SYN flooding Attack countermeasures in Next Generation Network

Razieh malekhoseini[1], Malekhoseini.r@gmail.com
Department of computer Engineering, yasouj branch
Islamic azad university of yasouj, yasouj, iran

Navab malekhoseini[2], navab.malek@yahoo.com
Department of computer Engineering, yasouj branch
Islamic azad university of yasouj, yasouj, iran

Abstract— **this paper propose countermeasures against syn flooding attack in the Next Generation Network (NGN), Applying a filtering and PSO algorithm to IP packets flowing from internet in to NGN. IP packets are checked and abnormal packets for syn flooding attack are detected at the internal router, then filter source IP address by security policy that is set in the firewall.**
In syn flooding attack some sources send a large number of TCP segments, without completing the third handshaking step to quickly exhaust connection resources of the under attack system or victim. After filtering mechanism, number of packets that have not detected, the victim by using queuing mechanism in which attack requests are recognized based on long service time. paper proposes a framework in which the defense issue is formulated as an optimization problem and employ filtering mechanism based on number of SYN/RST segment and particle swarm optimization(PSO) algorithm to optimally solve this problem. Finally by using opnet simulator, simulation results show that the proposed defense strategy improves the performance of the victim in term of efficient consumption of buffer space by attack & regular request.

Keywords-component; NGN; Denial of Service (DOS) Attack ;SYN Flooding; PSO, victim

Introduction

The internet has become an infrastructure that supports the basis of our highly networked information society. Moreover it has brought convenience to the lives of people and has infilterated general life deeply. However unlawful computer access from the internet by malicious users in still a serious threat. When telecommunication carries in the world proviced connection services to the internet from the Next Generation Network (NGN), the NGN Face similar threats. In this paper we propose mechanism against one type of Denial Of Service(DOS) attack , namely, SYN flooding in the NGN. DOS attack aim at obstructing regular service provisioning by systematically exhausting network and server resources. In flooding DOS attack, malicious users (attacker) send a large number of requests such that requests of legitimate users can not be efficiently handled as designated. Syn flooding is one of the most serious flooding DOS attack , that it is transport layer DOS attack. SYN attack exploits 3-way handshaking mechanism, that TCP connection use to establish a connection. When a client effort to start a TCP connection to another system, first, the client requests a connection by sending a SYN packet to system. Then in the second step of 3-way handshaking mechanism system returns a SYN-ACK packet to client. At the end of algorithm, client sends ACK packet to for replying or client acknowledgment the SYN-ACK packet. Finally connection established and data transfer commences. Fig 1 shows 3-way handshaking mechanism for establishing connection.

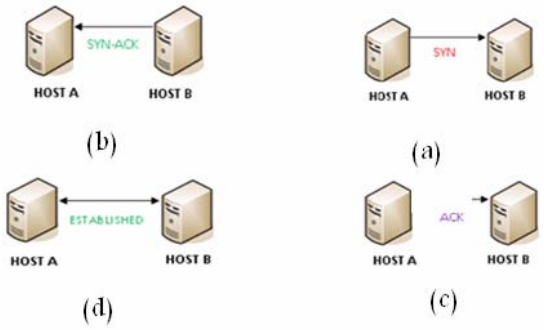

Fig1: 3-way handshaking mechanism

In the syn flooding attack, attacker use this mechanism to their benefit. The attacker sends a large number of syn packets to the victim. Victim must be answer with them by sending a SYN-ACK packet. When victim sends SYN-ACK packet to the client, really it allocate some of the buffer space. On the other hand it create a half open connection for it, and wait to receive ACK packet from it. Since resource of any system is limited, then, there are a limited number of connections a system can control. Once all of these are in use, waiting for connections that will never come, no new connection can be made whether valid or not. When system can not control new connections, any application that tries to establish TCP connections with this system fails in its attempt. there are some proposed defense for this attack.

