A Comparative Study of Defense Mechanisms against SYN Flooding Attack

Prathibha R.C
M Tech Student
Department of Computer Science and Engineering
SCT College of Engineering
Thiruvananthapuram, India

Rejimol Robinson R R
Assistant Professor
Department of Computer Science and Engineering
SCT College of Engineering
Thiruvananthapuram, India

ABSTRACT

Distributed Denial-of-Service (DDoS) flooding attacks are a serious threat to the security of the internet. A DDoS attack makes a machine or network resources not usable by the legitimate clients. A SYN flood is a form of denial-of-service attack. An attacker sends SYN requests continuously to a target system to consume enough server resources and to make the system unable to respond to legitimate traffic. It is a threat to the network as the flooding of packets may delay other legitimate users from accessing the server and in severe cases may result the server to be shut down, wasting valuable resources. The objective of this paper is to review the detection mechanisms for SYN flooding. The advantages and disadvantages for some detection schemes are examined and their performance is compared.

Keywords

Distributed Denial of Service (DDoS), Flooding attack, SYN-Flood

1. INTRODUCTION

Denial of service (DoS) attacks is an intended attempt to stop legitimate users from accessing a specific network resource. The Distributed Denial of Service (DDoS) attack exploits the client/server technology, combine it with multiple computers to use them as an attack platform, and the service is denied for one or several targets and hence it will increase the power of the DoS attack and results in the target to consume enough system resources until it cannot work normally. Different methods are there for launching DDoS attacks in the Internet. In the vulnerability attack, some malformed packets are sent to the victim system. This results in confusing a protocol or an application running on it. In the transport of network level flooding attack, involves an attacker trying to disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity or network resources (network/transport level flooding attacks) or to disrupt a legitimate user's services by exhausting the server (application level flooding attacks).

Today, DDoS attacks are generated using a network of well organized, remotely controlled and widely scattered Zombies or Botnet computers that are simultaneously and continuously sending a large amount of traffic and/or service requests to the target system. The target system's response becomes so slow so that it cannot be used or it crashes fully. Zombies or computers are made as a part of a botnet by the using worms, Trojan horses or backdoors. Attackers launch huge disruptive attacks by using the resources of the zombie computers. Furthermore, it is difficult for the defense mechanisms to recognize the original attacker because of the use of spoofed IP addresses by zombies under the control of the attacker.

2. TCP BASED DDoS ATTACK

The TCP's three way handshake mechanism and its limitation in maintaining half open connections are exploited by the SYN flood attack. The behavior of TCP control packets in a normal three way handshake is analyzed first and then in a SYN floods attack.

In the normal three way handshake shown in figure 1, first client sends a SYN(x) request to the server, which replies with a packet containing both the acknowledgement ACK(x+1) and the synchronization request SYN(y) and waits with a half-open connection in its memory space for the acknowledgement from the client. Upon receiving both ACK(x+1) and SYN(y) client will finish building the connection by sending ACK(y+1). When server get ACK(y+1), it removes previously stored half-open connections in its memory space. The released memory space on server makes it possible to handle further connection requests from clients and the network can run smoothly. x and y are respectively sequence numbers produced randomly by the server and the client during the three-way handshake.

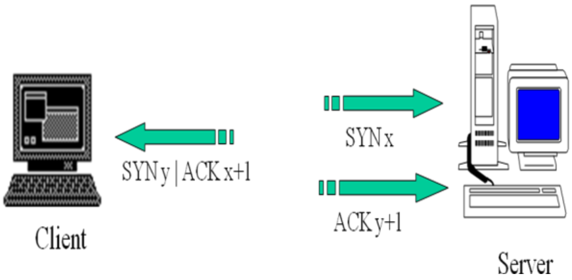

Fig 1: Normal 3-way handshake mechanism

The SYN flood attack is shown in figure 2. The working of SYN flood attack is in such a way that the client will not give the ACK response to the server, which it expects to receive. The malicious client either does not send the ACK packet, or it uses a spoofed source IP address. Spoofing the source address results in the server sending the SYN/ACK to a falsified IP address, but it will not respond with an ACK since it had never send the SYN request.

