International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 39404-39407
© Research India Publications. http://www.ripublication.com

The Quantitative Risk Assessment for Distributed Denial of Service Attacks

Tae Kyung Kim

Dept. of Tourism Management, Seoul Theological University,
101 Sosabon3-dong, Sosa-gu, Bucheon-City, Kyonggi-do, South Korea

Copyright © 2015 Tae Kyung Kim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
Many organizations establish and operate their own security plan to provide an appropriate information protection to keep their information assets safely. The risk management is important procedure to select a cost-effective information protection plan. We should perform a risk assessment procedure to manage the potential risk efficiently. These risk analysis and assessment method are effort to measure and find out the degree of risk within scientific and formal process. There are many studies associated with these effort based on the qualitative method. Although studies have been made on the degree of risk, there is little agreement on how the degree is divided and defined without the subjective opinions of estimators. Therefore we propose an enhanced method based on the quantitative measurement to provide an objective and common criteria. In this paper, we focus on the risk of distributed denial of service attacks. As an initial effort to address this problem, we suggest a loss scale and probability of occurrence for risk using some mathematics methods. Through the performance evaluation, the proposed method is shown that it is useful to estimate the degree of risk correctly.

Keywords: Distributed Denial of Service Attacks, Information Security Management System, Risk Assessment

1. Introduction

Many organizations establish their own information security management system to protect their information assets against numerous external security threats. This system is conFig.d five processes and it includes a policy establishment, range establishment, risk management, implementation, and post management. In these components, risk management processes makes that an administrator can select a cost-effective plan of information security and protect information assets by more efficient manner [1].

In this paper, we analyze the elements which are affected to the risk and propose an appropriate risk assessment method. In particular, we focus on the distributed denial of service attacks. We theoretically analyze the loss scale and use the probability distribution function of distributed denial of service attacks. Also, we propose a quantitative risk assessment method using statistical risk analysis. Distributed denial of service attacks are malicious attempts to make a network resource unavailable and it is caused critical damage to provide stable services [2, 3]. The cause of these attacks is the difference of physical resources such as a buffer and bandwidth between upper layer and lower layer in the system. This distinction causes a buffer overflow and traffic loss. The distributed denial of service attacks are occurred at an input point of a queue in a traffic processing node [4, 5, 6]. Since most of the risk analysis methods are depends on the qualitative evaluation and this evaluation is based on the subjective decision, this is not the proper way to estimate the risk degree exactly. In next chapter, we suggest the efficient risk assessment method with a quantitative way.

The remainder of this paper is divided into four sections. In section 2, we discuss several Eq.s related to a single source and multi-source distributed denial of service attacks. Also, we propose a suitable risk assessment method to provide objective criteria. In section 3, we evaluate the risk of DDoS attack under the various environments. Finally, section 4 concludes this paper.

2. Proposed Method for Risk Assessment

In this study, it is assumed that the distributed denials of service attacks are occurred in a single source. Generally, effective bandwidth means that it can accommodate the traffic of abnormal attack sessions or overload attack sessions to maintain the stable services of a system. When we know the maximum bandwidth of a system considering service requests and an inner buffer capacity of target node, we should make the model by supposing the worst case to calculate the effective bandwidth. Also, this bandwidth should ensure the availability of service without consideration of delay and traffic loss.

In this paper, on-off model is used to the proposed method. This model is used to allocate resources and control call admissions. It can be generalized as a set of on-state and off-state. On-state means the situation that traffic is entered as maximum input rate, and off-state indicates the case that traffic does not occur [7, 8]. As shown in Fig. 1, an occupancy time of each state can be expressed as follows in on-off model.

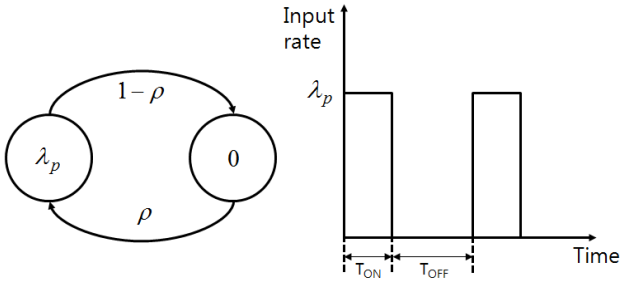

Fig. 1. ON-OFF model

In this Fig., λ_p is a maximum input traffic and ρ is the maximum input traffic rate. Also, T_{on} is the time when there is a maximum input traffic of inflow and T_{off} is the time when there is no input traffic in the system. T_{on} and T_{off} are shown Eq. (1) and Eq. (2) respectively.