I. RELATED WORK

protection mechanism that assure availability remain a difficult challenge for next generation network. Attack can come from a single source or many sources in distributed DOS(DDOS). They can occur at data link, network, transport, or application layers. They can be sudden or dramatic or gradual and subtle. Most network protocol were design without DOS protection and vulnearable by design. An example of an attack that attempt to exploit the resource allocation logic of the target(smith,2007)(i.e, a semantic attack) is the syn flood attack(peng et al, 2007) whereby the attacker sends a large number of TCP SYN Packets with a forged source address. Since the target will never receive ACK

packets to complete TCP handshakes, its operating system will eventually exhaust all possible available connections, therefore, preventing valid TCP-based services to start. DOS attack detection consist of either the identification of behavioral changes in peers(anomaly- based detection(Hussain et al., 2003; Mirkovic and Reiher, 2005)). Most machine learning and signal processing techniques could be applied for this purpose, such as neural networks (jalili et al., 2005), neuro fuzzy inference(he et al., 2005), radial basis functions(Gavrilis and Dermats, 2005), Genetic algorithms(Gavrilis et al., 2004), statistical signal analysis(Li et al., 2004; li., 2004; Xiang et al.,2004; Gu et al., 2005; Kulkarni and Bush., 2006; Hussain et al., 2004), Particle Swarm Optimization Algorithms(Jamali, sh., Shaker, GH.,2011) and wavelets(Li and Lee, 2005; yang et al., 2004).
All theses related works are valuable and researchers can use them for detection or/and prevention DOS attacks, specially SYN flooding attacks.

II. SYN/RST FILTERING MECHANISM

The mechanism of filtering operations are as follows:
1 - The number of SYN and RST packets to the TCP protocol
2 - disposal of non-normal traffic
The Internal router using a network analyzer to count the number of SYN packets and TCP RST flag-related charges. By comparing the obtained value and threshold value normal and abnormal traffic is detected from each other. Obviously, the observed value is greater than the threshold showing abnormal behavior or attack the network. if it detects an attack packet is discarded And half open connections from the IP address is terminated.
One of the most resources in the system is buffer or memory. In SYN flooding attack basic aim is consumption of buffer. Here we use proposed algorithm by two step. first, filtering attack packets based on number of SYN/RST segment, second we use queuing mechanism to present the defense map against SYN flooding attack. In this part our assumption is that, all connection requests share the same backlog buffer. When a request arrives the system, enter a buffer space of a backlog queue up on finding an inactive buffer space and if backlog queue is full this request is block. Now we assume any request can held for a limit period of time h, and m connection concurrent as half open connection are allowed. We must be have definite rules or limitation about h&m parameters for regular and attack requests.

A. Particle Swarm Optimization Algorithm

PSO employ for optimizing difficult numerical functions and based on metaphore of human social interaction, is able to process knowledge[8,9].

B. Pparticle structure of the problem

One of the most resources in the system is buffer or memory. In SYN flooding attack basic aim is consumption of buffer. Here we use proposed algorithm by two step. first, filtering attack packets based on number of SYN/RST segment, second we use queuing mechanism to present the defense map against SYN flooding attack. In this part our assumption is that, all connection requests share the same backlog buffer. When a request arrives the system, enter a buffer space of a backlog queue up on finding an inactive buffer space and if backlog queue is full this request is block. Now we assume any request can held for a limit period of time h, and m connection concurrent as half open connection are allowed. We must be have definite rules or limitation about h&m parameters for regular and attack requests.
Assumptions:

1- Regular request packets is held by exponentially distributed with parameter μ.

2- Arrivals of the regular and attack request packets are both poission process with rate $\lambda 1$ and $\lambda 2$, respectively

When victim under syn flooding attack , half open connection quickly consume all the backlog buffer and prevent which from further accepting new requests. H and m as its design parameters and employ the PSO algorithm particle. To defense against SYN Flooding attack our proposed mechanism must try to minimize number of lost connection and allocating buffer space to attack request
connections[13]. for this purpose we define these parameters:

1- Rejection prob
2- Buffer Usage
3- Attack Buffer Usage
4- Average active time
5- Attack Average Active Time

III. IMPLEMENTION AND SIMULATION RESULTS

The performance of the proposed mechanism was evaluated by using network simulator opnet 14.5. network topology for simulation was composed of a LAN, NGN and the internet which is shown in fig2. There are one FTP server, one custome application server and one remote login server that a regular user and attacker use them. The bandwidth of the access line between NGN and LAN was 10 mbps, and that of both internet and NGN was much broader 10 mbps.

