Research Journal of Applied Sciences, Engineering and Technology 10(12): 1414-1419, 2015
DOI: 10.19026/rjaset.10.1842
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: April 7, 2015 Accepted: April 22, 2015 Published: August 25, 2015

Research Article

Formalized of Model of Linear Kind for Differentiate Distributed Network Attacks on the Basis of a Weight Coefficients

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

Abstract: This study discusses the problem distributed network attacks, formalized of model of linear kind for differentiate distributed network attacks on the basis of a weight coefficients Structured the formalized mathematical models allow to consider structure of the On network to a basis big percent, a measure of influence of each type of attack that gives the fine chance effectively to design to protect information system taking into account information on threats. Based on classification of information threats, characteristic for distributed network attacks it is offered the formalized models of a linear look for differentiation of attacks on the basis of a method of weight coefficients. By these indicators and coefficients it is possible to define the main types of threats in computer systems allowing to design effectively systems of information security taking into account information threats.

Keywords: Client-server model of communication, distributed network attacks, formalized mathematical model, mathematical model

INTRODUCTION

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. 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).

The growth of cyber crime in recent years, allows unauthorized access to the resources of computer networks. Among the most widespread numerous attacks of malefactors to on computer networks is a interruption and distortions of a package traffic. The most devastating attack in today's time is an attack aimed at denial of service of legal services. In this case the initiator of attacks compromises knot user, operating its resources, for receiving full management of knot. The initiator of attacks directs a large number of a counterfeit traffic to knot user, consuming thus the capacity of essential volume that leads to impossibility to serve a legitimate traffic. To such class belong of attacks DoS (Denial of Service), DDoS (Distributed Denial of Service), DRDoS (Distributed Reflection Denial of Service) (Apiecionek *et al*., 2015).

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/DRDoS attacks, which deny certain users of computer network services (Stone, 2000).

“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. The main essence of DoS of attack to make the services working at the target car (for example, the website, the DNS server and so forth) temporarily inaccessible to alleged users. DDoS attacks are usually carried out on a web server on which there are vital services, such as bank services, electronic commerce, processing of personal information, credit cards (Denial-of-Service Attack, 2015).

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

Corresponding Author: G. Shangytbayeva, Kazakh National Technical University Named After K.I. Satpayev, Almaty 050013, Kazakhstan

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).

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 (Deepthi *et al*., 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 (Elliott, 2000).

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 (Lee, 2000; Yang *et al*., 2014).

MATERIALS AND METHODS

To build a system to protect computer networks identified the main types of threats and their impact on network security. On the basis of the classification of known attacks denial of service developed a formal mathematical model of linear species. In this model is used the method of weight factors. The constructed formalized mathematical models of probability of information DoS/DDoS/DRDoS-threats, that define the matrix activity network by which the attack is uniquely determined (Özçelik and Brooks, 2014).

Using the method of weighting coefficients developed a mathematical model of communication of client and server for the differentiation of attacks in computer networks containing probability compromised node number of paths from the access points to the destination. The comparative characteristics of the implementation of Denial of Service client-server system, allows us to distinguish what type of attacks carried out its initiator (Baba and Matsuda, 2002).

In this study we investigate the traffic and the analysis of its volume, which depends on the type of exposure to attacks DoS/DDoS/DRDoS. Describes the characteristics of computer network attacks during a Denial of Service using a large number of compromised nodes, reflecting the growth of generating traffic and significant work client-server system (Szczerba and Volkov, 2013).

For the solution of the task it is necessary to use classification of information threats, DoS/ DDoS/DRDoS of attacks and the formalized models to measure influence on productivity operation of a computer network.

It will allow solving effectively a problem of detection of attacks on access point of a computer network. Construct the formal mathematical models of probability of information threats, DoS/DDoS/DRDoS of attacks on the basis of the linear form by method of weight factors (Bhuyan *et al*., 2015).

To solve this problem it is advisable to use the classification of information threats and DoS/ DDoS/DRDoS attacks and mathematical models of the level of impact indicators to work a computer network. This will allow the use of indicators and of coefficients and to establish the degree of influence.

Based on the classification of information threats, prompted a formal mathematical model that is used to determine the influence of each parameter on the threat (Deepthi *et al*., 2015).

