Research Journal of Applied Sciences, Engineering and Technology 10(12): 1420-1424, 2015
DOI: 10.19026/rjaset.10.1843
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: April 7, 2015 Accepted: April 22, 2015 Published: August 25, 2015

Research Article

Detection Techniques of DOS/DDOS/DRDOS Attacks in Networks of Mass Service

[1]G. Shangytbayeva, [2]G. Kazbekova, [3]U. Imanbekova, [3]S. Munsyzbaeva and [4]N. Shangytbayev
[1]K. Zhubanov Aktobe Regional State University, Aktobe 030000, Kazakhstan
[2]Kazakh-Russian International University, Aktobe 030000, Kazakhstan
[3]Kazakh National Technical University Named After K.I. Satpayev, Almaty 050013, Kazakhstan
[4]Aktobe Polytechnic College, Aktobe 030000, Kazakhstan

Abstract: The study describes the basic network attacks such as "denial of service", algorithm of operation of malefactors with attacks of this type, techniques of detection of DOS/DDOS/DRDOS attacks in networks of mass service. For detection of DDoS-attacks is offered the valuation method of probability of loss of arbitrary request in case of its passing on networks of mass service. Developed the architecture and constructed program implementation of system of detection of DDoS-attacks. The developed technique allows to receive an adequate assessment of frequency of loss of requests on a network if the network of mass service is in the stationary mode.

Keywords: Denial of service attacks, detection of network attacks, distributed denial of service attacks, mass service, networked and distributed attacks

INTRODUCTION

DoS attacks can also target tangible system resources, such as computational resources (bandwidth, disk space, processor time); configuration information (routing information, etc.); state information (for example, unsolicited TCP session resetting). Moreover, a DoS attack can be designed to: execute malware that maxes out the processor, preventing usage; trigger errors in machine microcode or sequencing of instructions, forcing the computer into an unstable state; exploit operating system vulnerabilities to sap system resources; crash the operating system altogether (Lee, 2000; Ioannidis and Bellovin, 2002).

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.

DoS attack, Denial of Service attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic. This means that one computer and one internet connection is used to flood a server with Packets (TCP/UDP). The point of such a denial of service attack is to overload the targeted server's bandwidth and other resources. This will make the server inaccessible to others, thereby blocking the website or whatever else is hosted there. Unlike DoS-attacks ("Denial of Service") from DDos attack ("Distributed Denial of Service") is that in this case overload occurs as a result of requests from any particular internet site (Denial-of-Service Attack, 2015; Özçelik and Brooks, 2014).

In most respects it is similar to a DoS attack but the results are much, much different. Instead of one computer and one internet connection the DDoS attack utilizes many computers and many connections.

The computers behind such an attack are often distributed around the whole world and will be part of what is known as a botnet. The main difference between a DDoS attack vs. a DoS attack, therefore, is that the target server will be overload by hundreds or even thousands of requests in the case of the former as opposed to just one attacker in the case of the latter (Bhatia *et al*., 2014; Wang and Chien, 2003).

Therefore it is much, much harder for a server to withstand a DDoS attack as opposed to the simpler DoS incursion. Do not process a large number of requests, the server first starts just slowly and then stops completely. Inquiries most often have smart and senseless character that even more complicates operation of the server.

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.

The majority of DDoS-attacks use vulnerabilities in the main Internet Protocol (TCP/IP), namely, a method of processing query systems SYN (Dean *et al*., 2001).

Corresponding Author: G. Shangytbayeva, K. Zhubanov Aktobe Regional State University, Aktobe 030000, Kazakhstan

Allocate two main types of attacks which cause refusal in service. As a result of carrying out attack of the first type, work of all system or a network stops. The hacker sends to system data or packages which she doesn't expect and it leads to a stop of system or to its reset.

The second type of DDoS-attacks leads to overflow system or a local network using the vast amount of information that can't be processed. DDoS-attack consists in the continuous appeal to the site from many computers which are located in different parts of the world. In most cases these computers are infected with viruses which are operated by swindlers is centralized and eaten in the botnet.

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.

