximum session (5). $cyct10$-cycle time (10s). FB-Fewbad. MB-Manybad. OA-One Aggregate. MA-Multiple Aggregates. AttC-Attacking Capacity. RC–Recilient Capacity.

Both the attacker and the defense system prefer to choose an optimal strategy. Therefore, when DDoS attacks occur, they will finally stay at an optimal strategy and no one wants to move. So RC is the upper bound of the defense system's resilient capacity against DDoS attack and $AttC$ indicates the the upper bound of the attacking capacity of the attacker. When the defense system or the attacker move to another strategy their payoffs will be less than the upper bound.

We found most Nash equilibria occur when the target-droprate-rate is 0.03 and the number of zombies is MANYBAD. When the aggregate property is DEST, many Nash equilibria occur when the attacking traffic has multiple aggregates. We can also observe the optimal strategies from the *dominant strategies* in Figure 3 and Figure 4. For example in Figure 3(b), we found the drop rate (0.03) is the dominant strategy for the defense system, since $U_d(a_i, d_{droprate0.03}) > U_d(a_i, d_i)$ for all $a_i \in A_u$ and $d_i \in A_d \vee d_i \neq d_{droprate0.03}$. No matter what the attacker will do, the defense system always gets its highest resilient capacity when the drop rate is 0.03. In order to get high resilient capacity, the system should stay at the drop rate 0.03 and does not move. Therefore, there should be at least one optimal strategy under droprate (0.03) strategy. From the Table I, we found that there exists Nash equilibria under droprate 0.03.

4.5. Attack prediction

The attacker and defense system will definitely choose or ultimately converge to a Nash equilibrium strategy to fight each other. The distribution of Nash equilibria strategies shows which kind of strategies are most likely to be taken by the attacker and the defense system. The distribution of Nash equilibria strategies helps us to predict what the attacker will do even before the attack occurs and to suggest how to build a high resilient defense system.

Considering *ratio*, *number of zombies* and *system strategy*. the distribution of Nash equilibria is as follows.

(1) The attacking rate does not affect the Nash equilibria much, which is shown in Table II. The probability of the Nash equilibria for all ratios have little differences. It seems when the attacker sends more packets to the victim, the attacker should always occupy more bandwidth and get higher attacking capacity. But we found that Pushback works stable when the attacker increases the attacking rate. In other words, high attacking rate cannot help the attacker to maximize his attacking capacity.

TABLE II

THE NASH EQUILIBRIA DISTRIBUTION UNDER DIFFERENT ATTACKING TRAFFIC RATIO

Aggregate	30	35	40	45	50
DEST	0.2542	0.3051	0.0678	0.0678	0.3051
DESTPATT	0.2422	0.1111	0.1111	0.3333	0.2022
DESTPORT	0.2625	0.3000	0.0625	0.1250	0.2500
SOUR	0.1875	0.2500	0.2500	0.0625	0.2500

(2) Most Nash equilibria occur when the number of zombies is MANYBAD, which is shown in Table III. Under SOUR strategy, the probability that the Nash equilibrium happens is 1 when the number of zombies is MANYBAD. So when the attacker launches attacks, he had better use more zombies to maximize his interests. More zombies will not increase the costs of the attacker, since the attacker usually uses automatic tools to install agents.

(3) Most Nash equilibria occur when the target-drop-rate is 0.03 or when the maximum session is 5(DEST). The probability that the Nash equilibrium happens is at least 0.2 under target-drop-rate(0.03) strategy. Under DEST and maximum session (5) strategy, the probability that the Nash equilibrium happens is more than 0.5. So we should set Pushback with low target drop rate and large value of maximum session to maximize its resilience against DDoS attacks.

In order to get high interests, the attacker should use more zombies, CBR (UDP based) traffic and multiple aggregates. The defense system should use low target drop rate and large value of maximum session. Knowing the distribution of Nash equilibria, we can predict the profile of next action of the defense system and attacker. By calculating the Nash equilibria strategies, we can obtain more information about the next action.

5. DISCUSSION

Legitimate users' obtained service ratio and strategies The legitimate users' obtained service ratio depends on not only the strategies of themselves but also the strategies of the attacker and system. When the poor rate is high, the legitimate users earn low obtained service ratio since many packets are dropped by the defense system. For the defense system's strategy, legitimate users always get the highest obtained service ratio when the target-drop-rate is 0.03 and get the lowest obtained service ratio when the target-drop-rate is 0.07. Legitimate users earn higher obtained service ratio when the aggregate property is DESTPORT since the defense system can identify the malicious signature more accurately. Regarding the attacker's strategies, we found that the legitimate users earn high benefits when the number of zombies is FEWBAD. The other attacker's strategies, such as the traffic pattern, has little effect on the availabilities of legitimate users.

