

Queueing Analysis for Networks Under DoS Attack

Amar Aissani

University of Science and Technology Houari Boumediene (USTHB),
BP 32 El Alia, Bab-Ez-Zouar, 16111, Algeria
amraissani@yahoo.fr

Abstract. In this paper, we consider a queueing model of computer network under DoS attacks. The arrival of SYN packets contains two types: the regular request packets and the attack packets that request for connections. We assume that the connection requests arrive according to a Poisson processes and the service times are general but different for the two types of requests. A maximum number of connections can be served at the same time. Each half-open connection is held for at most a deterministic or random period of time (time-out). We obtain the steady-state probability distribution of the stochastic process describing the evolution of such a system. Next, we show how to compute some security metrics such as the loss-probability or the buffer occupancy percentage of half-open connections for attack packets.

Keywords: Network security, DoS attack, Queueing, Steady-state distribution, Timeout.

1 Introduction

Networks attacks today (Denial of service (DoS) attack, worm, Trojan horse and virus) are increasing in frequencies, severity and sophistication. They exploit bugs in a specific operating system or vulnerabilities in TCP/IP implementation and can cause serious problems to normal business operations [1-5,7-9]. In this paper, we concentrate on DoS attacks which can be classified into several types. In flooding attack, malicious users (attackers) may flood a network with a large volume of data in order to deliberately consume the basic and limited resources of a victim, such as the process control blocs and the maximum allowed connections. In particular, DoS attacks may disrupt the normal operation of physical components in the network, and may also manipulate data in transit such as encrypted data. The impact of a DoS attack on a particular system will vary depending on the protocols and applications involved. Crippling DoS (CDoS) attack, may cause the degradation of Quality of Service(QoS) or render the service unavailable. Distributed Denial-of-service (DDoS) attacks are simply DoS attacks performed by multiple agents simultaneously. (Some statistics about DoS attacks can be found in [1] and some used networks security metrics in [1-5,7-9].

These works provide also references about some defence mechanisms which have been proposed in the literature to defend against DoS attacks (anomaly-detection, signature-scan including blocking attack packets, tracing and filtering). Many defence

mechanisms have been proposed [7,9] (anomaly-detection and signature-scan techniques, for example). These mechanisms include blocking attack packets to reduce the intensity of attacks, tracing the packets to locate the attacking source and using the proactive measures to filter the attack packets [4,5,7].

Most of the cited works are experimental studies trying to characterise the behaviour of the DoS attacks and quantitatively estimating their impact on the basis of the effective detection and filtering techniques. Most of these studies use simple queueing models to analyse various network security metrics (consumption metrics, complexity metrics,...) [3] Some others use more sophisticated queueing models, but the analysis is also based on experimental simulation [2]. There is some attempts to give more formal framework in order to analytically study the impact of DoS attacks using Queueing theory (see Chang [7]). The motivation is that when an attack has an impact on a network parameter, then such parameter can be used as an attack detection metric [3].

We can mention also in this research direction the work of Khan & Traore [3] which use a simple model $M/M/1/K$ with round robin discipline to analyse the impact of DoS attacks on some parameters as response time or queue-growth-rate. Long et al [2] proposed an abstract queueing model showing the effect of DoS attacks on delay jitter and loss probability both at remote plant level and at controller level. C. Xenakis & al [8] develop an analytic model for an abstract model of UMTS mobile device. The analysis is carried out by modelling the IPsec processor and the transmitter as a system of two independent $M/G/1$ queues in tandem. Wang & al [4] use a two dimensional embedded Markov chain model to study the network under DoS attacks.

In this paper, we provide a next step in this direction in order to analytically characterise the security attributes of a network under DoS attacks such as the most prevalent SYN-flooding attack. We consider the model studied both in [4] and [5] by different methods. The goal is to quantify the damage that a successful attacker can have on the performance of the network such as the loss probability and buffer occupancy of half-open connections. The difference in our model is that the distribution of service times are arbitrarily distributed and we take into consideration the possibility of connection failures. On the other hand, it is obtained explicit formulas for the steady-state probabilities of the underlying stochastic process, which render the model more interesting from the computational point of view.

In the following section we describe the basic model of a network under flooding DoS attack and we derive the steady-state distribution of the network under such attack. In section 3, we consider some useful characteristics which can be used as security metrics. Section 4, is devoted to a discussion of the time-out, particularly the sensitivity of its distribution to the exponential assumption. In section 5 we consider numerical illustrations showing the effect of DoS attacks upon system performance. The accuracy of the model is tested by comparison with the similar model of [4] for different scenarios. Finally, in sections 7 and 8, we discuss the cases of Degradation of service DoS (DSDoS) attacks and non Poisson arrivals respectively.

