Modern Applied Science; Vol. 9, No. 8; 2015
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Mathematical Model of System of Protection of Computer Networks against Attacks DOS/DDOS

Shangytbayeva G. A.[1], Karpinski M. P.[2], Akhmetov B. S.[3], Yerekesheva M. M.[1] & Zhekambayeva M. N.[3]

[1] K. Zhubanov Aktobe Regional State University, Aktobe, Kazakhstan

[2] Academy of Technologies and the Humanities in Bielsko-Biala, Bielsko-Biala, Poland

[3] Kazakh National Technical University named after K.I.Satpayev, Almaty, Kazakhstan

Correspondence: Shangytbayeva Gulmira, K. Zhubanov Aktobe Regional State University, Aktobe, Kazakhstan. E-mail: shangytbaeva@mail.ru

Received: January 6, 2015 Accepted: February 18, 2015 Online Published: July 10, 2015

doi:10.5539/mas.v9n8p106 URL: http://dx.doi.org/10.5539/mas.v9n8p106

Abstract

In practice the most part of connections of subjects of a wide area network uses the virtual connections as this method is the dynamic protection of network connection and won't use static key information. Therefore, the interaction without establishing a virtual channel is one of the possible reasons for the success of remote attacks such as DoS / DDoS. An abstract considers the mathematical model of system of protection of computer networks against attacks such as DoS/DDoS, allowing in practice to detect attacks such as DoS / DDoS. Grounded way to prevent attacks through the use of network reconfiguration procedures, it is difficult for practical implementation attacks such as DoS / DDoS. The algorithm to create new virtual data channels to ensure a minimum amount of traffic regardless of reconfiguring computer network. The article presents an approach to detection of the distributed network attacks to refusal in service, the offered method increases efficiency of use of the calculated resource of a computer network at the big distributed network attacks to “Denial of Service”.

Keywords: computer network, routing, attacks, network attacks, DoS – attack, DDoS – attack, “Denial of Service”, detection of network attacks

1. Introduction

Computer network providing every opportunity for exchanging data between the client and server, but now widely distributed attack denial of service clients, the determination of distributed attacks in the network is particularly acute. The most common types of such attacks are DoS / DDoS attacks, which deny certain users of computer network services. 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 attacks are characterized by a straightforward implementation complexity and resistance, which poses new problems of researchers, who are still not yet resolved (Yang Z. X. et al., 2014).

Wide use of computer networks creates conditions for implementation of the attacks using standard algorithms of routing. It is known that the routing protocol in data transfer is rule set and arrangements on an exchange of information network between routers to determine the data path transfer which satisfies to the given parameters of quality of service and provides the balancing load of all computer network in general therefore the research problem of network traffic acquires special relevance (Wang J., & Chien, A, 2003).

To questions of the organization and creation of computer networks including to questions of routing, are devoted to the work of scientists M.Yu.Ilchenko, S.G. Bunina, A.S. Petrova and D. Davis, D. Barber, V. Price, V. Vilinger, D. Wilson, D. Rakhson, etc.

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 utilises 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 (Hussain, A., et al., 2003).

Therefore it 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 (Denial-of-service attack, 2015).

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 (Kihong Park & Heejo Lee, 2001).

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 (Goodrich, 2002).

The majority of DDoS-attacks use vulnerabilities in the main Internet Protocol (TCP/IP), namely, a method of processing a query systems SYN (Wang, H., et al., 2002).

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. Computers which enter in botnet, send to spams, participating, thus, in DDoS-attacks (Li Muh *et al.,* 2008).

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. 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. For implement of attacks like DoS / DDoS in the modern computer networks is characteristic multilevel routing in of which the computer network certain way breaks into the subnets and they working on standard protocols (Savage, S., et al., 2000). Most implementations of attacks like DoS / DDoS are calculated on the net with a homogeneous structure or on network with the fixed structure of domains. Frequent change of components of a computer network leads to change of its topology, composition and quantity of routing domains, influences efficiency of procedure of routing, and promotes operation of algorithms like DoS / DdoS (Park, K., & Lee, H., 2000). Therefore there is a need for development of new methods of protection of a computer network that will provide information transfer with the given parameters of quality of service at the minimum volume of traffic by development of a method of protection of traffic against the redundant information on the basis of determination of criterion of network transmission capacity and computing resources. The analysis of practical implementation of the attack in the wide area network allows to determine information security mechanisms in the computer networks on the basis of use of algorithms like DoS / DDoS. For elimination of the reasons of attacks to infrastructure and basic protocols of a network is advisable to change a configuration of computer system. At the first investigation phase it is necessary to analyze network traffic for preventing of unauthorized reading from physical transmission channel of data, it will allow to avoid interception of information leakage. This task successfully treated by creating of the virtual networks, of the the algorithms the tunneling, identification, authentication (Bhuyan, M. H., et al., 2015).

