International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 4(April 2013), PP.17-21
www.irjes.com

Provide a way to deal with SYN-Flooding Attacks in Next Generation Networks

Razieh malekhoseini[1], mohammad mosleh[2]
[1]*(MS Student of computer engineering , Islamic Azad university of Dezful, Dezful , Iran)*
[2]*(The faculty member of computer engineering , Islamic Azad university of Dezful, Dezful, Iran)*

ABSTRACT : *Next generation networks(NGN) are as a new structure for information networks and communication systems that need to research and investigation in several aspects such as quality of service (QOS), global access and most important, security and reliability time to full set up. in spite of creation of facilities for users and resolve of problems in previous technologies by emerging of new technologies and informations have new vulnearabilities. That we should know them throughout different aspect of investigations such as design, implementation and then counter them. Not only next generation network fallow this rule as a new structure in communication aspects, but also because of transmission of some basic technologies, some of the vulnearabilities in current networks transfer to them. Based on default standards of ITU-T, IPV6 is one of the basic protocols in next generation network. This protocol although is able to resolve some relative limits about buffer problems, but now is as a vulnearability point for creation of some attacks, such as denial of service(DOS) in next generation network. SYN flooding attack is one of the serious type of DOS attacks, that a network attacker by using it create a huge damage. In this thesis for defense of a victim system we carry out modeling by using of hybrid mechanism composed of filtering approach that based on number of SYN/FIN packet and simple queuing model for investigation half open connection which remain in system exceed of threshold time. Then by using of PSO algorithm in opnet software, simulate model. For prove performance we compare results of proposed approach with previous related work based on rejection probability, buffer usage, attack buffer usage, average active time and attack average active time Parameters , then present results by using tables and plots formats.*

Keywords : *Next Generation Network, security vulnearability, attack, victim, attacker, denial of service, SYN-Flooding Attack*

I. INTRODUCTION

The Next Generation Networks that also called next generation networks architecture is a general term that is used for certain type of structures and computer network technology. from an overall perspective the next generation networks, are including networks that normal have been the voice and data communications and also optionally may be include additional media such as video.

however, it should be noted that the NGN will not replace the existing network, but gradually the current network capabilities will developed to create new capital to the convergence of voice and data. for the transition of today's networks to the new network structure it is essential to minimize the required investment strategy in order to use a suitable strategy along with the benefits using of NGN structure. However, each step must be taken which lead to the structure of NGN. Next generation networks are based on internet technology, including proprietary protocols such as internet protocol (IPV6) and MPLS. According to the 2005 official ITU-T next generation networks can be defined as follows:

next generation networks are packet based network that can be able to provide telecom services and also have the ability to deploy multiple broad band and transmission technology with ensuring quality of service, so the dependent functions on network services and technology related functions of the transport layer are independent[8]. Despite the increasing use of IP protocol in telecommunication networks and changing of the protocol to a standard communication protocols, this protocol doesn’t still guarantee the quality of service. The IPV6 addressed some security issues as well as quality of service, but it still remained as a problem. On the other hand, one of the most important feature of the IP protocol is independency of it to the layer protocol, that it is highly affected on the feature of global communication networks. So this protocol provide an independent association of the protocol sub- layer networks such as PSTN, ATM, Frame Relay and also provide a broadband access, such as ADSL, which include various on- line application. Despite all the facilities that IP protocol provides, specially IPV6, but because of the using of algorithm 3-way handshaking, is still a potential development of some attacks such as SYN Flooding attack. SYN Flooding attack has a significant harmfulness effects, so it has attracted many researchers, and it is refferd to as a serious threat.

SYN Flooding attack uses the lack of TCP protocol in order to provide the communication between two computers. Communication process in TCP protocol uses a mechanism called 3-way handshaking algorithm. In this algorithm starter the connection(source) sends a SYN packet to the destination and the destination by receiving the packet, put it in backlog buffer line and create a half open connection and in response send a SYN-ACK packet to SYN packet in source. If the source responses to the sent packet by sending a packet of ACK, the half open connection ends and the resources allocated to it is released and the connection between the source and destination is established. But if there source IP address be spoofed the packet which way sent will remain unanswerable. So the half open connection will remain untill ends by the destination.

