International Journal of Computer and Communication Technology

Volume 5 | Issue 1 Article 5

January 2014

A Mathematical Model for Randomly-Occurring Low-Rate Denial of Service Attacks

Nahush Chaturvedi
Department of Computer and Information Science and Engineering, University of Florida, Gainesville, Florida, USA,, nahush@cise.ufl.edu

Hrushikesha Mohanty
Department of Computer and Information Sciences, University of Hyderabad, Hyderabad, India., mohanty.hcu@gmail.com

Recommended Citation
Chaturvedi, Nahush and Mohanty, Hrushikesha (2014) "A Mathematical Model for Randomly-Occurring Low-Rate Denial of Service Attacks," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 1 , Article 5.
DOI: 10.47893/IJCCT.2014.1215
Available at: https://www.interscience.in/ijcct/vol5/iss1/5

A Mathematical Model for Randomly-Occurring Low-Rate Denial of Service Attacks

Nahush Chaturvedi, Hrushikesha Mohanty
Department of Computer and Information Science and Engineering, Department of Computer and Information Sciences
University of Florida, Gainesville, Florida, USA, University of Hyderabad, Hyderabad, India
nahush@cise.ufl.edu, mohanty.hcu@gmail.com

Abstract*—Low rate attacks, or Denial-of-Service (DoS) attacks of the occasional misbehaviour, can throttle the throughput of robust timed-protocols, like the Transmission Control Protocol(TCP), by creating either periodic or exponentially distributed outages, or transmission disruptions. Such attacks are as effective as full-fledged DoS with high undetectability of the misbehaving network entity. In this paper, we present a mathematical model of Low-Rate. randomly occurring, Denial-of-Service attacks. By viewing the process as a two-state Continuous-Time Markov Chain(CTMC), we have successfully computed the transition and state probabilities of a compromised network entity that can behave normally, while in the normal state. and abnormally, when in the abnormal state.

Key words:* Low-rate Denial of Service Attacks, Transmission Control Protocol (TCP), stochastic processes, randomly-occurring outages, exponential distribution, Continuous Time Markov Chains.

I. INTRODUCTION

Denial-of-Service attacks, traditionally known as a benign network attack, can be twice as detrimental to transmissions by depleting resources for legitimate users and, from the time gained by the disruption, expediting the correlation of the communicating parties' identities with the packets received, thus endangering the privacy of the sender and the receiver of the message. While simple Denial-of-Service attacks involve bringing down the entire network in one blow through a compromised network entity, like a router, more evolved network attacks mandate the compromised entity to misbehave only at certain intervals of time while behaving normally the rest of the time. The idea has been dealt with extensively in [1], deeming these attacks Low-Rate Denial of Service attacks. These attacks can either be mounted by creating periodic or exponentially distributed outages. While [1] contains a thorough survey of such attacks through periodic outages, little has been done to model Low-Rate attacks through randomly occurring, or exponentially distributed, traffic disruptions.

The idea of a mathematical model of Low-Rate Denial of Service Attacks has been discussed in [4], [1] alongwith its effects on the overhead and the client-success probability, or the probability of finding a vacant slot in an application server queue. These attacks, however, utilise a compromised network entity's ability to predict a vacancy in the application server, while the attacks mentioned in [1] exploit the retransmission characteristics of the Transmission Control Protocol (TCP).

Our work, however, is protocol-independent and takes into consideration a very general pattern of compromised-entity- behaviour that could be applied to a variety of situatiions. The conditions that must be met for a server to be a potential target has been discussed in [5]. Finally, the methods and means of detecting Low-Rate Attacks have been discussed in [1], [2], [3], [5].
In this paper, we address the question of modelling Low-Rate DoS attacks with randomly occurring outages. The paper is organised as follows: Section 2 gives an intuitive introduc- tion to compromised-network-entity misbehaviour character- istics when mounting such attacks, while Section 3 contains a rigorous mathematical treatment of the subject. We present our conclusions in Section 4.

II. THE PRELIMINARIES

In Low-Rate Denial of Service Attacks, a compromised network entity creates transmission blackouts, referred to as

'outages', in which it overwhelms the target system with packets, thus denying network resources to legitimate users. These outages are created at specific time epochs, a statistics- term for time instants. The time intervals between consecutive outages, which is the time when the compromised entity behaves normally, can either be periodic or exponentially distributed, in which case, it becomes a random process. Fig.

1 illustrates the idea. The genesis of such attacks lies in [1], where low-rate attacks with periodic outages are modelled and investigated in terms of their effect on the throughput of the Transmission Control Protocol (TCP) and how its various flavours respond to these attacks, which exploit the Retrans- mission Time Out(RTO)

characteristic of TCP protocols. By creating outages of duration of the Round-Trip-Time(RTT) of packets after minRTO (minimum Retransmission Time Out) units of time, the throughput of a robust protocol like the TCP can be throttled.