Danger of the majority of DDoS-attacks is that at the first stages don't violate the exchange protocol of data. They manifest themselves when computable network resource becomes insufficiently. For preventing of such attacks quite properly configure the router and firewall.

For simplification of implementation of DoS / DDoS of algorithms the user should observe of rated speeds of data transfer, it will allow in practice to avoid algorithms of optimization of network traffic on which are realized of many attacks (Wu, Y., et al., 2015).

2. Methodology

The Method section describes in detail how the study was conducted, including dependence of the volume of traffic on the types of attacks DoS / DDoS, efficiency of methods of routing, etc (Klimenko, I. A., 2005).

From attacks such as flood can effectively dissociate themselves by division of the main communication channel into multiple virtual. This will allow to create other network interfaces in case of defeat of the channel DoS / DDoS of algorithms. Firewalls advisable to continuously strengthen and adjust so that internal network services were unavailable to the external user. It is expedient to set the analyzer of network traffic, value of its parameters will allow in time to identify the beginning of the attacks. Before the direct beginning of attack bots gradually increase a flow of packets on system. Therefore is necessary the continuous observation of over the router connected to the external network (Dean, D., et al., 2001).

The effectiveness of routing methods is directly dependent on the topology of the network and its size. Multilevel routing substantially depends on optimum partition of a computer network on domains routing. Thus, one of the main objectives of protecting the functioning of a computer network has network traffic, which is based on the principle of the minimum amount of network data. The task of protecting network data reduced to the problem of minimization of parameters of information transfer (Law, T., et al., 2005).

It is known that when using known routing protocols in the domain network topology change leads to growth of traffic the non-linear law, therefore reconfiguration of domains routing in the course of topology change of a network promotes reduction of volume of traffic and time of formation of ways of data transfer, and also complicates implementation of attack like DoS / DDoS. Based on an advanced mathematical model is defined the choice of quantity and the size of routing domains. For the purpose of support of maximum efficiency of functioning of a computer network, procedure should take into account changes the network topology. However the majority of routing protocols don't provide procedure of change of structure of routing domains. In this regard there is a need of development of new model of routing which at the expense of the accounting of attacks of a failure in service of resources of routing will allow to increase efficiency of information transfer in the computer networks. Thus it is necessary to consider conditions of feasibility of parameter values of network transmission capacity and computing resources. It is expedient to determine the parameters regulating the amount of the packets transferred on each communication link separately and total amount of the packets transferred during the update of routing tables (Stone, R., 2000).

The total volume of traffic is determined by this model (1):

$$V = \frac{T_{sys}}{\Delta t_{sys}} \sum_{i,j=1}^{N} P_i Q_j \tag{1}$$

Where:

Δt_{sys} – time of one clock period of system;

Q_j– amount of information, transferred for one clock period on each certain canal;

N – quantity of nodes on the computer networks;

P_j – the degree of a node is compromised;

T_{sys} – time during which in case of topology change of a network nodes distribute messages of message on restoration of routes (Bu, T., et al., 2004).

3. Results

In the Results section, summarize the collected data and the analysis performed on those data relevant to the discourse that is to follow. Report the data in sufficient detail to justify your conclusions. Mention all relevant results, including those that run counter to expectation; be sure to include small effect sizes (or statistically nonsignificant findings) when theory predicts large (or statistically significant) ones. Do not hide uncomfortable results by omission. Do not include individual scores or raw data with the exception, for example, of single-case designs or illustrative examples. In the spirit of data sharing, raw data, including study characteristics and indivldual effect sizes used in a meta -analysis, can be made available on supplemental online archives (Karpinski, M. P., 2011).

Researches showed that during implementation of attack of a type of DoS / DDoS increases the quantity of the compromised nodes and grows the total amount of traffic of V.

The results of numerical experiment presented in Figure 1.