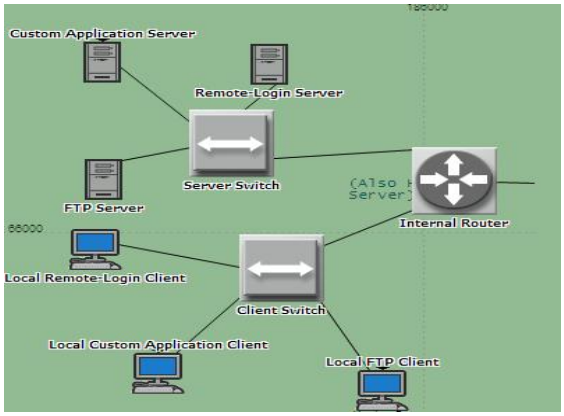

Figure 2: LAN topology

Filtering mechanism uses internal router to detect anomaly traffic by using comparing number of SYN and RST packets. By default number of SYN packets must be equal to number of RST packets. Then observing anomaly deference between them, indicate that anomaly traffic is occurred. Then queuing model process arrival packets to the LAN by using PSO algorithm, according default flowchart, which is shown in below[13].

1. Start
2. Initializing variable
3. Evaluate Objective function
4. If new objective function > best objective function then

   4.1 if new objective function> old objective function then

   4.1.1 use old h,m

   Else Evaluate new h,m

   Else Evaluate new h,m
5. Evaluate velocity and location h,m for next step
6. Set h,m for half connection(new and next steps)
7. If parameters are not suitable then go to step 3

8. End

Now consider a simulation by running four scenarios.
First scenario: arrival rate of attack requests equal to arrival rate of regular requests (k=1):
The aim of this scenario is simulation proposed algorithm (PSO_SFDD_Filtering) and prior related work (PSO_SFDD algorithm) by using same number of attack requests and regular requests under attack condition.
After run simulation we get these results:

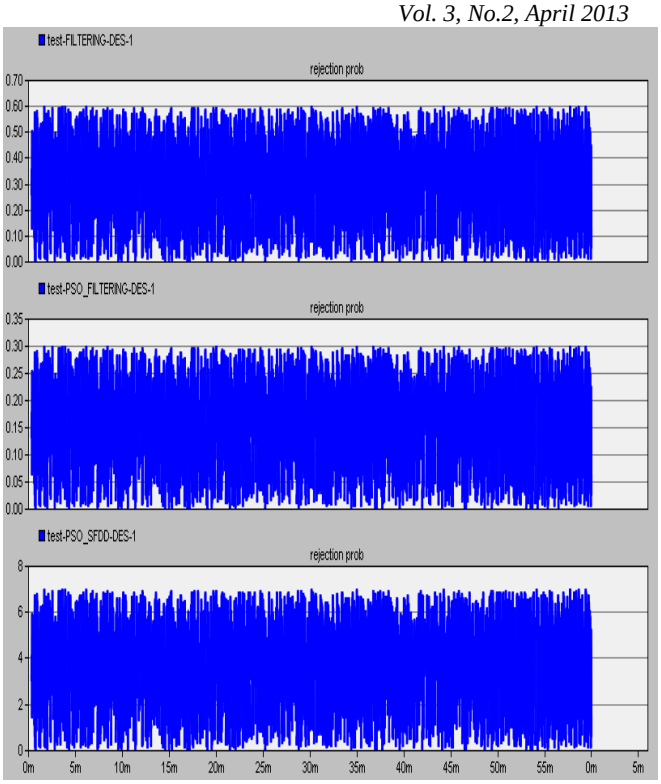

Figure 4: Rejection probability of requests(k=1)

