A MECHANISM FOR EARLY DETECTING DDOS ATTACKS BASED ON M/G/R PS QUEUE

Nguyen Hong Son

Department of Information and Communication Technology, Post and Telecommunication Institute of Technology, Ho Chi Minh City, Viet Nam

ABSTRACT

When service system is under DDoS attacks, it is important to detect anomaly signature at starting time of attack for timely applying prevention solutions. However, early DDoS detection is difficult task because the velocity of DDoS attacks is very high. This paper proposes a DDoS attack detection method by modeling service system as M/G/R PS queue and calculating monitoring parameters based on the model in odder to early detect symptom of DDoS attacks. The proposed method is validated by experimental system and it gives good results.

KEYWORDS

DDoS, Detection, M/G/R Processor Sharing queue

1. INTRODUCTION

The goal of any DoS attacks is to stop services in servers or to isolate servers from users. There are many ways for hackers to reach the goal. We can classify two main kinds of DoS ways which have ever been exploited by hackers in reality. In the first one, hackers manage to stop service from users by exploiting vulnerabilities in network services or system software in servers [31]. For example, hackers have exploited vulnerabilities of DNS system to poison DNS servers andweb sites were isolated from its clients bypoisoned DNS servers responding to queries of clients with wrong IP addresses. In the second, hackers make to exhaust resources of networks or resources of hosts. The common way is to send to target systems with a lot of requests, SYN flood attack, for instance. The bandwidth of link will be degraded by a lot of connections going through. The CPU power and memory capacity will quickly be emptied by having to handle enormous amount of requests and processing for responses [32]. The target servers cannot run for services in exhausted status. This is a key of the kind of DoS ways. The main challenge facing hackers in the second way is how to make number of requests enough to destroy target hosts. It is difficult for hackers to overload a target host with an attack computer having power smaller than the target host. However, hackers have overcome the challenge by using a great number of attack computers simultaneously. A lot of compromised computers on Internet were mobilized by hackers to join in their DoS attacks. The case of DoS attack is called distributed denial of service (DDoS). Nowadays, DDoS attack is still serious type of attacks and hardly to prevent. DDoS attack detection is an important task in DDoS attack mitigation; however, it is a difficult task.

DDoS attack detection is not significant if it was too late. In any case, DDoS defense mechanism must detect the attack as soon as possible and look for the source to prevent it.DDoS defense mechanism is a topic paid attention by many researchers. So far, variety of DDoS defense

DOI: 10.5121/ijnsa.2016.8502

mechanisms have been proposed, such as in [1], [2], [3], and [17]. All DDoS defense mechanisms belong to kind of network-based mechanism or kind of destination-based mechanism [4]. The defense mechanisms is proposed by authors in [5], [6], [7], [8] are network-based mechanisms which based on identifying and filtering IP traffic for detecting DDoS attacks. If DDoS attacks take place in application layer, network-based mechanisms is not useful solutions because they have no means for sensing any things in application layer. Application-level DDoS attacks have just been detected by destination-based defense mechanisms. The common principle of destination-based defense mechanisms is to look for a special signature which reflects actual DDoS attacks at early stage. Variety of theories have been applied to build destination-based defense mechanisms, such as using entropy in information theory [9], [10], [11], [12], game theory model in [17],artificial intelligent, learning machine, data mining [13], [14], [15], [16].

In this paper we propose a DDoS attack detection mechanism which can early detect DDoS attacks based on M/G/R Processor Sharing (PS) queue. It belongs to type of destination-based defense mechanism. The proposed mechanism is also aimed at application-level DDoS attacks. The idea behind of the proposed mechanism is to model service system (victim system of DDoS attacks) as a M/G/R PS queue and to apply theory results in [28] to identify signature of DDoS attacks early. The rest of paper is organized as following: Section 2 overviews related works from other authors. The M/G/R PS queue is introduced in section 3. Section 4 presents about modeling service computer as M/G/R PS queue. The proposed DDoS detection mechanism is described in section 5. Section 6 presents experimental results for validating the proposed method. The session 7 will close the paper by several conclusions.