$$T_{on} = \frac{B_s}{\lambda_p} \quad (1),$$

$$T_{off} = B_s\left(\frac{1}{\lambda_s} - \frac{1}{\lambda_p}\right) \quad (2),$$

$$b = \frac{B_s}{\lambda_p}\left(\lambda_p - \lambda_e\right), \quad \lambda_s \le \lambda_e \le \lambda_p \quad (3),$$

$$\lambda_e = \lambda_p\left(1 - \frac{b}{B_s}\right) \quad (4)$$

In Eq. (1), λ_p is the rate of maximum input traffic and B_s indicates a maximum burst size. Also, in Eq. (2), λ_s represents an average input traffic. The Eq. between effective bandwidth and buffer capacity can be expressed as follows. In Eq. (3), let b denote an effective buffer capacity and λ_e is an effective bandwidth. This Eq. can be represented differently as Eq. (4). Note that a given buffer capacity divided by effective bandwidth equals a maximum delay time.

$$D_{\max} = \frac{b}{\lambda_e} \quad (5),$$

$$b_{total} = \sum_{i=1}^{N} b_i = N \times b \quad (6),$$

$$\lambda_{total} = \sum_{i=1}^{N} \lambda_{e_i} = N \times \lambda_e \quad (7)$$

As another case, we discuss distributed denial of service attacks by distributed sources. In this environment, the traffic of distributed denial of service attacks has the same characteristic. Thus, when N independent and abnormal attack traffics occur in the system, we should find out a required buffer capacity and proper service bandwidth to provide stable services. These elements are represented Eq. (6) and (7), respectively. We use the fluid flow approximation to induce these Eq.s [9, 10]. On the contrary, if buffer capacity and service bandwidth is fixed, then acceptable number of attack sources is defined as follows.

$$C_{noloss} = \left\lfloor \frac{\lambda_{lower}}{\lambda_{e(attack)}} \right\rfloor \quad (8),$$

$$C_{loss} = \left\lceil \frac{\lambda_{lower} - \lambda_{usage}}{\lambda_{e(attack)}} \right\rceil = \left\lceil \frac{\lambda_{surplus}}{\lambda_{e(attack)}} \right\rceil \quad (9)$$

The denial of service by traffic loss occurs at the end position of an input buffer. If the normal average traffic usage of sublevel bandwidth is λ_{usage}, then point at which the loss occurs due to attack session traffic is case that the traffic exceeds the permitted capacity at average surplus bandwidth without average traffic usage. Let C_{loss} denote the minimum number of potential attack sources.

Finally, because abnormal attack session of distributed denial of service attacks occur traffic with same features, traffic loss scale for surplus bandwidth is represented as follows. Let P_{loss} denote the traffic loss scale.

$$P_{loss} = \sum_{C_{loss}}^{N}\left[\binom{N}{C_{loss}}\rho^{C_{loss}}(1-\rho)^{N-C_{loss}}\right] \quad (10),$$

$$p(X \le x; m) = \frac{e^{-m} \cdot m^x}{X!} = P_{occur} \quad (11)$$

This Eq. indicates sum of probability that causes the traffic loss when there are some attack attempts (N) occur more than the minimum number of potential attack sources(C_{loss}). The load monitoring is essential element to respond quickly when distributed denial of service attacks occur. The load monitoring can identify appropriate time which expected overload. It runs periodically and maintains statistics associated to traffic load and the number of attack sessions. Also, it controls the existing connection by using stateful session inspection based on session. Traffic overload should be defined as input traffic load to the network. Thus, the Poisson distribution can be used to this method.

In this Eq., x is traffic load and X is random variable of traffic load. p is probability that traffic load is less than x. Let P denote cumulative probability of the Poisson distribution that can be recognized as normal traffic. m is average of traffic load. Administrator decides that the value of normal state is P and it is overload state when traffic load(x) occurs in excess of the P. This value uses as threshold to cognize an abnormal state like an Eq. (12).

$$x' = \log_m \frac{X! \cdot P}{e^{-m}} \quad (12)$$

4. Performance Evaluation

We simulate each case that the number of attack attempts (N) is from 1 to 50. We assume that the maximum traffic rate (ρ) is 0.3. Also, we assume that the number of minimum attack sources which cause traffic loss (C_{loss}) is from 2, 5, and 10 in each case. Table 1 shows simulation environment of the proposed method.

