Mathematical Foundations for the Design of a Low-Rate DoS Attack to Iterative Servers (Short Paper)

Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, and Pedro García-Teodoro

Dpt. of Signal Theory, Telematics and Communications - University of Granada
c/ Daniel Saucedo Aranda, s/n - 18071 - Granada, Spain
gmacia@ugr.es, jedv@ugr.es, pgteodor@ugr.es

Abstract. A low-rate DoS attack to iterative servers has recently appeared as a new approach for defeating services using rates of traffic that could be adjusted to bypass security detection mechanisms. Although the fundamentals and effectiveness of these kind of attacks are known, it is not clear how to design the attack to achieve specific constraints based on the used rate and the efficiency in denial of service obtained. In this paper[1], a comprehensive mathematical framework that models the behaviour of the attack is presented. The main contribution of this model is to give a better understanding of the dynamics of these kind of attacks, in order to facilitate the development of detection and defense mechanisms.

1 Introduction

Recently, one of the most important problems in security are denial of service (DoS) attacks. The primary goal of these attacks is to deny legitimate users the access to specific resources [1]. This goal has been traditionally achieved by following several possible strategies. One of them is to exploit some vulnerability in a protocol or a service in such a way that an attacker, using a few resources, can defeat a machine with much more capacity. Another strategy consists in flooding the target service with a traffic that exhaust either the connectivity or some resources of the server.

So important are these kind of attacks that many big companies have suffered from their effects [2], reason for which much research has focused its activity on the development of detection and defense mechanisms. This way, several approaches have been proposed in the field of prevention, like egress [3] or ingress filtering [4], disabling unused services [5], honeypots [6], and others, while many efforts have been made in the field of detection through intrusion detection paradigms (IDS) [7].

A low-rate DoS attack to iterative servers has been recently presented in [8] as an attack capable of defeating an iterative server by using an adaptable traffic

[1] This work has been partially supported by the Spanish Government through MYCT (Project TSI2005-08145-C02-02, FEDER funds 70%).

P. Ning, S. Qing, and N. Li (Eds.): ICICS 2006, LNCS 4307, pp. 282–291, 2006.

rate according to the desired level of denial that the attacker wants to afflict to the server.

For other recently presented attacks, like the low-rate TCP targeted attack [9], some solutions in the field of detection and response [10] [11] have appeared. However, until now, neither defense nor prevention mechanisms have been proposed for [8], mainly due its novelty. In this line, there is a necessity for a more comprehensive analysis of the mechanisms that the intruder could use to carry out the attack in order to facilitate the development of detection and prevention measures. The goal of this study is to present such analysis, based on the development of a mathematical framework. The proposed model establishes the relation between the design parameters for the attack and the efficiency and rate values obtained.

The rest of this paper is organized as follows. Section 2 recapitulates the fundamentals of the attack introduced in [8]. In Section 3, some indicators to measure the effectiveness of the attack are proposed. Section 4 presents the mathematical models that support the design of the attack. Section 5 shows some experimental results for the validation of the models. Finally, some conclusions and future work are given.

2 Fundamentals of the Low-Rate DoS Attack

The scenario where the low-rate DoS attack [8] to iterative servers is analyzed consists of a generic client-server configuration in which an iterative server is going to receive aggregated traffic coming from both legitimate users and intruders. The server receives requests from the clients and responds to them after doing some processing. The low-rate DoS attack focuses the effort in the task of maintaining the destination service queue occupied with malicious requests for as long a period as possible. Due to the functioning of an iterative server, each time that a response or output to a request is generated, a position in the queue is freed. So, to achieve the goal, when an output is given, the intruder should occupy the new position in the queue as soon as possible. A vulnerability present in iterative servers, that allows to forecast the instant at which the next output is going to happen, is exploited for that purpose.

The fundamentals of the vulnerability and the attack are simple. By sending the requests in such a way that all of them ask for the same resource at the server, the time between consecutive answers or outputs, called the *inter-output time* τ, will be determined by the required service time, t_s, and so easily obtained. However, despite the solicited resource being always the same, the inter-output time is observed by the intruder as a random process, τ_{int}, because there are some variations in the service time caused by the round trip time (RTT), and the fact that each request is processed in a multitasking operating system. This random process is modelled by the authors in [8] as a normal variable with a mean value $\overline{t_s}$ and a variance of $var[t_s] + var[RTT]$.

