Research Journal of Applied Sciences 10 (2): 49-53, 2015
ISSN: 1815-932X

Systems of Protection of Computer Networks from Distributed Network Attacks to Denial of Service

[1]Gulmira A. Shangytbayeva, [2]Bahytzhan S. Akhmetov, [2]Mikolaj P. Karpinski,
[1]Roza N. Beysembekova and [3]Erbol A. Ospanov
[1]Kazakh National Technical University Named after K.I. Satpayev,
Satpayev Street 22a, 050013 Almaty, Republic of Kazakhstan
[2]Academy of Technologies and the Humanities in Bielsko-Biala,
2 Willowa Street, 43-309 Bielsko-Biala, Poland
[3]Semey State University Named after Shakarim,
Glinka Street 20a, 071410 Semey, Republic of Kazakhstan

Abstract: The study discusses the mathematical model of system of protection of computer networks against attacks to denial of service, allowing in practice to detect attacks such as denial of service. Grounded way to prevent attacks through the use of network reconfiguration procedures, it is difficult for practical implementation attacks such as denial of service. The algorithm to create new virtual data channels to ensure a minimum amount of traffic regardless of reconfiguring computer network. This method helps to ensure the minimum amount of traffic regardless of the reconfiguration of the network.

Key words: Information security, computer network, network attacks, DOS-attacks, DDOS-attacks, attacks to denial of service

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 straight forward implementation complexity and resistance which poses new problems of researchers who are still not yet resolved.

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 (Li *et al*., 2008).

To questions of the organization and creation of computer networks including to questions of routing are devoted to the research 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.

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. 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. 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

Corresponding Author: Gulmira A. Shangytbayeva, Kazakh National Technical University Named after K.I. Satpayev, Satpayev Street 22a, 050013 Almaty, Republic of Kazakhstan

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 (Wang and Chien, 2003; Bhuyan *et al*., 2015; Wu *et al*., 2014; Yang *et al*., 2014; Ioannidis and Bellovin, 2002).

Danger of the majority of DdoS attacks is that at the first stages do not 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 (Stone, 2000).

MATERIALS AND METHODS

The study 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.

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.

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 (Bu *et al*., 2004; Klimenko, 2002; Law *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 do not 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. The total volume of traffic is determined by this model (Eq. 1):

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

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_i = 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

RESULTS AND DISCUSSION

In the study, 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

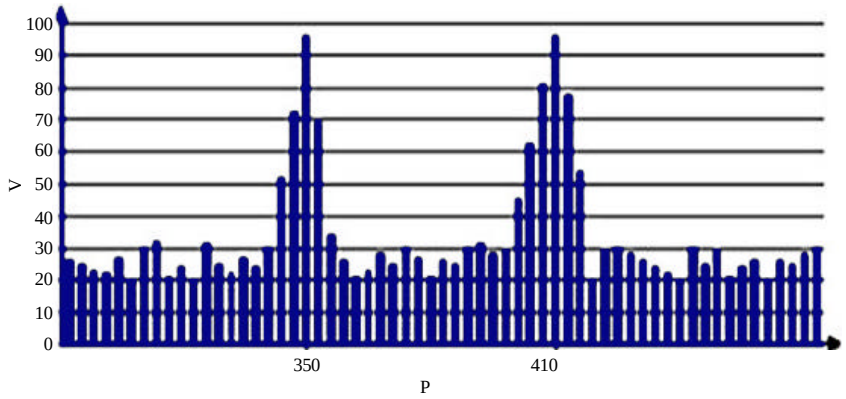

Fig. 1: The dependence of the volume of traffic on the type of attacks DoS/DDoS

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 (encouraged by APA and other professional associations and sometimes required by funding agencies), raw data including study characteristics and indivldual effect sizes used in a meta analysis can be made available on supplemental online archives (Hussain *et al*., 2003; Zhukov and Davydenko, 2008; Karpinski, 2011; Elliott, 2000; Nicholas and Gulmira, 2015; Aleksander *et al*., 2012; Park and Lee, 2001; John, 1998; Park and Lee, 2000).

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 Fig. 1. The results of the model experiment are presented in Fig. 2.

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. 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 (Song and Perrig, 2000; Wang *et al*., 2002; Goodrich, 2008; Burch and Cheswick, 2000; Baba and Matsuda, 2002; Savage *et al*., 2000; Dean *et al*., 2001).