2. RELATED WORKS

Up to now, DDoS attack is the most common attack that hackers use to shut down service from user in networks. Researchers have attempted to develop effective ways for preventing the attacks. In general, almost methods use such sequence as: data collecting, preprocessing or filter, and processing for detecting anomaly signature from DDoS attacks. Thus, all DDoS defense methods belong to kind of reactive mechanism; it means that waiting for attacks in place, detecting them, and appling prevention ways latter. We have still no effective proactive mechanism for preventing DDoS attacks. There are two common methods of anomaly detection used in reactive mechanisms: statistical analyze and appling technology of learning machine or artificial intelligent. Authors in [18] based on calculating entropy and statistic of packet attributes to detect DDoS attacks. They also proposed a prototype for responding DDoS attacks recently detected.

Other entropy-based mechanisms, such as [19],[20],[21], packet headers are represented as independent information symbols with unique probability of occurrence. It based on calculating entropy of stochastic request packets in a period of time. According to the algorithms, deviations of two values of entropy from two consecutive calculations are compared with a preset threshold. Whenever the threshold is exceeded, the system was under a DDoS attack.

In other methods, detection algorithms are continuously trained based on network events in order to update filter criteria by using learning machine or artificial intelligent technology. It is a common method for DDoS detection in [22],[23],[24].Some common algorithms in network intrusion and anomaly detection are Multilayer Perceptron, Gaussian Classifier, K-means Clustering and Markov model [25].

M/G/R Processor Sharing queue was used by authors in [26], [27], [28] to discover relationship between the degradation of the TCP flows and utilization of link that transports the TCP flows.

Based on the relationship, we can know whether TCP flows are in degradation by observing their throughput. Especially, in [28] provided a new view of the relationship which expresses relationship between degradation of TCP flows and utilization of link by using link utilization variance. An important feature of the variance is to increase with link utilization mean; however, it will be decrease when certain saturation threshold is exceeded.The feature can be exploited to build a way that allows to early detecting degradation of TCP flows from their throughput. We recognize that degradation of TCP flows is the same as degradation of service in computer under DDoS attacks. Thus, the feature is applied to build a destination-based DDoS detection mechanism in this paper. The service computer will be modeled as a M/G/R PS queue and its parameters will be replaced by suitable parameters in expressions in [28].

3. M/G/R PROCESSOR SHARING QUEUE

M/G/1 Processor Sharing queue differs from M/G/1 queue in manner of customer service. Both queues have only one server and the server of M/G/1 queue just serves one customer at a time until finish. So, if more customers arrive at busy M/G/1 queue, they must wait for server available. Unlike the server of M/G/1 queue, the server of M/G/1 PS queue serves customers simultaneously and there is no queue in the M/G/1 PS queue ! Customers always reach service upon arrival and capacity of the server is fairly shared between them. Because of the behavior, M/G/1 PS becomes an important modeling tool, such as modeling TCP flows in Internet. Naturally, TCP connections are fairly shared bandwidth of network link [29].

M/G/R PS queue is the same as M/G/1 PS queue but which have *R* servers. The arrivals follow a Poisson process and the service times distribution is general. Customers entering the system are served immediately by *R* servers. When the system has*N* customers, all of them are in service. In case of R greater than N, each customer is simultaneously served by just one server. Thus, service rate for each customer is equal the service rate of server. However, each customer will receive service rate less than service rate of server in case of N greater than R. In the case, total capacity of R servers are equally shared by N customers and the system is the same as M/G/1 PS queue [30].

4. M/G/R PS MODEL

The idea behind the M/G/R Processor Sharing model in our context is to look at processing service requests at service computer, such web site. A service computer is referred to as processor sharing system;it servesmany clients simultaneously by sharing system performance. The computer responds to all service requests fairly. If we consider each service request as a customer and they share executive capacity of computer, we can apply M/G/R PS to model behavior of respond processing in the system. According to the model, when number of customers is greater than R, the executive capacity will be fairly share for all current customers. In this paper, we use theory results from [28] with R replaced by number of client; degradation of service computer performance is expressed by expression (1)

$$D(R,\rho) = 1 + \frac{C(\lfloor R \rfloor,\rho)}{(1-\rho)R}\left(1 - (1-\rho)(R - \lfloor R \rfloor)\right) \qquad (1)$$

with C is maximum executive capacity of service computer, ρ is resource utilization, and C(R, ρ) is Erlang's C equation. The parameter ρ in our model is formulated by expression (2)

$$\rho = \frac{1}{2}\left(\frac{1}{PT}\int_0^T P_t(t)dt + \frac{1}{MT}\int_0^T M_t(t)dt\right) \qquad (2)$$