Table 1. Simulation Environment

Type	Parameter	Value
Traffic loss scale (P_{loss})	ρ	0.3
	N	1 ~ 50
	C_{loss}	2, 5, 10
Possibility of risk occurrence (P_{occur})	m	5, 10, 15
	x	1~50

Fig. 2 shows the traffic loss scale. In this Fig., the solid line, dot-dashed line and dotted line indicate the change of the number of minimum attack sources is 2, 5, and 10 respectively. We can recognize that the minimum number of potential attack sources increases as the number of attack attempts increases.

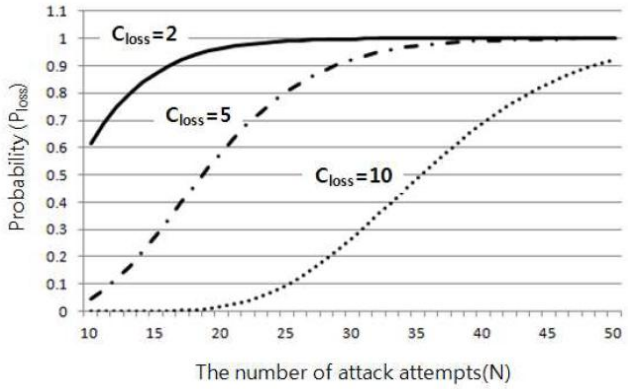

Fig. 2. Traffic loss scale

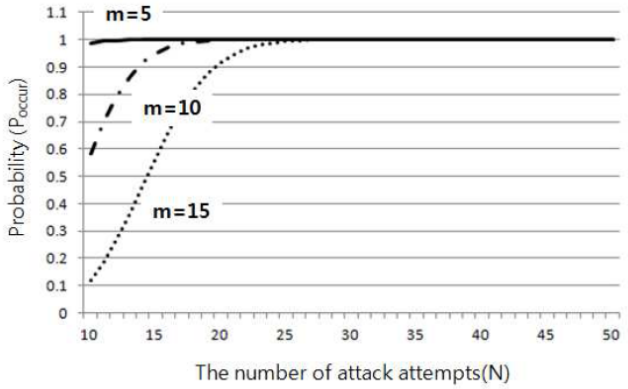

Fig. 3. Possibility of risk occurrence

Fig. 3 shows the possibility of risk occurrence. In this Fig., the solid line, dot-dashed line and dotted line indicate the change of the average number of sources is 5, 10 and 15, respectively. It is likely that the average number of sources increases as the number of attack attempts increases.

Let P_{risk} denote risk degree and it is represented the product of traffic loss scale and possibility of risk occurrence. It is defined as shown in Eq. (13).

$$P_{risk} = P_{loss} \times P_{occur} \quad (13)$$

Based on the Eq. (13), we evaluate the risk degree in three cases that the average number of sources is 5, 10 and 15, respectively. Fig. 4 shows the risk degree when the average number of sources is 5. In this Fig., the solid line and dot-dashed line indicate change of the minimum number of potential attack sources is 2 and 5 respectively. The Fig. shows that the risk degree increases as the number of attack attempts increases in general. If the number of attack attempts is 13, then risk degree is 0.2 and 0.8 when the minimum number of potential attack sources is 2 and 5 respectively. Thus, the risk degree is greatly influenced the minimum number of potential attack sources.

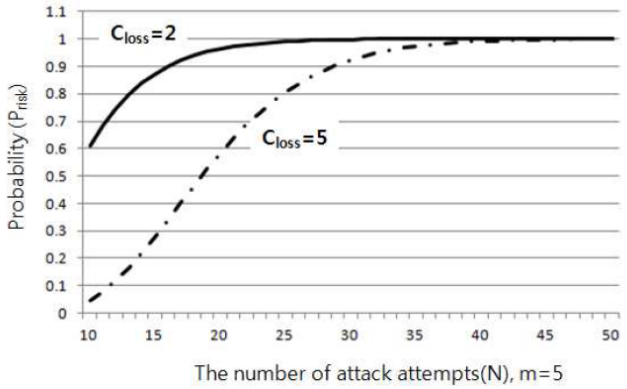

Fig. 4. The risk degree (m=5)

Fig. 5 and Fig. 6 shows the risk degree when the average number of sources is 10, and 15 respectively.