This mode of communication has weaknesses that uses by the attacker of SYN Flooding attacks for occupying system resources. Thus, the attacker sends SYN packets with spoofed IP addresses, and SYN- ACK packets from destination are sent to the same spoofed IP addresses. So the half open connections is created and will remain until end by the destination. It is clear after the number of half open connections reached to the maximum number of half connections that the system can provide, the system would be unable to accept new connections and provide service to other users.

II. RELATED WORK

In recent years, extensive research has been conducted on countering to these attacks that some of them are mentioned in the following.

Wang and colleagus in 2003 tried to detect SYN flooding attacks by using of SYN and SYN/ ack packets in the TCP protected header.

Genelatakis in 2005 by using of signature- based approach attempted to detect SYN flooding attacks.

In 2007 ehlertos used an upgrade of the DADD for SYN flooding attacks related to DNS cache.

See in [17] use the analysis of traffic rate(TRA) for modeling of the rate of TCP flags. TCP flag rate is a measurement of the proportion of the packets to the total number of TCP packet with chosen set flags. Additionally, they use the rate of protocol. The rate of protocol is a measure of the proportion of packets in a selected protocol to the total input packets. Ten features were considered in this analysis and separately normal packets models for attack packets as a series of SVM.

Attacka as DOS, DDOS, DRDOS are labeled according to the class. Dr jamali in 2011 has achieved beneficial results by identifying SYN flooding attacks and by using particle swarm optimization algorithm.

III. THE PROPOSED ALGORITHM

In this paper by considering of the topology of the network, we began to launch a SYN flooding attack. Then in order to evaluate the proposed method, we use filtering based on SYN and FIN packets and then by using particle swarm algorithm in opnet simulation environment, and we will present the result in the form of tables & graphs. Filtering model based on comparing the number of SYN and FIN in the TCP protocol flags is as follows. Based on the definition of communication and using of TCP protocol there should be relative agreemented between the different flags.

Obviously, the observed differences in these features indicate an abnormal behavior or the occurrence of an attack. For example based on the work proposed by wang[15, 41] the huge difference between the number of SYN and FIN packets on the TCP flags showing the SYN- flooding attack. Although this weakness has long been recognized, but still is used by the attacker to disable a service. Therefore this work based on the number of SYN and FIN packet on TCP packets identify some attacks and will waste the marked packets as an attack packet. In the second part of the algorithm of the queuing modeling and by considering of the following parameters we perform a suitable approach for the method based on particle swarm optimization algorithm (PSO).

- Statistical characteristics of incoming requests
- Queue capacity and parameters for behavioral analysis

- Statistical characteristics of incoming requests

In this study we use Statistical distributions to investigate the behavior of the system under SYN flooding attacks and for packets arrival rate for normal and attack packets.

Based on proposal on the paper [24], we consider regular arrival rate of packets to the target system, the poisson distribution with rate average that k is the strinking of the attack packets to the normal packets. For the maintain half open communications in regular request we use exponential distribution with mean µ. It should be noted half open communications of attacking packets is retained as long as h.

-Queue capacity and parameters for behavioral analysis

In this queuing system, the queue length is equal to the maximum number of half open connections that the system can make . if there an free space in queue, legal application and attack with respect to statistical distributions and by making a half open relationship, take in queue and enter to the system.

However, if the queue is full, the request s will be blocked. Based on the proposed algorithm and for different values of h and m we simulate the system behavior. We define the objective function by the following proposed parameters.

The probability of packet loss(rejection prob): a packet is blocked when the server can not response to received request to create contact because of the buffer filtering. So, rejection prob are defined as the number of packets blocked to the total number of imported packets to the server.

Regular request buffer occupancy percentage (RRBOP): after the setting up of half open connection, if possible, a buffer is allocated it. We define the average ratio number of half open connections created by normal requests to the maximum number of half open connection thet the server can provide[13].