2 The Basic Model

We consider the model described in [4,5] in which the input queue and service times are stochastic processes. In general, the arrival of SYN packets contains two types:

the regular request packets (first type) which describe the packet flow under network normal status and the attack packets (second type) that request for connections. The victim has a connection buffer of the backlog queue, in which at most N half-open connections are allowed simultaneously, so a maximum number of connections N can be served at the same time. We assume that the connection requests arrive according to a Poisson process with rate λ . This assumption is conform to some experimental studies [11], at least when the network is heavily used. Let $S^{(i)}$ be the service time of i th type of request packet with distribution function $H_i(x) = P(S^{(i)} < x)$, $i = 1, 2$. We assume that $H_i(0+) = 1$. The arrivals of the regular request packets (from legitimate users) and the attack packets (from malicious users) are both Poisson processes with rate λ_1 and λ_2 respectively. The two arrival processes are independent of each other and of the holding times for half-open connections.

Let $\nu(t)$ and $\mu(t)$ be the numbers of the regular request packets and the attack packets at time t , respectively. It indicates the number of connections used by legitimate users and malicious users respectively. It is obvious that at any time $t \geq 0$, we have $\nu(t) + \mu(t) \leq N$, so that a maximum number of both legitimate and malicious connections N can be served in the same time. All connection requests that arrive when the server is in saturated state, $\nu(t) + \mu(t) = N$, will be rejected.

Let $\zeta(t) = \{\nu(t), \mu(t); \alpha_1(t), \dots, \alpha_{\nu(t)}; \beta_1(t), \dots, \beta_{\mu(t)}\}$ be the stochastic process where the discrete component is defined on the state space $IN \otimes IN$ and $\alpha_i(t) \in IR_+$ is the residual service time of a regular packet on the server $N^\circ i$ and $\beta_j(t) \in IR^+$ the residual service time of a malicious packet on the server $N^\circ j$

$$F_{i,j}(t; x^{(i)}, y^{(j)}) = P\{\nu(t) = i, \mu(t) = j; \alpha^{(i)}(t) < x^{(i)}; \beta^{(j)}(t) < y^{(j)}\}$$

$$0 \leq i + j \leq N$$

Here we have denoted by $x^{(i)} = (x_1, \dots, x_i)$, $y^{(j)} = (y_1, \dots, y_j)$ and $\alpha^{(i)}(t) < x^{(i)}$

means that $\alpha_k(t) < x_k, \forall k = 1, \dots, i$.

If $\max(\tau_1, \tau_2) < \infty$, then the stochastic process $\{\zeta(t), t \geq 0\}$ has a stationary ergodic distribution. By using a method similar to that of Sebastianov [11] (see also [6]) we can find that the steady-state probability distribution is solution of the following equilibrium system of partial differential equations

$$\sum_{p=1}^i \frac{\partial F_{i,j}}{\partial x_p} + \sum_{q=1}^j \frac{\partial F_{i,j}}{\partial y_q} - (\lambda_1 + \lambda_2)(1 - \delta_{i+j,N}) + \frac{\lambda_1}{i} \sum_{p=1}^i F_{i-1,j}(x(i,p); y^{(j)})H_1(x_p) +$$

$$+ \frac{\lambda_2}{j} \sum_{q=1}^j F_{i,j-1}(x^{(i)}; y^{(j,q)})H_2(y_q) = \sum_{p=1}^i \frac{\partial F_{i,j}(x_1, \dots, x_{p-1}, 0, x_{p+1}, \dots, x_i; y^{(j)})}{\partial x_p} +$$

$$\sum_{q=1}^j \frac{\partial F_{i,j}(x^{(i)}; y_1, \dots, y_{q-1}, 0, y_{q+1}, \dots, y_j)}{\partial y_q} + (i+1) \frac{\partial F_{i+1,j}(x_1, \dots, x_i, 0; y^{(j)})}{\partial x_{i+1}} + (j+1) \frac{\partial F_{i,j+1}(x^{(i)}; y_1, \dots, y_j, 0)}{\partial y_{j+1}},$$

where $x^{(i,p)} = (x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_i)$ and $y^{(j,q)} = (y_1, \dots, y_{q-1}, y_{q+1}, \dots, y_j)$