Having analyzed classification of DoS/DDoS/ DRDoS of attacks, it is possible to offer the formalized mathematical model which allows defining a level of influence of indexes of attacks on computer networks:

$$\begin{aligned} P_{IT} &= \alpha_i\,(P_{Konf}, P_{Chel}, P_{Dost}) \\ P_{DoS} &= \beta_i\,(P_{Smurf}, P_{Fraggle}, P_{SYNFlood}, P_{DNS}) \\ P_{DDoS} &= \delta_i\,(P_{Trinoo}, P_{TFN/TFN2K}, P_{Stacheldraht}) \\ P_{DRDoS} &= \mu_i\,(P_{Smurf}, P_{Fraggle}, P_{DNS}, P_{SNMP}) \end{aligned} \qquad (1)$$

where,

$\alpha_i, \beta_i, \delta_i, \mu_i$: Weighting coefficients of influence of indexes of DoS, DDoS, DRDoS of attacks

where,

$$\sum_{i=1}^{4}\beta_i = 1,\ \sum_{i=1}^{3}\delta_i = 1,\ \sum_{i=1}^{4}\mu_i = 1$$

The weighting factors determine the contribution of the main types of attacks, DoS/DDoS/DRDoS computer networks and allow these attacks to take into account in the design and operation of information security systems.

By these indexes and coefficients it is possible to define the main types of threats and their influence of the security level of computer networks allowing to design effectively systems of information security taking into account information threats (Savage *et al*., 2000).

To solve the task should use the classification of information threats, DoS/DDoS/DRDoS attacks and formalized models (2) measure the impact on job performance computer network.

This will effectively solve the problem of detecting attacks on computer network access point. Construct formal mathematical models of probability of information threats, DoS/DDoS/DRDoS attacks based on the linear form of the method of weighting coefficients (Li *et al*., 2008):

$$\begin{aligned}
&P\_IT\_\ (P) = \alpha_1 P_{Konf} + \alpha_2\ P_{Chel} + \alpha_3 P_{Dost}\\
&P\_DoS\ (P) = \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS}\\
&P\_DDoS\ (P) = \delta_1 P_{Trinoo} + \delta_2 P_{TFN/TFN2K} + \delta_3 P_{Stacheldraht}\\
&P\_DRDoS\ (P) = \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}
\end{aligned} \tag{2}$$

where,

$P\_IT\_\ (P)$: Probability of information threats

$P\_DoS\ (P)$: Probability of DoS attacks

$P\_DDoS\ (P)$: Probability of DDoS attacks

$P\_DRDoS\ (P)$: Probability of DRDoS attacks

α_i : Weighting coefficients, where $\alpha_i \in [0; 1]$

β_i : Weighting coefficients, where $\beta_i \in [0; 1]$

δ_i : Weighting coefficients, where $\delta_i \in [0; 1]$

μ_i : Weighting coefficients, where $\mu_i \in [0; 1]$

These mathematical model defining the matrix network activity, according to which make conclusions about the realization of attack:

$$\alpha_{IT} = \begin{bmatrix} \alpha_1^a & \alpha_2^a & \alpha_3^a \\ \alpha_1^b & \alpha_2^b & \alpha_3^b \\ \alpha_1^c & \alpha_2^c & \alpha_3^c \\ \alpha_1^d & \alpha_2^d & \alpha_3^d \\ \alpha_1^e & \alpha_2^e & \alpha_3^e \\ \alpha_1^f & \alpha_2^f & \alpha_3^f \\ \alpha_1^g & \alpha_2^g & \alpha_3^g \end{bmatrix}, \beta_{DoS} = \begin{bmatrix} \beta_1^a & \beta_2^a & \beta_3^a & \beta_4^a \\ \beta_1^b & \beta_2^b & \beta_3^b & \beta_4^b \\ \beta_1^c & \beta_2^c & \beta_3^c & \beta_4^c \\ \beta_1^d & \beta_2^d & \beta_3^d & \beta_4^d \\ \beta_1^e & \beta_2^e & \beta_3^e & \beta_4^e \\ \beta_1^f & \beta_2^f & \beta_3^f & \beta_4^f \\ \beta_1^g & \beta_2^g & \beta_3^g & \beta_4^g \end{bmatrix}$$

$$\delta_{DDoS} = \begin{bmatrix} \delta_1^a & \delta_2^a & \delta_3^a \\ \delta_1^b & \delta_2^b & \delta_3^b \\ \delta_1^c & \delta_2^c & \delta_3^c \\ \delta_1^d & \delta_2^d & \delta_3^d \\ \delta_1^e & \delta_2^e & \delta_3^e \\ \delta_1^f & \delta_2^f & \delta_3^f \\ \delta_1^g & \delta_2^g & \delta_3^g \end{bmatrix}, \mu_{DRDoS} = \begin{bmatrix} \mu_1^a & \mu_2^a & \mu_3^a & \mu_4^a \\ \mu_1^b & \mu_2^b & \mu_3^b & \mu_4^b \\ \mu_1^c & \mu_2^c & \mu_3^c & \mu_4^c \\ \mu_1^d & \mu_2^d & \mu_3^d & \mu_4^d \\ \mu_1^e & \mu_2^e & \mu_3^e & \mu_4^e \\ \mu_1^f & \mu_2^f & \mu_3^f & \mu_4^f \\ \mu_1^g & \mu_2^g & \mu_3^g & \mu_4^g \end{bmatrix} \tag{3}$$