Attack request buffer occupancy percentage (ARBOP):

This parameter defined as the average ratio number of half open connections created by attackes requests to the maximum number of half open connections that the server can provide[13]. The objective function by using these parameters reduces to the following:

- Decrease the loss rate request
- Increases the percentage and time of buffer accupancy by the legitimate requests.

IV. TOPOLOGY USED IN THE SIMULATION

In simulation in order to demonstrate the performance of proposed algorithm the following scenarios is made and their results can be compared with each other. Figure 1 shows the topology used in the simulation.

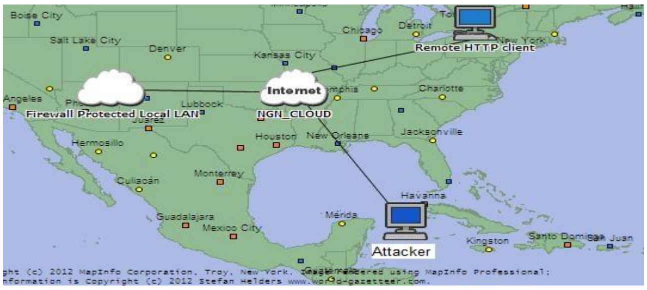


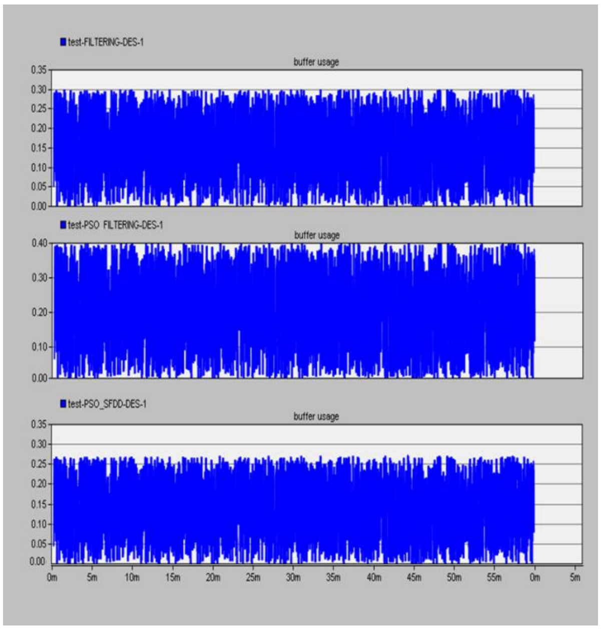
fig1:topology in simulation

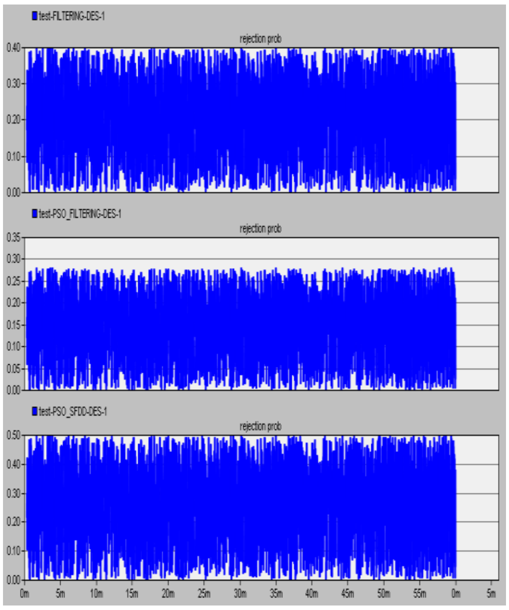
- Scenario1: the arrival rate of the attack requests is lower than the arrival rate of legal requests.
- Scenario2: the arrival rate of attack requests change accidentally during the attack.

In both scenarios, by comparing of the proposed method (PSO-Filtering) and pervious method (PSO-SFDD) a method which use the PSO algorithm, graphs and tables of simulation is presented.