Where

- P: total of CPU capacity
- $P_t(t)$: consume of CPU capacity at time of t
- T: period of calculate time
- M: total of main memory capacity
- $M_t(t)$: occupied capacity of main memory at time of t

5. THE MECHANISM FOR EARLY DETECTING DDOS ATTACKS BASED ON M/G/R/PS MODEL

As presented in [28], the M/G/R PS model does not allow to direct calculating degradation D(R, ρ). Thus, relationship between utilization variance and degradation of performance was formulated for detecting symptom of degradation in performance easily. It switches to calculate index of degradation I(ρ) by expression(3)

$$I(\rho) := \frac{1-\frac{V_U(\tau)/\rho}{V_0}}{1-\rho} \qquad (3)$$

Where $V_U(\tau)$ is the variance of τ samples, ρ is the resource utilization, and $V_0$is the variance of request when resource of computer is not saturated, it is calculated by (4)

$$V_0 := \lim_{\rho \to 0} \frac{V_u(\tau)}{\rho} \qquad (4)$$

so variations in resource degradation can be detected by I(ρ). However, I(ρ) can not help to specify degradation in a certain time frame. Indeed, we just get whether degree of degradation exceeds a reference value. By setting up a controlled environment or actual system, we can determine the V_0 and calculate a threshold. The threshold is set to corresponding with resource saturation. As recommended in [28], the threshold should be three times deviation of I(ρ) plus its mean in case of low utilization ρ<0.5. Expression (3) uses a parameter (τ) to indicate the number of previous samples to calculate the variance.

The method of early DDoS attack detection in this paper is constructed by determining degradation in available resource of service computer via the above M/G/R PS model. Under DDoS attack during, available resources become to smaller and indicated by the index I(ρ). For getting I(ρ), we first calculate the parameters $V_U(\tau)$, V_0, and ρ. The variance $V_U(\tau)$ is derived from sampling *k* samples of service computer resources in period Δt with during of sample τ, and $V_U(\tau)$ is formulated as (5).

$$V_U(\tau) = \delta^2[\rho] = \frac{\Delta t}{\tau} \sum_{i=1}^{k} (\rho_i - E[\rho])^2 \qquad (5)$$

We get V_0 from actual system, by setting up the mechanism in actual system an run it in normal condition (no DDoS attack), select during τ seconds and k samples, calculate Vu(τ)/ρ, repeat several times, get value of mean, and the value is V_0.

The detection algorithm is implemented as a program which runs on protected systems. The program continuously samples system resources and calculates necessary parameters for calculating degradation index I(ρ). Whenever the value of index exceeds a preset threshold, signature of DDoS attack is detected and the program signals an alarm to detectors. The threshold

is selected how to detect DDoS attacks as soon as possible by monitoring an actual system under DDoS attack in controlled environments.

6. VALIDATING THE PROPOSED MECHANISM

In order to validating the proposed mechanism, we apply the system introduced in[31]. The system is illustrated in figure 1. The M/G/R PS-based DDoS detection method is validated by comparing with entropy-based DDoS detection method. The entropy-based DDoSdetection mechanism bases on calculating entropy of stochastic requests in a period of time, proposed in [21]. According to the algorithm, if deviation of two values of entropy from two consecutive calculations exceeds a preset threshold, the system was under a DDoS attack. Two DDoS detection methods are implemented in the experimental system by two plugins: plugin 1 and plugin 2 which run simultaneously on the same protected system (web server).