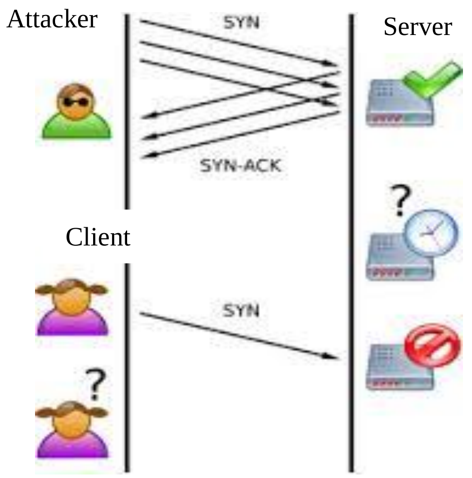

Fig 2: SYN Flood Attack

Network congestion could also result in missing ACK. So the server will have to wait for the ACK up to the time out period. But in an attack, there will be many half-open connections and they will bind server resources so that new connections cannot be made. This results in a denial of service to legitimate traffic. If operating system functions are starved of resources in this way, some systems may also malfunction badly or even crash.

The SYN-flooding attack can cause significant financial losses in the client server network. When a server receives a SYN request, a SYN/ACK packet is returned to the client. The connection in the server is maintained in a half-open state until it receives an ACK packet from the client or up to the TCP connection timeout period. However, to keep all such half-open connections, the server has an inbuilt backlog queue in its system memory. Since this backlog queue is of only finite size, once its limit is reached to the, all connection requests will be dropped within SYN-flooding attack's time.

3. PERFORMANCE MEASURES

There is no unique set of consistent metrics to evaluate the mitigation and defense mechanisms to address DDoS attacks. Some of the metrics used for performance measurement includes defense strength(accuracy), scalability, delay, system performance degradation, implementation complexity etc.

Table 1: Performance measurement outcomes

		DDoS defense decision	
		Negative	**Positive**
DDoS defense decision	**Negative**	A	B
	Positive	C	D

The strength of a defense mechanism can be measured by various metrics by checking how much does it can prevent, detect, and stop the attacks. These metrics could be defined based on the decision or prediction that each defense mechanism makes. Defense mechanisms either detect and respond to the attacks or miss them. Based on their responses, there are four possible outcomes as shown in table 1.

The outcome A is called true negative (i.e, the desired outcome was negative and the outcome of the defense mechanism was negative as well), B is called false negative (i.e, the desired outcome was positive and the outcome of the defense mechanism was negative), C is called false positive (i.e., the desired outcome was negative and the outcome of the defense mechanism was positive), and D is called true positive (i.e., the desired outcome was positive and the outcome of the defense mechanism was also positive).

Based on the above outcomes, six metrics can be used for measurement of performance [1]:

3.1. Accuracy ((A+D)/(A+B+C+D)): Ratio of the correct outcomes of the defense mechanism (true positives and true negatives) over the total outcomes of the defense mechanism.

3.2. Sensitivity (D/(B+D)): Ratio of true positives over total desired positive outcomes.

3.3. Specificity (A/(A+C)): Ratio of true negatives over total desired negative outcomes.

3.4. Precision (D/(C+D)): Ratio of true positives over the total positive outcomes of the defense mechanism.

3.5. *Reliability or False positive rate* (C/(C+D)): Ratio of false positive outcomes of the defense mechanism over total positive outcomes of the defense mechanism.

3.6. False negative rate (B/(A+B)): Ratio of false negative outcomes of the defense mechanism over total negative outcomes of the defense mechanism.

4. DoS DETECTION SCHEMES

The detection schemes for SYN flooding attacks have been broadly classified into three categories – detection schemes based on router data structure, statistical analysis and artificial intelligence [2].

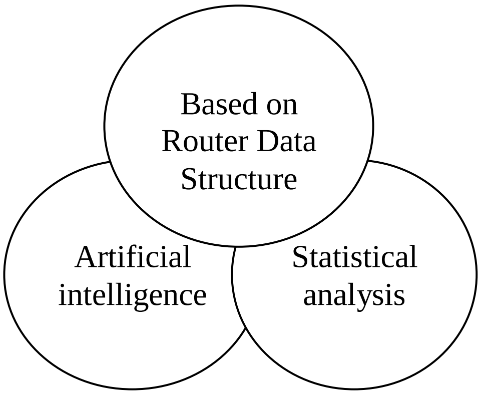

Fig 3: Classification of detection schemes

4.1 Router Mechanism

Detection mechanisms can be implemented on the routers of the autonomous systems inside networks. Detecting attack traffic and creating a proper response to stop it at intermediate networks is the goal of router mechanisms.

