Journal of Engineering and Applied Sciences 9 (10-12): 368-371, 2014
ISSN: 1816-949X

Architecture and Program Realization of System of Detection of Network Attacks to Denial of Service

[1]Shangytbayeva Gulmira and [2]Karpinski Mikolaj
[1]Kazakh National Technical University Named after K.I. Satpayev, Almaty, Kazakhstan
[2]Academy of Technologies and the Humanities in Bielsko-Biala, Poland

Abstract: The study presents approach to detection of the distributed network attacks the "Denial of Service". In study, the technique is offered is developed architecture and is constructed realization of system of detection of network attacks like "Denial of Service". The technique is based on modeling of the studied network by networks of mass service with the subsequent assessment of probability of losses of demands in a network.

Key words: Network attacks, DoS-attack, DDoS-attack, "Denial of Service", detection of network attacks

INTRODUCTION

If you work in the field of computer technologies or in the field of network safety, I am sure that is familiar to you the term "denial of service" which in popular speech is called as "DoS attack". Currently, it is one of the most common types of network attacks carried out on the internet.

"Denial of Service" or "DoS attack" are one of types of network attacks are intended "to flood" target networks or cars with a large number of a useless traffic, so that overload the attacked machine (Bhatia *et al*., 2014).

The most common type of Denial of Service attack involves flooding the target resource with external communication requests. This overload prevents the resource from responding to legitimate traffic or slows its response so significantly that it is rendered effectively unavailable (Ioannidis and Bellovin, 2002).

Resources targeted in a DoS attack can be a specific computer, a port or service on the targeted system an entire network, a component of a given network any system component. DoS attacks may also target human-system communications (e.g., disabling an alarm or printer) or human-response systems (e.g., disabling an important technician's phone or laptop) (Dean *et al*., 2001; Bhuyan *et al*., 2015).

DDoS is the acronym for Distributed Denial of Service. DDoS is denial of service network resource resulting in multiple distributed (i.e., originating from different internet access points) requests.

DDoS attack the distributed attack like refusal in service which is one of the most widespread and dangerous network attacks. DDOS is a type of DOS attack where multiple compromised systems which are usually infected with a Trojan are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack (Elliott, 2000; Hussain *et al*., 2003).

DDoS attack, the incoming traffic flooding the victim originates from many different sources potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin (Ozcelik and Brooks, 2015).

The widespread DOS option of the attack known as DDoS (Distributed Denial of Service the distributed refusal in service) attack became very popular in recent years as it is very powerful and difficult to detected attacks.

DoS attack takes one place of an origin and attack of DDoS comes from several IP addresses distributed on several networks (Garber, 2000).

All the data from those servers adds up to significant bandwidth, enough to congest the target's internet connectivity. With bandwidth maxed out, "normal" traffic cannot be serviced and legitimate clients ca not connect. Any server open to the internet and running UDP-based services can potentially be used as a reflector (Li *et al*., 2008).

With the constant development of computer networks and the increasing number of users grows and the number of new types of attacks to denial of service.

Corresponding Author: Shangytbayeva Gulmira, Kazakh National Technical University Named after K.I. Satpayev, Almaty, Kazakhstan

DoS/DDoS/DRDoS attacks are characterized by a straightforward implementation complexity and resistance which poses new problems of researchers who are still not yet resolved. Analysis of recent publications shows that exercise is accompanied by attacks: interception of confidential information to unauthorized use of network bandwidth and computational resources, the spread of false information, violation of network administration (Hautio and Weckstrom, 1999; Wang and Chien, 2003).

Objective of the study: This research is directed on studying of the distributed network attacks like "Denial in Service" and methods, models and architecture of network attacks to refusal in service.

Literature review: Traditional mechanisms of security firewalls and signature-based intrusion detection systems are not effective means for detection of low-active network attacks like "Denial of Service" (DDoS-attacks) of applied level and protection against them.

The fundamental prerequisite for intrusion detection is to build the control characteristics of the network traffic when in standard conditions followed by a search of anomalies in traffic patterns (deviation from the control characteristics).