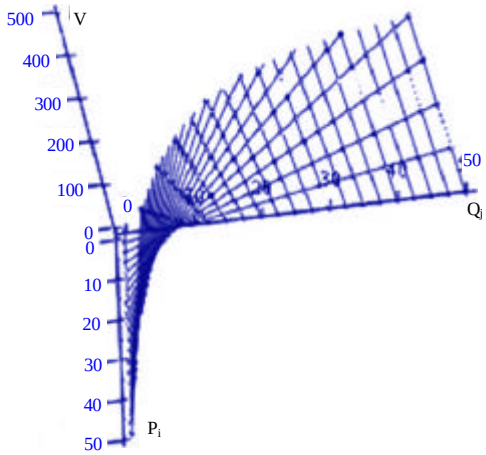

Fig. 2: The dependence of the volume of traffic from the degree of a compromise node

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.

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 (Song and Perrig, 2001; Savage *et al*., 2000; Snoeren *et al*., 2001).

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.

CONCLUSION

In study, 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., M.P. Karpinski and U.O. Yatsykovska, 2012. Features of denial-of-service attacks in information systems. Inform. Math. Meth. Simulat., 2: 129-113.

Baba, T. and S. Matsuda, 2002. Tracing network attacks to their sources. IEEE Internet Comput., 6: 20-26.

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.

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source. Proceedings of the 14th USENIX Conference on System Administration, December 3-8, 2000, New Orleans, Louisiana, USA., pp: 319-327.

Dean D., M. Franklin and A. Stubblefield, 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.

Goodrich, M.T., 2008. Probabilistic packet marking for large-scale IP traceback. IEEE/ACM Trans. Network., 16: 15-24.

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.

John, D.H., 1998. An analysis of security incidents on the internet. Ph.D. Thesis, Ph.D. Thesis, Carnegie Mellon Univerisity, Pennsylvania.

Karpinski, M.P., 2011. Modeling network traffic computer network in implementation attacks such as DOS/DDOS. Information Security, American Psychological Association, Ethical Standards of Psychologists, Washington, DC., USA., pp: 143-146.

Klimenko, I.A., 2002. A method of dynamic routing with support for required level of quality of service in mobile networks without a fixed infrastructure. Problems Inform. Control: SAT Sci., 15: 102-112.

Law, T.K.T., D.K.Y. Yau and J.C.S. Lui, 2005. You can run, but you can't hide: An effective statistical methodology to trace back DDos attackers. IEEE Trans. Parallel Distrib. Syst., 16: 799-813.

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

Nicholas, K. and S. Gulmira, 2015. Architecture and program realization of system of detection of network attacks to denial of service. Proceedings of the International Conference on Global Issues in Multidisciplinary Academic Research, January 05-06, Dubai, UAE, pp: 55-55.

Park, K. and H. Lee, 2000. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. Computer Science Technical Reports No. 00-013, Department of Computer Sciences, Purdue University, West Lafayette, IN., August 2000.

Park, K. and H. Lee, 2001. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, August 27-31, 2001, San Diego, CA., USA., pp: 15-26.

Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2000. Practical network support for IP traceback. Proceedings of the conference on Applications, Technologies, Architectures and Protocols for Computer Communication, August 28-September 1, 2000, Stockholm, Sweden, pp: 295-306.

Snoeren, A.C., C. Partridge, L.A. Sanchez, Jones, C.E., F. Tchakountio, S.T. Kent and W.T. Strayer, 2001. Hash-based IP traceback. Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, August 27-31, 2001, San Diego, California, USA., pp: 3-14.

Song, D. and A. Perrig, 2000. Advanced and authenticated marking schemes for IP traceback. Technical Reports UCB/CSD-00-1107, Computer Science Department, University of California, Berkeley.

Song, D.X. and A. Perrig, 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the 20th Annual Joint Conference on IEEE Computer and Communications Societies, April 22-26, 2001, Anchorage, AK., USA., pp: 878-886.

Stone, R., 2000. Centertrack: An IP overlay network for tracking DoS floods. Proceedings of the 9th USENIX Security Symposium, August 14-17, 2000, Denver, Colorado, USA., pp: 107-118.

Wang, H., D. Zhang and K.G. Shin, 2002. Detecting SYN flooding attacks. Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies. June 23-27, 2002, New York, USA., pp: 1530-1539.

Wang, J. and A. Chien, 2003. Using overlay networks to resist denial-of-service attacks. Proceedings of the 10th ACM Conference on Computer and Communication Security, October 27-30, 2003, Washington, DC., USA -.

Wu, Y., Z. Zhao, F. Bao and R.H. Deng, 2014. Software puzzle: A countermeasure to resource-inflated denial-of-service attacks. IEEE Trans. Inform. Forensics Secur., 10: 168-177.

Yang, Z.X., X.L. Qin, W.R. Li, Y.J. Yang, 2014. A DDoS detection approach based on CNN in cloud computing. Applied Mech. Mater., 513: 579-584.

Zhukov, I.A. and I. Davydenko, 2008. Distributed traffic management in mobile networks. Electron. Control Syst., 2: 161-167.