International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 3, Issue 2 (February 2014), PP.10-15

SYN-Flooding Attack detecting by using PSO algorithm based on FIPS algorithm

Razieh Malekhoseini[1], Sadegh Karami mehrian [2]

[1](*Faculty of Engineering , Department of Computer , Yasouj Branch, Islamic Azad University, Kohgiloyeh & Bovirahmad Province, Yasouj ,Iran)*

[2](*Department of Computer , Yasouj Branch, Islamic Azad University, Kohgiloyeh & Bovirahmad Province, Yasouj ,Iran)*

Abstract:- security issues in computer networking have always been of great important and network providers always intend to improve the security situation. Protocols, software, hard ware and applications can be prone point security intrusion. One of the main methods for preventing and reducing of intrusion and the destructive operation is detecting points of the vulnerability and provide mechanism to deal with them. One of the most important challenges in network environments is the attacks that cause preventing of suitable services to legitimate users. These types of attacks are known as denial of service attacks and between them, SYN-Flooding attack has the more damages. In fact using of the TCP protocol to establish a connection between source and destination will cause these attacks. In this paper we explain the mechanisms for detecting and dropping attack packets and illegal traffics by using of the PSO algorithm based on FIPS algorithm

Keywords:- SYN Flooding Attack, PSO, FIPS, Victim, attack, network, Denial of service

I. INTRODUCTION

One of the most important aims in using of computer networks is creating of suitable facilities for sharing of resources and reduce network costs. Basic issues in networks environment providing reliable network infrastructure for legal users. For this purpose we should detect the network vulnerability point and resolve them. One of the major challenges that researchers attend them is countermeasure the type of network attacks known as denial of service attacks. Denial of service attack aim to down system and depletion of resources.

Then they threat network resources and victim's system. In fact such attack by imposing of in additional burden the network and the disruption of vital services cause a disruption in servicing to legitimate users. If we consider the security issue from three aspects of confidentiality, integrity and availability then the issue of DOS attacks that threaten system availability. SYN-Flooding attack is a type of malisuios DOS attacks that cause the waste of victim resources by sendin huge volumes of SYN packets.[1]

Because of the weakness 3-Way handshaking algorithm in TCP protocol in order to establish connection between sender and receiver SYN-Attack can be occurs. Since the TCP protocol of communication protocol is very important in today's electronic society, so completely avoidance of this kind of attack is not possible. We must seek the ways to reduce the impact of this kind of malicious attacks on the network. Among of the methods that have already been proposed to detect and deal with this type of attacks, the method based on collective intelligence have more applicable. Accordingly in this paper we use PSO algorithm based on FIPS algorithm as one of the collective intelligence algorithm. The method of PSO optimized was introduce in 1995 by James kennedy and Russel Eberhart. Spacing search of PSO algorithm containg a series of hypotical organism that cause to rise a wide variety of algorithm based on the connection them to each other and forming a specific topology. PSO algorithm based on information sharing between members or groups of particles in the search space. In the PSO algorithm, every answer to question indicates the position of a particle in a search space. All the particles in the search space have fitness value that is obtained by objective function. It should be noted that the aim of objective function is optimize the proposed solution. The types of location of particles in the search space and using of the information for each of the particles in the search space represent a concept called neighbors. Neighborhood causes formation of various type of topology for this algorithm. One of the most widely used type of proposed topologies in PSO algorithm is using of full connected topology. Each particle in full connected topology can be associated with all the particles in the search space. On the other hand, each particle tends to follow the movement of the best member of s of search space. This type of connection cause to form FIPS algorithmo which used for gather information about the particles in search space. FIPS is decide based on information available to all nodes in the neighborhood of the particles in search space and used the concept of weight that indicate the value of each particle uses. in fact the particles tend to particle which have more weight. FIPS is a graphical depiction of a complete graph in which each particle with all particles are

in neighboring community. Figure 1 shows the connection of neighboring particles community made up 8 vertex based on FIPS algorithm.[2,3]

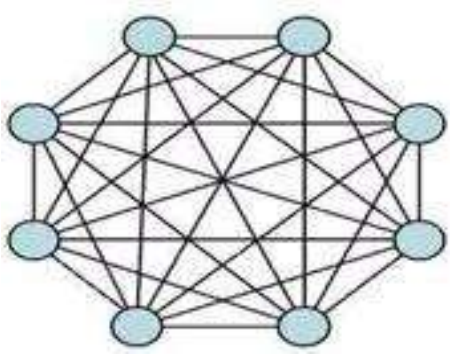

Fig1.full connected topology in forming of FIPS algorithm

TCP is a connected protocol subset of groups of common protocols in transport layer of OSI references model which currently is as one of the widely used protocols. In fact is an integral part of internet.