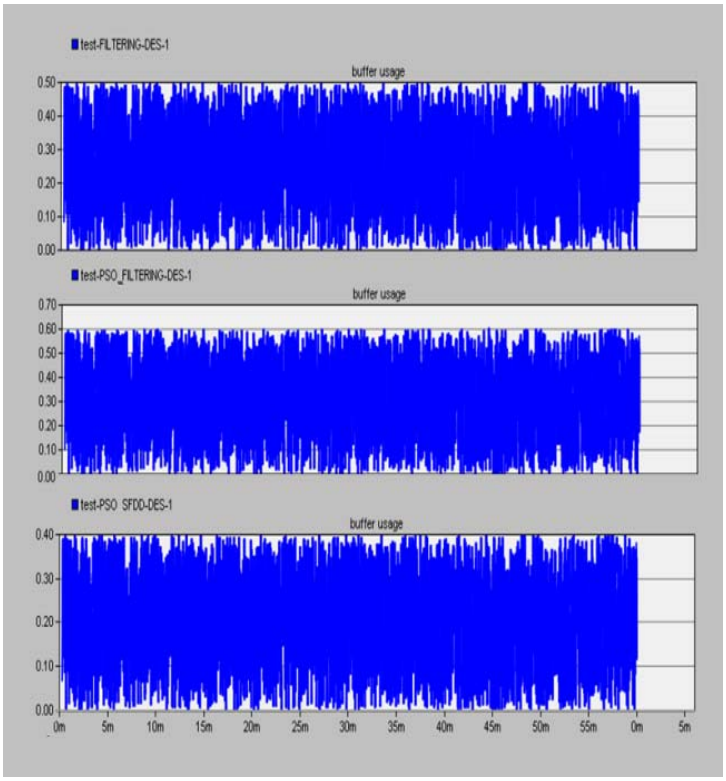

Figure5: Percentage of Buffer Usage(k=1)

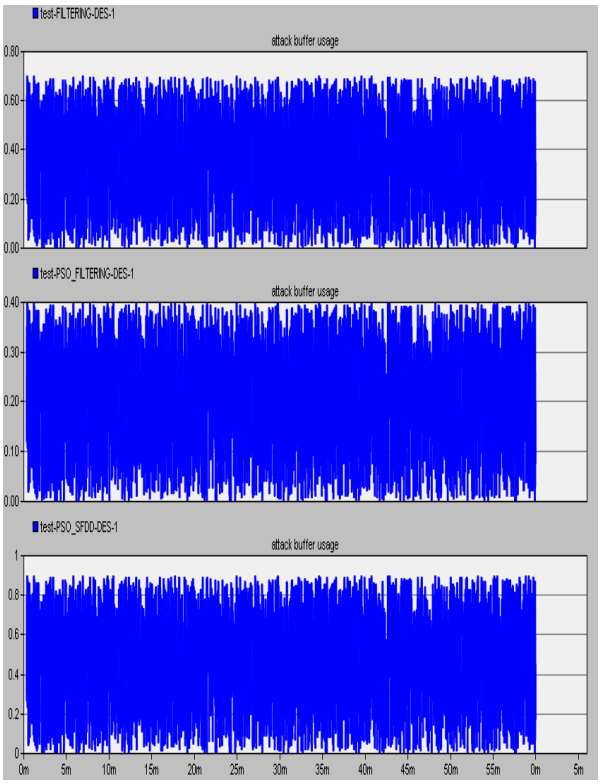

Figure6: Percentage of Attack Buffer Usage(k=1)

TABLE1: result values for First scenario(k=1)

Criteria	PSO_SFDD	PSO_SFDD_Filtering
Rejection probability of requests	0.7	0.3
Percentage of Buffer Usage	%39	%60
Percentage of Attack Buffer Usage	%85	%39

According to the value from table2, we can conclude PSO_SFDD_Filtering algorithm has good performance than PSO_SFDD algorithm . In our proposed algorithm (PSO_SFDD_Filtering) , Rejection probability of requests has 20% improvement, Buffer Usage has 15% improvement and Attack Buffer Usage parameter has 21% improvement than PSO_SFDD algorithm.