Legitimate users' strategies also affect the capacity of system and attacker. For example, when the poor rate increases, the resilient capacity of the defense system goes down since

TABLE III

THE NASH EQUILIBRIA DISTRIBUTION UNDER DIFFERENT COMBINATION OF USERS [A]

Aggregate Property	FFF	FFM	FMF	FMM	MFF	MFM	MMF	MMM
DEST	0	0	0.0169	0	0.1186	0	0.2373	0.6271
DESTPATT	0	0	0	0.3333	0	0	0.3333	0.3333
DESTPORT	0	0.2500	0	0	0.1875	0.4375	0.1250	0
SOUR	0	0	0	0	0	0.1250	0	0.8750

[a] F–Few, M–Many. The first F or M is for the number of zombies, the second and the third one are the number of poor and good users.

more legitimate packets are dropped by the system. When the number of legitimate users is MANY, the resilient capacity of the defense system goes up since the legitimate traffic distributed widely.

Changing the network scenarios We use ns-2 as our simulator, the topology and strategies are based on the pushback simulation scenario. We found that the experimental results consist to the real cases and speculation. For example, we found that deploying more zombies is good for the attacker. In real DDoS attacks, an attacker really prefers to use more zombies. That the lower target-drop-rate is good for system matches our speculation. When the target-drop-rate is low, the limit on the controlled aggregates will be lower and more bad packets will be dropped by the defense system.

When the topology, the strategies, the defense system or some other parameters changed, if the defense system is signature based rate limiting and the DDoS attack is bandwidth consumed, though the upper bound of capacity and the Nash equilibria strategies will change, our game theoretic analysis framework can still apply to analyze the game if mechanisms of the attacker and defense system changed. For example, the defense system is a trace back system, we may need a new model since the interests changed. But our game theoretic analysis frame still can be applied to enhance people's understanding the interactions between the defense system and the attacker.

6. RELATED WORK

In recent years, the researches of DDoS mainly focus on the attack analysis [5], [6], intrusion detection [2], [25] and such defense mechanisms as traceback [3], [23], [26], rate-limiting [9], [14], [16] and filtering [7], [18], [20]. Intrusion detection is used to determine whether the network is under attacking. Traceback provides the information about where the attacking traffics come from. Filtering mechanisms try to filter out the attack stream completely based on some detection methods. Rate-limiting method impose a rate limit on a stream that has been identified as malicious by the detection mechanisms. All the work focus on mitigating the effects of attacks, which cannot solve the problems about what are the optimal strategies for the attacker and the defense system, what the attacker and the defense system will do to maximize their benefits. Game theory can help us to solve the problems.

Game theory is widely used in the network field such as high-speed network [21], routing policy [10] and flow control [15]. Game theory is a primary tool to handle strategic interdependence, which is the fundamental characteristics of the attack-defense relationship in computer security. Kodialam proposed a zero-sum game to detect the malicious packets in [19]. In [22], Syverson proposed a two-person game between the good network and evil network. They showed that networks of n interacting nodes need not to be represented by an n-person game: they can often be represented in a two-person game. Lye et al view the interaction between an attacker and the administrator as a two-player stochastic game and construct a model for the game in [13]. They give Nash equilibria strategies of the players and explain how to use these results to enhance the security of network. In [4], Browne use static games to analyze attacks of military network. A defending team, which determine whether to run a worm detector based on the outcome of combined attack and defense actions. Our previous work [11], [12] presented a general incentive-based method to model attacker's intent, objectives and strategies. We used the same game-theoretic approach. However, we focused more on the modeling and framework instead of detailed analyses and simulations in this paper.

Our work differs from previous work in that (1)none of them model the game about defending DDoS attacks before, (2)we use Bayesian game to model defending DDoS attacks and analyze the game based on the motivation, strategies and capacities of the attacker and the defense system. (3)propose a game theoretic analysis framework and a novel family of analyses, (4)give a detailed analytic and simulation results to show how to use our approach to analyze the game.

7. CONCLUSIONS

In this paper, we proposed a Bayesian game theoretic analysis to infer "How resilient is the Internet against DDoS attacks?" from the angle of modeling and computing the motives, strategies and payoffs of the defender, namely the Internet, and the DDoS attacker. We model countering Class B DDoS attacks as a Bayesian game. We do a high volume of simulations to compute an approximate solution of the game. And we propose a family of Nash equilibrium based resilience analyses. Our analysis not only estimates the *upper* bound of the Internet's resilience under Class B DDoS attacks, but also shows which kinds of Class B DDoS attacks are more likely to be enforced by the attacker in our simulation. Our analysis may substantially improve people's understanding about the nature of (a) the DDoS threat and (b) the Internet's resilience against this threat.

In the future work, we plan to (a) use more advanced "testbeds" such as EmuLab and real world testbeds and (b) do more analytical study to validate and refine the findings discovered throughout this research.

REFERENCES

[1] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[2] Stefan Axelsson. Intrusion detection systems: A survey and taxonomy. Technical Report 99-15, Chalmers Univ., March 2000.

[3] S.M. Bellovin. Icmp traceback message. Technical report, IETF, 2001.