Scenario1: the arrival rate of the attack requests is lower than the arrival rate of legal requests (k=0.1):

The purpose of this Scenario is to show the state of system in case of arrival rate of attack requests is much less than arrival rate of legitimate requests.





The probability of blocking requests(k=0.1) Percentage of the buffer occupied by regular requests(k=0.1)
fig2: arrival rate of attack requests(k=0.1)

TABLE 1: the result of the simulation in terms(k=0.1)

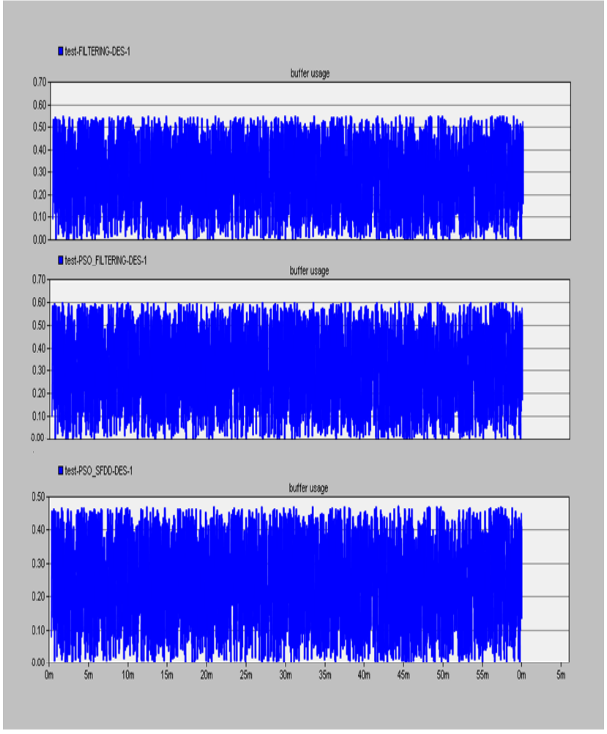
criteria	PSO_SFDD	PSO_SFDD_Filtering
The probability of blocking requests	0.48	0.28
Percentage of the buffer occupied by regular requests	27%	%38
Percentage of the buffer occupied by attack requests	58%	%29

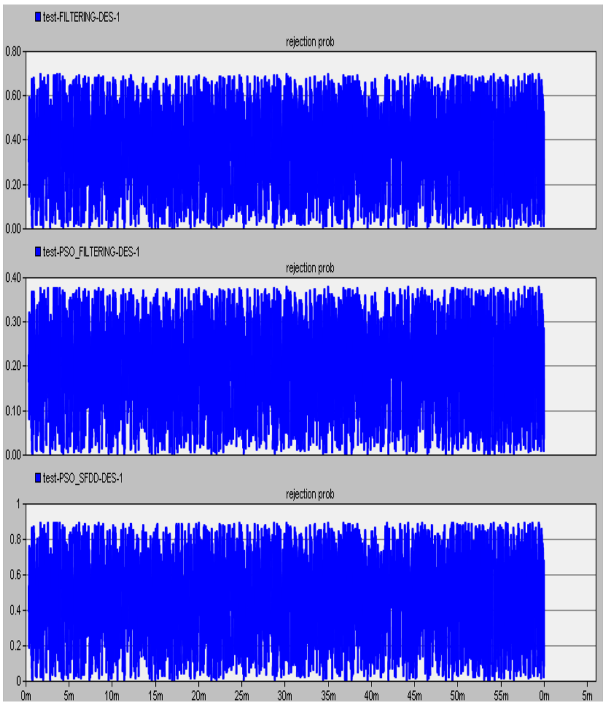
A conclusion section must be included and should indicate clearly the advantages, limitations, and possible applications of the paper. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extentions.

Consistant with the values obtained from table1 we can conclude that, PSO_SFDD_Filtering algorithm with further improve in the parameters listed in any amount, may requests blocking with 17% efficiency improved, Percentage of the buffer occupied by regular requests with 14% efficiency improved and Percentage of the buffer occupied by attack requests with 20% efficiency improved has provided a better process for impact and reduce the impact of deny service attacks in type of SYN- flooding.