Second scenario: variable attack density (k=[0,2]):

In this scenario, we simulate proposed algorithm (PSO_SFDD_Filtering) and PSO_SFDD approach with test random arrival rate for attack request under attack condition, then we set k parameter by uniform distribution in range of [0,2].

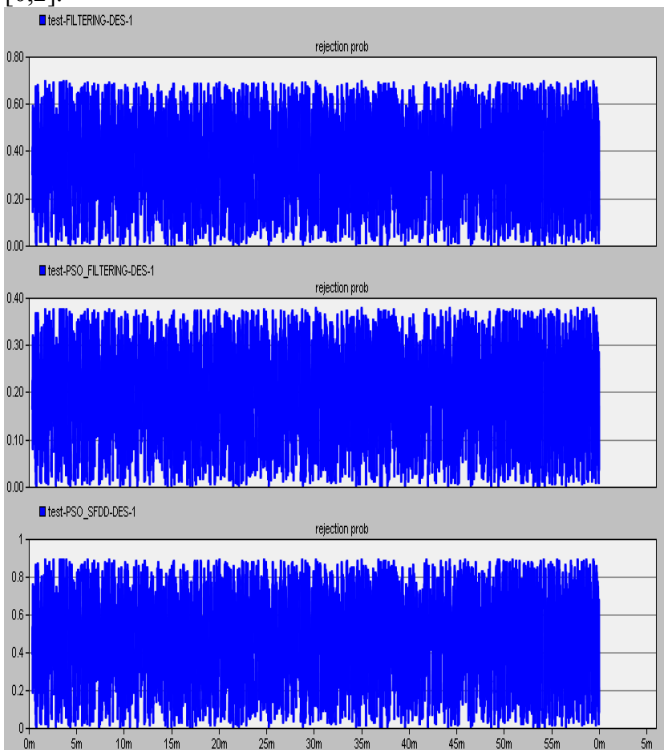

Figure7: Rejection probability of requests(k=[0,2])

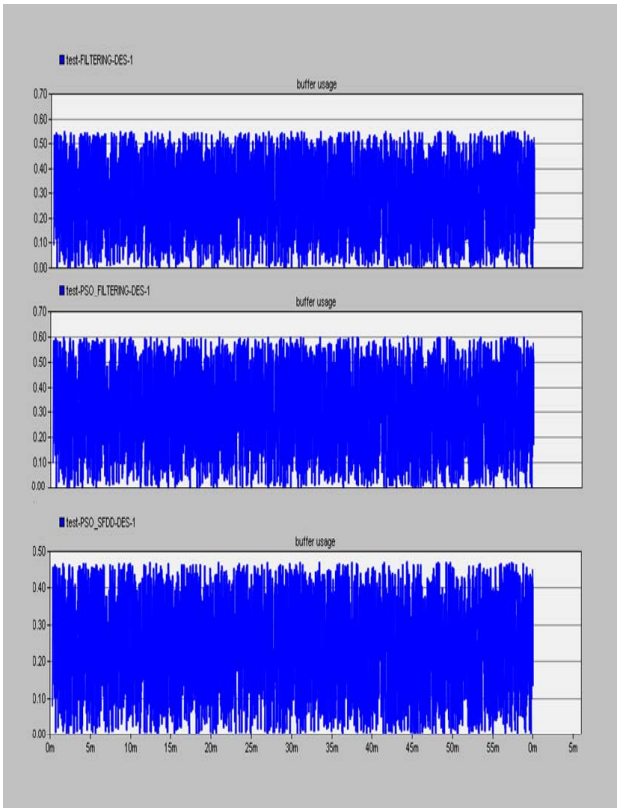

Figure8: Percentage of Buffer Usage(k=[0,2])