4.1.1 Three Counter Defense Mechanism

This router-based three counter defense mechanism [3] is used to mitigate SYN floods. This scheme first detects the attack and then mitigates it. A counting Bloom Filter is used in detection of attack to store the 4-tuple of counted SYN packets. The 4-tuple includes source and destination IP and Port. When a FIN or RST packet comes, it is counted only if its 4-tuple is already stored in Bloom Filter. Thus malicious FIN or RST packets are not counted. The number of SYN packets is more than FIN and RST packets at the time of SYN flood. The efficient detection scheme detects various SYN flooding attacks. The mitigation phase makes use of the client's persistence, i.e, client's reaction to packet loss in later retransmissions. If a legitimate client's SYN packet is lost, it would be retransmitted several times before giving up. Mitigation scheme will definitely drop the first SYN packet of each connection request, and the second SYN packet is allowed to go. If a connection completes the three-way handshake, then its subsequent SYN packets are passed. Otherwise, the subsequent SYN packets are passed only with certain probability. This scheme can mitigate the SYN floods effectively, as only a small portion of SYN flooding packets reach the victim.

4.1.2 Detecting SYN flooding attack in edge routers

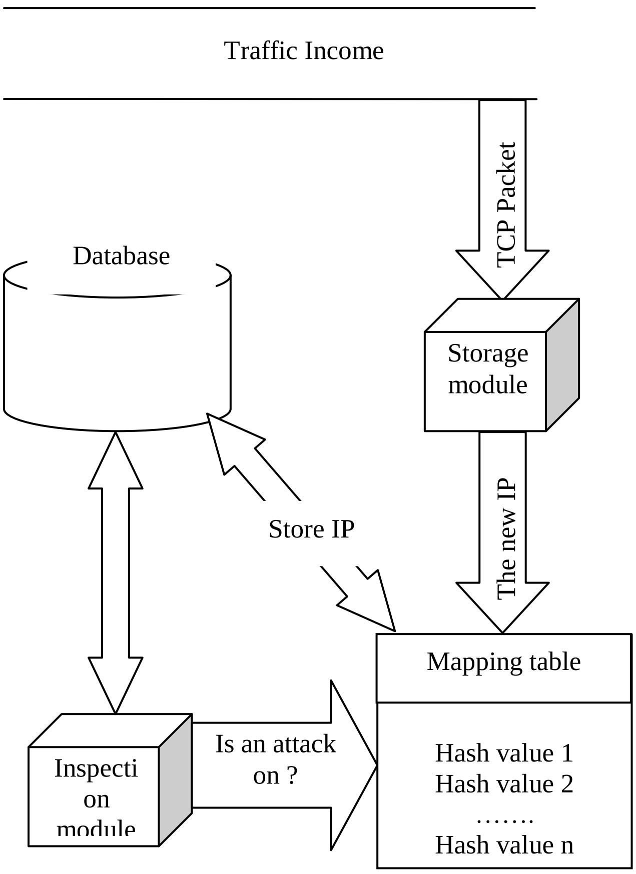

Fig 4 : The structure of defense mechanism

The edge router defense mechanism continuously monitors the TCP control packets that pass through the domain [4]. The structure of defense mechanism is shown in figure 4 given above. This detection approach mainly has a storage module and an inspection module. The storage module makes use of the hash function for storing information about source and destination addresses into the database. The inspection module makes use of the mapping table constructed in the storage process to detect whether any abnormal cases occurred. If any suspicious events are identified, then the detection module can be used to identify whether the abnormal events are caused by attack or not and thus it could detect the SYN flood attack.

4.2 Statistical Analysis

Statistical analyses have been undertaken in using the sample flow of statistics to detect attacks.

4.2.1 Detection based on Statistical test

The statistics of normal SYN arrival rate is investigated and then confirmed that it follows normal distribution [5]. Use one-sample Kolmogorov-Smirnov (K-S) test to decide if the samples come from a population with a normal distribution. The SYN arrival rates (SAR) sampling distribution of normal traffic is fitted to a normal distribution. That is, the data of normal SAR follow a normal distribution.