Therefor in such circumstances that we are required to use this protocol inherently we cannot completely prevent unwanted conditions which occur because of the security weakness of such protocols. So we look for ways to reduce the impact of adverse conditions due to the weakness of such protocols. One of the most devasting attacks ever occurred in the content of network attacks are SYN-Flooding attack where a large number of unanswered SYN packets leading to unwanted traffic on the network.

In fact TCP protocol works to establish connection between source and destination by 3 way handshaking based on 3 packets called SYN, SYN-ACK and ACK according to the following:

1- Source send SYN packet to destination.

2- The destination by receiving SYN packet store in back log buffer and attempts to create a half open connections. Then by sending SYN-ACK packet to the source declare its. at this stage, destination has considered a part of it's resources such as buffer space for a half open connection.

3- The source by receiving SYN-ACK packet and acknowledgment the acceptance of request by destination send the ACK packet. In this stage the destination by receiving an ack packet, release all resources that allocated to the creation of half-open connections and create the actual relationship between source and destination. **Figure 2** shows the steps above**.[2]**

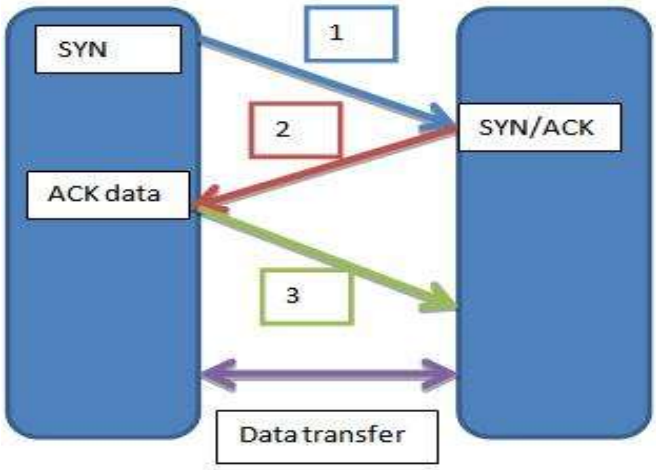

Fig2. The complete 3 Way handshaking in TCP

The above process is completed when source and destination are legal and they have legitimate request. If the source is attacker, then this process in the second step is stoped and leading to a waste of destination's resource. Actually attacker by spoofing IP addresses and attempts to fill the victim's back log buffer cause to wasted resources and victim system is down to the received request from legitimate users, then denial of service is occurred. In other words an attacker based on SYN-Flooding tacke place according to the following process:

1- The source send SYN packet to the destination

2- The destination create a half open connection by receiving a SYN packet and store the recived packet in back log buffer, then send a SYN-ACK packet to response the attacker.

3- Waiting for receiving ACK packet from destination!....[4]

In the third stage the waiting of victim's system never stop, because attacker don't send ACK packet for it and allocate a part of victim's resource until to restart.

This problem is serious when the attacker send huge packet to destination by spoofing IP address. In this condition the victim's system crash and over all cannot service any type of request whether, legal or illegal. Figure3 shows attack mechanism of SYN-Flooding.**[4]**

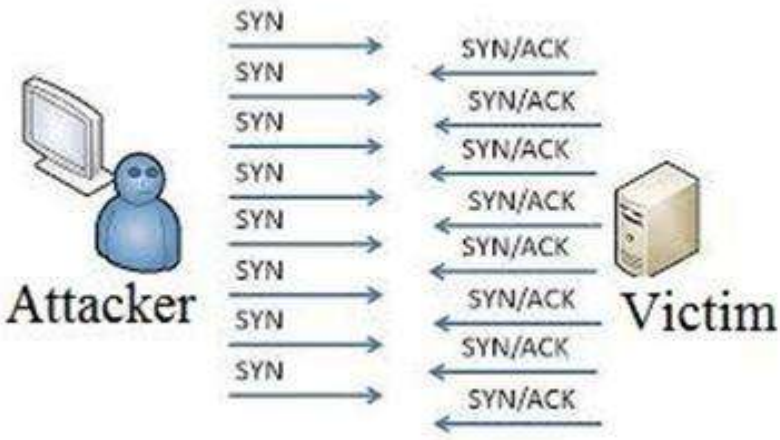

Fig3. SYN-Flooding attack mechanism

The remarkable point is that with high level famous with TCP protocol and it's parameters, we can easily discover the traffic situation in SYN-Flooding attack. i.e SYN, FIN and RST parameters contribtted to this order. The following pictures show changes in regular and irregular traffic flow.