Scenario2: the arrival rate of attack requests change accidentally during the attack

The purpose of this Scenario is to show the state of system in case of arrival rate of attack requests change accidentally during the attack by k=[0,2].





The probabilitof blocking requests (k=[0,2])

Percentage of the buffer occupied by regular requests(k=[0,2])

Fig3: arrival rate of attack requests((k=[0,2])
TABLE2: THE RESULTS OF THE SIMULATION IN TERMS(K=[0,2])

criteria	PSO_SFDD	PSO_SFDD_Filtering
The probability of blocking requests	0.88	0.38
Percentage of the buffer occupied by regular requests	47%	%59
Percentage of the buffer occupied by attack requests	82%	%53

Consistant with the values obtained from table2 we can conclude that, PSO_SFDD_Filtering algorithm with further improve in the parameters listed in any amount, may requests blocking with 23% efficiency improved, Percentage of the buffer occupied by regular requests with 12% efficiency improved and   Percentage of the buffer occupied by attack requests with 15% efficiency improved has provided a better process for impact and reduce the impact of deny service attacks in type of SYN- flooding.

V. Conclusions

In this paper a new method (PSO_SFDD_Filtering) for prevention of SYN-Flooding attack is proposed. Simulations demonstrate that our system is effective facing attack.

REFERENCES

[1] ITUT Rec. Y.2001, General Overview of NGN.

[2] ITUT,Rec. Y.2011, General Principles and General Reference Model for Next Generation Networks.

[3] ND1612 Generic IP Connectivity for PSTN/ISDN/PSDN Service between UK Next Generation Networks ,2009

[4] M. Roesch, Snort – lightweight intrusion detection for networks, 13th USENIX Large Installation System Administration Conference (LISA ’99), Seattle, USA,1999, pp.229–238.

[5] N. Carugi, B. Hirschman, A. Narita, Introduction to the ITUT NGN Focus Group Release 1: Target Environment, Services, and Capabilities”, IEEE Communications Magazine, 2005, pp. 4248.

[6] H.Wang, , D.Zhang, , KG .Shin,, Detecting SYN flooding attacks, in: Proceedings of IEEE INFOCOM. 2002,pp.1-26.

[8] S.Atay, M. Masera, Challenges for the security analysis of Next Generation Networks,TUBITAK under Grant of Bideb2219 post-Doctorate Research Fellowship, 2008.

[9] J.Kennedy, R.Eberhart, ,Particle swarm optimization, Proc. IEEE Int.Conf. Neural Networks, 1995,pp.1942-1948.

[10] Y.Okada, Y.Nishikawa, DoS attack countermeasures in NGN using private security policy, APSITT, 2010, pp.123-129.

[13] SH.Jamali, ,GH. Shaker, defence against SYN Flooding Attacks By Employing PSO Algorithm. Compouter and mathematics with application, Elsevier, 2011,pp.214-221

[14] D.Geneiatakis, T.Dagiuklas, G.,Kambourakis, C.Lambrinoudakis, S.Gritzalis,S.Ehlert, D.Sisalem, , Survey of security vulnerabilities in session initiation protocol, IEEE Communications, Surveys and Tutorials, vol.8, No. 3, 2006,pp. 68-81.

[15] R.Lee, D.Karig, P.McGregor, Z.Shi, Enlisting Hardware Architecture to Thwart Malicious Code Injection”, Proceedings of the International Conference on Security in Pervasive Computing (SPC-2003), LNCS 2802, 2003,pp. 237-252.

[16] D.Mankins, R. Krishnan, C. Boyd,J. Zao, M. Frentz, Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing, Computer Security Applications Conference. ACSAC 2001. Proceedings 17th Annual,2001, pp. 411-421.

[17] D.Zagar, K. Grigc, IPV6 security threats and possible solutions, WAC 2006, 2006,pp. 1-7.