SECURITY METHODS AGAINST TCP SYN FLOODING DDOS ATTACKS IN WIRELESS NETWORKS- A SURVEY

Parveen Kakkar[1], Dr. Pooja Sharma[2], Dr. Krishan Kumar[3]
[1]Research Scholar Computer Science Department IKGPTU Kapurthala, Punjab, India.
[2]Asstt. Professor (CSE), IKGPTU main campus Kapurthala, Punjab, India
[3]Professor, UIET, Punjab University Chandigarh, 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 unavailable for its legitimate users. This paper considers attacks on Wireless sensor networks. Wireless Networks is collection of large number of nodes which are of limited capabilities to collect sensitive information. With the advancement in technology, Security is one of the major concerns these days. There are so many attacks possible on wireless networks, in Distributed-Denial of Service (DDOS) attacks, malicious nodes adapts many attacks such as flooding attack, to halt the overall functioning of network. Due to the continuous evolution of new attacks worldwide, many DDoS attack defense methods have been proposed. This paper presents the recent trends and incidents of attacks, challenges in Wireless Networks, 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: TCP SYN Flooding Attack, Edge Router, Packet Flow, Swarm Intelligence, Denial of Services (DoS)

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 lots 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].

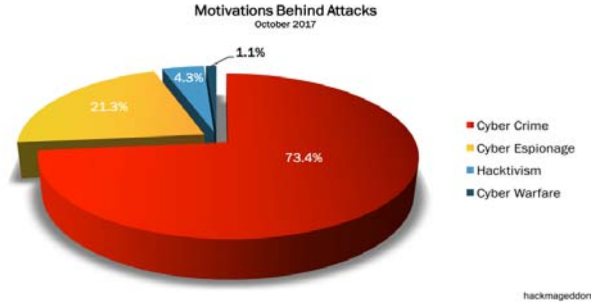


Figure 1 Motivation behind Cyber Attacks in Oct, 2017 [2]

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

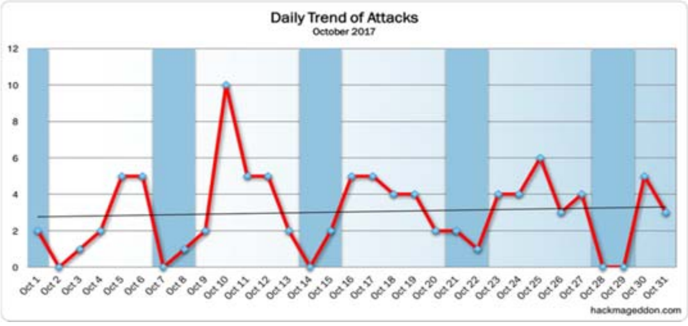


Figure 2 Daily trends of Attack in Oct 2017 [2]

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.

DoS attacks produce damages in different areas, such as in financial and resource losses. Also, they overexert/exhaust the network or its resources such as bandwidth, energy, and power. In addition, these attacks cripple the network and impede/disrupt one of the most important security requirements which is the availability condition [4], where these security requirements include the integrity, confidentiality, and availability of the transmitted data. The definitions of these requirements as follows: 1) privacy or confidentiality, which refer to the defense and security of information against unlawful release; 2) honesty, which pertains to preventing any unlawful and inappropriate change of information; and 3) availability, which denotes exclusion/ deterrence and retrieval from the errors of the hardware and the software, and from the denial of access of harmful, rendering the unavailability of the database system [5]. In other words, confidentiality denotes the restrictions encountered when obtaining various kinds of data. Honesty is the assurance that there is no information whereas availability ensures that data and related resources can be accessed by the lawful and authorized users when needed [6, 7, 8]. It is quite possible to support the information existing on the Web by following techniques which defend the attacks of DoS, including the techniques related to machine-learning [9]. According to Nawneet Raj, [43, 44], the three security requirements are defined as follows. First, confidentiality guarantees that the confidential data is not legitimated/ released to unlawful users. Confidential data, for example, may include necessary martial choices or confidential data concerning a specific location. The absence of similar data to the adversaries may result in unwanted consequences. Second, the principles of honesty refer to the exchange of information among the nodes, it is neither damaged nor altered. Messages may be altered either by accident as a result of favorable failures, or they may be altered on purpose by harmful nodes in the network, as in the case of the loss of radio broadcast or flows in the hardware. Third, availability guarantees the readiness of the data all the time, and that the communication channels operations are completed in an appropriate way, as this is conducted to access the information. Availability prohibits the DoS attack. Disruption sets the accessibility of the jeopardized source.

