Solution for TCP/IP Flooding

Report BSCIS DCN,

Minhaj, Yahya,

Abstract: TCP stands for transmission control protocol. It was defined by Internet Engineering Task Force (IETF). It is used in establishing and maintaining communication between applications on different computers and provide full duplex acknowledgement and flow control service to upper layer protocol and application. [2][3][4][5]
In this report proposes solution for TCP SYN flood.

***Key Words*— TCP (Transmission Control Protocol). SYN (Synchronous), DoS (Denial of Service), DDos (Distributed DoS)**

I. INTRODUCTION

The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network. The two main protocols in the internet protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.
IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message. [19][18] [17][16]

TCP/IP functionality is divided into four layers, each of which include specific protocols.

- **The Application Layer:** The application layer provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).[1][6][7][8]
- **The Transport Layer:** The transport layer is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and UDP, which is sometimes used instead of TCP for special purposes.
- **The Network Layer:** Also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the ICMP, which is used for error reporting.[9][11][10]
- **The Physical Layer:** The physical layer consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for LANs and the ARP.

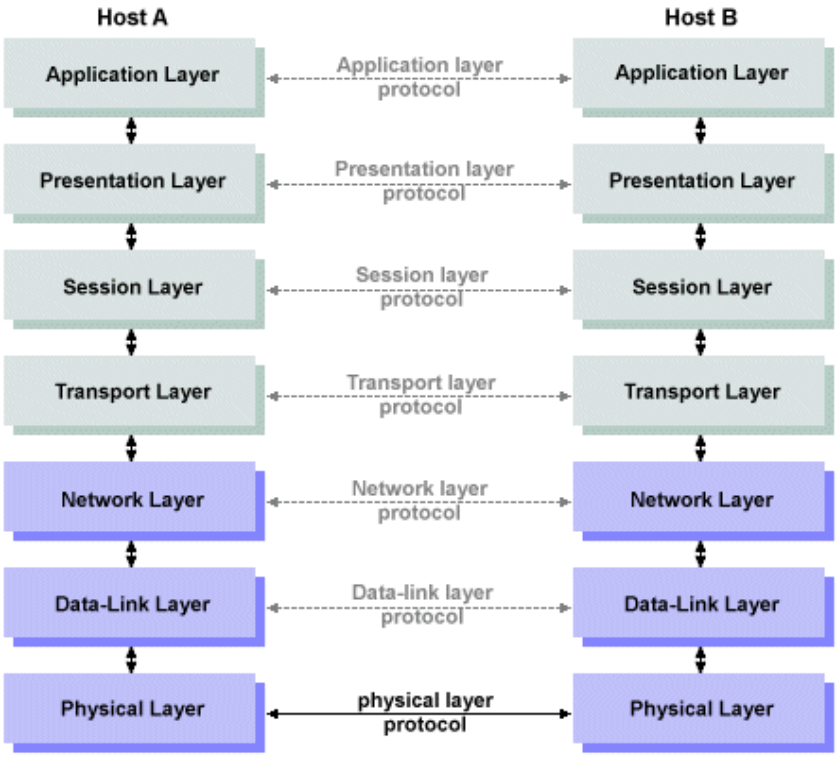


Figure 1: OSI Model.

TCP stands for transmission control protocol. It was defined by Internet Engineering Task Force (IETF). It is used in establishing and maintaining communication between applications on different computers and provide full duplex acknowledgement and flow control service to upper layer protocol and application. Figure 2 shows how packets are exchanged with other layers. [2][3][4][5]