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" 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

Computers which enter in botnet, send to spams, participating, thus, in DDoS-attacks.

How does DDoS works shown in the following diagram (Fig. 1).

Unlike the attack DoS, where an attacker uses to attack a single computer or network to attack a target, DDoS attack proceeds from the numerous computers and servers which are previously infected, belonging to usually various networks. Since as the attacker uses computers and servers from different networks and even different countries, the incoming traffic, at first, does not cause suspicion among security services, since it is difficult to detect (Hautio and Weckstrom, 1999).

The distributed attack "refusal in service" overloads a target network or system. The idea of attack consists in use of different sources (demons) for attack and "owners" for management. The most known utilities of the DDoS organization-this Tribal Flood Network (TFN), TFN2K, Trinoo and Stacheldraht (Li *et al*., 2008).

In the Fig. 2 shows the architecture of a DDoS-attacks.

Figure 3 shows an example of an organization DDoS.

DDoS is Denial of Service network resource resulting in multiple distributed 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.

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.

The widespread DOS option of the attack known as DDoS (Distributed Denial of Service-the distributed refusal in service) attack became very popular in

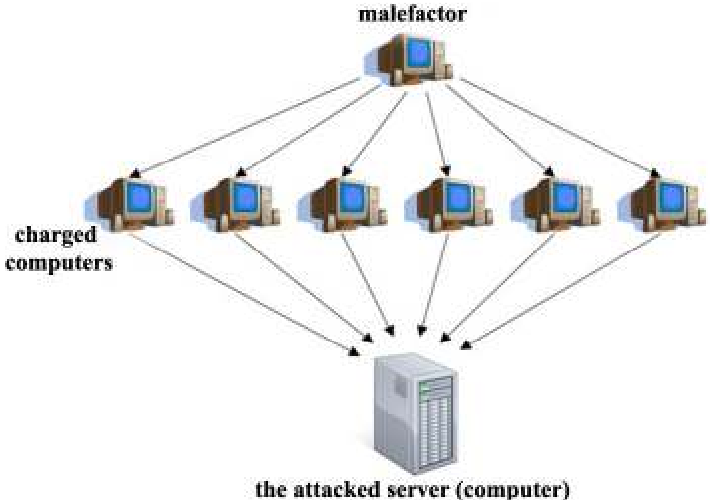

Fig. 1: The distributed DDoS attack

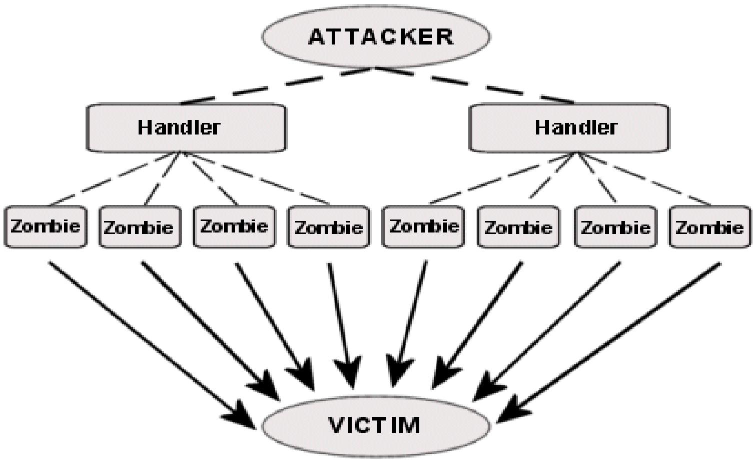

Fig. 2: Architecture of a DDoS-attacks

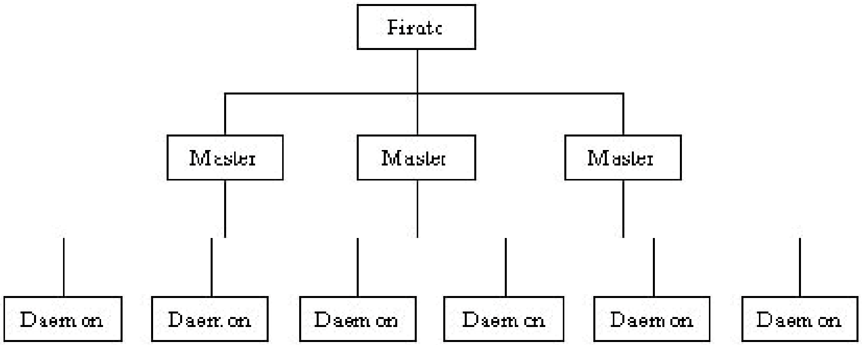

Fig. 3: The distributed attack "denial of service"

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.