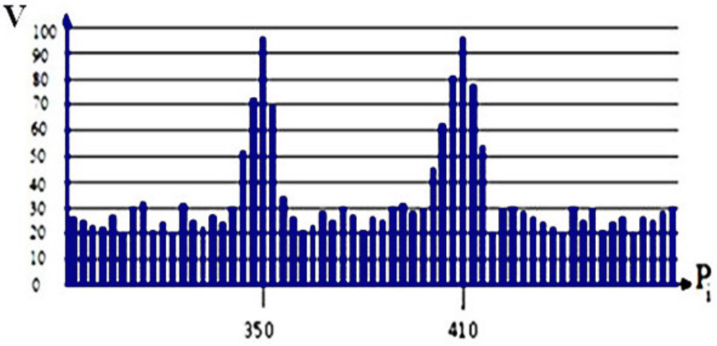

Figure 1. The dependence of the volume of traffic on the type of attacks DoS / DDoS

The results of the model experiment are presented in Figure 2.

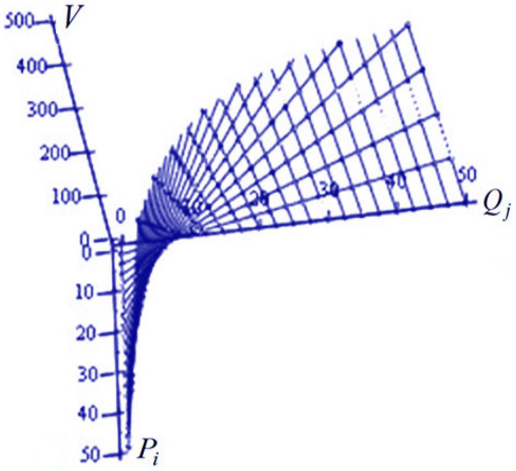

Figure 2. The dependence of the volume of traffic from the degree of a compromise node

The analysis of a figure shows that in attack promptly increases traffic volume in channels of a network, the most part of traffic uses an algorithm like DoS / DDoS. It's pretty much slows down the work network. To prevent such situations, it is advisable to use the traffic analyzers that control the amount of packets in the network (John, D. H., 1998). Also it is necessary to execute procedure of routing by means of distributed system of agents of routing provided that routing in the domain is carried out by the agent who is a part of this domain, and routing between domains is executed at the interoperability layer of agents of routing. This is due to the fact that the exchange of official information on the network is carried out by the same channels as the transmission of useful information (Aleksander, M. A., et al., 2012).

4. Discussion

In this paper for the detection of DDoS-attacks provided a method for estimating the probability of loss of any requests during its passage through of networks (Karpinski, N., & Shangytbayeva, G., 2005).

After presenting the results, you are in a position to evaluate and analyze, interpret their implications. Here you will examine, analyze, interpret, and qualify the results and draw inferences and conclusions from them.

The analysis of the data provided research shows that in attack time traffic volume in channels of a network promptly increases, and the most part of traffic is used by attack like DoS / DDoS. it's pretty much slows down the network (Baba, T., & Matsuda, S., 2002).

For increase of efficiency of procedure of routing in operation is offered to separate data on the virtual links. For this purpose, a plurality of workstations and virtual channels between them arranged in the form of a local area computer network. A method of forming and dynamic reconfiguration of routing domains can increase the efficiency procedure routing of computer network. Formation and dynamic reconfiguration of domains is carried out by means of specialized system of routing which basic functions is determination of quantity and layout of workstations, updates of the routing information and a choice of a way, meets the requirements of stability and the minimum temporal time delay.

To prevent attacks appropriate to introduce in the system of additional detectors of monitoring of traffic of a network. These detectors instruct the executing modules in different network segments. As a result, before the attacked flow it is formed the screen, the separating attacks from an internal network. Routes are elected dynamically or statically so as to use only the physical security of the subnet, nodes of switching and channels. Transmission of data having security tags through certain subnet, switching nodes and channels advisable to prohibit the security policy.

This research is directed on studying of the distributed network attacks such as DoS / DDoS and methods, models and architecture of network attacks to refusal in service.

On the basis of the presented methodology the developed architecture and is constructed program realization of system of detection of DDoS-attacks. (Shangytbayeva, G., et al., 2015) According to the results is published scientific articles. The methodology developed in this study got considerable support. (Shangytbayeva, G., & Beysembekova, R., 2015).

Conclusion

In article improved mathematical model of total traffic, allows in practice to reveal attacks like DoS / DDoS. Use of the received results allows to raise the network security level at the expense of the organization of multi-level of protocols routing. For preventing specified attacks appropriate to introduce a system of additional detectors traffic monitoring network. Reasonably a method of preventing of attacks on the basis of use of procedure of reconfiguration of a network that allowed to complicate practical implementation of attack like DoS / DDoS, by creation of new virtual links of data transfer. This method provides the minimum volume of traffic irrespective of reconfiguration of a computer network.