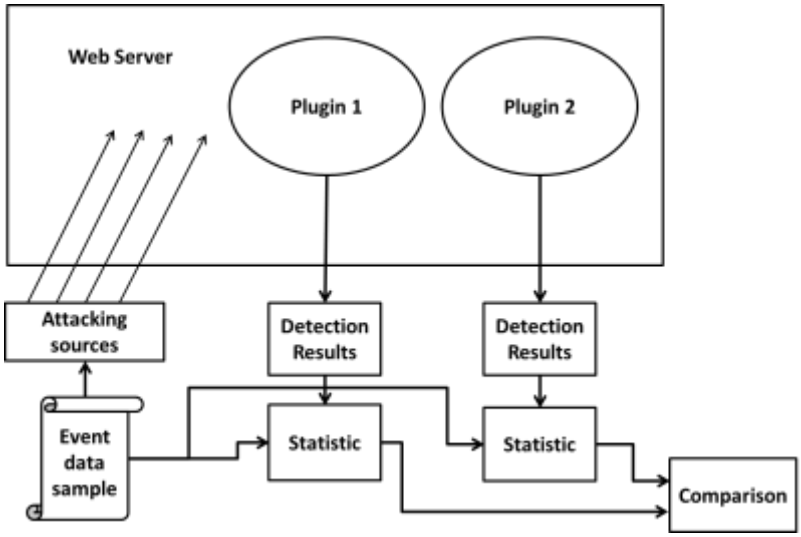

Figure 1. The experimental system in [31]

Several EDSs (Event Data Samples) were specified for testing. The first EDS, called EDS 1, includes chains of 5 seconds of attack interleaved by 10 seconds of non attack. By collecting detection results from the testing system, statistics of four quantities TP (true positive), FP (false positive), TN (true negative) and FN (false negative) are illustrated in figure 2.

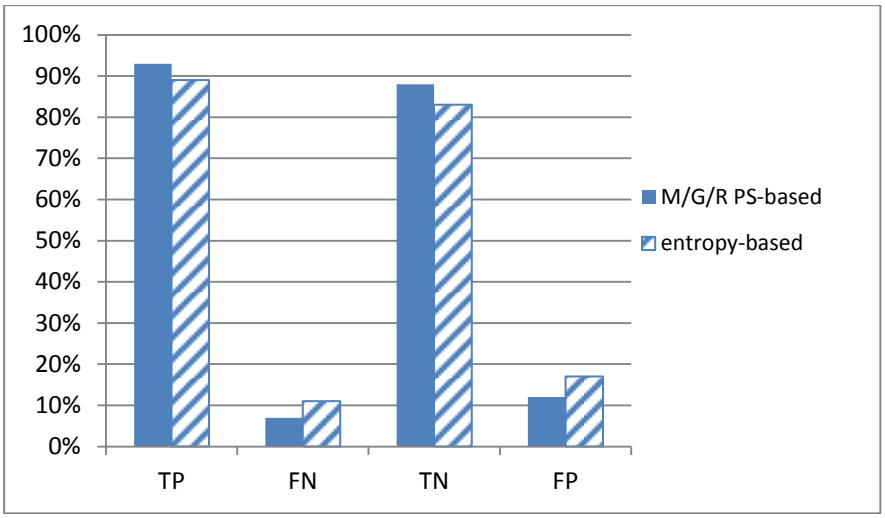

Figure 2. Results of testing for the case of using EDS1

Figure 2 shows that TP and TN rate of M/G/R PS-based detection mechanism are higher than in entropy-based detection mechanism, TP rate of 92% and TN rate of 88%. The rates of entropy-based detection mechanism are just at 89% and 83%, respectively. In terms of error indication, both rates of FP and FN from the proposed mechanism are smaller than the rates of entropy-based detection mechanism.

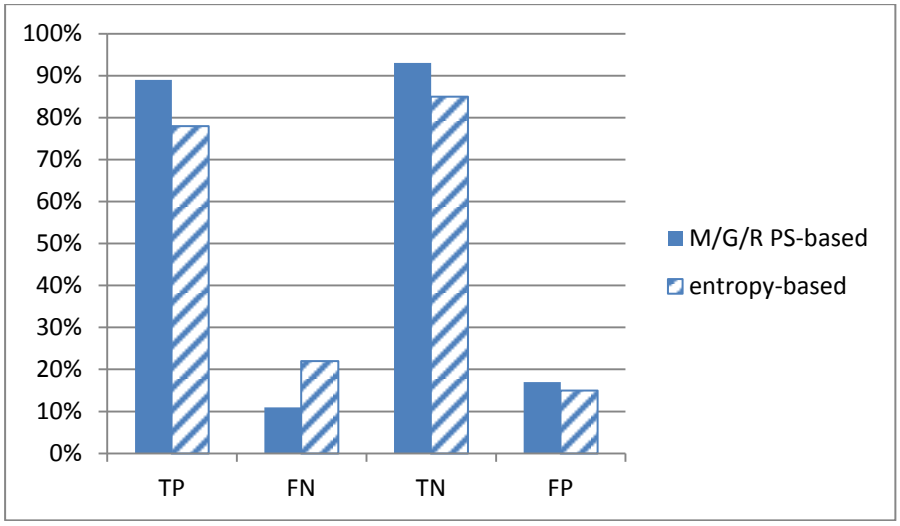

Figure 3. Results of testing for the case of using EDS2.

