A Comparative Survey of TCP SYN Flooding DDoS Attacks Defense Methods

[1]Ankush Parashar, [2]Parveen Kakkar, [3]Krishan Kumar Saluja
[1]Research Scholar, [2]Assistant Professor, [3]Associate Professor
[1] Computer Science Department,
[1]DAV Institute of Engineering and Technology, Jalandhar, India

Abstract: TCP SYN Flooding is a type of DoS (Denial of Services) attack which utilizes the vulnerabilities in Connection establishment phase of TCP. In this attack, some sources send a large number of TCP SYN packets, without completing the third handshake step to quickly exhaust connection resources of the victim machine and make the server/machine unavailable for its legitimate users. Due to the continuous evolution of new attacks worldwide, many DDoS attack defense methods have been proposed. In this paper, we present the recent trends and incidents in attacks, comprehensive review of TCP SYN Flooding DDoS attacks methods, description of SYN Flooding attack, advantages and disadvantages of attack defense methods with the General comparison of the SYN Flooding defense methods.

Index Terms **- SYN Flooding Attack, Edge Router, Packet Flow, Swarm Intelligence, Denial Of Service**

I. INTRODUCTION

DDoS is a Distributed Denial of Service attack where one system is attacked by the number of compromised systems, which are infected with the Trojan, causing DoS (Denial of Service) attack. A DoS attack which is large-scale cooperative and social attack, launched from an infected host causing server unavailable for the legitimate users. The frequency of DDoS attacks is also increasing. Last year, 44 percent witnessed more than 51 attacks per month. This year, that proportion has risen to 53 percent [1]. DDoS attacks shows about growing threats to businesses and Internet providers around the world. While many techniques have been proposed to detect these attacks, they are either not efficient or not effective enough. Even though lot of efforts have been made to provide defense from these attacks but still they are serious problems on the internet yet. Traditionally, DoS attacks aim at degrading the availability and quality of services, by consuming the service resources to make it unavailable. Nowadays, the work of most of the important and vital services dependent on fast development of the technologies and their operation is almost inconceivable without Internet usage, so any interruption in the operation of the Internet can be very inconvenient. Considering the fact that the internet was actually designed for openness and scalability without much worry about security, it is clear that the mischievous users can use the design weaknesses of the Internet to break havoc in the operation of most of services. According to the last investigation, cybercrime and hacktivism became the fundamental motivation behind cyber-attacks (Fig. 1) [2].

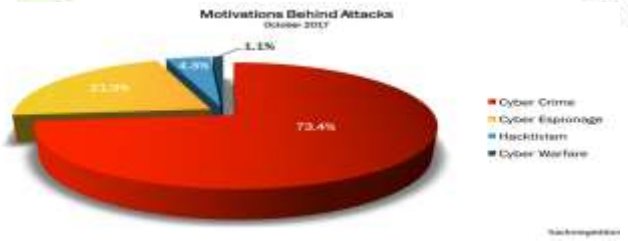

Figure 1 Motivation behind Cyber Attacks in October, 2017 [2]

The **Daily Trend of Attacks**, which shows a slow start, immediately followed by a plain, then a peak is there, and finally a stable value until the end of the month [1].These trends can be seen by graph given in Fig. 2

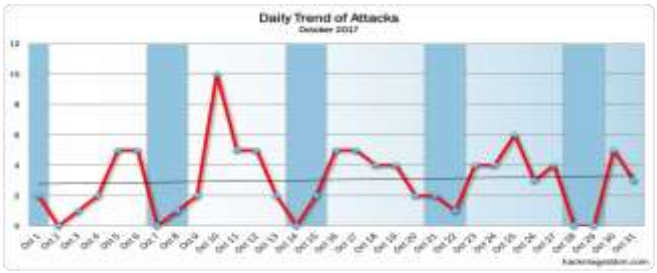

Figure 2 Daily trends of Attack in Oct 2017 [2]

In addition, today, with the propagation of technology, the use of net connections and the Internet is very important in most areas of our lives, such as in education, travel, health, recreation, and so on. Most people use their mobile devices, including their laptops, iPods, and mobile phones, in any location. Therefore, the number of users, including mobile users, has increased. The International Telecommunication Union (ITU) [3] developed key Information and Communication Technologies (ICT) indicators for developed and developing countries, as well as globally and according to that In 104 countries, more than 80% (830 million) of the youth population are online. Out of which 39% (320 million) are from China and India[10][11].