These weight factors can be determined by the experimental method. That is, to design architecture of the networks provided in a Fig. 1 and to set intensity of different type of attacks to a network (Bhatia *et al*., 2014).

Thus, having taken total quantity of attacks for 100%, it is possible to define, how many processes will belong to each type of attacks. Then the coefficients will be calculated according to the following equation:

$$\begin{aligned}
&\alpha_1^a = \frac{n_{Конф.}^a}{100\%}, \alpha_2^a = \frac{n_{Цел.}^a}{100\%}, \alpha_3^a = \frac{n_{Дост.}^a}{100\%},\\
&\beta_1^a = \frac{n_{Smurf}^a}{100\%}, \beta_2^a = \frac{n_{Fraggle}^a}{100\%}, \beta_3^a = \frac{n_{SYNFlood}^a}{100\%}, \beta_4^a = \frac{n_{DNS}^a}{100\%},\\
&\delta_1^a = \frac{n_{Trinoo}^a}{100\%}, \delta_2^a = \frac{n_{TFN/TFN2K}^a}{100\%}, \delta_3^a = \frac{n_{Stacheldraht}^a}{100\%},\\
&\mu_1^a = \frac{n_{Smurf}^a}{100\%}, \mu_2^a = \frac{n_{Fraggle}^a}{100\%}, \mu_3^a = \frac{n_{DNS}^a}{100\%}, \mu_4^a = \frac{n_{SNMP}^a}{100\%},
\end{aligned} \tag{4}$$

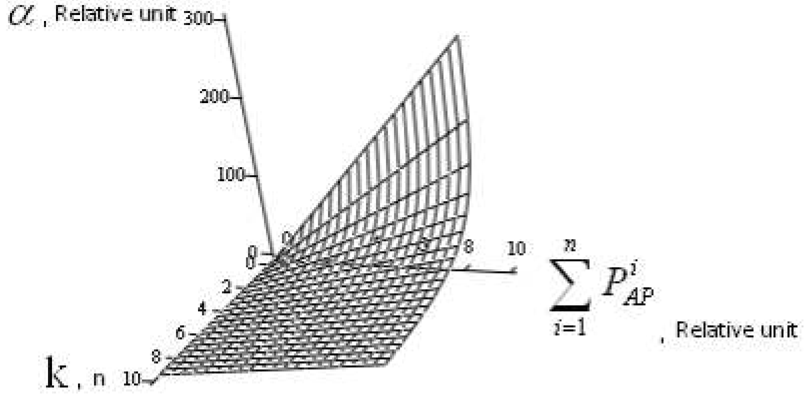

Fig. 1: Dependence of probability weights compromised access points and number of whatever routs:
α: Weighting coefficient; k: The number of paths from the access points to the destination AP to T; n: Number of nodes; $\sum_{i=1}^{n} P_i\, AP$: The total number of probably compromised access points

where,

n^{a}_{DoS} : Quantity of indexes of attacks of a type of DoS to a network of type a)

n^{a}_{DDoS} : Quantity of indexes of attacks of a type of DDoS to a network of type a)

n^{a}_{DRDoS} : Quantity of indexes of attacks of a type of DRDoS to a network of type a)

Similarly also are defined all remaining indexes.

The research has shown that all types of attacks evenly affecting computer network. With increasing probability kinds of attacks the probability of information threats and DoS/DDoS/DRDoS attack increases directly proportional. The denial of service attack has the greatest impact on network performance. But to discern what kind of attack is practically implemented, these models do not allow (Hautio and Weckstrom, 1999).