The threshold, Maximum SYN packet Arrival Rates (MSAR) is the boundary between normal SAR and high rate attack The t-test is used to verify the difference between

i) normal SAR and attack SAR, and
ii) the number of SYN and ACK packets.

Figure 5 below depicts the flowchart of traffic identification. When the incoming packets are received, the host system calculates SAR based on the sampling period (*M*). Then we have to compare incoming SAR and normal SAR with two-sample t-test. If significant difference is seen between two groups, then there is high-rate attack. Otherwise, test the difference between the number of SYN and ACK packets for identifying the behavior of the flow. If there is significant difference, the flow has a possibility to be attack.

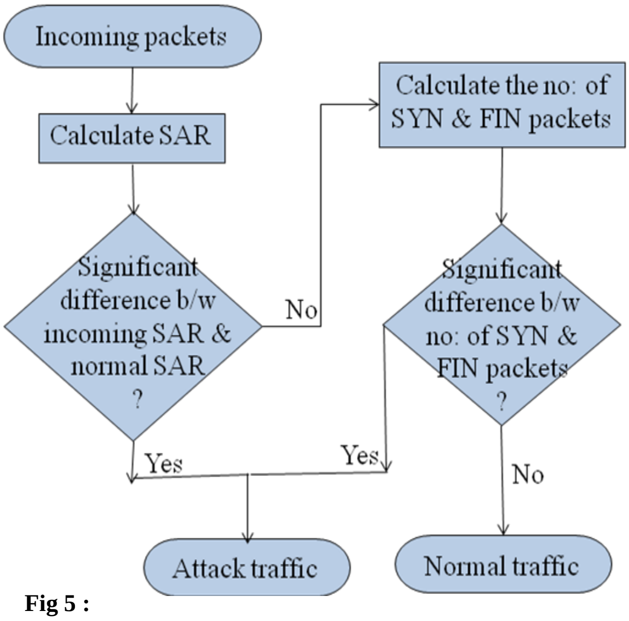
Incoming packets
Calculate SAR
Significant difference b/w incoming SAR & normal SAR ?
No
Calculate the no: of SYN & FIN packets
Significant difference b/w no: of SYN & FIN packets ?
Yes
Yes
No
Attack traffic
Normal traffic