Different layers in the Open Systems Interconnection (OSI) reference pattern are targeted by DoS attacks. The Media Access Control (MAC) layer is affected by a certain kind of DoS attack [5,6] that is known as a jamming attack; the network layer is influenced and affected by black hole attacks, gray hole attacks, and wormhole attacks. The transport layer is targeted by TCP synchronized (SYN) overflowing attacks, session takeover attacks, and repudiation attacks, all of which are types of DoS attacks [12] Our main focus is on the TCP SYN Flooding attacks. The various DDoS attack incidents happened across the world which are harmful to the particular organization are follows:

- In December 2013, a DDoS attack hit the website of China's Central Bank. This attack was planned as reprisal over restrictions of currency [14]
- Series of 200 gigabyte per second DDoS attack detected on Dyn DNS in October 2016.
- In 2010, PayPal website was attacked by a DDoS attack that results huge financial losses.[16].
- A DoS attack was launched against the name servers of the distribution network of Akamai's (CDN), which blocked all access to many websites for nearly 120 minutes in June 2004 [17].
- A domain name server (DNS) was targeted by a DoS attack in 2002. Which causes difficulty to access some Websites because of this attack [15].
- Attack on Twitter and Reddit which was of 1.2Tbps and it used a botnet of 10Million bots.
- In November 2016, DDoS attacks were made against the environmental control systems in apartment buildings in Finland, resulting in the systems shutting down and leaving the inhabitants literally in the cold for up to two days.[1]

There are Drawbacks/Challenges in TCP which causes the TCP SYN Flooding attacks. The two main reasons of TCP SYN flood attacks, The first is the feature of TCP which enables an attacker to consume major resources at a server, while less using its own resources. The second is that a server cannot control the packets it receives, especially the SYN packets can easily reach a server without its approval[13]

II. DoS AND DDoS ATTACKS

A DoS attack starts by utilizing a computer and a connection to the Internet, while a DDoS attack is launched by utilizing many computers and Internet connections. In addition, DDoS have many cooperated systems called zombies, handlers, or masters that collectively launch this attack. The attacker constructs an attack network with the cooperated nodes or zombies or bots. Zombies are used to launch the attack by giving commands of control to them by attacker. The attack goals of DDoS include making sure that legitimate users cannot access the resources or to degrading the performance of resources for admissible users of the system. In other words, they prohibit admissible users from utilizing the resources of the network such as Web services, a Website, or computer systems [4].

A. Classification of attacks

Broadly DDoS attacks are classified into three categories based on the type and quantity of traffic they used for the attacks. These attacks are classified as Volumetric attack, Protocol Attacks and Application Layer Attacks.

- Volumetric Attacks: This attack uses the huge amount of traffic which saturate the bandwidth of the target attacked site. These attacks are easy to generate by using simple amplification techniques. E.g. UDP Flood and TCP Flood. The magnitude of this attack is measured in bits per seconds (Bps) or Packets per second.
- TCP State-Exhaustion Attacks: This type of attacks exploits the weakness in layer 3 and layer 4 protocol and it consumes the connection state tables of the server or of intermediate critical communication devices like firewalls, load balancers etc. and make

it in-accessible to users. The TCP SYN Flood, Ping of Death, fragmented packet attacks, Smurf Attacks and more comes in this category. Protocol attacks consumes all the processing capacity of the server. This attack is measured in Bits per second.