It is not difficult to see that the solution of this equation is of the form

$$F_{i,j}(x^{(i)}; y^{(j)}) = \frac{\lambda_1^i \lambda_2^j}{i! j!} F_{00} \times \Pi(H_1, x^{(i)}) \times \Pi(H_2, y^{(j)}), \tag{1}$$

$$\Pi(H, x^{(i)}) = \prod_{p=1}^i \int_0^{x_p} [1 - H(u)] du$$

Since

$$\lim_{\substack{x_p \rightarrow \infty, 1 \leq p \leq i \\ y_q \rightarrow \infty, 1 \leq q \leq j}} F_{i,j}(x^{(i)}; y^{(j)}) = \frac{(\lambda_1 \tau_1)^i (\lambda_2 \tau_2)^j}{i! j!} F_{00},$$

then, the unknown constant can be found from the normalisation condition

$$F_{00} \sum_{i=0}^N \sum_{j=0}^{N-i} \frac{(\lambda_1 \tau_1)^i (\lambda_2 \tau_2)^j}{i! j!} = 1,$$

Next, we get

$$F_{00} = \left[\sum_{\substack{i,j=0 \\ 0 \leq i+j \leq N}} \frac{(\lambda_1 \tau_1)^i (\lambda_2 \tau_2)^j}{i! j!} \right]^{-1}, \tag{2}$$

Finally, we obtain the probability that the server is in a specific state (i, j) , indicating that i regular packets and j attack packets are in the system

$$p_{i,j} = \frac{(\lambda_1 \tau_1)^i (\lambda_2 \tau_2)^j}{i! j!} \left[\sum_{\substack{i,j=0 \\ 0 \leq i+j \leq N}} \frac{(\lambda_1 \tau_1)^i (\lambda_2 \tau_2)^j}{i! j!} \right]^{-1}, 0 \leq i + j \leq N, \tag{3}$$

Particular case. If $H_1(x) = 1 - e^{-\mu_1 x}, x \geq 0$ and $H_2(x) = 1 - e^{-\mu_2 x}, x \geq 0$, and $\rho_i = \lambda_i / \mu_i, i = 1, 2$ then we obtain

$$p_{i,j} = \frac{(\rho_1)^i (\rho_2)^j}{i! j!} \left[\sum_{\substack{i,j=0 \\ 0 \leq i+j \leq N}} \frac{(\rho_1)^i (\rho_2)^j}{i! j!} \right]^{-1}, \tag{4}$$

3 Security Metrics

Now, from the above results, we can derive some security metrics which characterise the performance of the network under DoS attack. They are similar to that of [4,5].

Connection loss probability is a basic measure which can be obtained from the stationary distribution as follows

$$P_{loss} = \sum_{i=0}^N p_{i,N-i} ,$$

We can use this characteristic as a detection intrusion metric by fixing threshold value $\varepsilon = \varepsilon(N)$ small enough to indicate the network security status; if $P_{loss} \geq \varepsilon$, then the network is under DoS attack.

Another performance measure which can be used as security metric is the buffer occupancy percentage of half-open connections for regular traffic. It is characterised by the mean ratio of the number of regular half-open connections to the maximum allowable number of half-open connections

$$P_r = \frac{1}{N} \sum_{i=0}^N i \sum_{j=0}^{N-i} p_{i,j} ,$$

Similarly, the buffer occupancy percentage of half-open connections for attack packets is

$$P_a = \frac{1}{N} \sum_{i=0}^N \sum_{j=0}^{N-i} j p_{i,j} ,$$

It represents the mean ratio of the number of attack packets to the maximum allowable number of half-open connections.

4 Time Out

In realistic situations [4,5] of SYN-flood attacks, each half-open connection is held for at most a deterministic (or random) period of time B which is time interval from the epoch that the half-open connection begins to the epoch that the connection is dropped. The event “*connection arrived*” represents a SYN message and the event “*connection completed*” corresponds to ACK message being received by the server. In the case of SSL connection depletion attack, N_1 and N_2 represent the number of legitimate and malicious completed TCP connections respectively, that have not yet established a secure channel and for which the negotiation phase is still in progress.

The *connection arrived* event represents the *Client hello* message being received by the server and the *connection completed* event represents the corresponding *Finished message* being sent by the server. It is even possible to consider a nested model, each level representing a different layer in the protocol stack [5].