1.1 Wireless Networks

Wireless Networks consists of small sensor nodes communicated through radio links. They are used in many applications like (agriculture, health, home, industrial, and military) for monitoring and data collection purpose. Its main advantage is that it is easy to deploy in harsh environments, where infrastructure is difficult to deploy [67].

In many applications (like military, medical and industrial) security is very crucial requirement. Due to so many limitations in WNs, the traditional security methods cannot be directly implemented. There limitations include limited battery power, power to communicate and compute. Furthermore the area for deployment of WNs may be public locations, where intruder can physically take over sensor nodes and take all information. Moreover due to energy failures some nodes may die, or new nodes can join the network and the channel used for communication is very insecure. Hence more efficient security approaches are required which consider all these constraints [68]. Wireless Network mainly contains one or few Base Station (BS) or Sink and hundreds or thousands of sensor nodes. Sensors have limited capacity whereas base stations are having more capabilities and are used to communicate with other networks. Sensor nodes are deployed at random, and responsible for data collection, whereas base stations are responsible for data aggregation and management of the network. BS sends aggregated data through internet to the user [66] (Fig. 3) Denial of Service Attack (implemented by attacker by targeting the scheme of routing) occurs due to the failure of nodes unintentionally and also due to malicious action. In DoS attack, the resources available at the victim node are exhausted by receiving unnecessary packets which are not meant or entitled for that node. DoS attack is not only for adversary nodes but also for those events which dismisses the capability of network to provide services in Wireless Network

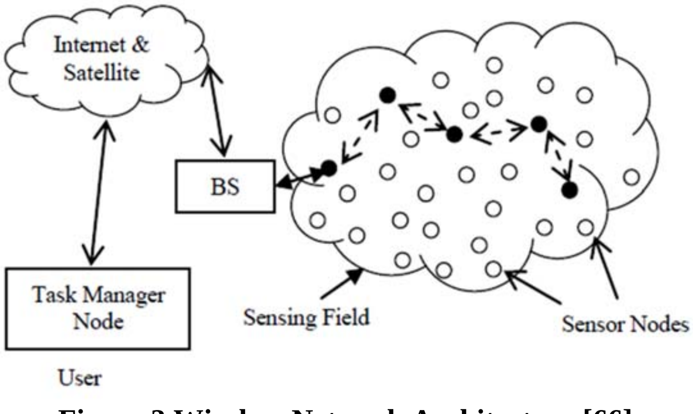


Figure 3 Wireless Network Architecture [66]

Wireless networks are more vulnerable to malicious attacks than traditional wireless networks [69]. Threats to WNs can be classed in a number of ways, based on the capabilities of the attacker, the level of access by the attacker and the level of intervention by the attacker. Firstly, an attacker can utilize devices with the same capabilities as the sensor nodes in the network, either by introducing sensor nodes to the networks deployment area or subverting some of the nodes in the network under attack. With this approach the scope of attacks is limited as the attacker only has the same resources as the nodes under attack, especially in terms of energy and processing power. The alternative is that the attacker uses a personal computer/laptop, or potentially an even more powerful dedicated device, equipped with the appropriate radio, which can possibly transmit at a much higher power level than the radios on the sensor motes. This option opens up many more avenues of attack due to the much greater energy supply, processing power, memory and much lower communication latency. Defending against this class of attacker is the primary difficulty when trying to secure a sensor network. Attacks can also be classed as being outsider or insider attacks. With an outsider attack, an attacker does not become part of the network. An outsider attacker can choose to passively eavesdrop on the network communication, which is very difficult to detect. However using a sufficiently strong cipher to preserve confidentiality is generally the only defense needed against this type of attack. An outsider attacker can also actively influence the communication channel. This can be done by interrupting (i.e. jamming) or modifying network packets or injecting false packets into the network. Authentication, integrity and replay protection techniques can detect and prevent modification and injection of packets. Interruption attacks, while often easy to detect, are difficult to defend against, especially when dealing with a PC/laptop class attacker. An insider attack involves running malicious code on nodes that are valid members of the network. In this case the attacker often has access to at least some legitimate secret cryptographic keys used in the network. The only defense against an insider attack is to detect these malicious nodes, generally a very difficult problem, revoke the keys they know, and ignore any future communication originating at these nodes. A problem faced by WNs that is not faced by other ad-hoc wireless networks is ability of the attacker to gain physical access to the sensor nodes. This is the case due to the unattended and accessible nature of WN deployments. This physical access opens up a number of attacks, including reprogramming the sensor nodes with malicious code, retrieving secret information, such as cryptographic keys, from