SYN	**28%**
SYN/ACK	27%
FIN/ACK	28%
FIN/ACK/PSH	26%
FIN	28%
RST	28%
RST/ACK	27%

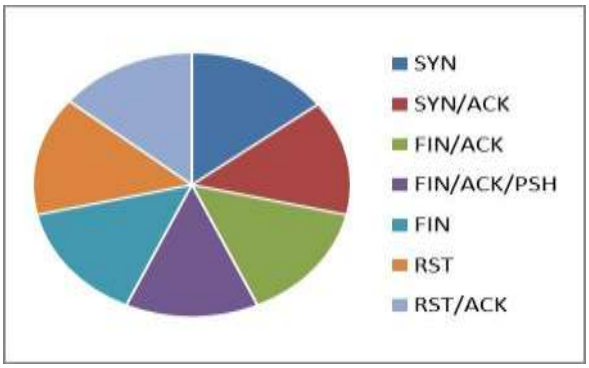

Fig4. The changes of SYN, FIN and RST in regular traffic

SYN	**28%**
SYN/ACK	24%
FIN/ACK	39%
FIN/ACK/PSH	4%
FIN	0%
RST	3%
RST/ACK	3%

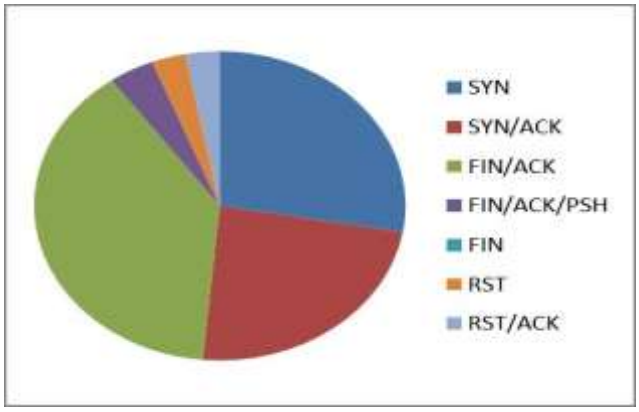

Fig5. The changes of SYN, FIN and RST in irregular traffic

In figure5, data shows that not each try to establish a connection is successful and that not each connection can be established.

II. FRAMEWORKS

As we observed in the section of 3-Way handshaking algorithm discribtion a part of information is saved in a placed called back log buffer. So in this mechanism, we use queue data structure called Q with capacity of M to maintain the attack and legal requests. If Q is full, any kind of request whether legal or attack is discarded. If a packet is legal and Q is empty, in this case it is kept in queue and naturally after a time it goes out after creating a connection between source and destination. . If a packet is legal and Q is empty, in this case it is kept in queue and normally never be removed because the 3 way hand shaking algorithm has not completed. Therefore based on thr track of creating connection between source and destination and departure of legislative packet we define the threshold parameter which based on, it the exit rate of attack packets is also determined. In fact, if a packet exceeded the threshold remain in queue it must be a type of attack and should be discarded. [2,6,7]

Threshold is defined based on the queue capacity and according to the following equation:

$\alpha=[m/2]$ (1)

Since the value of M is obtained based on PSO algorithm and any time that search space is chaining, so it is dynamic. PSO algorithm by considering of the FIPS algorithm uses the velocity equations and particles motion according to the following equations:

$Xi=[Xi,1,Xi,2,Xi,3,\ldots\ldots,Xi,m]$ (2) ,location vector

$Vi=[Vi,1,Vi,2,Vi,3,\ldots\ldots,Vi,m]$ (3) ,velocity vector

According to the relations of (2) and (3), we use the following equation to calculate the value of m. $mi+1=mi+Vi+1best$ (4)

After calculating, the value of dynamically is calculated at each step according to the relation of (4) and is used in the objective function to optimize the solution.