MATERIALS AND METHODS

To detect anomalies may apply statistical criteria (standard deviation, chi-square deviation from the standard normal distribution, a significant increase in entropy and so on) a clustering, a method of detection of a point of transition, spectral analysis and others (Apiecionek *et al*., 2015).

Each of the below specified methods and models have certain merits and demerits and is not universal for detection of all types of network attacks. Often enough to calculate the parameters of data streams in computer networks use mathematical models in the form of queuing networks (Bu *et al*., 2004).

In this study for the detection of DDoS-attacks provided a method for estimating the probability of loss of any requests during its passage through of networks (Szczerba and Szczerba, 2012; Szczerba and Volkov, 2013).

RESULTS

Because the application layer attacks on various network services occur independently within each service for modeling nodes can be used single-server queue length m.

Considering separate knot of networks of mass service, it is possible to assume that all network in general and the chosen knot in particular function in the stationary mode. Externally, supplied poisson flow applications with parameter 8. The knot contains one device of service of demands for which intensity μ their processing. After processing the application leaves from knot. If during receipt of the application the device is busy processing other requests, then the application becomes in line. If the demand arrives and the turn is completely filled, the demand is lost.

Let for knots of a network is set vector of intensities of the entering flows of application $\vec{\lambda}$ vector of intensities processing of applications $\vec{\mu}$ and substochastic matrix of probabilities of transitions of applications of p.

In research presents iterative procedure of calculation of a vector of intensities $\vec{\rho}$ of the streams for calculating the vector of intensities within the nodes of the original network flows (the total flux from the outside and from other nodes) and adjusted substochastic matrix of probabilities of transitions of applications $\tilde{p}$.

Proceeding from need of an assessment of probability of losses of demands for a network is offered the technique of creation of the chain of Markov with discrete time corresponding to a way of any application on knots. To do this, enter shaded state of this chain, i.e. is an ordered pair of numbers (i; d) where i corresponds to number of knot in which there is a demand (changes ranging from 1-J), d quantity of the taken places in turn of knot (changes ranging from i to m_i+1). Condition (i; m_i+1) corresponds to a crowded queue at node I. The initial distribution of the chain $\hat{p}$ can be calculated as (Eq. 1):

$$\hat{p}\{(i,d)\} = \frac{\lambda_i}{\sum_{j=1}^{J}\lambda_j} \times \frac{\frac{\rho_i^{d-1}}{\mu_i^{d-1}}\left(1-\frac{\rho_i}{\mu_i}\right)}{1-\frac{\rho_i^{m_i}}{\mu_i^{m_i}}} \quad (1)$$

Besides are entered two additional States (S) and (F). The first corresponds to successful processing of the demand and the second loss of the demand. The initial probabilities of these states are zero. Next is defined the matrix of probabilities of transitions $\hat{p}$ of Markov's chain corresponding to a way of any application on knots. States (S) and (F) are not reported. Chain having got to one of these states, already out of it comes out. Transition probability from a status (i; d) in a status (j; w) it is possible to calculate on a Eq. 2:

$$p\{(i,d)\to j,w)\} = \tilde{p}_{ij}\frac{\frac{\rho_j^{w-1}}{\mu_j^{w-1}}\left(1-\frac{\rho_j}{\mu_j}\right)}{1-\frac{\rho_j^{m_j}}{\mu_j^{m_j}}} \quad (2)$$

where, $\tilde{p}_{ij}$ elements of the corrected substochastic matrix of probabilities of transitions of $\tilde{P}$ requests correction is necessary as the matrix of P is set for networks of mass service without loss of requests. The probability of successful processing of the request in a node is equal to (Eq. 3):

$$p\{(i,d)\rightarrow S)\} = \tilde{p}_i^* \quad (3)$$

where, $\tilde{p}_i^*$ probability of successful processing of the request in a node i (then the request leaves a network); it is calculated during iterative procedure on the basis of a matrix of P and:

$$p_i^* = 1 - \sum_{k=1}^{J} Pik$$

If the request is in the crowded queue, the probability of its loss (transition of a circuit to a status (F)) is equal (Eq. 4):

$$p = \{(i, m_i + 1) \rightarrow F)\} = 1 \quad (4)$$

All other probabilities are = 0. For an assessment of probability of loss of the request in case of a stationary operation mode of a network it is necessary to calculate the member of a vector $\hat{p}^{(k)}\{(F)\}$ corresponding to a status (F) on k-m a step of the given Markov chain where $\hat{p}^{(k)} = \hat{p} \times (\hat{p})^k$.