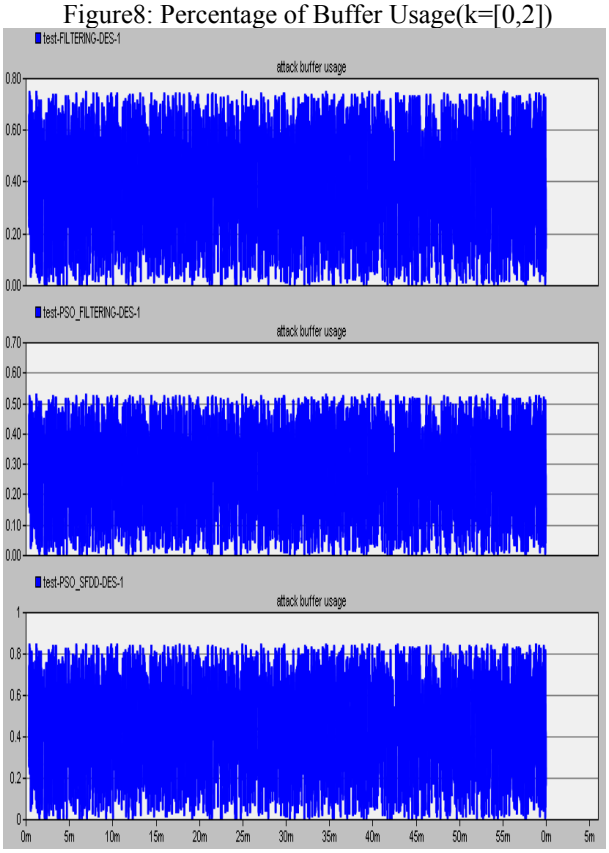

Figure9: Percentage of Attack Buffer Usage(k=[0,2])

TABLE2: result values for First scenario (k=[0,2])

Criteria	PSO_SFDD	PSO_SFDD_Filtering
Rejection probability of requests	0.88	0.38
Percentage of Buffer Usage	%47	%59
Percentage of Attack Buffer Usage	%82	%53

According to the value from table2, we can conclude PSO_SFDD_Filtering algorithm has good performance than PSO_SFDD algorithm []. In our proposed algorithm (PSO_SFDD_Filtering) , Rejection probability of requests has 23% improvement, Buffer Usage has 12% improvement and Attack Buffer Usage parameter has 15% improvement than PSO_SFDD algorithm.

Third scenario: arrival rate of attack requests lower than arrival rate of regular requests (k=0.1):
The purpose of this scenario is to demonstrate the system at the arrival rate of requests arrival rate of requests for legal attack, much less. results of the scenarios in Figures 10 to 12 and is shown in Table 3.