- Application-Layer Attacks: These attacks exploit a weakness in layer 7 protocol and are the most sophisticated of attack and most challenging to identify/ mitigate because they generate the attacking traffic at very low rate so detection with general flow based mechanisms are difficult. HTTP Flood, attack on DNS services are the example of Application layer attacks. These are slow-and-low attacks. The goal of these attacks is to crash the web server and it is measured in requests per second.

B. TCP SYN Flooding Attack

In SYN flood attack, the "SYN" stands for the Synchronize flag in TCP headers. The SYN flag gets set when a system first sends a packet in a TCP connection, and indicates that the receiving system should store the sequence number included in this packet.

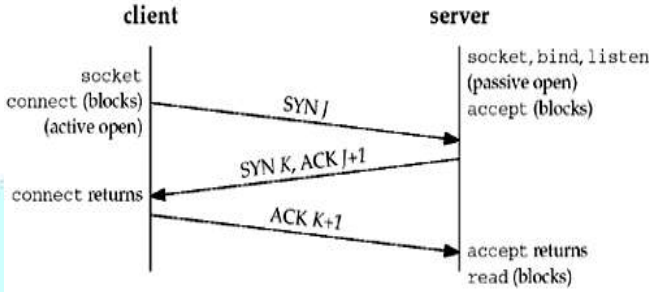

Figure 3 TCP three-way Handshake procedure

The TCP three-way handshake procedure shown in Figure 3 works as follows

- A client sends a SYN packet to a server to perform an active open request
- The server reserves connection resources (backlog queue) to track the TCP state on receiving a SYN packet and replies with a SYN/ACK packet in response.
- Finally, the client sends an ACK back to the server as an acknowledgement, and the connection is established when receiving this ACK on the server side.

During SYN flood attack, an attacker generates a large number of SYN requests but never sends the ACK packets to complete the connections. Since the victim server allocates resources to track the TCP state for each received SYN packet, its backlog queue can be easily exhausted and all the new incoming SYN requests are dropped. Furthermore, many other system resources, such as CPU and network bandwidth, are occupied.

There are three types of SYN flooding attacks[18], which are going out in the nowadays Internet networks: Direct Attack, Spoofing Attack and Distributed Direct Attack. If attackers rapidly send SYN segments without spoofing their IP source address, this will cause direct attack. On the other hand, in the SYN spoofing attack uses IP address spoofing, which might be considered more complex than the method used in a direct attack. During this type of attacks the attacker will sent SYN packets spoofed with the legitimate user source address to victim and then victim will respond with SYN-ACK to the legitimate user. A distributed SYN flooding attack is the most dangerous amongst mentioned types of SYN flooding attacks. During this type of SYN flooding attack the attacker takes advantage of numerous zombie machines/processes throughout the Internet. In the case, the zombies use direct attacks, but in order to increase the effectiveness even further, each zombie could use a spoofing attack and multiple spoofed IP addresses.

III. TCP SYN FLOODING DDOS DEFENSE METHODS

Three are different methods for defense against SYN Flooding DDoS attacks. In this section we will describe these methods and we will also discuss their advantages and disadvantages.

A. Backscatter Analysis

Reference [19], presented a new technique, called "backscatter analysis", that provides an estimate of worldwide denial-of service activity. It uses darknet traffic to estimate worldwide attacks at a single observation point. A darknet is composed of blocks of dark addresses, which are unused but routable addresses. When dark addresses are spoofed to launch attacks, they might receive responding traffic from victims. The responding traffic is called backscatter. Through analyzing backscatter, a large quantity of DDoS attacks can be observed, among which SYN flooding attacks are the most prevalent ones [20]. Nevertheless, the dark addresses are hard to obtain since the IPv4 address space is almost exhausted.