In fact a PSO algorithm is used to optimize the objective function obtained from the condition of problem. In this problem the ultimate goalis increasing the space occupied by the legitimate demands and further reduce the occupied buffer space by the attack applying. So, the objective function of this problem will receive to a appropriate response by optimization of the following relation:

$$\text{Objective function}=\frac{\text{regular buffer usage}}{\text{attack buffer usage}} \quad (5)$$

In the relation of (5) the fraction is optimized by increasing the value of numerator (regular buffer usage), and reducing the value of denominator (attack buffer usage). By the objective function ant time and comparing it to the objective function obtained from the previous steps of all particles in community, we can calculate the parameters of the queue and the threshold at any moment. The substantial point in the calculation of objective function is the attention to the best overall and the best location obtained from the all particles in community.

III. SIMULATION

We use the opnet simulator for the operation of simulation and by considering of the following two scenarios and bellow rules [8]:

1- the topology used for the operations of simulation shown in figure 6

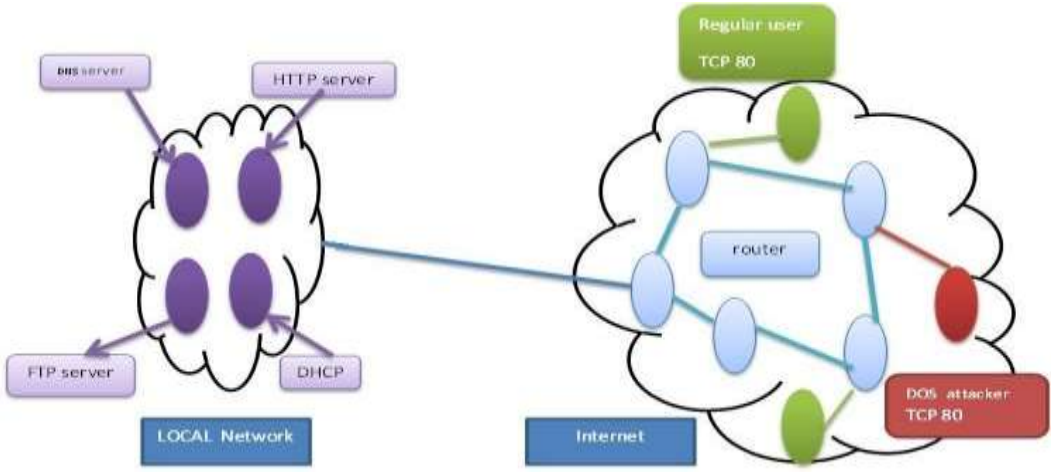

Fig6. Network's topology for simulation

2- The ratio or intensity of attacking request to legal requests is shown by the variable of k.
3- scenario1: the arrival rate of attacking requests is equal to the arrival rate of legal requests.(k=1)
4- scenario2: the arrival rate of attacking requests is [m/2] of the arrival rate of legal requests.(k=[m/2]) The results of the simulation operation for both of the above scenarios are as following:

scenario1: the arrival rate of attacking requests is equal to the arrival rate of legal requests.(k=1)
scenario2: the arrival rate of attacking requests is [m/2] of the arrival rate of legal requests.(k=[m/2])