Installation of parameter k happens to the help of additional iterative procedure. According to the results of calculation is calculated $\tilde{p}_N^{(k)}$ the probability that the kth step of a given Markov chain application is still in the network, i.e., E. Is not lost and is not processed in full (Eq. 5):

$$\hat{p}_N^{(k)} = 1 - \hat{p}^{(k)}\{(F)\} - \hat{p}^{(k)}\{(S)\} \quad (5)$$

If as a result of computation $\hat{p}_N^{(k)}$ exceeds the given accuracy some beforehand, k increases and calculation repeats until is reached the given accuracy of the specified probability.

DISCUSSION

On the basis of the presented methodology the developed architecture and is constructed program realization of system of detection of DDoS-attacks. The methodology developed in this study got considerable support.

CONCLUSION

The developed technique allows to receive an adequate assessment of frequency of loss of demands in a network in case the network of mass service is in the stationary mode. At emergence DDoS-attack knots of networks of mass service leave the stationary mode for some time, after is set the stationary mode with other parameters. For the period of transition between the modes the technique is inapplicable. As transition time between the modes depends on topology of a network and parameters of knots, the assessment of efficiency of the developed technique and its comparative analysis with other approaches represents a separate task.

REFERENCES

Apiecionek, L., J.M. Czerniak and W.T. Dobrosielski, 2015. Quality of services method as a DDoS protection tool. Adv. Intell. Syst. Comput., 323: 225-234.

Bhatia, S., D. Schmidt, G. Mohay and A. Tickle, 2014. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. Comput. Security, 40: 95-107.

Bhuyan, M.H., D.K. Bhattacharyya and J.K. Kalita, 2015. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit. Lett., 51: 1-7.

Bu, T., S. Norden and T. Woo, 2004. Trading resiliency for security: Model and algorithms. Proceedings of the 12th IEEE International Conference on Network Protocols, October 5-8, 2004, IEEE Computer Society, Washington DC. USA., pp: 218-227.

Dean D., M. Franklin and A. Stubble?eld, 2001. An algebraic approach to IP traceback. Proceedings of the Network and Distributed System Security Symposium, February 8-9, 2001, Sand Diego, CA., USA., pp: 3-12.

Elliott, J., 2000. Distributed denial of service attacks and the zombie ant effect. IT Professional, 2: 55-57.

Garber, L., 2000. Denial-of-service attacks rip the internet. Computer, 33: 12-17.

Hautio, J. and T. Weckstrom, 1999. Denial of service attacks. March 1999. http: //www.hut.fi/u/tweckstr/hakkeri/DoS_paper.html.

Hussain, A., J. Heidemann and C. Papadopoulos, 2003. A framework for classifying denial of service attacks. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, August 25-29, 2003, Karlsruhe, Germany, pp: 99-110.

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router-based defense against DDoS attacks. Proceedings of the 9th Symposium Network and Distributed System Security, February 6-8, 2002, San Diego, California, USA., pp: 1-12.

Li, M., M. Li and X. Jiang, 2008. DDoS attacks detection model and its application. WSEAS Trans. Comput., 7: 1159-1168.

Ozcelik, I. and R.R. Brooks, 2015. Deceiving entropy based DoS detection. Comput. Security, 48: 234-245.

Szczerba, E.V. and D.A. Volkov, 2013. Development of the system architecture of distributed detection of network attacks such as denial of service. Magazine Applied Discrete Mathematics Application, Issue No. 6, pp: 68-70.

Szczerba, E.V. and M.V. Szczerba, 2012. Development of the system architecture of distributed detection of network attacks such as denial of service. Scientific Herald of Omsk. Ser. Appliances Machinery Technology, 113: 280-283.

Wang, J. and A.A. Chien, 2003. Using overlay networks to resist denial of service attacks. Proceedings of the ACM Conference on Computer and Communucation Security, October 2003, Washington DC., USA., pp: 1-13.