B. Firewalls

They enhance the capabilities of firewall and proposed an algorithm to detect and mitigate the effect of SYN Flooding attacks. It is a three-way counter algorithm and uses the honeypots based scheme. The results show that 97.5% identification, detection and mitigation using proposed technique. The basic idea here is to use honeypots which attracts the hackers and then it records their information and this information is used for classification of attacker and legitimate users. Cloud security is also discussed in this paper. Device capturing and packet sniffing are the two main steps in this system. C# language is used for packet sniffing and for defining set of rules for detection and mitigation. Database is used for storing the sync packets and to perform operations on them[32].

C. WSAND

In reference[21] author has proposed the work to detect the SYN Flood attacks with WSAND algorithm using Netflow data at the live network border. They have worked with Netflow because with the IPv4 exhaustion darknet are difficult to get so Netflow is used. A complete scenario of position of attacker, a victim and attacking address is designed. Then algorithm WSAND to detect attack is proposed. They have used SYN/SYN+ACK pair. With the help of this technique, internal zombies who use real addresses for the attacks can be identified. Similar to darknets, back scatter can be observed at live networks. It detect attacks targeting inside host and internal Bots.

D. Game Theoretical Approach

Authors of [28] presented an algorithm to detect the SYN Flooding attacks in Mobile Ad hoc Networks at early stage using game theory. Malicious nodes delay the communication before launching the SYN Flood attack. This technique is exploits to detect the malicious node in Mobile Ad hoc networks. This algorithm forms a game between the malicious node and multimedia server. The robustness of algorithm is check by using parameters related to the multimedia communication. NASH Equilibrium is used to get the cost or benefit of the attacker and network which is an optimal solution for players. The quality of algorithm is checked by parameters like PDR, Control Overhead, throughput, End to End Delay, Jitter.

E. SLICOTS

SLICOTS (SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks) is an algorithm for detection and defense against SYN Flooding attacks in SDN. SLICOTS is the name of the algorithm that is implemented at the Control plane of the SDN which effectively install the rules to OF Switch at the time of attack. SLICOTS is implemented as a control plane extension module of the OpenDayLight controller[8]. Whenever the request comes the SLICOTS temporarily install the rules into Switch and when the half open connection exceeds some value than it understand that it is SYN Flood attack so then install a rule to blocks the requesting malicious host at the switch and hence defend from the attack.[30]

F. Fuzzy Based Systems

Fuzzy logic is used to detect intrusion because it deals with uncertainty and uncertainty is one of the characteristic of intrusion analysis. The proposed fuzzy based system is compared with the decision tree, a machine learning technique and results shown that in predicting SYN Flooding attacks the performance difference of the proposed system is negligible with respect to the decision tree[9]. They have detected SYN Flood denial of service attacks in NSL KDD dataset.[31].

G. DCA (Dendric Cell Algorithm)

A novel approach to detect DDoS attacks using dendritic cell algorithm. DCA is a kind of artificial immune system in the evolutionary algorithm that can be used as an anomaly detection. The DCA is also designed to solve the problem in network intrusion detection. In this author tries to make a design of TCP Flood DDoS attack detection using artificial immune systems, especially dendritic cell algorithm. Dendritic cell algorithm (DCA) is a kind of artificial immune systems that use danger theory concept. The DCA is a population-based algorithm that consists many individual dendritic cells as an agent. Each cell can collect and represent data items. Mapping between human immunology and computer security is established and various signal are mapped according to the computer security.[33]

IV. RELATED WORK: TCP SYN FLOODING ATTACKS DEFENSE MECHANISMS

Over the past years several methods have been proposed to detect the SYN Flooding attack [22]-[25]. They use the characteristics of the attack and normal conditions to detect the attacks and they also focus on the characteristics of TCP packets. According to this these works can be roughly classified as

1. In [22]-[23] SYN-FIN(RST) method is used and author utilized the normalized difference between the number of SYNs packets and the number of FIN (RST) packets in a time interval. If the rate of SYNs packets is much higher than that of FIN (RST) packets by a non-parametric cumulative sum algorithm, the router recognizes that some attacking traffic is mixed into the current traffic. The disadvantage is that when attacker sends SYN and FIN packets simultaneously it becomes useless.
2. SYN-SYN+ACK method is used in [24][29], is a detection algorithm that uses the difference between the number of outgoing SYN and incoming SYN+ACK packets.