It is possible to take into account these phenomena by modifying the equilibrium equations and then solve them. But, in this study we take a more rapid argumentation. According to our assumptions, connections completed events are generated at intervals of time from the *connection arrived* events, if the *time_out* has not elapsed. Otherwise, *connection expired* events are generated at time-out intervals from the *connection arrived* event, so that the effective legitimate service time S_B is

$$S_B = \begin{cases} S, & \text{if } S \leq B \\ B, & \text{if } S > B \end{cases} ,$$

Then the probability distribution of S_B is

$$H_{S_B}(x) = H_2(x)H_2(B) + \chi(B < x)\bar{H}_2(B) ,$$

It is not difficult to show that the mean time-out is

$$\tau_B = E(S_B) = B\bar{H}_2(x) + \int_0^B x dH_2(x) , \tag{5}$$

$$\tau_b^{(2)} = B\bar{H}_2(B) = \int_0^B x^2 dH_2(x) , \tag{6}$$

In particular, if $H_2(\cdot)$ belongs to the class of NBUE (New Better than Used) probability distributions with mean $\bar{\tau} = \frac{1}{\mu}$, then $S_B \leq_{st} S_{\text{exp}}$ i.e. S_B is stochastically smaller than a random variable S_{exp} with distribution function $H_{\text{exp}}(x) = e^{-\mu B} \delta(x-B) + [1 - e^{-\mu x}] [1 - e^{-\mu B}]$ and the mean time-out $\tau_B \leq \tau_{\text{exp}} = \frac{1 - e^{-\mu B}}{\mu}$ suggested in [5] for the effective mean service time of legitimate connections.

Now we can modify the probability of the event *connection failed* as follow $\phi = \phi_r + \phi_e$ where ϕ_r is the probability of the event *connection rejected* : it occurs when the server was not able to serve the connection because no more connection channels were available (the queue is full), and ϕ_e is the probability of the event *connection expired*: the server tried to serve the connection but the communication timed out and the connection was dropped.

If $\infty^{(i)}$ means that $x_k = \infty, 1 \leq k \leq i$, then in stationary regime, we have

$$\phi_e = 1 - \sum_{i=0}^N \sum_{j=0}^{N-i} \frac{\lambda_1^i \lambda_2^j}{i! j!} F_{00} \times \Pi(H_1, \infty^{(i)}) \times \prod_{q=1}^j \int [1 - H_2(u)] du ,$$

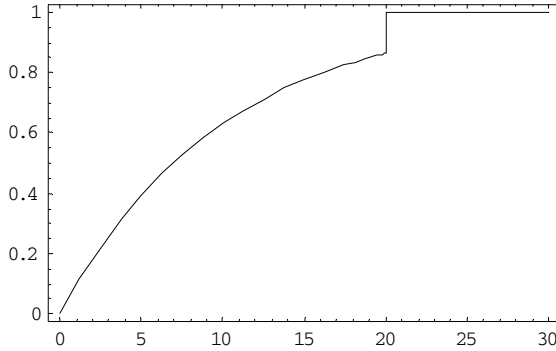
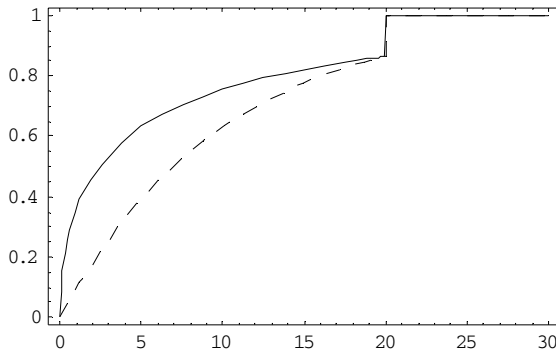


Fig. 1. Time-out distribution function for exponential service distribution ($\mu = 0.1$)



- - - -
 exponential service distribution ($\mu = 0.1$)
 ———
 Weibull service ($\lambda = 0.2, \alpha = 0.5$)

Consider now the problem of approximating analytically the time_out distribution. Consider two such distributions F and G , X and Y being the corresponding random variables. For example, G can be the exponential distribution used as approximating distribution in [4,5]. How we can estimate the deviation of the unknown F from the approximating one G ? If for example $F <_* G$ and have the first two moments common, then $F = G$, where $<_*$ is the star stochastic order. The two corresponding random variables are ordered in this sense if and only if the random variable $Z = \Lambda_G(X)$ has an increasing failure rate average (IFRA) distribution.