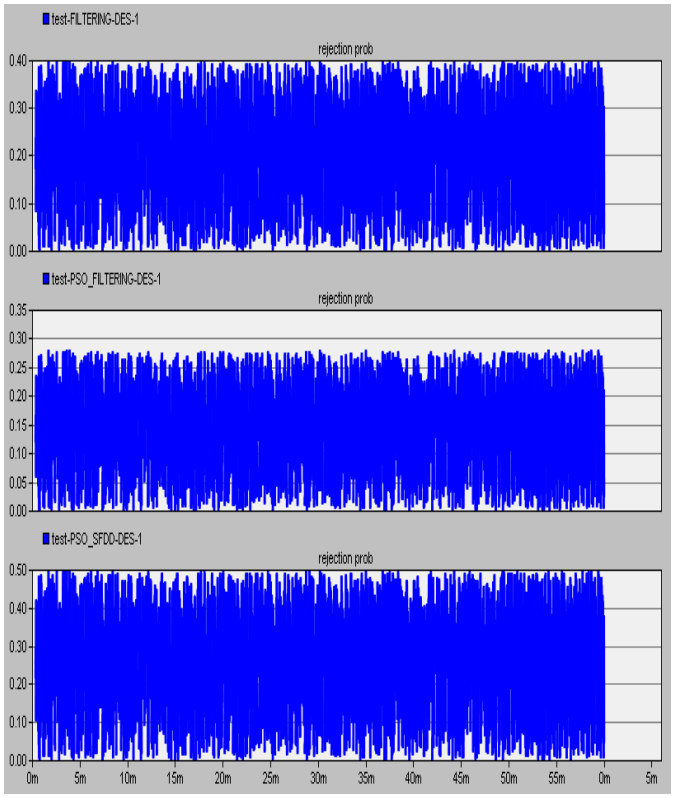

Figure10: Rejection probability of requests(k=0.1)

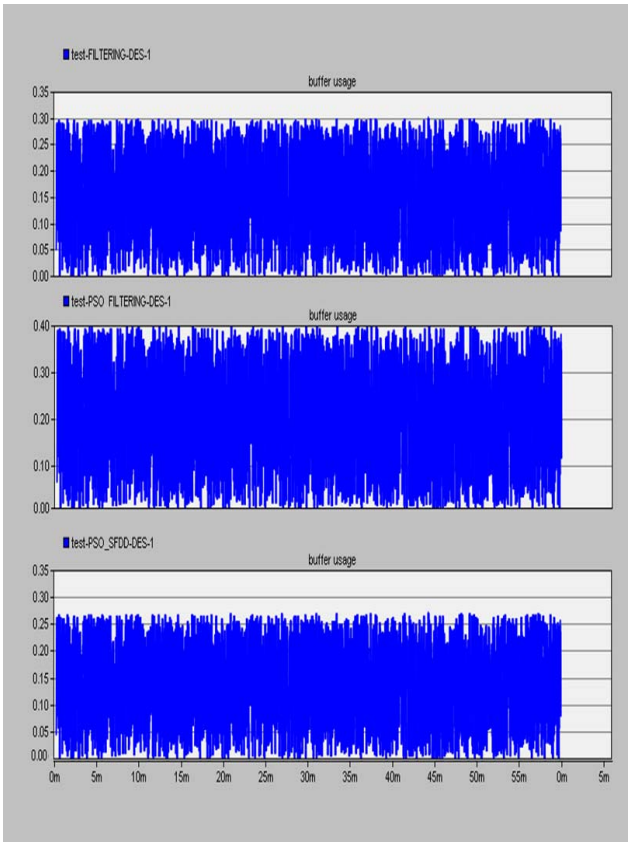

Figure11: Percentage of Buffer Usage(k=0.1)

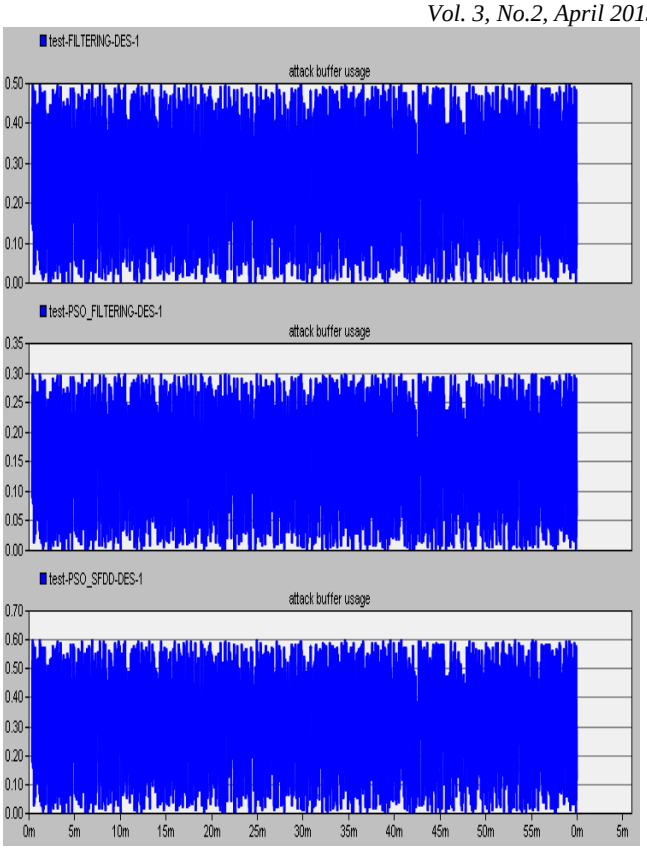

Figure12: Percentage of Attack Buffer Usage(k=0.1)