the nodes or even just physically destroying the nodes. The only defense against the first two attacks is to use tamper proof hardware but this is both very expensive and generally not very effective against a determined attacker [70]. The only defense against physically destroying the nodes is to encase the nodes in strong, destruction resistant enclosures, but this solution is usually cost prohibitive, not to mention the effect such cases can have on radio communication or the operation of the sensors themselves.

1.1.1 Attacks on Wireless Network

In order to better organize the presentation, attacks can be classified based on how the attack is initially launched. The reason for this is that considering an attack as an intrusion, any IDS should be able to detect it from the moment the attack is launched. Using this rationale, three types of attacks identified [80]: (a) attacks launched by introducing one or more additional dishonest nodes in the network; (b) attacks launched by weaken one or more existing network nodes; and (c) attacks launched by turning one or more nodes of existing system into malicious ones.

A. Type A attacks

Node Replication/Clone attack: In this type of attack, the attacker inserts replicated nodes at specific network points; she can then easily manipulate the information passing through these cloned nodes and, more generally, a specific segment of the network [88]. **False Node attack:** An intruder inserts a node to the WN; she then feeds it with false data or prevents the passage of true data. The wrong data can spread to all nodes, destroying the whole network [81]. **Sybil attack:** In a Sybil attack a single node duplicates itself and appears in multiple locations at once. This malicious node will send incorrect information to another node in the network [81], [87].

B. Type B attacks

Node Outage attack: Node outage occurs when an attacker manages to stop one or more nodes from functioning properly, e.g. by depleting their power source [81]. **Unfairness:** This kind of attack does not entirely prevent legitimate access to the channel, but could result in marginal performance degradation, [85]. **Routing Loop Attack:** This kind of attack will deplete the resources of every node in a loop. Moreover, it can cause the isolation of the destination and few packets are not able to reach the destination [86]. **Physical attack:** The attacker destroys one or more sensors permanently, so that the losses are irreversible [81]. The physical attack can be further classified into two main categories according to a) the degree of control the attacker gains; and b) the time span during which the regular operation of a node is interrupted.

C. Type C attacks

Node Malfunction attack: The attacker forces a node to generate inaccurate data that could expose the integrity