References

Aleksander, M. A., Karpinski, M. P., & Yatsykovska, U. O. (2012). Features of Denial of Service attacks in information systems. *Informatics and Mathematical Methods in Simulation, 2*(2), 129-130.

Baba, T., & Matsuda, S. (2002). Tracing network attacks to their sources. *IEEE Internet Computing, 6*(2), 20-26.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters,* (51), 1-7.

Bu, T., Norden, S., & Woo, T. (2004). Trading resiliency for security: Model and algorithms. *In Proc. 12th IEEE International Conference on Network Protocols,* pp. 218-227),

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

Denial-of-service attack. (2015, February). In Wikipedia, the free encyclopedia. Retrieved February 2, 2015, from http://en.wikipedia.org/wiki/Denial-of-service_attack

Goodrich, M. T. (2002). *Efficient packet marking for large-scale IP traceback.* In 9th ACM Conf. on Computer and Communications Security (CCS). pp. 117–126.

Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). *A framework for classifying denial of service attacks.* (pp. 99-110), Proc. ACM SIGCOMM. Karlsruhe, Germany.

John, D. H. (1998, August). *An Analysis of Security Incidents on the Internet*. Ph.D. thesis, Carnegie Mellon Univerisity.

Karpinski, M. P. (2011). *Modeling network traffic computer network in implementation attacks such as DOS / DDOS.* (5), 143-146. Information Security, American Psychological Association. Ethical standards of psychologists. Washington, DC: American Psychological Association.

Karpinski, N., & Shangytbayeva, G. (2015, 05-06 January). *Architecture and Program Realization of System of Detection of Network Attacks to Denial of Service.* (pp. 55), International Conference on "Global Issues in Multidisciplinary Academic Research" GIMAR-2015, Dubai, UAE.

Kihong, P., & Lee, H. (2001, August). *On the Effectiveness of Route-Based Packet Filtering for Distributed DoS*

Attack Prevention in Power-Law Internets, (pp. 15-26), Proc. of ACM SIGCOMM '01.

Klimenko, I. A. (2005). *A method of dynamic routing with support for required level of quality of service in mobile networks without a fixed infrastructure.* (Vol. 15. pp. 102-112). Problems of Information and Control: Sat. Sciences. pr. M.: NAU.

Law, T., Yau, D., & Lui, J. (2005). *You can run, but you can not hide: An effective statistical methodology to trace back ddos attackers,* 16(9), 799-813. IEEE Transactions on Parallel and Distributed Systems.

Li, M., Li, M., & Jiang, X. (2008). DDoS attacks detection model and its application (Vol. 7, No. 8, pp. 1159-1168). WSEAS Trans. Computers.

Park, K., & Lee, H. (2000, June). *On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack,* Tech. Rep. CSD-00-013, Department of Computer Sciences, Purdue University.

Savage, S., Wetherall, D., Karlin, A. R., & Anderson, T. (2000). *Practical network support for IP traceback* (pp. 295-306). In Conference on SIGCOMM.

Shangytbayeva, G., & Beysembekova, R. (2015, 21-22 March). *Integrated approach to the detection of distributed network attacks. International Conference on Mechanical*, Electronic and Information Technology Engineering, Chongqing, China.

Shangytbayeva, G., Akhmetov, B., & Beysembekova, R. (2015, 25-26 February). *Analysis of Methods Organization of the Modelling of Protection of Systems Client-Server.* International Conference on "Multidisciplinary Innovation in Business Engineering Science & Technology". Manila, Philippine.

Stone, R. (2000, August). Centertrack: An IP overlay network for tracking DoS floods. In Proc. of 9th USENIX Security Symposium.

Wang, H., Zhang, D., & Shin, K. G. (2002). *Detecting SYN flooding attacks.* (pp. 1530-1539), Proc. IEEE INFOCOM'2002. New York.

Wang, J., & Chien, A. (2003, October). *Using overlay networks to resist denial of service attacks.* Submitted to ACM Conference on Computer and Communication Security.

Wu, Y., Zhao, Z., Bao, F., & Deng, R. H. (2015). *Software puzzle: A countermeasure to resource-inflated denial-of-service attacks.* IEEE Transactions on Information Forensics and Security.

Yang, Z. X., Qin, X. L., Li, W. R., & Yang, Y. J. (2014). *A DDoS detection approach based on CNN in cloud computing.* Applied Mechanics and Materials.

Copyrights