The intruder sends the requests in such a way that they arrive at the server in the minimum possible time after a position is freed. Moreover, the traffic

generated by the intruder should be low-rate. For the attainment of these two objectives, an ON/OFF attack waveform, synchronized with the outputs from the server, is used.

The attack waveform is characterized by the following parameters: (a) An *interval* (Δ) that is the time elapsed between the sending of two consecutive packets during the interval of activity; (b) an *ontime interval* (t_{ontime}) that consists on an activity interval during which an attempt to seizure a freed position in the service queue is made by emitting request packets at a rate given by $1/\Delta$; and also by (c) an *offtime interval* ($t_{offtime}$), that is, an inactivity interval previous to *ontime* in the period of attack, during which no attack packets are transmitted.

The selection of different values for these defined parameters of the attack yields in a variety of combinations between the denial efficiency achieved by the attack, and the traffic rate generated against the server. Intuitively, a higher rate will result in more denial efficiency and vice versa. However, this intuitive conclusion does not fit the need of quantitative tools for the evaluation of the effects of the attack.

To address this problem, a main task has to be afforded: that of defining a formal model which allows to relate the performance of the attack (in terms of efficiency and rate) with its operational parameters (Δ, $t_{offtime}$, t_{ontime}) and the target server and network characteristics. The following sections will deal with this objective.

3 Indicators for Evaluating the Attack

The evaluation of the attack in terms of the efficiency obtained and the rate of traffic involved leads, as a preliminary task, to the definition of some indicators to measure these features.

The following indicators are defined:

- *Effort* (E): it is the ratio between the traffic rate generated by the intruder and the maximum traffic rate accepted by the server (server capacity).
- *User perceived performance* (*UPP*): it is the ratio between the number of legitimate users requests processed by the server, and the total number of requests sent by them.
- *Mean idle time* ($\overline{T}_{idle}$): this indicator is defined for a scenario where legitimate users send no traffic. In this environment, $\overline{T}_{idle}$ is the percentage of time during which the system has any free positions in the service queue, related to the total duration of the attack.

As defined, the *effort* gives an idea about the traffic rate that the intruder needs to generate for the attack to succeed. On the other hand, both *UPP* and $\overline{T}_{idle}$ specify how to measure the efficiency of the attack. The value of *UPP* points out the DoS degree experienced by the legitimate users. Although it may be a good indicator to compare attack configurations, it is dependent on the characteristics of the legitimate users traffic. Because of this, the indicator $\overline{T}_{idle}$

is also defined to measure the efficiency of the attack; by using it the probability of seizure a position for a legitimate user can be deducted. As it is referred to a scenario free of legitimate users traffic, there is no dependence on it.

The aim of the attack is thus to minimize *UPP*. This will be similar to minimize $\overline{T}_{idle}$, because doing this, the probability of a legitimate user to seize a free position in the queue is reduced. On the other hand, the intruder will also try to minimize the *effort* needed to carry out the attack by choosing optimized settings for the parameters. In this way, the attack will become less detectable by intrusion detection systems based on high-rate detection.

Despite it seems that a reduction in the *UPP* value implies a higher *effort* as an expense and vice versa, it is desirable to find a quantitative relation between the setting of the parameters of the attack and the values obtained for the indicators previously defined. In the following section, some mathematical models that addresses this problem are discussed.

4 Mathematical Modelling for the Attack Behaviour

To address the issue of finding a quantitative relationship between a specific setting of the parameters of the attack and the values for the indicators that evaluate it, a mathematical framework is proposed in the following.

4.1 Mathematical Model for the Mean Idle Time

The *mean idle time* is defined as the percentage of the time during which at least a free position is available. In the evaluation of this indicator, a period of an attack, that is, an *offtime* interval followed by an activity interval (*ontime*) is taken as the observation period.

Fig. 1 represents the observed attack period (ON/OFF pattern), along with the curve of probability (normal distribution as proposed in [8]) for the generation of an output at the server. The instants for the arrival of attack packets (during the *ontime interval*) are represented by vertical arrows. These arrivals occur at the instants $a_i (i \geq 1)$. We will refer, henceforth, to the instants a_i at which an attack packet arrives at the server as *calculation points* in the model. A special calculation point, a_0, which does not correspond to the instant of a packet arrival is also defined. The position of this point is, by definition, at a time $\overline{RTT}$ before the reception of the first attack packet in the observation period, that is, $a_0 = a_1 - \overline{RTT}$.