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 can't connect. Any server open to the Internet and running UDP-based services can potentially be used as a reflector.

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. 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 (Bhuyan *et al*., 2015).

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 isn't 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 AND DISCUSSION

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 λ. 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 work 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 to 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 (Bu *et al*., 2004).

The initial distribution of the chain $\hat{p}$ can be calculated as (1):

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

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) aren't 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 formula (2):

$$p\{(i,d) \rightarrow j,w)\} = \widetilde{p_{ij}}\,\frac{\frac{\rho_j^{w-1}}{\mu_j^{w-1}}\left(1-\frac{\rho_j}{\mu_j}\right)}{1-\frac{\rho_j^{m_j}}{\mu_j^{m_j}}} \tag{2}$$

where $\widetilde{P_{ij}}$-elements of the corrected sub-stochastic 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 (3):

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

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:

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

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

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

All other probabilities are equal to zero.

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 $\hat{p}^{(k)} = \hat{p}\cdot(\hat{P})^{k}$.

Installation of parameter k happens to the help of additional iterative procedure.

According to the results of calculation is calculated $\hat{p}_N^{(k)}$-the probability that the k-th step of a given Markov chain application is still in the network, i.e., E. Is not lost and is not processed in full (5):

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

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.

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 (Elliott, 2000; Hussain *et al*., 2003).

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, Ł., J.M. Czerniak and W.T. Dobrosielski, 2015. Quality of services method as a DDoS protection tool. Adv. Intel. Sys. 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. Secur., 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 Recogn. Lett., 51: 1-7.

Bu, T., S. Norden and T. Woo, 2004. Trading resiliency for security: Model and algorithms. Proceeding of the 12th IEEE International Conference on Network Protocols, pp: 218-227.

Dean, D., M. Franklin and A. Stubblefield, 2001. An algebraic approach to IP traceback. Proceeding of the Network and Distributed System Security Symposium (NDSS), pp: 3-12.

Denial-of-Service Attack, 2015. Wikipedia, the Free Encyclopedia. Retrieved from: http://en.wikipedia.org/wiki/Denial-of-service_attack. (Accessed on: February 2, 2015)

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

Hautio, J. and T. Weckstrom, 1999. Denial of Service Attacks. Retrieved from: http://www.hut.Fi/u/tweckstr/hakkeri/DoSpaper.html.

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

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router-based defense against DDoS attacks. Proceeding of the Network and Distributed System Security Symposium (NDSS, 2002). Reston, VA, USA, pp: 100-108.

Lee, G., 2000. Denial-of-Service attacks rip the internet. Computer, 33(4): 12-17.

Li, M., M. Li and X. Jiang, 2008. DDoS attacks detection model and its application. WSEAS T. Comput., 7(8): 1159-1168.

Özçelik, I. and R. Brooks, 2014. Deceiving entropy based DoS detection. Comput. Secur., 48: 234-245.

Szczerba, E.V. and M.V. Szczerba, 2012. Development of the system architecture of distributed detection of network attacks such as "Denial of Service". Sci. Herald Omsk. Ser. Appl. Mach. Technol., 3(113): 280-283.

Szczerba, E.V. and D.A. Volkov, 2013. Development of the system architecture of distributed detection of network attacks such as "Denial of Service". Appl. Discrete Math. Appl., pp: 68-70.

Wang, J. and A.A. Chien, 2003. Using overlay networks to resist denial of service attacks. Proceeding of the ACM Conference on Computer and Communucation Security.