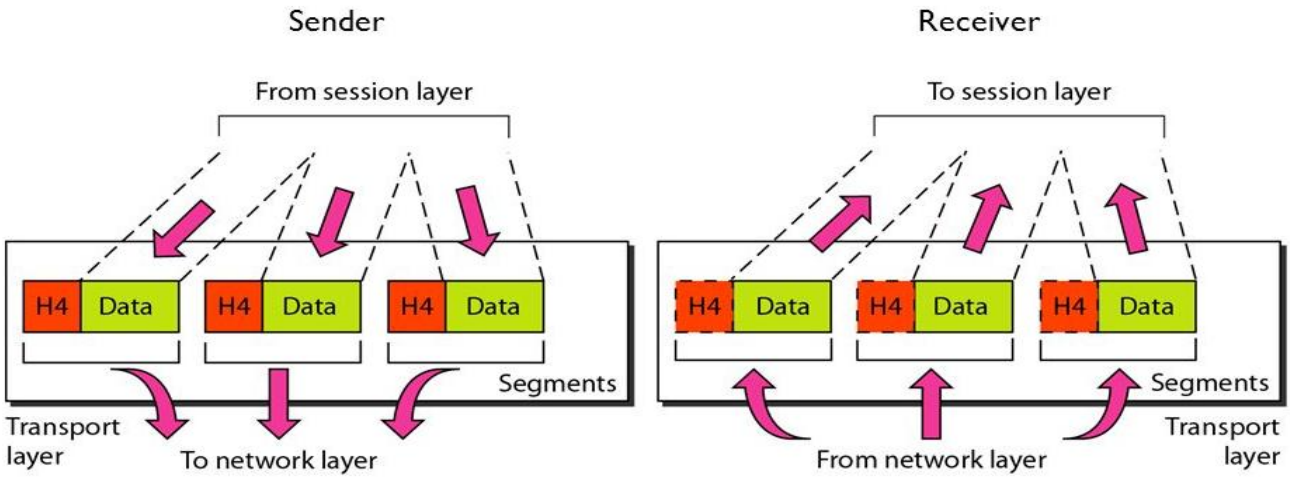


Figure 2: TCP Packet Exchange.

Following are the goals for which TCP is designed, endorsed in Figure 3:

- Route should be established for as long as needed.
- Reliable delivery.
- Technology should permit dissimilar systems to exchange data.
- Interconnections across long distances.

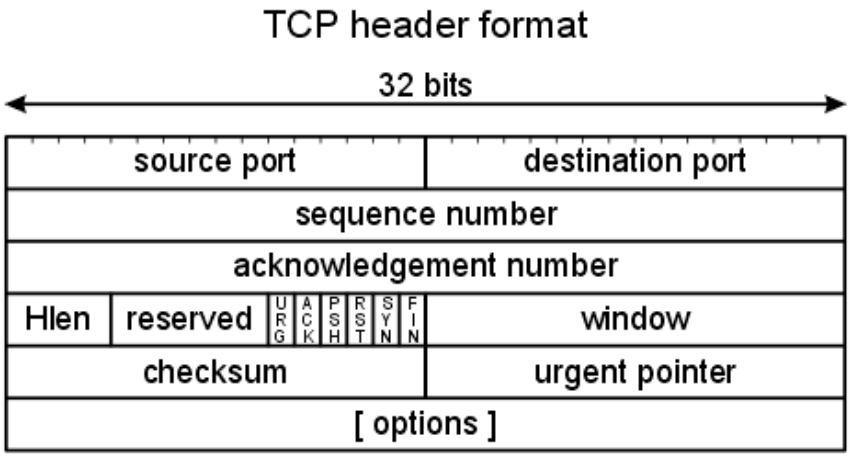


Figure 3: TCP Header Format.

In the next section we explain TCP operation in detail with the help of sequence chart.

II. TCP OPERATIONS

Figure 4 shows the sequence flow of a TCP connection.