It has been shown [13] that when the two distributions share the first moment, but the second moments are known, then the deviation of the two distributions can be estimated by

$$\sup_{x \geq 0} |F(x) - G(x)| \leq 3b^{2/3} [\zeta(X, Y)]^{1/3},$$

where b is the supremum of the density of either F or G and $\zeta(X, Y)$ is the average metric given by

$$\zeta(X, Y) = \int_0^\infty \int_0^\infty [F(u) - G(u)] du dx$$

From now, we assume that $X <_* Y$, $E(X) \leq E(Y)$ (if $E(X) < E(Y)$, then $F(x) < G(x)$ for some x and the second moments of F and G are finite). Then the average metric can be expressed through the two first moments

$$\zeta(X, Y) = \frac{1}{2} [E(Y^2) - E(X^2)].$$

So, $F = G$ if and only if the two moments are equal.

Now, if the approximating distribution G (or F) has a density uniformly bounded by b , then we have a family of bounds of the form

$$\sup_{x \geq 0} |F(x) - G(x)| \leq 3 \left[\frac{b^2(\alpha)}{2} \{v(\alpha) - E(x^2)\} \right]^{1/3}, \tag{6}$$

where $b(\alpha) = \sup_{x \geq 0} \alpha g(x) \bar{G}^{\alpha-1}(x)$, $v(\alpha) = \int_0^\infty 2x \bar{G}^\alpha(x) dx$.

This bound comes from the fact that $F <_* G$ is equivalent to $F <_* (1 - \bar{G}^\alpha)$ for each $\alpha > 0$. So the range of α in (6) is $\alpha_1 < \alpha \leq \alpha_2$, where α_1 is the largest value of α such that $\bar{F} = 1 - F$ is completely dominated by \bar{G}^α , and α_2 is such that the first moment of $1 - \bar{G}^{\alpha_2}$ is the same as that of F . In some cases the ‘‘best possible approximation’’ can be obtained by minimizing the right-hand side with respect to α over the interval $(\alpha_1, \alpha_2]$.

For example, if H_2 is an IFRA distribution with first two moments μ_1 and μ_2 , then H_B is also an IFRA distribution (at least for random time-out which can be chosen as an IFRA random variable) and the approximating time-out distribution is exponential as in [4,5], with

$$\sup_{x \geq 0} |F(x) - e^{-\alpha x}| \leq \varepsilon(B) = 3 \left[1 - \tau_B^{(2)} / (2(\tau_B)^2) \right]^{1/3}, \quad \forall 0 < \alpha \leq 1 / \tau_B$$

Here $\alpha_1 = 0$, $\alpha_2 = 1 / \tau_B$, and the minimal deviation is obtained for this last value of α .

This bound holds in fact for all upper non parametric distributions, in particular *NBU*, *NBUE*, *HNBUE*.

Consider for example, the following IFRA distribution $H_2(x) = (1 - e^{-x})(1 - e^{-2x})$, then figure 3 shows evolution of the error $\varepsilon(B)$ in (6) as a function of the mean timeout B .

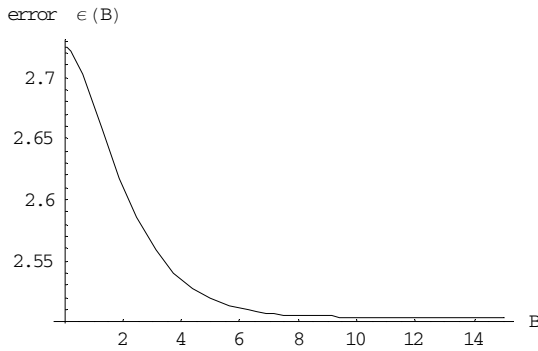


Fig. 3. Evolution of the upper error bound $\epsilon(B)$ as a function of B

5 Numerical Examples

We consider now some numerical examples showing the effect of DoS attacks on some performance metrics.

First, we test the accuracy of our model (model 2) with the similar model of Wang (2007) [4] (model 1). In that work the basic numerical data are as follows. Let $\lambda_1 = 10$ packets/sec be the parameter of the Poisson arrival process of regular request packets ; $\lambda_2 = k\lambda_1$ is the parameter of the Poisson arrival process of attack request packets. In this case, the attack parameter k may be understood as the ratio of arrival rates between the attack packets and the regular request packets. The service time distribution is exponential $H_1(x) = H_2(x) = 1 - e^{-\mu x}$, with mean $\mu^{-1} = 100$ sec. Note that it is not difficult from our formula to take different distributions of service time for regular and attack requests, for example a Weibull distribution.