In this paper, we have attempted to model low-rate attacks with randomly-occurring outages. Assuming that a misbehav- ing network entity has two states, the normal and the abnormal states, and that normal and abnormal behaviour on the system's part is the outcome of the system being in these states, we view the alternation between the normal and abnormal states as a stochastic process. Since normal behaviour, lasting for the time

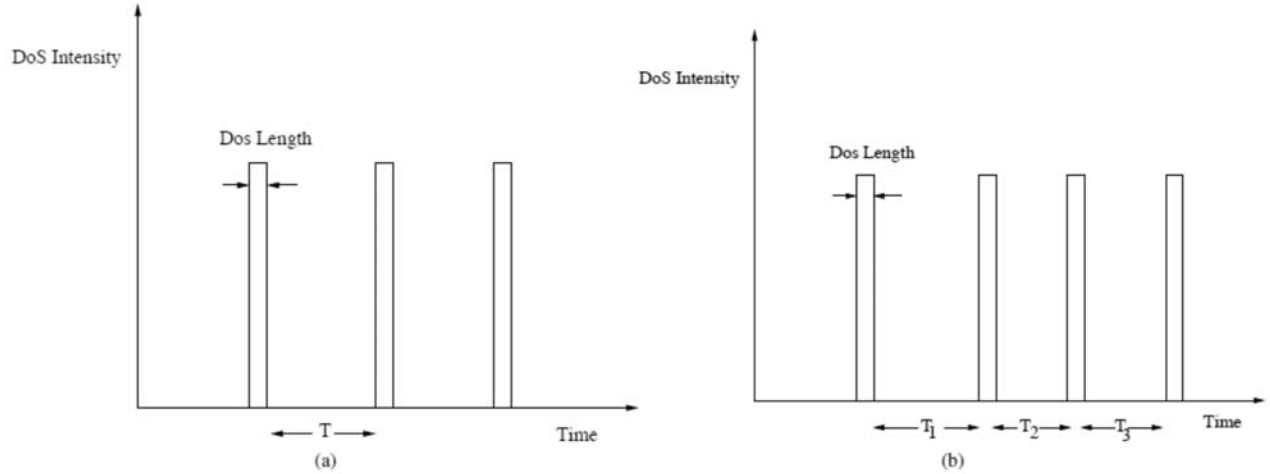

Fig. 1: (a) Low-rate attacks with periodically occurring outages. (b) Low-rate attacks with randomly occurring outages.

between consecutive outages, is the outcome of the time spent in the normal state, we arrive at the following conclusions

Time interval between consecutive outages = Time spent in the normal state
Duration of an outage = Time spent in the abnormal state

Hence, the conditional probability of the system being in state, say u, at time epoch (t + s), given that the system is in state u at time epoch t, is then the same as the probability of the system spending s or more units of time in state u starting from time epoch t. Since this duration is random, and hence statisfying the Markovian property of memorylessness, the aforementioned conditional probability distribution is an exponential one. These ideas are discussed more rigorously in the next section.
Intuitively, undetectability demands the probability of a misbehaving router assuming the abnormal state to be less than the router assuming the normal state. Hence, the chances of the router being in the normal state are greater than it being in the abnormal state. On a time scale, this would imply that the time spent by the router in the normal state is greater than the time spent in the abnormal state. Thus, the time spent in a particular state u is of vital importance. In the next section, a more rigorous mathematical treatment of the ideas, discussed in this section, leading to the computation of the probabilities of the system being in the normal and abnormal states.

III. THE MODEL

Let the state space of a misbehaving router, S, be given by

$S = \{N,A\}$

where N refers to the normal state of a misbehaving router and A denotes the abnormal state of a router.
For any general state space comprising states u and v, let U_t be a random variable denoting the time spent in state u starting from, and X_t be another random variable denoting the state at, epoch t. Then

(Ut e" s) a"(Xt' = u, t d" t' d" (t + s))a"(Xt+s = u, Xt = u) (1)
Ò! P (Ut e" s) = P (Xt+s = u, = u) (2)
Ò! P (Ut e" s) = P (Xt+s = u | Xt = u)P (Xt = u) (3)