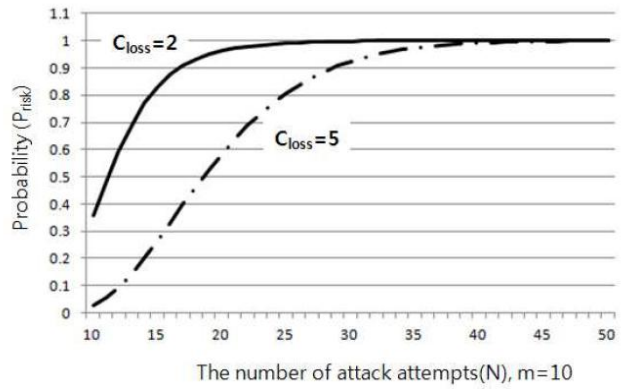

Fig. 5. Risk degree (m=10)

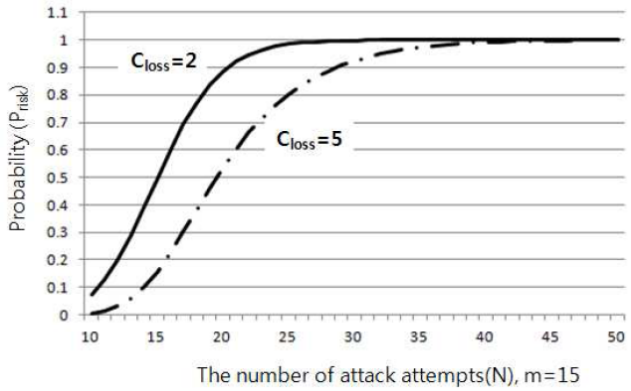

Fig. 6. Risk degree (m=15)

As shown these Figs, the risk degree is influenced the average number of sources. In particular, if the minimum number of potential attack source is low, then the risk degree is more affected the average number of sources.

5. Conclusions

Many organizations define the information security management system to protect their assets safely. In general, the system has five procedures such as policy establishment, range establishment, risk management, implementation, and post management. In these components, a risk analysis is important procedure to support security against threat by unauthorized attacker and vulnerability of systems in the organization. There are many methodologies associated with a risk assessment. However, most of them depend on a qualitative assessment based on the grade which estimated by experts.

In this paper, we assume that the risk is the product of traffic loss scale and the possibility of occurrence to provide a quantitative evaluation. In the many attacks, we focus on the distributed denial of service attacks and propose the efficient risk assessment method by quantitative way. As shown in the simulation results, the risk degree is affected by an average number of attack sources and the minimum number of potential attack sources. Also, we can estimate the risk degree to the values exactly.

Acknowledgements.

The author wishes to thank the editor and anonymous referees for their helpful comments for improving this paper. This research was supported by 2015 Seoul theological university research grant.

References

[1] A. Elwalid, D. Mitra, Effective bandwidth of general markovian traffic sources and admission control of high speed network, *IEEE TRANS on Networking*, Vol.1, No.3, pp. 329-341, 1993.

[2] A. Aikebaier, T. Enokido, M. Takizawa, Trustworthy Group Making Algorithm in Distributed Systems, *Human-centric Computing and Information Sciences* (*HCIS*), 2011.

[3] Aly M. El-Semary, M. Gadal-Haqq M. Mostafa, Distributed and Scalable Intrusion Detection System Based on Agents and Intelligent Techniques, *Journal of Information Processing System* (*JIPS*), Vol. 4, No. 4, pp. 481-500, 2010.

[4] R. Guerin, L. Gun, "A unified approach to bandwidth allocation and access control in fast packet-switched networks, *Proc. IEEE INFOCOM*, 1992.

[5] B.-J. Kim, I.-K. Kim, Robust Real-time Intrusion Detection System, *Journal of Information Processing System* (*JIPS*), Vol. 1, No.1, pp. 9-13, 2005.

[6] E. Andreeva, B. Mennink, B. Preneel, Security Properties of Domain Extenders for Cryptographic Hash Functions, *Journal of Information Processing System* (*JIPS*), Vol. 6, No. 4, pp. 453-480, 2010.

[7] A. Elwalid, D. Mitra, R. Wentworth, A new approach for allocating buffers and bandwidth to heterogeneous, regulated traffic in an ATM node, *IEEE J. on Select Area in Communication*, Vol. 13, No. 6, pp. 1115-1127, 1995.

[8] G. Ramamurthy, Q. Ren, Multi-class connection admission control policy for high speed ATM switches, *Proc. IEEE INFOCOM '97*, pp. 965-974, 1997.

[9] L. Kosten, Liquid models for a type of information storage problems, *Delft Prog. Rep.: Math. And Inform. Eng.*, Vol. 11, pp.71-86, 1986.

[10] R. Guerin, H. Ahmadi, M. Nagshineh, Equivalent capacity and its application to bandwidth allocation in high-speed networks, *IEEE J. on Select Area in Communication*, Vol. 9, No. 7, pp. 968-981, 1991.

Received: Month xx, 20xx