We consider the following scenarios:

Scenario 1. Let the mean time-out $B = 5$.

Scenario 2. Let the maximum allowable number of half-open connections $N = 20$.

For the first scenario, the values of the loss probabilities for both models 1 and 2 are given in table 1 for different values of the attack parameters k . Also, we considered different scenarios about the values of $N = 10, 20, 50$. As in [4], we observe that the loss probability increases with the increase of the attack traffic load. On the other hand, the values of P_{loss} for both models are similar, particularly for great values of k . The deviation between two models comes from the different nature of the assumptions about the mean time-out. Note however that our model 1 is more interesting from the computational point of view. Indeed, Wang & al [4] claim a computational complexity of $O(N^6)$ on a sequential machine , and $O(N^{5.7})$ on a parallel machine. Our method gives an explicit formula with complexity no greater than $O(N)$, in order to compute the normalisation constant.

Table 1. Comparison of loss probabilities for model 1 and model 2 (scenario 1: $B = 5$)

$k \downarrow$	$N \rightarrow$	$N = 10$		$N = 20$		$N = 40$	
		Model1	Model2	Model1	Model2	Model1	Model2
$k = 0$		0.01	--	--	--	--	--
$k = 0.2$		0.5	0.8324	--	0.6665	--	0.3456
$k = 0.4$		0.9	0.8559	0.45	0.7128	0.001	0.4321
$k = 0.7$		0.9	0.8809	0.9	0.7624	0.2	0.5279
$k = 1$		0.9	0.8986	0.9	0.7975	0.82	0.5966
$k = 1.25$		0.9	0.9097	0.9	0.8197	0.9	0.6404
$k = 1.6$		0.9	0.9218	0.9	0.8437	0.9	0.6880
$k = 1.9$		0.9	--	0.9	0.8597	0.9	0.7198
$k = 2.3$		0.9	--	0.9	0.8766	0.9	0.7534

The corresponding loss probabilities for the second scenario are given for both models in table 2, when the maximum number of allowed half-open connections is set to be $N = 20$. Other scenarios showing the mean ratio of the number of regular half-connections to the maximum allowable number of half-open connections versus the attack load result in similar tables and plots that are omitted here for brevity. In all scenarios, we observe small deviations between studied characteristics, while the computation time is considerably improved.

Table 2. Comparison of loss probabilities for model 1 and model 2 (scenario 2: $N = 20$)

$k \downarrow$	$B \rightarrow$	$B = 1$		$B = 10$		$B = 50s$	
		Model1	Model2	Model1	Model2	Model1	Model2
$k = 0$		0	--	--	--	--	--
$k = 0.2$		0.5	0.8324	--	0.6665	--	0.3456
$k = 0.4$		0.9	0.85596	0.45	0.7128	0.001	0.4321
$k = 0.7$		0.9	0.8809	0.9	0.7624	0.2	0.5279
$k = 1$		0.9	0.8986	0.9	0.7975	0.82	0.5966
$k = 1.25$		0.9	0.9097	--	0.8197	0.9	0.6404
$k = 1.6$		0.9	0.9218	--	0.8437	0.9	0.6880
$k = 1.9$		0.9	--	--	0.8597	--	0.7198
$k = 2.3$		0.9	--	--	0.8766	--	0.7534

Figure 4, shows the connection loss probability P_{loss} as a function of the attack traffic load with different settings for the maximum allowable number of half-open connections N . We use again the basic data of the work[4].

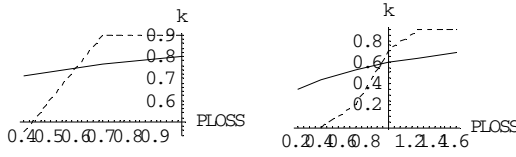


Fig. 4. Effect of the attack parameter k on the connection loss probability for different values of $N = 10, 40$ ($H^{(i)}(x) = 1 - e^{-\mu x}$). The dashed line corresponds to model 1.

In a second set of experiments (Fig.5), we take a non exponential service distribution. We choose a Weibull distribution $H_i(x) = 1 - e^{-(\lambda x)^\alpha}$, with $\lambda = 0.02$ and $\alpha = 0.5$, so it has the same mean as the previous example, with a coefficient of variation greater than one. Figure 5, shows the effect of the attack for different scenarios about the maximum number of allowable half-open connections.