To determine the types of attack that is implemented, form the mathematical model of communication and customer service, which includes the likelihood compromise node and the number of ways to whatever they access points:

$\alpha_1^{\alpha} = \frac{3}{8}.\frac{1}{k_e^a} = 0.375, \alpha_1^b = \frac{3}{8}.\frac{1}{k_e^b} = 0.15, \alpha_1^c = \frac{3}{8}.\frac{1}{k_e^c} = 0.15,$

$\alpha_1^d = \frac{3}{8}.\frac{1}{k_e^d} = 0.125, \alpha_1^e = \frac{3}{8}.\frac{1}{k_e^e} = 0.15, \alpha_1^f = \frac{3}{8}.\frac{1}{k_e^f} = 0.15,$

$\alpha_1^g = \frac{3}{8}.\frac{1}{k_e^g} = 0.75\ \alpha_2^a = \frac{1}{8}.\frac{1}{k_e^a} = 0.125, \alpha_2^b = \frac{1}{8}.\frac{1}{k_e^b} = 0.05,$

$\alpha_2^c = \frac{1}{8}.\frac{1}{k_e^c} = 0.05\ \alpha_2^d = \frac{1}{8}.\frac{1}{k_e^d} = 0.375, \alpha_2^e = \frac{1}{8}.\frac{1}{k_e^e} = 0.05,$

$\alpha_2^f = \frac{1}{8}.\frac{1}{k_e^f} = 0.05\ \alpha_2^g = \frac{1}{8}.\frac{1}{k_e^g} = 0.0625, \alpha_3^a = \frac{1}{2}.\frac{1}{k_e^a} = 0.5,$

$\alpha_3^b = \frac{1}{2}.\frac{1}{k_e^b} = 0.2\ \alpha_3^c = \frac{1}{2}.\frac{1}{k_e^c} = 0.2, \alpha_3^d = \frac{1}{2}.\frac{1}{k_e^d} = 0.166,$

$\alpha_3^e = \frac{1}{2}.\frac{1}{k_e^e} = 0.2\ \alpha_3^f = \frac{1}{2}.\frac{1}{k_e^f} = 0.2, \alpha_3^g = \frac{1}{2}.\frac{1}{k_e^g} = 0.25$

where,

$\alpha^a{}_i$, $\alpha^b{}_i$, $\alpha^c{}_i$, $\alpha^d{}_i$, $\alpha^e{}_i$, $\alpha^f{}_i$, $\alpha^g{}_i$: Weighting coefficient

a, *b*, *c*, *d*, *e*, *f*, *g*: Model of communication

i : Types of attacks DoS/DDoS/DRDoS

k : Number of possible paths from AP to T

We determine these coefficients by an experimental method, by designing architecture, allowing defining intensity of attacks to a network.

For calculation of coefficients k_e^a, k_e^b, k_e^c, k_e^d, k_e^e, k_e^f, k_e^g we will use a formula (5):

$$k_e = \frac{n_3}{n_e} \tag{5}$$

where,

n_3 : The number of bonds

n_e : The number of components:

$k_e^a = \frac{2}{2} = 1;\ k_e^b = \frac{5}{2} = 2.5;\ k_e^c = \frac{5}{2} = 2.5;\ k_e^d = \frac{6}{2} = 3;\ k_e^e = \frac{5}{2} = 2.5; k_e^e = \frac{5}{2} = 2.5; k_e^g = \frac{4}{2} = 2$

RESULTS AND DISCUSSION

It should be noted that the greatest coefficient the communication model the client-server type d). Therefore it is expedient to use it for ensuring safe transfer of information streams in computer networks.

Here are the results of numerical experiment with the model (5) in graphic form (Fig. 1).

In the illustration: α-weighting coefficient, k-the number of paths from the access points to the destination AP to T, n-number of nodes, $\sum_{i=1}^{n} P_i\, AP$ -the total number of probably compromised access points.

The research have shown that as the number of ways to whatever they can from client to server network activity is low, so the practical realization of attack is difficult to determine. For small values k, the active of network is growing rapidly, the attack is

Table 1:Comparative characteristics of attacks DoS/DDoS/DRDoS, computer network

Type of attack		Route, k Min	Indefinite	Determined	Passing through the compromised node
DoS	Smurf	-	+	-	-
	Fraggle	-	+	-	-
	SYN flood	-	+	-	+
	DNS	-	-	+	-
DDoS	Trinoo	-	+	-	+
	TAN/TF2K	-	-	+	+
	Stacheldraht	-	+	-	+
DRDoS	Smurf	-	+	-	+
	Fraggle	-	+	-	+
	DNS	-	+	-	+
	SNMP	-	+	-	+

determined unambiguously. Level of the compromised nodes has a little impact on network activity in general, since these units do not determine the process routing (Hussain *et al*., 2003).

To distinguish between that attacks was realized, we use Table 1 which analyzed the way to and through compromised node.

It should be noted that the attacks and DNS TAN/TF2K implemented on a specific path, because in a computer network they are easy to detect by analyzing traffic. Traffic activity increases significantly in the implementation of such attacks. In other cases it is difficult to determine the type of threat (Yang *et al*., 2014).