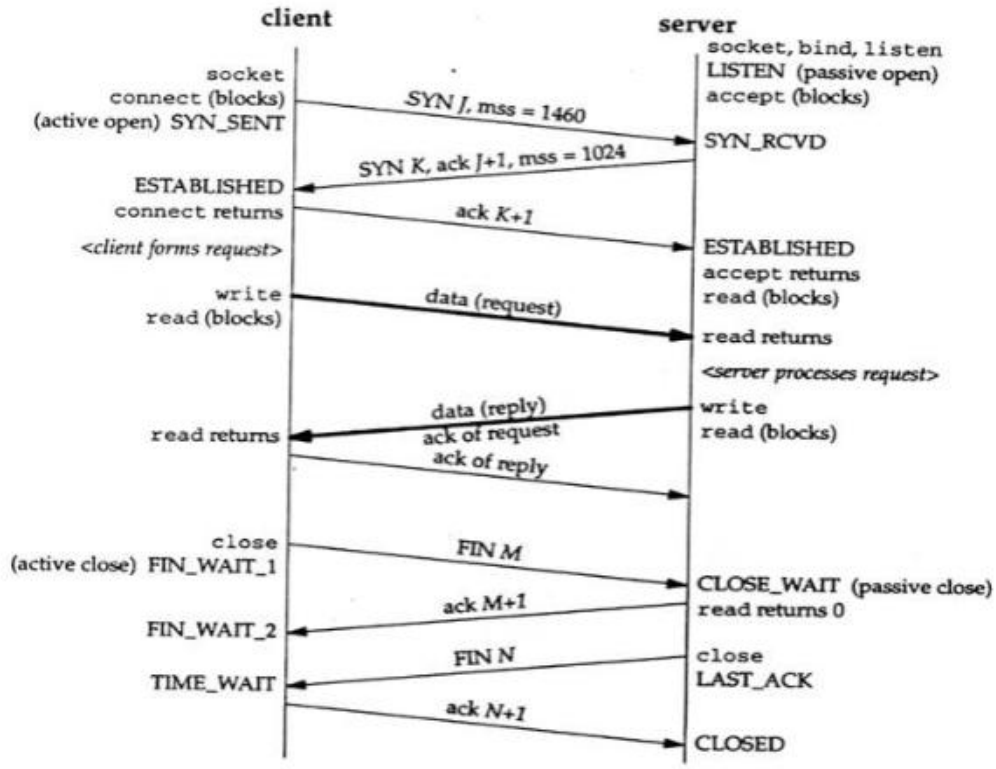


Figure 4: Sequence Chart of TCP.

TCP has following main functions:

• **Connection setup and teardown** (TCP establishes a connection known as a logical circuit between the remote host ports first then link ports or processes, maintains the connection throughout the communication and then tears down the connection when it is no more needed.)

• **Multiplexing** (Multiplexing capability enables TCP to establish and maintain multiple communication paths between two hosts simultaneously)

• **Data transfer**(receives data from upper layer and passes it down to IP(Internet Protocol) for addressing and delivery. On the destination end it takes the packets from IP and sends them to upper layers.)
• **Flow control** (Flow control guarantees that incoming traffic does not overwhelm a host's receive buffer. When congestion occurs, a host reduces its window size and when congestion no longer exists, a host can increase the size.)
• **Reliability**(Reliability comes from TCP's guaranteed delivery of packets. The receiving host does not send an ACK if datagrams become lost in transit. TCP deals with damaged frames through a CRC(Cyclic Redundancy Check) field contained within the TCP header.)
• **Precedence and security** (the higher the precedence level, the higher the security level.) [21][20]

III. DOS Attack

A DoS attack tries to make a resource unavailable to its users by overloading it with malicious requests. That means that during the attack period, regular traffic toward resource will be either slowed down or completely interrupted.