3. In reference [25] the key is to match the SYN packets and CliACK packets. CliACK packets are ACK which client sent in the TCP handshake process.

There are lot of methods for detecting and mitigating the SYN Flooding DDoS attacks and these methods may be categorized in three classes on the basis of technique they are using

- Router Based Data Structure -Bloom Filter based Methods
- Packet Flow Statistical Analysis based Methods
- Swarm Intelligence and Soft Computing Based Methods

In this section a comparison and their advantages and disadvantages with the technique of each methods are summarized in the Table 1.

TABLE 1: ADVANTAGES AND DISADVANTAGES OF SYN FLOODING DDOS DEFENSE METHODS

Reference	Category	Technique Used	Advantages	Disadvantages
S. Changhua et al. [34]	Edge Router Based Data Structure	This technique uses the Bloom filter (BF) in an edge router to detect SYN flood attack. it records the packet information of TCP-FIN pair.	IT uses the Change Point Detection method based on Cumulative Sum (CUSUM) for avoidance of discrepancy in TCP and resending of SYN	1.Bloom Filter generate the False Positive. 2.if FIN is used in next SYN packet it results in inefficient technique.
H. Tang, et al [35]	Edge Router Based Data Structure	It record the TCP sessions statistics (IPTTL) of SYN packets with Bloom Filters and compare it with SYN packets to detect the Attacker's packet.	Records the TTL from statistical measurement with bloom filter data Structure. Shows great results when packets sent based on groups.	False Positive cause the difficulty to measure the detection accuracy. False positive and False negative Results have been seen in using bloom filter data structure in multiple packets' case.
C. Chin-Ling [36]	Packet Flow Statistical Analysis	Statistics method based on mean to detect the SYN flood attack is developed in this technique. The matching process is conducted by comparing the difference between the incoming traffic rate and normal traffic incoming rate.	Main advantage of this technique is low computational overhead because the proposed scheme does not hold the three-way handshake states but only statistically analysis the SYNs and ACKs segments.	1.This technique cannot overcome the low-rate SYN flooding attack which happens on condition that the arrival rate difference between attacks and normal. 2.False Negative (FN)and False Positive(FP) are produced. 3.The shutdown of the available resources happen when attacks are at low rate.
G. Kanwal, &Rshma, C [7]	Packet Flow Statistical Analysis	The methodology is to deploy the real time detection system at the leaf router to detect and monitor the Dos attack.	System can detect the attacker, victim, normal user by a quick identification method.	This technique takes the CPU time and Consumes memory
S. Jamali and V. Shaker[26]	Swarm Intelligence and Soft Computing	(PSO_SYN) PSO algorithm is used to mitigate the effect of SYN Flooding attack	This methods shows good results i.e. it reduces the effect of SYN flooding attack.	Algorithm sometimes trapped in local best solutions.

Reference	Category	Technique Used	Advantages	Disadvantages
Ruiping Lua and Kin Choong Yow [27]	Swarm Intelligence and Soft Computing	Intelligent Water Drop algorithm is used to mitigate the DDoS attack with Swarm nodes.	This method provide location anonymity, security of server increases, attacker will not get the location of the server which led to secured server.	Overhead of maintaining so much swarm nodes.

A. Comparison based on General Parameters

Different methods use different parameters for example so we must take general parameters. Comparison of all these methods based on the general and basic parameters like CPU time, Memory Consumption, False Positive, accuracy of attack detection at high rates of attack as well as low rate of attacks, weather method can be used in real or non-real time, unknown attack detection, scalability is made in this section. Comparisons based on these parameters are summarized in the Table2.