Although in the example shown in Fig. 1 there are only three attack packets due to the chosen value for the *interval* Δ, it could be generically defined a set of calculation points $\mathcal{A} = \{a_0, a_1, \ldots, a_n\}$, where $n = floor[t_{ontime}/\Delta]$. These calculations points will be used by the model as references for the mathematical expressions.

The calculation points delimit a set of intervals at which we will calculate the instantaneous values of *idle time*, T_i. Following, the values of T_i are specified for each interval delimited by the calculation points.

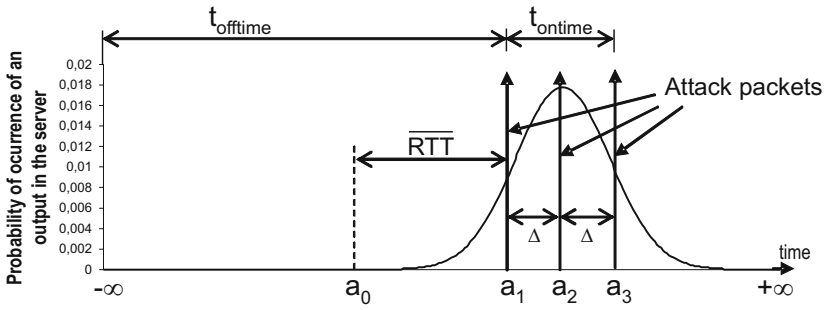

Fig. 1. Diagram of occurrence for an output: probability function and associated calculation points

If the output occurs within the interval $(-\infty, a_0)$, the value of T_i will be $\overline{RTT}$. In effect, when an answer is given by the server, it travels to the intruder and just then a new request is generated as a response to the reception of the output. This new request has to reach the server again. The whole process implies a time equal to $\overline{RTT}$. When the output rises at an instant t situated within the interval (a_{i-1}, a_i), for all the possible values of a_i in $\mathcal{A}$, and assuming that the intervals between two consecutive calculation points are short enough to keep the condition $\Delta = a_i - a_{i-1} \leq \overline{RTT}$, the *idle time* will take the value $(a_i - t)$. Finally, when the output occurs during the interval (a_n, ∞), we have the same case as in the first interval, and thus the value of the originated *idle time* is $\overline{RTT}$.

Thus, for the case in which $\Delta \leq \overline{RTT}$ is assumed, the *mean idle time* in a period of attack can be obtained from the instantaneous values previously deducted as:

$$\overline{T}_{idle_{(\Delta \leq \overline{RTT})}} = \frac{1}{T_p} \cdot \left[\int_{-\infty}^{a_0} \overline{RTT} \cdot f(t)dt + \int_{a_0}^{a_1} (a_1 - t) \cdot f(t)dt + \right.$$
$$\left. + \ldots + \int_{a_{n-1}}^{a_n} (a_n - t) \cdot f(t)dt + \int_{a_n}^{\infty} \overline{RTT} \cdot f(t)dt \right] \quad (1)$$

where $f(t)$ is the probability function for the generation of an output at the instant t and T_p is the duration of an attack period, that is, $T_p = t_{offtime} + t_{ontime}$. As it can be seen, the model is independent of the proposed distribution. If a normal distribution is taken and, for the sake of simplicity, a temporal translation is considered to get a mean value for the distribution equal to zero, the resolution of the equation leads to

$$\overline{T}_{idle_{(\Delta \leq \overline{RTT})}} = \frac{1}{T_p} \cdot \left[\overline{RTT} \cdot \Big(F(a_0) + 1 - F(a_n) \Big) + \right. \quad (2)$$
$$\left. + \sum_{i=1}^{n} a_i \cdot \Big(F(a_i) - F(a_{i-1}) \Big) + \frac{\sigma}{\sqrt{2\pi}} \cdot (e^{-\frac{a_n^2}{2\sigma^2}} - e^{-\frac{a_0^2}{2\sigma^2}}) \right]$$

where the operator $F(t)$ means the value of the distribution function associated to $f(t)$ at the instant t.