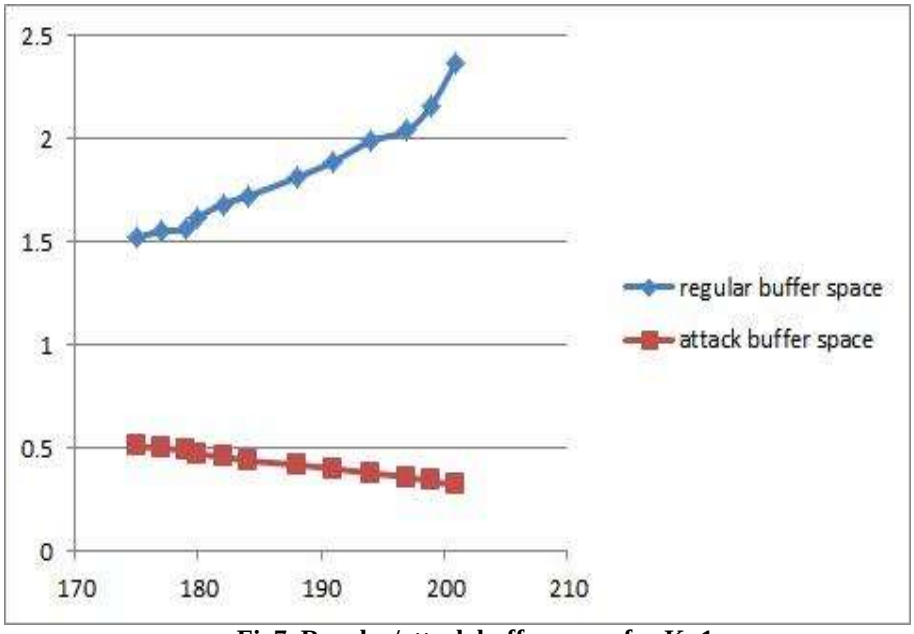

Fig7. Regular/attack buffer space for K=1

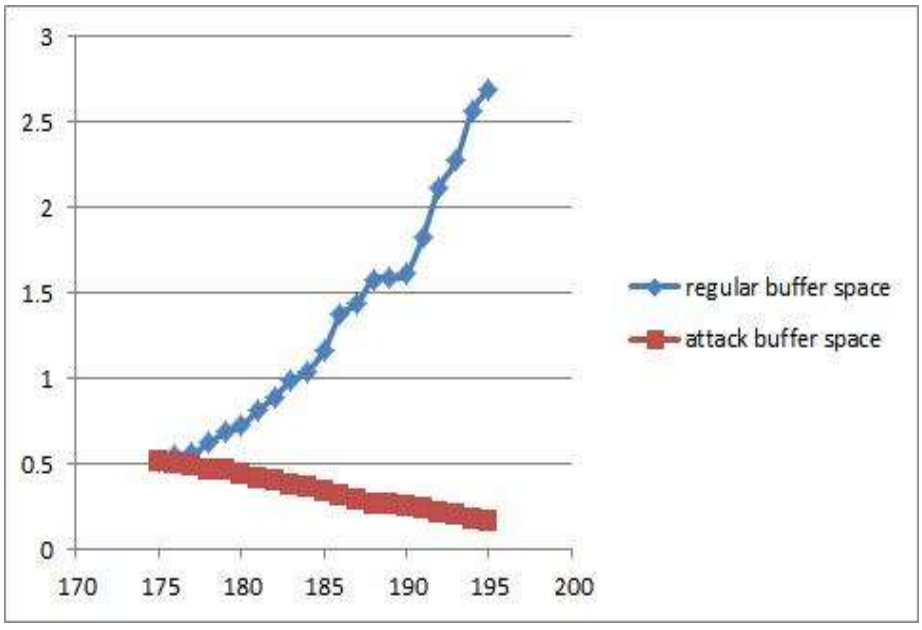

Fig7. Regular/attack buffer space for K=[m/2]

IV. CONCLUSION

In this paper, we propose the PSO algorithm based on FIPS algorithm for detecting SYN flooding attacks. We employ a buffer space usage parameter can be used by regular and attack request, then we simulated two scenarios and results argue that PSO algorithm can well reflect the different features of DOS attacks, which are different from normal traffic. In both scenarios buffer space usage by regular requests are greater than from buffer usage by attack requests.

REFERENCES

[1]. W. Wang, S. Gombault. Efficient detection of DDoS attacks with important attributes, Proceedings of the Third International Conference on Risks and Security of Internet and Systems, 2008, 61–67.

[2]. S.jamali, G.shaker, PSO-SFDD:Defence against SYN Flooding DOS attacks by employing PSO algorithm, computer and mathematics with applications,2001

[3]. H.Wang, D. Zhang, and K.G. Shi, Detecting SYN flooding attacks, Proceedings of the IEEE Infocom, 2002, 1530–1539.

[4]. G.Carl, G. Kesidis, R.R. Brooks, and S. Rai. Denial-of-service attack – detection techniques. IEEE Internet Computing, 2006, 10(1): 82–89.

[5]. J. Martin, Denial of service (dos) attacks, http://www.securitydocs.com/library/2616,2011.

[6]. G.Zhang, S.Ehlert, T.Magedanz, D.Sisalem, 'Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding', Principles, Systems and Applications of IP Telecommunications (IPTComm 2007), New York, USA, 2007, pp.57–66.

[7]. l.Yu-hua, Z.hong-ai, Y.ying-jie, A DOS attack simulation assessment Method Based on QOS, international conference on computer science and network technology, 2011, 1041-1045.

[8]. Y.Okada, Y. Nishikawa, N. Sato, DoS attack countermeasures in NGN using private security policy, APSITT, 2010