TABLE 2. GENERAL COMPARISON BETWEEN DEFENSE MECHANISMS

Reference	Category	CPU Time	Memory Required	R/N`	Scalability	Unknown attack detection	False Positive	Accuracy Detection	
								High traffic rate	Low traffic rate
S. Changhua et al. [34]	Edge Router	Flexible	Flexible	R	Yes	Yes	High	Very good	No
H. Tang, et al [35]	Edge Router	Low	Low	R	Yes	Yes	High	Good	Good
C. Chin-Ling [36]	Packet Flow	NA	NA	N	No	No	High	Good	No
G. Kanwal, &Rshma, C [7]	Packet Flow	High	High	R	Yes	Yes	NA	Good	NA
S. Jamali and V. Shaker [26]	SI and SC	Flexible	Flexible	R	Yes	NA	NA	Good	Good
Ruiping Lua et al. [27]	SI and SC	High	High	R	Yes	NA	NA	Good	Good

V. CONCLUSION

In this paper the DoS and DDoS SYN Flooding attacks and their trends over the past with attack incidents worldwide have been described. DDoS attacks have been classified into three categories which are Volumetric Attacks, TCP State-Exhaustion Attacks and Application-Layer Attacks. TCP SYN Flooding attack is explained also the reasons in Transmission Control Protocol which causes the SYN Flooding attack. Some of New Defense Methods of SYN Flooding attack are also summarized in related work with advantages and disadvantages of each. These methods Categorized based on the methods they are using which are Edge router based data structure methods, Packet Flow Statistical analysis based method, Soft computing and Swarm Intelligence based methods. The comparison of the existing defense mechanisms shows that most approaches are not capable of fulfilling all the requirements for real time systems the advantages and disadvantages of various schemes are examined and prepared a general comparison of all these papers on the basis of some common parameters. Performance parameters need to be balanced against each other.

REFERENCES

[1] A. Networks, "The 12th annual worldwide infrastructure securityreport(wisr),"https://www.arbornetworks.com/insight-into-the-global-threat-landscape/

[2] October 2017 Cyber Attack Statistics, Available: http://hackmageddon.com/category/security/cyber-attacks-statistics/

[3] ITU website, 2017-05-24 [Online]. Available:http://www.itu.int/en/ITUD/Statistics/Pages/stat/default.aspx

[4] A. Alsumayt and J. Haggerty, "A survey of the mitigation methods against dos attacks on Manets," in Science and Information Conference(SAI), 2014, pp. 538–544, Aug 2014.

[5] E. Bertino; R. Sandhu, "Database security - concepts, approaches, and challenges", Volume: 2, Issue: 1, IEEE Transactions on Dependable and Secure Computing, 2005.

[6] Anita and Les Labuschagne, A Framework Comparing Information Security Risk Analysis Methodology, 2005.

[7] G. Kanwal, & Rshma, C. , "Detection of DDoS Attacks Using Data Mining," *International Journal of Computing and Business Research (IJCBR)*, vol. 2, pp. 1-10., 2011.

[8] Nadya El Moussaid, Ahmed Toumanari, Maryam El Azhari, "Security analysis as software-defined security for SDN environment", Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 87 - 92.

[9] T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in *International Conference on Information Security and Assurance*, 2008, pp. 321-325.

[10] P. Ning, A. Liu, W. Du, Mitigating DoS attacks against broadcast authentication in wireless sensor networks, 2008, ACM journal name Vol No 20.

[11] Madhurya, M., B. Ananda Krishna, and T. Subhashini. "Implementation of Enhanced Security Algorithms in Mobile Ad Hoc Networks." International Journal of Computer Network & Information Security 6.2 (2014).

[12] Jawandhiya, Pradip M., et al. "A Survey of Mobile Ad Hoc Network Attacks." International Journal of Engineering Science and Technology 2.9 (2010): 4063-4071.