In a common design of the attack, the value of Δ is low enough to accomplish the condition $\Delta \leq \overline{RTT}$. However, although expression (2) provides the value of $\overline{T}_{idle}$ for the previous condition, the model could be easily adapted to the opposite condition, that is, $\Delta > \overline{RTT}$, considering that the intervals for which the instantaneous *idle time* varies are only those within (a_1, a_n). In effect, each one of these intervals are now split into two parts where the value for T_i is different.

This value is:

$$T_{i_{(\Delta>\overline{RTT})}}^{(a_{i-1},a_i)} = \begin{cases} a_i - t & \text{if} \quad a_i - \overline{RTT} < t < a_i \\ \overline{RTT} & \text{if} \quad a_{i-1} < t < a_i - \overline{RTT} \end{cases} \tag{3}$$

And, as a consequence, a new expression for the evaluation of the *mean idle time* is yielded:

$$\overline{T}_{idle_{(\Delta>\overline{RTT})}} = \frac{1}{T_p} \cdot \left[\int_{-\infty}^{a_0} \overline{RTT} \cdot f(t)dt + \sum_{i=1}^{n} \left(\int_{a_{i-1}}^{a_i - \overline{RTT}} \overline{RTT} \cdot f(t)dt + \right. \right.$$
$$\left. \left. + \int_{a_i - \overline{RTT}}^{a_i} (a_i - t) \cdot f(t)dt \right) + \int_{a_n}^{\infty} \overline{RTT} \cdot f(t)dt \right] \tag{4}$$

In the proposed model, the server characteristics are considered in the $f(t)$ term. Besides, the main network factor that affects the attack is the round trip time, which is also included in the model through the mean value $\overline{RTT}$, and its variance, $var[RTT]$ (included in the distribution $f(t)$). Finally, the setting of the attack is reflected on the calculation points of the expression. In effect, their positions depend on the parameters of the attack, that is, $t_{offtime}$, t_{ontime}, and the considered value for Δ.

4.2 Mathematical Model for the User Perceived Performance

The legitimate users packet arrivals are modelled in [8] by a Poisson distribution. This implies that the probability of packet reception from a legitimate user during a period of time is given by the exponential distribution function of mean value λ: $F(T) = 1 - e^{-\lambda T}$, that represents the arrival rate of packets from the legitimate users.

The calculation of *UPP* implies the evaluation of the probability for a legitimate user to capture a position in the service queue during a period of the attack. Intuitively, this probability is derived from the originated *mean idle time*, that is, an user will capture a position in the queue with more probability as the position is free during more time. As $\overline{T}_{idle}$ is given by the summing up of contributions from the different intervals delimited by the calculation points (see Fig. 1), the probability for the k-th interval, that is (a_{k-1}, a_k), is affected by the *idle time* originated during this interval, T_{idle}^k, that is

$$T_{idle}^{k} = \frac{1}{a_k - a_{k-1}} \int_{a_{k-1}}^{a_k} T_i^{(a_{k-1},a_k)} f(t)dt \tag{5}$$

However, these terms, as defined above, does not consider the presence of traffic coming from legitimate users. In effect, the *mean idle time* will take different values depending whether the considered output corresponds to either a user or the intruder. When the output is sent to a legitimate user, the intruder will not receive it and consequently a new attack packet will not generated. Therefore, the maximum value of T_i will not be $\overline{RTT}$.

In considering the above effect, and for the sake of simplicity, two approximations are made. First, the condition $\Delta \leq \overline{RTT}$ is retained, as discussed in the previous section, with the expression (1) being used to calculate the *mean idle time*. Second, the effect of the variation of the *mean idle time* is not considered when the packets coming from legitimate users arrive at the server in the intervals within a_0 and a_n. This is not an unreasonable approximation, due to the fact that the variation in the originated *idle time* for these intervals is up to Δ, if the intervals (a_1, a_n) are considered, and $\overline{RTT}$ for the interval (a_0, a_1). However, the experimental results shown later in Section 5 confirm the goodness of these approximations.