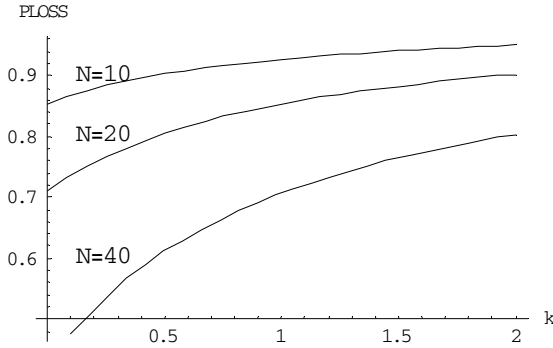


Fig. 5. Effect of the attack parameter k on the connection loss probability for different values of $N = 10, 20, 40$ ($H^{(i)}(x) = 1 - e^{-(\lambda x)^\alpha}$).

6 Degradation of Service DoS Attack

In this section we discuss the case of DSDoS attack where service becomes unavailable for a random restoration period of time. These DSDoS attacks occur according to the following process. If at any time, a connection is in course, then the life time of the connection (the period between beginnings of service until such an attack occurs) is a random variable ξ with distribution function $F(x)$. We assume that when such an attack occurs, a connection is interrupted with the loss of packet in service at this time. A restoration begins for a random period of time η with distribution function $G(x)$. On the other hand all arriving packets (regulars or attackers) finding all connections unavailable (busy or out of order) are lost. In this case we have again a solution of the form

$$F_{i,j,k}(x^{(i)}; y^{(j)}, u^{(k)}, v^{(l)}) = \frac{\lambda_1^i \lambda_2^j \gamma_1^k \gamma_2^l}{i! j! k! l!} F_0 \times \Pi(H_1, x^{(i)}) \times \Pi(H_2, y^{(j)}) \times \Pi(G_1, u^{(k)}) \times \Pi(G_2, v^{(l)}),$$

where $\gamma_i = \int_0^\infty [1 - H_i(x)] dF(x)$ and $1 \leq i + j + k + l \leq N$.

The underlying markovian process is ergodic if $\max(E(\xi), E(\eta), E(\tau_1), E(\tau_2)) < \infty$.

7 Non Poisson Arrivals

Consider now the case of non Poisson arrival processes of regular or attack packets. It is indeed difficult to obtain an explicit solution for the modified basic process. However, we can obtain some useful assertions concerning the condition of non saturation of the system.

Let t_n^1 (resp. t_n^2) be the instant of the n -th regular (resp. attack) packet and $\xi_n^i = t_{n+1}^i - t_n^i, (i = 1, 2), n = 0, 1, \dots$. Also, let τ_n^i be the service time of the n th packet of type $i, i = 1, 2$.

Now we consider the process $q_{((i,j))}(x)$ indicating that i legitimate connections and j malicious connections after a period of x units from the last arrivals, $q_{((i,j))} = q_{((i,j))}(0)$.

We assume that the sequence $\left\{ \xi_n^i, \tau_n^i, -\infty < n < \infty \right\}$ is stationary (in the strict sense) and ergodic.

We follow the methodology of Borovkov [12] which consists to construct a judicious sequence of stationary events $\left\{ A_{(i,j)} \right\}$ from a positive event A_0 , by iteration $A_{(i,j)} = T^{i+j} A_0$. Here T is the shift transformation of measurable sets of the σ -algebra generated by the sequences of input random variables $\left\{ \xi_n^i, \tau_n^i, -\infty < n < \infty \right\}$ corresponding to the measure preserving transformation on such measurable random variables. The event $B = \bigcup_{i+j \leq -m+1} A_{(i,j)}$ is such that $TB \supset B$ and

$P(TB) = P(B)$. Hence, $TB = B$ except perhaps on a negligible set (with zero probability). In view of the metric transitivity of our sequence, $P(B) = 0$ or $P(B) = 1$.

In order to have the last case, we need to choose a positive event A_0 , so from the inequality $P(B) \geq P(A_0) > 0$, we will deduce that $P(B) = 1$. Finally, it follows that the sequence of processes $\left\{ q_{n+k}^{(i,j)}(x) \right\}$ converges to a stationary process $\left\{ q^{(i,j)}(x) \right\}$ satisfying $P(q^{(0,0)}(0) = 1)$. The convergence is understood here in a strong sense.