Research have shown that the formal mathematical model of probability information of threats and DoS/DDoS/DRDoS attacks based on the linear form of the method of weighting coefficients do not allow to discern what kind of attack is practically implemented in a computer network, because with increasing probabilities of attack types increases directly proportional probability information of threats and attacks DoS/DDoS/DRDoS.

Dependence of probability weights compromised access points and ways of whatever they have shown that for small values k active network is growing rapidly and clearly defined attack. When increasing the number of ways to whatever they can from the client to the server, practical realization of attack is difficult to determine because of the low activity of the network. Level nodes of compromise have a little impact on network activity in general, since these units do not determine the process routing.

CONCLUSION

On the basis of the presented technique developed the architecture and constructed program realization of system of detection of DoS/DDoS/DRDoS attacks. The developed technique allows obtaining an adequate assessment of the frequency of losses in the network applications if the queuing network is in the stationary mode. At emergence DoS/DDoS/DRDoS attacks knots of networks of mass service leave the stationary mode for some time then 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 of technique and its comparative analysis with other approaches represents a separate task:

- Based on the classification of information threats specific to attacks such as DoS/DDoS/DRDoS is suggested formal model of a linear type of attack to differentiate on the basis of weighting factors. With these parameters and coefficients can define the main types of threats in computer networks to effectively design information protection system based on information threats.
- Are developed matrixes of network activity, with which you can draw conclusions about the implementation of the attack. The analysis of the offered models showed that all types of attacks influence operation of computer networks. With increase in probabilities of varieties of attacks the probability of information threats like DoS/DDoS/DRDoS increases in direct ratio. However, to discern exactly what a particular attack is practically implemented, these models do not allow (Bu *et al*., 2004).
- It is shown that to distinguish an attack it is advisable to take advantage of the proposed method, which examines the way the attack and its passage through the compromised node.
- To determine the type of attack, implemented formulated a mathematical model of communication of client and server that contains the probability of compromised node number of paths from the access points to the destination. Conducted model experiment showed that an increase in the number of paths from the client to the server network activity is low, making it difficult to implement the attack (Aleksander *et al*., 2012).
- Is offered the method probable markings of packets for tracing of attacks to a failure in service in which process of recovery of the message happens in two stages for achievement of high reliability of message passing.
- Are illuminated feasibility of determination of the parameters regulating the volume of the packets transferred on each communication link separately and total amount of packets. Results of computer simulation showed that in time attack promptly increases traffic volume in channels of a network, most of the traffic uses the attack type of DoS/DDoS/DRDoS (Karpinski and Shangytbayeva, 2015).
- Is proved that for the reinforced intensity of attack and increase in a factor of uncertainty the initiator of attacks uses counterfeit packets of other nodes. Therefore it is expedient to carry out the analysis of value of a factor of uncertainty for a resource of computer networks by means of the received ratio.
- To track the source of the attack method developed probabilistic packet marking, in which the recovery process messages in two stages to achieve high reliability of messaging each word (Szczerba and Szczerba, 2012).

REFERENCES

Aleksander, M.A., M.P. Karpinski and U.O. Yatsykovska, 2012. Features of Denial of Service attacks in information systems. Inform. Math. Methods Simul., 2(2): 129-130.

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.

Baba, T. and S. Matsuda, 2002. Tracing network attacks to their sources. IEEE Internet Comput., 6(2): 20-26.

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.

Deepthi, S., K.S. Hemanth, D. Rajesh and M. Kalyani, 2015. A Novel Approach for DDoS Mitigation with Router. Adv. Intel. Sys. Comput., 308: 701-707.

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. (Accessed on: March, 2014)

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.

Karpinski, N. and G. Shangytbayeva, 2015. Architecture and program realization of system of detection of network attacks to denial of service. Proceeding of the International Conference on Global Issues in Multidisciplinary Academic Research (GIMAR, 2015). Dubai, UAE, pp: 55.

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

Savage, S., D. Wetherall, A.R. Karlin and T. Anderson, 2000. Practical network support for IP traceback. Proceeding of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communication (SIGCOMM, 2000), pp: 295-306.

Stone, R., 2000. Centertrack: An IP overlay network for tracking DoS floods. Proceeding of the 9th Conference on USENIX Security Symposium, 9: 15.

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., pp: 68-70.

Yang, Z.X., X.L. Qin, W.R. Li and Y.J. Yang, 2014. A DDoS detection approach based on CNN in cloud computing. Appl. Mech. Mater., 513-517: 579-584.