Thus, only the first interval $(-\infty, a_0)$ and the last one (a_n, ∞) are going to be affected by the above effect, thus their expressions being:

$$\begin{aligned} T_{idle}^{0} &= F(a_0)\left[\overline{RTT}\cdot(1-P_u) + min\left[\frac{1}{\lambda}, \overline{t_s} - t_{ontime}\right]\cdot P_u\right] \\ T_{idle}^{n+1} &= (1-F(a_n))\left[\overline{RTT}(1-P_u) + \ min\left[\frac{1}{\lambda}, \overline{t_s} - t_{ontime}\right] P_u\right] \end{aligned} \tag{6}$$

where P_u is the probability for a legitimate user to seizure a position in the service queue during a complete period of the attack. It will be given by the sum of the corresponding terms from the different intervals:

$$P_u = \sum_{k=0}^{n+1} \left(1 - e^{-\lambda T_{idle}^{k}}\right) \tag{7}$$

where n is the index of the last calculation point.

It is important to notice that the calculation of the expressions for T_{idle}^{k} and P_u should be made recursively, due to the fact that there is a crossed dependency between them. In all the experiments made, the value of P_u converges in a reduced number of iterations.

Once the value for P_u is obtained, the final expression for the *UPP*, for an attack of duration T, with C seizures, is given by:

$$UPP = \frac{P_u \cdot C}{T/\lambda} \tag{8}$$

4.3 Mathematical Model for the Effort of the Attack

The *effort* is determined by the number of packets sent to the server during the attack. Two factors contribute to the generation of attack packets. First, the

activity period, *ontime*, during which these packets are generated at a rate $1/\Delta$. Second, the new packet sent as a response to the reception of an output by the intruder.

For the calculation of the *effort* an assumption will be made: the intruder will receive the answers from the server after the sending of all the packets corresponding to the *ontime* interval. This is similar to suppose that the attack period is not going to be restarted during *ontime*, being the number of packets generated $floor(t_{ontime}/\Delta) + 1$.

As previously discussed, not all the outputs are received by the intruder, and so no new attack packets are always sent. The percentage of attack periods at which an output is not received from the server is given by *UPP*. Thus, in these attack periods no additional attack packet is generated as a response to the output.

Considering that during the observation period, that is, an attack period, only one request is accepted by the server, the final expression for the *effort* is:

$$E = \left(floor(\frac{t_{ontime}}{\Delta}) + 1 \right) + (1 - UPP) \tag{9}$$

5 Conformance Analysis for the Mathematical Models

The purpose at this point is to validate the theoretical framework presented in the above Sections with experimental results obtained from simulations made within Network Simulator 2 (NS2) [12]. The values obtained from the proposed mathematical models are contrasted with those obtained through some experimental simulations to check their validity.

To check how accurate and precise are the expressions proposed for *mean idle time*, *effort* and *user perceived performance* in the mathematical models, we have evaluated the behaviour in a set of scenarios with different configurations for both the attack and server parameters. The results from these experiments have been compared to the values derived from the mathematical model, obtaining a very good approximation between them. Fig. 2 shows the corresponding values of *mean idle time, UPP* and *effort* for 13 simulations. The maximum variation in $\overline{T}_{idle}$ (see Fig. 2.a) given by the model is 3,77%, with a mean value of 1,71%, what is a very good approximation. The results for *UPP* are showed in absolute values (Fig. 2.b). The obtained values from the model approximate well to the simulated ones, with a mean variation of 0,4% and a maximum of 1,46%. Finally, it can be observed in the comparison for the effort (Fig. 2.c) that the model approximates well the simulated values, with a mean variation of 1,42% and a maximum of 4,02%.

As a conclusion, the approximations made in the mathematical model are accurate enough to consider it as a tool to evaluate the potential effect of an attack starting from the knowledge of its design parameters.