Fig 5 :
Flowchart of traffic identification

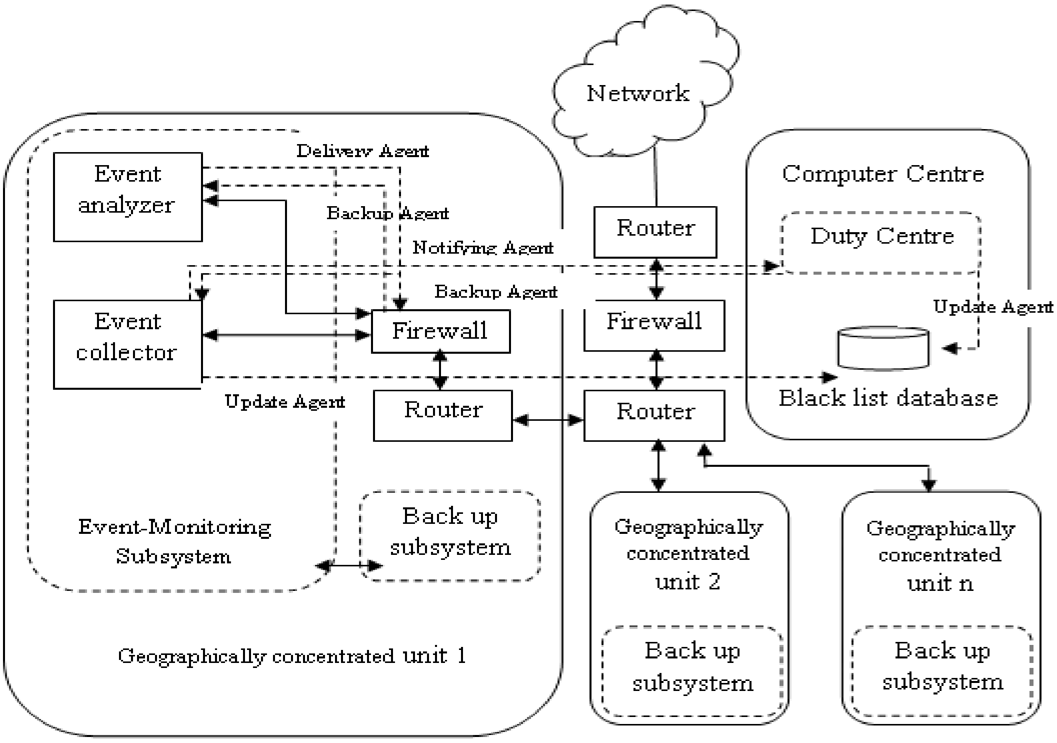

Fig 6: AIDS System Architecture

4.2.2 Detection System using Chi-Square Statistic Approach

The main components of the AIDS (Autonomous Intrusion Detection System) [6] are event monitoring subsystems, backup subsystems, mobile agents, a duty center and a black list database.

The event monitoring subsystem protects geographically concentrated subnets, ie subnets located together or nearby. An example is a building with several subnets owned by different departments or the same department. The source and destination addresses of packets are monitored to detect the DoS/DDoS attacks. When an attack is detected, it dispatches a mobile agent to send attacker's IP address to the black list database. The black list database consists of hackers' information and intrusion details. It also periodically dispatches another mobile agent to send the packet statistics to the duty center, which is the coordinator of an AIDS installed in a specific location, for further detecting whether or not there occurred a DDoS attack. If the DDoS attack actually exists, the duty center dispatches a mobile agent to record attackers' information in the black list database. Thus a firewall can filter out packets issued by known hackers using the black list database.

If any host system is under a DoS/DDoS attack, and loses its detection capability, then another node will be chosen from the backup subsystem and is requested to become substitute of the attacked one.

4.3 Artificial Intelligence

Neural network and fuzzy logic was adopted to design and implement intrusion detection systems for denial of service attacks.

4.3.1 Detection Based on Distributed Time-Delay Neural Network(DTDNN)

The intrusion detection system [7] using Distributed Time-Delay Neural Network is shown in Figure 7.

The data pre- processor module of IDS collects and formats the data to be analyzed by the detection algorithm. KDD99 dataset is used as database to train and test the system performance. The first step of preprocessing is to select important features from dataset. The second step of preprocessing is to convert the selected 35 features into standardized numeric representation. A 36th element was assigned to each record based on a determination of whether this event represented part of an attack on a network; this element was used during training as target output of the neural network for each record.

The detection module analyzes and detects intrusion using artificial neural network. Neural net used as detection module because of the utilization of a neural network in the detection of intrusion would be the flexibility that the network would provide. Distributed Time-Delay Neural Network (DTDNN) is used as detection module in IDSs. Depending on the outcome from the detection module alert filter send a warning email to stop the intruder.