[4] R. Browne. C4i defensive infrastructure for survivability against multi-mode attacks. In *Proc. 21st Century Military Communication-Architectures and Technologies for Information Superiority*, 2000.

[5] D. Dittrich. The dos projects 'trinoo' distributed denial of service attack tool,the 'stacheldraht' distributed denial of service attack tool, the 'tribe flood network' distributed denial of service attack tool, 1999.

[6] D. Dittrich, S. Dietrich, and N. Long. An analysis of the 'shaft' distributed denial of service attack tool, 2000.

[7] P. Ferguson and D. Senie. Rfc 2827 – network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing. Technical report, IETF, 2000.

[8] R. Gibbons. *Game Theory for Applied Economics*. Princeton University Press, 1992.

[9] T.M. Gil and M. Poletto. Multops:a data-structure for bandwidth attack detection. In *Proc. of 10th Usenix Security Symposium 2001*, 2001.

[10] J.P. Hespanha and S. Bohacek. Preliminary results in routing games.

[11] P. Liu and W. Zang. Incentive-based modeling and inference of attacker intent, objectives and strategies. In *Proc. of 10 ACM Conference on Computer and Communications Security*, 2003.

[12] P. Liu, W. Zang, and M. Yu. Incentive-based modeling and inference of attacker intent, objectives and strategies. *ACM Transactions on Information and Systems Security*, 8(1):78–118, 2005.

[13] K. Lye and J.M.Wing. Game strategies in network security. In *Proc. 15th IEEE Computer Security Foundation Workshop*, 2002.

[14] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Controlling high bandwidth aggregates in the network. Technical report, ACIRI, 2001.

[15] R.T. Maheswaran and T. Basar. Multi-user flow control as a nash game: Performance of various algorithms. In *Proc. of IEEE Conference on Decision and Control 1998*, 1998.

[16] Mananet. Reverse firewall.

[17] J. Mirkovic, J. Martin, and P. Reiher. A taxonomy of ddos attacks and ddos defense mechanisms. Technical report, UCLA. UCLA CSD Technical Report no. 020018.

[18] J. Mirkovic, G. Prier, and P. Reiher. Attacking ddos at the source. In *ICNP 2002*, pages 312–321, 2002.

[19] M.Kodialam and T.V.Lakshman. Detecting network intrusions via sampling: A game theoretic approach. In *Proc. of IEEE INFOCOM 2003*, 2003.

[20] K. Park and H. Lee. On the effectiveness of router-based packet filtering for distributed dos attack prevention in power-law internets. In *Proc. ACM SIGCOMM 2001*, 2001.

[21] K. Park, M. Sitharam, and S. Chen. Quality of service provision in noncooperative networks:heterogeneous preferences, multi-dimensional qos vectors and burstiness. In *Proc. International Conference on Information and Computation Economics*, 1998.

[22] P.F.Syverson. A different look at secure distributed computation. In *Proc. 10th IEEE Computer Security Foundations Workshop*, 1997.

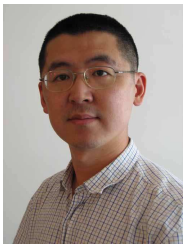
[23] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical network support for ip traceback. In *Proc. ACM SIGCOMM 2000*, 2000.

[24] Computer Emergency Respronse Team. Cert advisory ca-2000-01 denial-of-service development. Technical report, Carnegie Mellon University, 2000. http://www.cert.org/advisories/CA-2000-01.html.

[25] H. Wang, D. Zhang, and K.G. Shin. Detecting syn flooding attacks. In *Proc. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.*, pages 1530–1539, 2002.

[26] F. Wu and L. Zhang. Draft – intention-driven icmp trace-back. Technical report, IETF, 2001.

Wanyu Zang received the M.S. degrees in Computer Science from the Northeastern University, China, in 1998 and Ph.D. degree in Computer Science from Nanjing University, China in 2001. She is currently a visiting assistant professor at Computer Science department of Western Illinois University. Her research interests include computer security and wireless networks.



Meng Yu received the M.S. degrees in Computer Science from the Northeastern University, China, in 1998 and Ph.D. degree in Computer Science from Nanjing University, China in 2001. He has been worked as a postdoctoral research scholar at University of Maryland, Baltimore County and Penn. State University, University Park from 2002 to 2004. He is currently an assistant professor at Computer Science department of Western Illinois University. His research interests include computer security, especial on distributed and database systems.

Peng Liu received his B.S. and M.S. degrees from the University of Science and Technology of China, and his Ph.D. degree from George Mason University in 1999. He is an associate professor of Information Sciences and Technology and director of the Cyber Security Lab at Penn State. His research interests are in all areas of computer and network security. Dr. Liu has published a book and about 70 refereed technical papers. His research has been sponsored by DARPA, NSF, DOE, DHS, AFRL, NSA, CISCO, HP, Japan JSPS, and Penn State. Dr. Liu is a recipient of the DOE Early CAREER PI Award.