TABLE3: result values for First scenario (k=0.1)

Criteria	PSO_SFDD	PSO_SFDD_Filtering
Rejection probability of requests	0.48	0.28
Percentage of Buffer Usage	%27	%38
Percentage of Attack Buffer Usage	%58	%29

According to the value from table3, we can conclude PSO_SFDD_Filtering algorithm has good performance than PSO_SFDD algorithm . In our proposed algorithm (PSO_SFDD_Filtering) , Rejection probability of requests has 17% improvement, Buffer Usage has 14% improvement and Attack Buffer Usage parameter has 20% improvement than PSO_SFDD algorithm.

IV. CONCLUSION

Next generation network protocol TCP / IP and IPV6 Internet Protocol is vulnerable to attacks and weaknesses of the protocol used to launch an attack SYN-Flooding is a series of denial of service attacks. The attack is the historical background of the current network has suffered a lot of damage. In this paper a new method (PSO_SFDD_Filtering) for prevention of SYN-Flooding attack based on hybrid approach 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, , 1999, Snort – lightweight intrusion detection for networks, 13th USENIX Large Installation System Administration Conference (LISA '99), Seattle, USA, pp.229–238.
[5] N. Carugi, B. Hirschman, A. Narita, 2005, Introduction to the ITUT NGN Focus Group Release 1: Target Environment, Services, and Capabilities", IEEE Communications Magazine, pp. 4248.
[6] H.Wang, D.Zhang, KG.Shin,,2002, Detecting SYN flooding attacks, in: Proceedings of IEEE INFOCOM. pp.1-26.
[8] S.Atay, M. Masera., 2008, Challenges for the security analysis of Next Generation Networks, TUBITAK under Grant of Bideb2219 post-Doctorate Research Fellowship.
[9] J.Kennedy, R.Eberhart, 1995,Particle swarm optimization, Proc. IEEE Int.Conf. Neural Networks, pp.1942-1948.
[10] Y.Okada, Y.Nishikawa, 2010, DoS attack countermeasures in NGN using private security policy, APSITT,pp.123-129.
[13] sh.Jamali, GH.Shaker, 2011, defense against SYN Flooding Attacks By Employing PSO Algorithm. Compouter and mathematics with application, Elsevier,pp.214-221.
[14] D.Geneiatakis, T.Dagiuklas, G.,Kambourakis, C. Lambrinoudakis, S.Gritzalis, S.Ehlert, , D.Sisalem, , 2006, Survey of security vulnerabilities in session initiation protocol, IEEE Communications, Surveys and Tutorials, vol.8, No. 3, pp. 68-81.
[15] R .Lee, D.Karig , McGregor, P.,Shi, Z.,2003,Enlisting Hardware Architecture to Thwart Malicious Code Injection", Proceedings of the International Conference on Security in Pervasive Computing (SPC-2003), LNCS 2802, pp. 237-252.
[16] D.Mankins, R.Krishnan, C.Boyd , J.Zao , M.Frentz, 2001,Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing, Computer Security Applications Conference. ACSAC 2001. Proceedings 17th Annual, pp. 411-421.
[17] D.Zagar, K.Grigc, 2006, IPV6 security threats and possible solutions, WAC 2006, pp. 1-7.
[18]Hussain.A,Heidemann.J, Papadopoulos.C. A framework for classifying denial of service attacks. In: SIGCOMM'03:Proceeding of 2003 conference on applications, technologies, architectures and protocols for computer communications; 2003. P.99-110