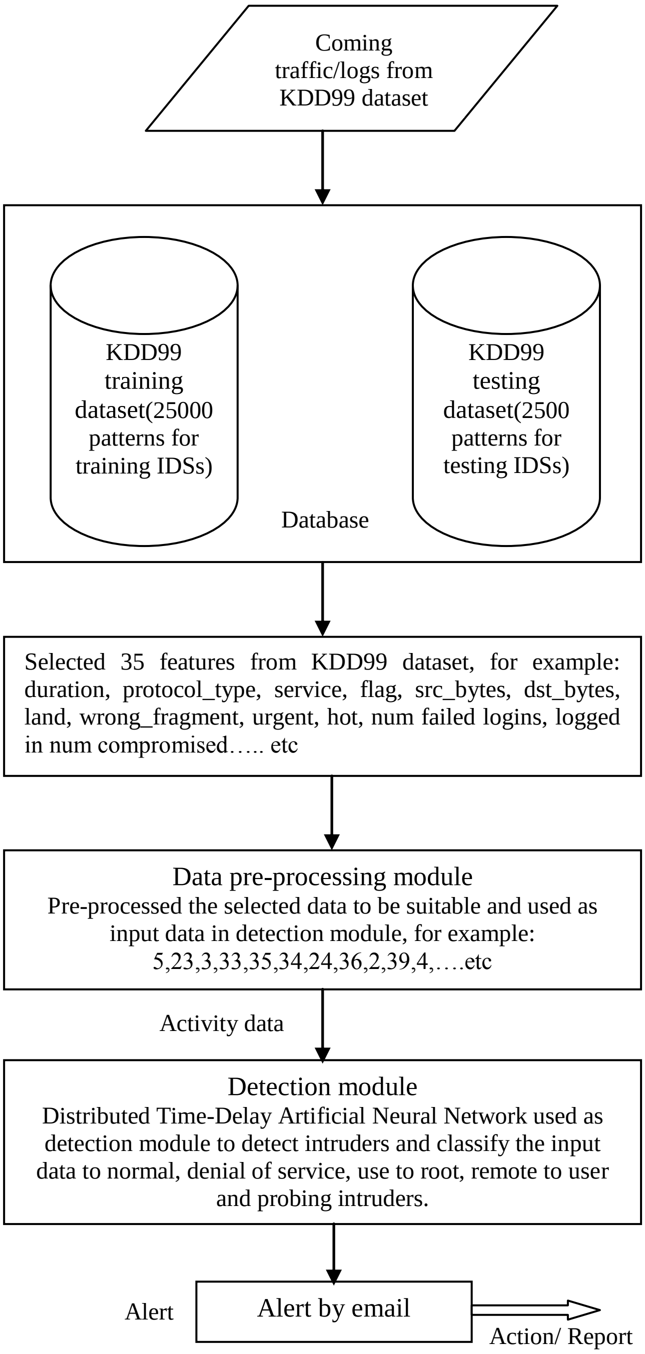
Coming traffic/logs from KDD99 dataset
KDD99 training dataset(25000 patterns for training IDSs)
KDD99 testing dataset(2500 patterns for testing IDSs)
Database
Selected 35 features from KDD99 dataset, for example: duration, protocol_type, service, flag, src_bytes, dst_bytes, land, wrong_fragment, urgent, hot, num failed logins, logged in num compromised….. etc
Data pre-processing module
Pre-processed the selected data to be suitable and used as input data in detection module, for example: 5,23,3,33,35,34,24,36,2,39,4,….etc
Activity data
Detection module
Distributed Time-Delay Artificial Neural Network used as detection module to detect intruders and classify the input data to normal, denial of service, use to root, remote to user and probing intruders.
Alert
Alert by email
Action/ Report

Fig 7: Structure Intrusion Detection System

4.3.2 Adaptive Distributed Mechanism Based on Machine Learning

The adaptive distributed mechanism [8] can be used for the detecting and stopping distributed flooding attacks and network abuses early. Nodes or elements in intermediate network share the available information about their local traffic data to improve the global traffic perspective. The learning ability is independent for each node. So each node has the ability to perform in different ways based on its current situation in the network and local traffic conditions. This property ensures that the parameters required for distinguishing attacks from non-attacks need not be set manually. Threshold values can be learned from experience. It is shown that this mechanism is more accurate and faster than static filters or single-machine adaptive mechanisms used for detecting distributed flooding attacks.

The current status of the network is shared by each element to its neighboring nodes, and then aggregates the local information and the received information so that it can model and classify the receiving traffic. This mechanism allows the elements to know about the behavior of its portion of network, and adjusting the classifiers based on its location and the traffic. Chosen subset of the intermediate network nodes are belongs to an overlay network. Nodes in the overlay network will be equipped with detection and classification capabilities. Overlay network nodes will exchange data about threats and warnings that could occur. The nodes chosen to be in the overlay network are important nodes that see most of the traffic. CUSUM algorithm determines when the traffic towards a particular node changes significantly and the Naive Bayes method declares when an attack is occurring.

The learning component allows the system to create, adjust, and renew the behavior models. Each element of the network learns from its local traffic patterns and shares this information with the other elements so that each one has aggregated information about the whole network. This information is collected in a local model or classifier. At prediction time, information about the state of the network is again circulated among the nodes, but the information is this time passed through the classifier, and it will determine whether messages send to a given destination belong to an attack or not.

5. COMPARISON

The parameters such as CPU time, memory consumption, false positive, false negative, accuracy of detection at high rates and low rates may be used to calculate the performance of Denial of Service (DoS) detection schemes as shown in Table 2 [2].