For example, a concrete sufficient conditions for $P(A_0) > 0$ to hold is that

$$P(\tau^{(i)} \leq m\xi^{(i)}) > 0, i=1,2, \text{ and } \max[E(\tau^{(1)}), E(\tau^{(2)})] < \infty$$

Another sufficient condition is the following: there exists x_0 such that for all $x \geq x_0, \Delta > 0$

$$P(\tau^{(i)} \in (x, x + \Delta) > 0), \max[E(\tau^{(1)}), E(\tau^{(2)})] < \infty$$

8 Conclusion

In this paper we proposed a new model for the analysis and security performance evaluation of computer networks. The model is interesting in the sense that its stochastic nature allows to capture attacker behaviour, system's response to attack and intrusion. The model takes into consideration the traditional failure processes in the Reliability sense So it can be included in more general simulation software environment. The accuracy of the model has been tested with a similar model for different scenarios about the input parameters. The developed model is particularly interesting from the computational point of view.

Further study may be evidently oriented to the case when the arrival processes are non Poisson although some experimental studies claim that the Poisson assumption is acceptable. Of course, an important effort need to be given to the simulation of real DoS attacks. However, the analytical nature of the model allows to conduct simulations by using some relevant data or few execution traces of a real system. So, we can draw conclusions under quite general assumptions about the parametric probability distributions. We also conjecture that the model in this form is insensitive to these distributions i. e. the loss probability depends only on the first moments of these distributions. An interesting problem is the optimisation of the above mentioned security metrics relatively to some controllable parameters and according to the envisaged technical architecture. Note finally, that a particular attention must be given to other types of DoS attacks as the crippling DoS attack or degradation Quality of Service (QoS) attacks [5].

Acknowledgements

The author is grateful to the referees for their comments. This work has been supported in parts by CNEPRU B00220060089 and Tassili 06 MDU 687 project grants.

References

1. Moore, D., Voelker, G., Savage, S.: Inferring Internet Denial-of-Service Activity. In: Proceedings of the 2001 USENIX Security Symposium, pp. 9–22. IEEE Press, New York (2001)
2. Long, M., Wu, C.-H., Hung, Y.: Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation. IEEE Transactions on Industrial Informatics 1(2), 85–96 (2005)

3. Khan, S., Traore, I.: Queue-based Analysis of DoS Attacks. In: Proceedings IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, pp. 266–273. IEEE Press, New York (2005)
4. Wang, Y., Lin, C., Li, Q.-L., Fang, Y.: A Queueing Analysis for the Denial of Service (DoS) Attacks. *Computer Networks* 51, 3564–3573 (2007)
5. Boteanu, D., Fernandez, J.M., McHugh, J., Mullins, J.: Queue Management as a DoS counter-measure? In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) *ISC 2007*. LNCS, vol. 4779, pp. 263–280. Springer, Heidelberg (2007)
6. Gnedenko, B.V., Kovalenko, I.N.: *Introduction to Queueing Theory*, Nauka, Moscow (1967)
7. Chang, R.K.C.: Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A tutorial. *IEEE Communications Magazine* 40(10), 42–51 (2002)
8. Xenakis, C., Laoutaris, N., Merakos, L., Stavrakis, L.: A Generic Characterization of the Overheads Imposed by IPsec and Associated Cryptographic Algorithms. *Computer Networks* 5(17), 3225–3241 (2006)
9. Mirkovic, J., Reiher, P.: A Taxonomy of DDoS Defence Mechanisms. *SIGCOMM Comput. Commun. Rev.* 34(2), 39–53 (2004)
10. Sevastianov, B.A.: An Ergodic Theorem for Markov Processes and its Application to Telephone Systems with Refusals. *Theory of Probability and its applications*, Tom II 1, 106–116 (1957)
11. Foster, L., Cao, J., Cleveland, W., Lin, D., Sun, D.: Internet traffic tends toward Poisson and independent as the load increases. In: Denison, D., Hansen, M., Holmes, C., Mallick, B., Yu, B. (eds.) *Nonlinear estimation and Classification*. LNCS, vol. 171, pp. 83–110. Springer, Heidelberg (2003)
12. Borovkov, A.A.: *Ergodicity and Stability of Stochastic Processes*. Wiley Series in Prob. & Stat. J. Wiley & Sons, Chichester (1998)
13. Sengupta, D., Deshpande, J.V.: Some Results on the Relative Ageing of Two Life Distributions. *J.Appl. Prob.* 31, 991–1003 (1994)