IV. Distributed DOS

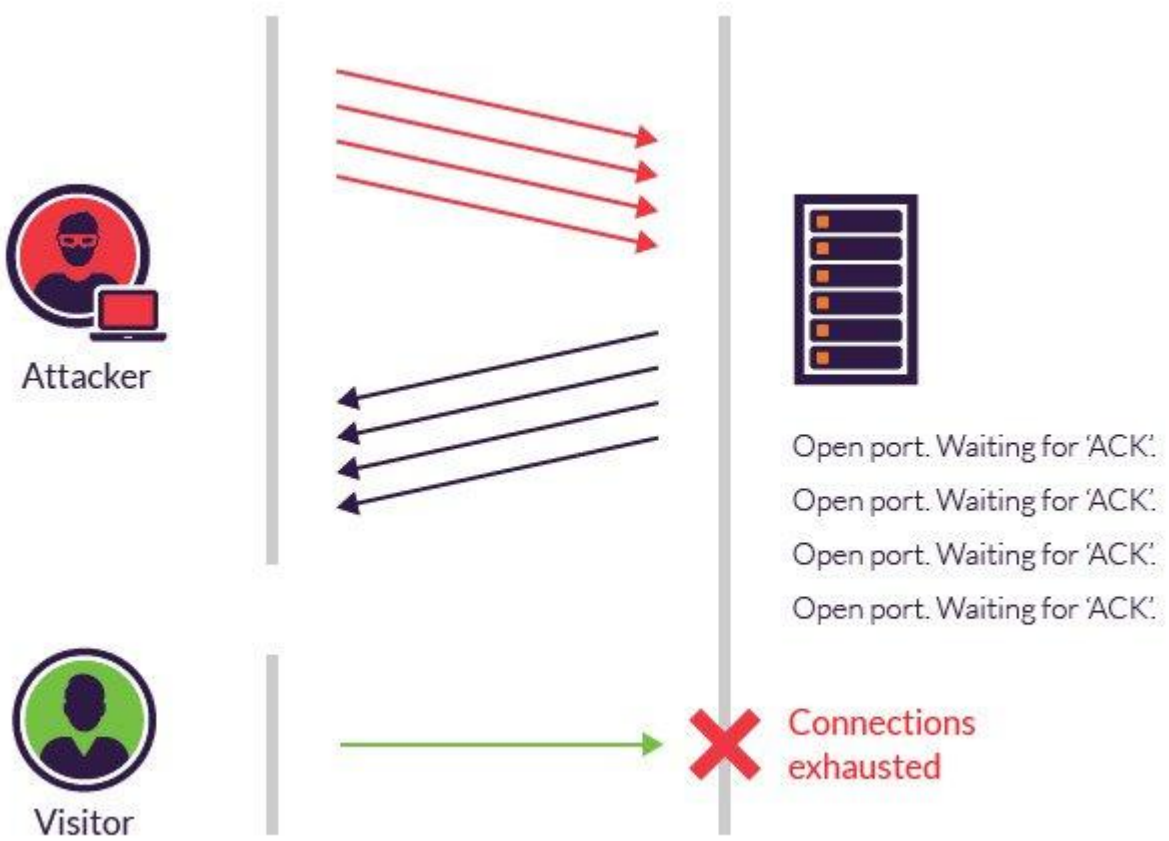
A DoS attack coming from number of source IP addresses, making it difficult to manually filter or drop traffic from these sources is known as Distributed DoS attack. The source computers behind this type of an attack are often distributed across the globe.

V. problem

When a client and server establish a normal TCP "three-way handshake," the exchange looks like this:

1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.
The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.



Progres
sion of a SYN flood.

During this time, the server cannot close down the connection by sending an RST packet, and the connection stays open. Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open – and indeed SYN flood attacks are also referred to as "half-open" attacks. Eventually, as the server's connection overflow tables fill, service to legitimate clients will be denied, and the server may even malfunction or crash.

While the "classic" SYN flood described above tries to exhaust network ports, SYN packets can also be used in DDoS attacks that try to clog your pipes with fake packets to achieve network saturation. The type of packet is not important. Still, SYN packets are often used because they are the least likely to be rejected by default. [23][22]

VI. SOLUTIONS

Firewalls can be set up to have simple rules to allow or deny protocols, ports or IP addresses. In the case of a simple attack coming from a small number of unusual IP addresses for instance, one could put up a simple rule to drop all incoming traffic from those attackers. The firewall does not have to use a lot of resources because a SYN request matching a rule with inbound policy is neither logged nor appears in real time status nor in the access cache until it is categorized as a valid TCP connection. To further protect the server, you can assign limits to the total amount of sessions and the maximum number of sessions coming from one source. If one of the limits are exceeded, further connection attempts are ignored. [25][24]

The second solution is SYN cookies. SYN cookies is a technical attack mitigation technique whereby the server replies to TCP SYN requests with crafted SYN+ACK, without inserting a new record to its SYN Queue. Only when the client replies this crafted response a new record is added. This technique is used to protect the server SYN Queue from filling up under TCP SYN floods.

VII. CONCLUSIONS

This article talked about SYN flooding attacks and discussed two solutions. The first solution was to implement a firewall and the second solution was setting up a threshold on the amount of communications that can take place between client and server. Both solutions solve the problem of SYN flooding attacks effectively [29][28] [27][26].

VIII. REFERENCES

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8] T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.

[18] SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: LivingExamples, Challenges, Advantages”, Tech. Rep. SITI-TR- 11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP- Tele Workshop, Porto, Portugal, Dec. 2009.

[25] SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[26] T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE- SW-13-05, 2013.

[28] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.

[29] Zeeshan Haider, Kiramat Ullah and T. Jamal, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.