Table 2 :Comparison of performance

Category	**Router based data structure**		**Statistical analysis**		**Artificial intelligence**	
Technique	[3]	[4]	[5]	[6]	[7]	[8]
CPU Time	Flexible	Flexible	NA	High	High	High
Memory Consumption	Flexible	Flexible	NA	High	High	High
False Positive	High	High	High	High	Flexible	Low
False Negative	NA	NA	Low	NA	NA	Flexible
High Rate Traffic Accuracy Detection	Very good	Very good	Good	Good	Good	Good
Low Rate Traffic Accuracy Detection	No	Fair	No	No	No	No

6. CONCLUSION

The SYN flooding is a type of Denial of Service attack which is harmful to the network. It is a threat to the network as the flooding of packets may delay other legitimate users from accessing the server and in severe cases may result the server to be shut down, wasting valuable resources. Various SYN flooding attack detection schemes are reviewed and their advantages and disadvantages are examined.

Technique	Method	Advantages	Disadvantages
3 counter mechanism	Network based router method	-Stateless -Low computational overhead	-Inefficient when every SYN packet retransmitted twice.
Detection on edge router	Network based router method	-Guarantees that each packet sent by client is valid as much as possible.	- Integration process of storing packet information is difficult when congestion occurs in the network flow.
Statistical scheme	Statistical analysis of traffic	-Low false positive and false negative rate. -Short detection time	- Cannot overcome the low-rate SYN flooding attack and consuming resources leads to shut down the available resources.
Chi square approach	Statistical agent based intrusion detection system	-Statistically analyze amount and variation of packet issued by the sender.	- Does not reflect the behavior and reliability of agent based IDS. -Limits the performance of communication because of the overhead in sending packets.
Distributed time delay NN	Artificial intelligence scheme	- Build offline detecting system.	- Requires retraining to improve analysis on varying input data.
Adaptive Distributed Mechanism	Machine learning	-Faster detection and more accuracy.	-When a service is under attack, all traffic is to be blocked.

7. REFERENCES

[1] Saman Taghavi Zargar, James Joshi & David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”, Communications Surveys & Tutorials, IEEE, Volume:15 , Issue: 4, pp. 2049-2069, March 2013.

[2] Mehdi Ebady Manna, Angela Amphawan, “Review of SYN flooding attack detection mechanism”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[3] S. Changhua, Jindou, F., Lei, S., & Bin, L., "A Novel Router-based Scheme to Mitigate SYN Flooding DDoS Attacks," in IEEE INFOCOM (Poster), Anchorage, Alaska, USA, 2007.

[4] L. Yun, Ye, G., & Guiyi, W., "Detect SYN Flooding Attack in Edge Routers," International Journal of Security and Its Applications (IJSIA), vol. 3, pp. 31-45, 2009.

[5] C. Chin-Ling, " A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test," Journal of Universal Computer Science, vol. 15, pp. 488-503,2009.

[6] L. Fang-Yie, & Chia-Chi, P., "Detecting DoS and DDoS Attacks using Chi-Square," in Fifth International Conference on Information Assurance and Security (IAS), Xian, 2009, pp. 255 – 258.

[7] L. M. Ibrahim, "Anomly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network (DTDNN)," Journal of Engineering Science and Technology, vol. 5, pp. 457-471, 2010.

[8] Josep L. Berral, Nicolas Poggi, Javier Alonso, Ricard Gavalda, Jordi Torres, Manish Parashar , “Adaptive Distributed Mechanism Against Flooding Network Attacks Based on Machine Learning”, Proceedings of ACM workshop on AISec, pp. 43-50, 2008.

[9] B. Al-Duwairi and G. Manimaran, “ Intentional Dropping: A novel scheme for SYN flooding mitigation”, in Global Internet Symposium, 2005.

[10] T. Peng, C.Leckie, and K. Ramamohanaroa, “Survey of network based defense mechanisms countering the DoS and DDoS Defense problems”, ACM Comput. Surv. 39, 1, /article 3, April 2007.

[11] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms”, ACM SIGCOMM Computer Communications Review, vol.24, no. 2, pp. 39-53, April 2004.

[12] R.K.C. Chang, “Defending against flooding-based distributed denial of service attacks: A tutorial”, Computer J. IEEE Commun. Magazine, Vol.40, no.10, pp. 42-51, 2002.