In the second testing case, EDS2 includes chains of 10 seconds of attack interleaved by 10 seconds of non attack. It extends periods of attack longer than in case of EDS1. Results of the testing case are described in figure 3. Figure 3 shows that the rates of correct indication from the proposed mechanism are still higher than the rates from entropy-based detection mechanism, TP rate of 89% and TN rate of 93% comparing with 78% and 85%, respectively. In terms of error indication, FN rate of the proposed mechanism is still smaller than the FN rate of entropy-based detection mechanism, 11% comparing with 22%. However, value of FP rate from the proposed mechanism is greater than the rate from entropy-based detection mechanism, value of 17% comparing with 15%, but two values are not much different.

7. CONCLUSIONS

Service systems were modeled as a M/G/R PS and the new method for early detecting DDoS attacks was presented in this paper. The method is one of host-based DDoS detection methods that detects signature of attack early by sampling system resources and fast calculating parameter of resource degradation. Experimental results show that the method has good sensitivity to detection, the rates of correct indication are very high, and the rates of error indication are low. Moreover, implementation of the method is easily and it is rather suitable for detecting application-level DDoS attacks.

REFERENCES

[1] J.Mirkovic, P. Reiher; "A taxonomy of DDoS attack and DDoS defense mechanisms"; ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[2] T. Peng, C. Leckie, K. Ramamohanarao; "Survey of network-based defense mechanisms countering the DoS and DDoS problems"; ACM Comput. Surv. 39, 1, Article 3, April 2007.

[3] RioRey; "Taxonomy of DDoS Attacks"; RioRey Taxonomy Rev 2.3 2012, 2012. [online] http://www.riorey.com/x-resources/2012/RioRey Taxonomy DDoS Attacks 2012.pdf.

[4] Saman Taghavi Zargar, James Joshi,David Tipper; "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks"; Communications Surveys & Tutorials, IEEE ,Volume 15, Issue 4, 2013.

[5] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao; "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks"; IEEE Trans. On Dependable and Secure Computing, vol. 3, no. 2, pp. 141-155, 2006.

[6] S. Changhua, Jindou, F., Lei, S., & Bin, L.; "A Novel Router-based Scheme to Mitigate SYN Flooding DDoS Attacks"; in IEEE INFOCOM (Poster), Anchorage, Alaska, USA, 2007.

[7] M. Abliz; "Internet Denial of Service Attacks and Defense Mechanisms"; University of Pittsburgh, Department of Computer Science, Technical Report. TR-11-178, March 2011.

[8] Cheng, J., Yin, J., Liu, Y., Cai, Z., Wu, C.; "DDoS attack detection using IP address feature interaction"; Proceedings of the 1st International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, pp. 113–118. IEEE CS, 4-6 November 2009.

[9] Krishan Kumar, Joshil, Kuldip Singh; "A Distributed Approach using Entropy to Detect DDOS Attacks in ISP Domain"; International conference on signal processing, communications and networking 2007, Chennai: IEEExplore Digital Library Press , pp. 331 – 337, 22-24 Feb. 2007.

[10] Shui Yu, Wanlei Zhou, Robin DOSs; "Information Theory Based Detection Against Network Behavior Mimicking DDOS Attacks"; Communications Letters, IEEE Vol. 12(4), pp. 318 -321, April 2008.

[11] Shui Yu, Wanlei Zhou; "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks"; Sixth Annual IEEE International Conference on Pervasive Computing and Communications, Hong Kong IEEE CS Press, pp.566 – 571, 17-21 March 2008.

[12] Giseop No, Ilkyeun Ra; "Adaptive DDoS Detector Design Using Fast Entropy Computation Method"; The Fifth IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011.

[13] Hwang, K., Dave, P., Tanachaiwiwat, S. NetShield; "Protocol anomaly detection with datamining against DDoS attacks"; Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, pp. 8–10. Springerverlag. , 8-10 September, 2003.