[13] Sun, Changhua, Chengchen Hu, and Bin Liu. "SACK2: effective SYN flood detection against skillful spoofs." *IET information security* 6.3 (2012): 149-156.

[14] Xin, F. A. N. G., et al. "DDoS Attacks Based on Protocol Analysis of Network Intrusion Detection System Research [J]." Netinfo Security 4(2012): 016.

[15] Cherazi, Golriz, and Susanne Koch. "Denial of Service Attacks in IP Networks." (2002).

[16] Arora, Ketki, Krishan Kumar, and Monika Sachdeva. "Impact Analysis of Recent DDoS Attacks." International Journal on Computer Science &Engineering 3.2 (2011).

[17] Sachdeva, Monika, et al. "DDoS Incidents and their Impact: A Review." International Arab Journal of Information Technology(IAJIT) 7.1 (2010).

[18] Bogdanoski, M., Shuminoski, T. and Risteski, A., 2013. "Analysis of the SYN flood DoS attack". *International Journal of Computer Network and Information Security*, 5(8), p.1.

[19] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Transactions on Computer Systems (TOCS), vol. 24, no. 2,pp. 115–139, 2006.

[20] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, "Internet background radiation revisited," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. ACM, 2010, pp. 62–74.

[21] Miao, L., Ding, W. and Gong, J., 2015, April. "A real-time method for detecting internet-wide SYN flooding attacks". In *Local and Metropolitan Area Networks (LANMAN), 2015 IEEE International Workshop on* (pp. 16). IEEE.

[22] H. Wang, D. Zhang, and K. G. Shin, "Detecting syn flooding attacks," in INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3. IEEE, 2002, pp. 1530–1539.

[23] C. Sun, J. Fan, L. Shi, and B. Liu, "A novel router-based scheme to mitigate syn flooding ddos attacks," IEEE INFOCOM (Student Poster),2007.

[24] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of dos attacks," Dependable and Secure Computing, IEEE Transactions on, vol. 1, no. 4, pp. 193–208, 2004.

[25] C. Sun, C. Hu, Y. Zhou, X. Xiao, and B. Liu, "A more accurate scheme to detect syn flood attacks," in INFOCOM Workshops 2009, IEEE. IEEE, 2009, pp. 1–2.

[26] S. Jamali and V. Shaker, "Defense against SYN flooding attacks: A particle swarm optimization approach," Computers & Electrical Engineering, vol. 40, no. 6, pp. 2013–2025, 2014

[27] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011

[28] Geetha K, Sreenath N. Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. Springer: Arabian Journal for Science and Engineering. 2016; 41(3):1161-72

[29] Sun C, Hu C, Liu B: SACK^2: effective SYN flood detection against skillful spoofs. *IET Inf Secure* 2012, 6(3):149–156. 10.1049/iet-ifs.2010.0158

[30] R. Mohammadi, R. Javidan and M. Conti, "SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks," in *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 487-497, June 2017

[31] Mkuzangwe N.N.P., Nelwamondo F.V. (2017) A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack. In: Nguyen N., Tojo S., Nguyen L., Trawiński B. (eds) Intelligent Information and Database Systems. ACIIDS 2017. Lecture Notes in Computer Science, vol 10192. Springer, Cham

[32] Hussain, Khalid, et al. "An Adaptive SYN Flooding Attack Mitigation in DDOS Environment." *IJCSNS* 16.7 (2016): 27

[33] Gilang Ramadhan, Yusuf Kurniawan, Chang-Soo Kim "Design of TCP SYN Flood DDoS Attack Detection Using Artificial Immune Systems", 2016 IEEE 6th International Conference on System Engineering and Technology (ICSET), October 3-4, 2016 Bandung – Indonesia, Pg. 72-76

[34] 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.

[35] H. Tang, *et al.*, "Traceback-based Bloomfilter IPS in defending SYN flooding attack," in *5th International Conference on Wireless Communications, Networking and Mobile Computing*, China, 2009, pp. 1-6.

[36] 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.