Let us look at (1). The random variable Ut is a continuous random variable and so P(U_t = s) = 0. Therefore, it must be the case that either P(U_t d" s) or P(Ut e" s). Since we are concerned with finding the probability that a compromised router would spend a time interval of s units in state u (that is to say, starting from time epoch t, the system would be in state u at epoch (t + s)), and since P(U_t = s) = 0, U_t being a continuous random variable, the only way we can be sure that the system would indeed spend a time of s units in the state u is by assuming P(U_t e" s). In other words, the minimum amount of time spent in state u would be s units of time. The assumption that P(U_t d" s) would mean that the maximum amount of time spent in state u is s units of time, but we cannot be sure that starting at epoch t, the system would definitely be in state u at epoch (t + s) since a state transition could occur much earlier than time epoch (t + s). Bearing this in mind, the right-hand-side of (1) would have to be written as P($X_{t'}$ = u; t d" t' d" (t + s)). Of course, the actual time epoch, starting from time epoch t, at which the transition takes place, could be greater than (t+s), but, s being the minimum amount of time spent in state u (from the left-hand-side of (1)), we can be sure that the system would be in state u at time epoch (t + s). This gives us (1) in its stated form.

From the definition, it is clear that the system is in state u at epoch t and thus
P (Xt = u) = 1 (4)
Substituting (4) in (3), we get
P (Ut ≥ s) = P (Xt+s = u | Xt = u) (5)

The equation above tells us that Ut and Xt+s = u given that Xt = u are identically distributed. While there is no restriction on the probability of the random variable Ut , the most general case, in the context of modelling misbehaviour, is that of Ut (the time spent in state u starting from epoch t) being a random process and thus Markovian(memoryless). Since Ut is a continuous random variable constituting a Markovian process and since the exponential distribution is the only probability distribution satisfying the Markovian property, we have

$$P(U_t \geq s) = \alpha(u) \int_s^{\infty} e^{-\alpha(u)t} dt \quad (6)$$

where á(u) is a function associating with state u the expected number of times the system is in state u per unit time. Mathematically,

$$\alpha : S \mapsto [0, 1] \quad (7)$$

The reason for the chosen co-domain will soon be clear. Also, note that

$$\alpha(u) = \frac{1}{\lambda},\ u \in S$$

where ë refers to the expected holding time of state u. Substituting (6) in (5), we have

$$P(X_{t+s} = u \mid X_t = u) = \alpha(u) \int_s^{\infty} e^{-\alpha(u)t} dt = e^{-\alpha(u)s} \quad (8)$$

$$\Rightarrow \quad P(X_{t+s} = u \mid X_t = u) = e^{-\alpha(u)s} \quad (9)$$

In a two-state system, with the states being u and v, we can say that

$$P(X_{t+s} = v \mid X_t = u) = 1 - P(X_{t+s} = u \mid X_t = u) \quad (10)$$

$$P(X_{t+s} = v \mid X_t = u) = 1 - e^{-\alpha(u)s} \quad (11)$$

From (9), we have

Now, we wish to determine the state matrix, ð(t), containing the probabilities of the system being in states u and v at time epoch t. We know that

$$\boldsymbol{\pi}(t) = \boldsymbol{\pi}(0) e^{\mathbf{Q}t} e^{-t} \quad (12)$$

$$\alpha(u) = \frac{1}{\lambda},\ u \in S$$

$$q_{uu} = 1 - \alpha(u) \quad (13)$$

$$\mathbf{Q} = [q_{ij}]_{|S| \times |S|}, q_{ij} = \lim_{s \to 0} \left(\frac{P(X_{t+s} = j \mid X_t = i)}{s} \right) \quad (13)$$

and Q is defined thus
where |S| refers to the number of states the system can assume. Ours is a two state system and thus |S| = 2.

From (11) and (13) we have

Since q_{uv} [0, 1] u, vS, we have the constraint that á (u) [0, 1] u S and thus the co-domain in the definition of á in (7). Since

we have the constraint that the expected holding time for any state should be greater than or equal to 1 viz. ë e" 1 ∀ u S. The units of measurement of the average holding times of each state vary from each other as we shall see later in this

document. We notice from (14) that the greater the expected holding time of a particular state u, the lower the probability of the system making a transition to state v.
Expressing the results in (14) and (15) for our statespace as a matrix, we have

$$Q = \begin{array}{c} \\ N \\ A \end{array} \begin{array}{c} \begin{array}{cc} N & A \end{array} \\ \begin{pmatrix} (1-\frac{1}{\lambda}) & \frac{1}{\lambda} \\ \frac{1}{\lambda'} & (1-\frac{1}{\lambda'}) \end{pmatrix} \end{array} \qquad (16)$$

where ë = 1/á(N) and ë' = 1/á(A). Now, the units of measurement of _ and _0 are of vital importance. The following table shows the default timeout values for the TCP and SCTP protocols for the Windows and Linux operating systems. As is obvious from the table above, the Timeout

TABLE I: Timeout values for TCP and SCTP protocols in the Windows and Linux operating systems