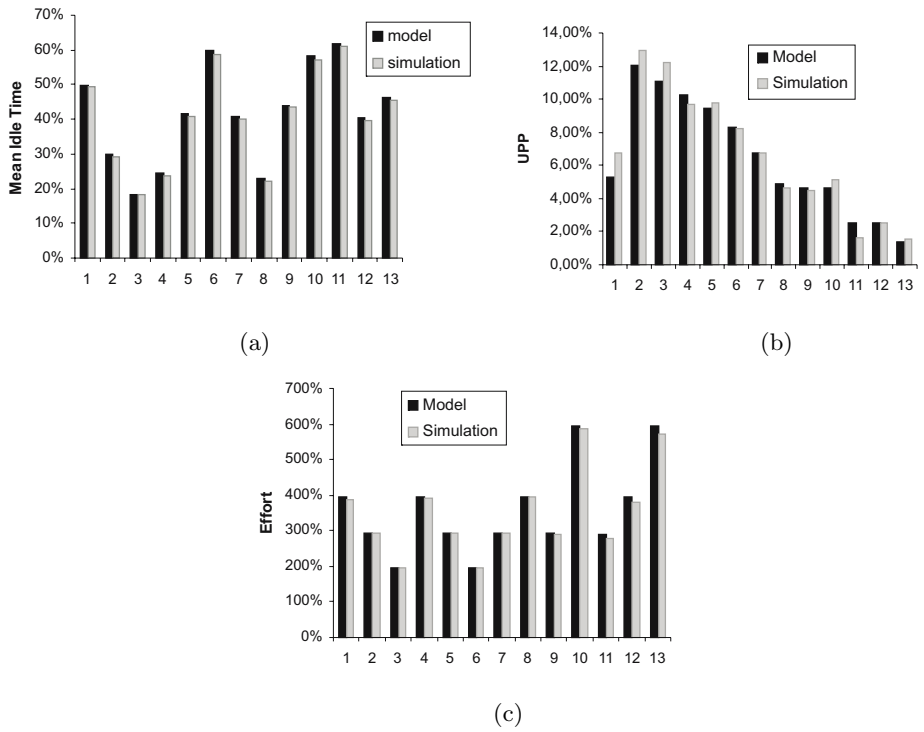

Fig. 2. Comparison between the values of (a) *mean idle time*, and (b) *UPP* from simulation and mathematical models, for 13 different scenarios

6 Conclusions and Future Work

This study is oriented to find the relationship between the design parameters of the low-rate DoS attack to monoprocess servers in [8], and the results obtained from this attack. A comprehensive study over the attack is made and some indicators to measure both the efficiency and the rate involved in a specific setting of the attack have been defined. But the main contribution of this work concerns the mathematical models that allow to quantitatively obtain the values for these defined indicators starting from a specific setting of the design parameters of the attack.

As a consequence of this study, a deeper understanding of the fundamentals of the attack is achieved. It should lead to the development of defense and response mechanisms that protect the target systems. As a future work, we plan to extend the mathematical models to concurrent systems attacked by the same mechanisms. The preliminary results we have obtained in this field show that it is possible not only to attack these systems with a similar mechanism but also it is likely to find a mathematical framework to analyze these attacks.

References

1. CERT coordination Center. Denial of Service Attacks. Available from <http://www.cert.org/tech_tips/denial_of_service.html>
2. M. Williams. Ebay, Amazon, Buy.com hit by attacks, 02/09/00. IDG News Service, 02/09/2000. http://www.nwfusion.com/news/2000/0209attack.html
3. Global Incident Analysis Center - Special Notice - Egress filtering. Available from <http://www.sans.org/y2k/egress.htm>.
4. P. Ferguson, D. Senie, Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing, RFC 2827, 2001.
5. X.Geng, A.B.Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2(4)(2000) 36-42.
6. N.Weiler, Honeypots for Distributed Denial of Service, in: Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109-114.
7. Axelsson S. Intrusion detection systems: a survey and taxonomy. Department of Computer Engineering, Chalmers University, Goteborg, Sweden. Technical Report 99-15; March 2000.
8. G. Maciá-Fernández, J. E. Díaz-Verdejo, P. García-Teodoro, Low Rate DoS Attack to Monoprocess Servers; LNCS Vol. 3934, pp. 43-57. 3rd Conf. on Security in Pervasive Computing, March 2006.
9. A. Kuzmanovic and E. Knightly, Low Rate TCP-targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants), in Proc. ACM SIGCOMM 2003, Aug. 2003, pp. 75-86.
10. H.Sun, J.C.S. Lui, and D.K.Y.Yau, Defending Against Low-Rate TCP Attacks: Dynamic Detection and Protection, in Proc. IEEE Conference on Network Protocols (ICNP2004), Oct. 2004, pp. 196-205.
11. A. Shevtekar, K. Anantharam and N. Ansari, Low Rate TCP Denial-of-Service Attack Detection at Edge Routers, in IEEE Communications Letters, vol 9, no. 4, pp. 363-365, April 2005.
12. Network Simulator 2. Available at: http://www.isi.edu/nsnam/ns/