[14] R. Jalili, F. ImaniMehr; "Detection of Distributed Denial of Service Attacks Using Statistical Pre-Prossesor and Unsupervised Neural Network"; ISPEC, Springer-Verlag Berlin Heidelberg, pp.192-203, 2005.

[15] Y. C. Wu, H. R. Tseng, W. Yang, R. H. Jan; "DDoS detection and traceback with decision tree and grey relational analysis"; International Journal of Ad Hoc Ubiquitous Computing., vol. 7, no. 2, pp. 121-136, 2011.

[16] Wang, J., Phan, R. C. W., Whitley, J. N., Parish, D. J.; "Augmented attack tree modeling of distributed denial of services and tree based attack detection method"; Proceedings of the 10th IEEE

International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS, 2010.
[17] G Dayanandam, T V Rao, S Pavan Kumar Reddy, Ravinuthala Sruthi; “Password Based Scheme and Group Testing for Defending DDOS Attacks”; International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013.
[18] D. Schnackenberg, R. Balupari, D, Kindred L. Feinstein, "Statistical Approaches to DDoS Attack Detection and Response," in DARPA Information Survivability Conference and Expedition, vol. 2003, Apr.
[19] Z. Qin, L. Ou, J. Liu, A. X. Liu J. Zhang, "An Advanced Entropy-Based DDoS Detection Scheme," in International Conference on Information, Networking and Automation, pp. 67-71, 2010
[20]I. Ra G. No, "An efficient and reliable DDoS attack detection using fast entropy computation method," in International Symposium on Communication and Information technology, pp. 1223-1228, 2009
[21] S. Renuka Devi, P. Yogesh; “Detection Of Application Layer DDoS Attacks Using Information Theory Based Metrics”; CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 217–223, DOI : 10.5121/csit.2012.2223, 2012
[22] Hwang, K., Dave, P., Tanachaiwiwat, S. NetShield; “Protocol anomaly detection with datamining against DDoS attacks”; Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, pp. 8–10. Springerverlag. , 8-10 September, 2003
[23] R. Jalili, F. ImaniMehr; “Detection of Distributed Denial of Service Attacks Using Statistical Pre-Prossesor and Unsupervised Neural Network”; ISPEC, Springer-Verlag Berlin Heidelberg, pp.192-203, 2005
[24] Y. C. Wu, H. R. Tseng, W. Yang, R. H. Jan; “DDoS detection and traceback with decision tree and grey relational analysis”; International Journal of Ad Hoc Ubiquitous Computing., vol. 7, no. 2, pp. 121-136, 2011
[25] D. O,Brien S. Seufert, "Machine Learning for Automatic Defence against Distributed Denial of Service Attack," in ICC, pp. 1217-1222, 2007
[26] Kawahara, R.; Ishibashi, K.; Asaka, T.; Ori, K., “A method of IP traffic management using TCP flow statistics,” IEEE Global Telecommunications Conference, GLOBECOM ’03, vol. 7, pp. 4059-4063, 2003
[27] Kawahara, R.; Ishibashi, K.; Asaka, T.; Sumita, S.; Abe, T., “A method of bandwidth dimensioning and management using flow statistics [IP networks],” IEEE Global Telecommunications Conference, GLOBECOM’04, vol. 2, pp. 670-674, 2004
[28] Ishibashi, K.; Kawahara, R.; Asaka, T.; Aida, M.; Ono, S.; Asano,S., “Detection of TCP performance degradation using link utilization statistics,” IEICE Transactions on Communications, pp. 47-56, 1989
[29] J. Roberts, U. Mocci, J. Virtamo (eds.): Broadband Network Teletraffic, Springer, 1996
[30] Dr. János Sztrik, Basic Queueing Theory, University of Debrecen, Faculty of Informatics.
[31] Nguyen Hong Son, A System For Validating And Comparing Host-Based Ddos Detection Mechanisms, International Journal of Network Security & Its Application (IJNSA) Vol.7, No.6, 2015.
[32] Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials, 2014.

AUTHOR

Son Nguyen Hong received his B.Sc. in Computer Engineering from Ho Chi Minh City University of Technology, his M.Sc. and PhD in Communication Engineering from the Post and Telecommunication Institute of Technology Hanoi. His current research interests include communication engineering, network security, computer engineering and cloud computing.