PROTOCOL	MINIMUM TIMEOUT VALUE (in milliseconds)	
	Windows	Linux
TCP	3000	3000
SCTP	3000	3000

value is of the order of seconds as opposed to milliseconds. According to [1], the optimal time to be spent in the normal state is of the order of the minimum retransmission timeout value of the TCP protocol, and thus is to be measured in seconds, while the holding time of the abnormal state is to be of the order of the RTT value maintained by the protocol, which is usually in milliseconds. Since the minimum holding times of ë and ë' are 1000ms and 1ms respectively, the average holding times would have to be greater these values. This is in total agreement with our values. Thus
Since our conceptualisation requires the expected duration of

$$\lambda > 1000ms$$
$$\lambda' > 1ms$$

normal behaviour to exceed that of abnormal behaviour, we have ë > ë'.

Given Q, $e^{Qt}e^{-t}$ computes to

$$e^{Qt}e^{-t} = \begin{pmatrix} \frac{\lambda+\lambda' e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} & \frac{\lambda'-\lambda' e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} \\ \frac{\lambda-\lambda e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} & \frac{\lambda'+\lambda e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} \end{pmatrix} \qquad (17)$$

$$\pi(0) = \begin{pmatrix} 1 & 0 \end{pmatrix} \qquad (18)$$

We assume that a misbehaving router at epoch t = 0 is always in the normal state. Hence,

From (12), (17) and (18) we have

$$\pi(t) = \begin{array}{c} \begin{array}{cc} N & A \end{array} \\ \begin{pmatrix} \frac{\lambda+\lambda' e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} & \frac{\lambda'-\lambda' e^{-t\left(\frac{\lambda+\lambda'}{\lambda\lambda'}\right)}}{\lambda+\lambda'} \end{pmatrix} \end{array} \qquad (19)$$

We have thus computed the probabilities of the system being in each and every state in its statespace. To verify these probabilities, we use the Weak Law of Large Numbers [6], [7]. From (19), we have that

$$\lim_{t\to\infty} P(X_t = N) = \left(\frac{\lambda}{\lambda+\lambda'}\right) \qquad (20)$$

hat,

$$\lim_{t\to\infty} P(X_t = A) = \left(\frac{\lambda'}{\lambda+\lambda'}\right) \qquad (21)$$

$$P(X_t = A) = \frac{\qquad}{\lambda+\lambda'} \qquad \frac{\qquad}{+\lambda'}$$

Equations (20) and (21) tell us that, for very large t and for one average normal-abnormal-state cycle duration lasting for (ë + ë') milliseconds, the system tends to spend average times ë and ë' in the normal and the abnormal states respectively. Comparing this to the number of heads in a sequence of coin flips, we note that, for a very large number of coin flips, the probability of getting a head tends to 1/2, the average value. The same idea applies to our case, thereby verifying our probabilities.

IV. CONCLUSION AND FUTURE DIRECTIONS

In this paper we have determined the probabilities of a compromised system, mounting Low-Rate DoS attacks, behaving both normally and abnormally. So, this work, in a way, is an extension of the work in [1]. We intend to use these probabilities to primarily detect and forestall attacks of this kind either through Hidden Markov Models (HMMs) or Artificial Immune Systems (AIS) with the design of more robust

protocols exhibiting immunity to attacks of this nature being the secondary motive.

REFERENCES

[1] Kuzmanovic, A., Knightly, E.: Low Rate TCP-Targeted Denial of Service Attacks (the Shrew vs. the Mice and the Elephants).In: Proceedings of ACM SIGCOMM, pp. 75-86, Karlsruhe, Germany(2003)

[2] Thatte, G., Mitra, U., Heidermann, J.: Detection of Low-Rate Attacks in Computer Networks. In: Proc. 11th IEEE Global Internet Symp., pp. 1-6, IEEE, Phoenix(2008).

[3] Luo, X., Chan, E., Chang, R.K.: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals. EURASIP J. Adv. Signal Process. 2009, 1-13 (2009)

[4] Maci´a-Fern´andez, G., D´yaz-Verdejo, J.E., Garc´ya-Teodoro, P.: Mathematical Model for Low-Rate DoS Attacks against Application Servers. Trans. Info. For. Sec.,4,3,519-529(2009)

[5] Maci´a-Fern´andez, G., D´yaz-Verdejo, J.E., Garc´ya-Teodoro, P.: LoRDAS: A Low-Rate DoS Attack against Application Servers. In: Proc. Of CRITIS'07, 5141, pp. 197-209, LNCS, Spain(2008)

[6] Feller, W., An Introduction to Probability Theory and Its Applications Vol. 1, 3rd ed. New York: Wiley, 1968.

[7] Feller, W., An Introduction to Probability Theory and Its Applications Vol. 1, 3rd ed. New York: Wiley, 1968.