of the sensor network, especially if the node is a cluster head in the network [81]. **Passive Information Gathering attack:** An attacker monitors the messages which contain the physical locations of the sensor nodes and intercepts the content of messages [81], [83]. **Monitor and Eavesdropping:** The attacker monitors the data traffic in order to discover the communication content [81]. **Traffic Analysis:** This is the process of intercepting and examining messages in order to deduce information from communication patterns [81]. **Camouflage Adversaries:** In this type of attack the attacker camouflages one or more malicious nodes to act as normal, in order to attract and misroute the packets to affect the entire network [81]. **Man-in-the-middle:** The attacker connects all the potential victims together, trying to transmit and receive messages among them. Moreover, the attacker is able to intercept all messages that the victims exchange and to force new ones [81]. **Masquerade attack:** It can take the form of: (1) inserting messages into the network using a false identity, (2) replaying previously intercepted messages, (3) spoofing a network service or d) taking the address of another host or service, essentially becoming that host or service. This type of attack is also called Fabricate information attack. **Message Corruption attack:** The attacker modifies the content of the message that a node broadcasts; thus the integrity of the message is compromised [81]. **Spoofed, altered and replayed routing information attack:** By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. [81],[87],[85]. **Selective Forwarding attack:** Malicious nodes are able to refuse forwarding certain packets and simply drop them, ensuring that they are not transmitted any further. [81], [87], [85]. **Sinkhole attack:** The attacker makes a compromised node look attractive to surrounding nodes by forging routing information. The surrounding nodes will choose the compromised node as the next node to route their data through [81], [87],[88],[83],[85]. **Wormhole attack:** A malicious node receives packets from one location of network, forwards them through a wormhole link and releases them into another location. [81],[88],[83],[85]. **HELLO flood attack:** This attack uses Hello packets that are required especially in routing protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in radio range of the sender [81],[87],[83],[85]. **Jamming attack:** A malicious node attempts to jam the frequencies of the radio used for communication between the nodes in the network [87]- [88],[85]. **Tampering:** The attacker can alter or replace sensors and parts of computational and sensitive hardware and can also extract information such as cryptographic keys to gain unrestricted access to higher communication layers [87],[88],[85]. **Collision:** The collision attack occurs when two nodes attempt to transmit packets on the same frequency at the same time. After that, a change will occur in the data, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid [81],[87],[85]. **Exhaustion:** the exhaustion attack is similar to collision attack but with the slight difference that a malicious node may conduct a collision attack repeatedly in order to exhaust the power supply of the communicating nodes [81],[87],[85]. **Acknowledgment spoofing:** An attacker can spoof the acknowledgments of overheard packets in order to provide false information to the neighboring nodes [85]. **Blackhole:** The attacker listens to the route request and then replies to the target node saying that it has the shortest path to the base station. The blackhole node can drop the packets, selectively forward those to the base station or to the next node, or even can change the content of the packets [85]. **Neglect and greed:** In this type of attack a malicious node may drop packets, deny transmitting legitimate packets or give excessive priority to the transmitted messages. **Homing:** An attacker tries to identify and target the nodes that act as leaders. Leaders could be the cluster heads in the sensor network or the cryptographic key managers [85]. **Misdirection:** The role of a malicious node is to direct the legitimate packets to a wrong path with no route to the intended destination [87],[85]. **Repetition attack:** In this type of attack, an attacker retransmits the same message several times in the network. **Message Delay attack:** an attacker retransmits a message after a defined timeout is occurred[88]. **Flooding attack:** A malicious node requests for continuous connection in order to flood a great number of packets. It does not drop the packets of the network but only floods them [87],[88],[85]. **Desynchronization:** In this type of attack the connection between two end points can be interrupted by desynchronization. The adversary forges messages to one or both end points [87],[85]. **Overwhelming attack:** The attacker deluges the network nodes with large volumes of traffic to a base station [85]. **Path-base DoS attack:** An attacker floods a path to the base station with either replayed or injected packets in order to waste secure energy resources [87],[85]. **Network Partition attack:** Node accessibility is violated even though there is a path between the nodes [84]. **Simple Broadcast Flooding:** The attacker floods the network with broadcast messages. The false information passes through the whole network [84]. **Simple Target Flooding:** The attacker tries to flood the network through some specific nodes [84]. **False Identity Broadcast Flooding:** This is similar to simple broadcast flooding but with the difference that the attacker deceives the network with wrong source node ID [84]. **False Identity Target Flooding:** This attack is similar to simple target flooding, but the attacker deceives the network with wrong source node ID [84]. **Node Subversion attack:** In this attack, the sensor network can be compromised if the attacker captures a node and it reveals its information including disclosure of cryptographic keys [81]. **Deluge (reprogramming) attack:** In many deployed networks reprogramming nodes is feasible. This process is not always secure and this can allow an attacker to handle a large portion of the network and deceive the process [85]. **Pseudorandom number attacks:** A random number is always used to prevent a replay attack. Because true random numbers are difficult to generate, pseudorandom numbers are used. However, under certain conditions, the pseudorandom number sequence can be revealed to an attacker [82]. **Digital signature attacks:** The RSA public key algorithm can be used to generate a digital signature. The user can get the signature of a message and use the signature and the message to fake another message's signature [82]. **Hash collision attacks:** A collision attack tries to find two messages with the same hash, but the attacker cannot pick what the hash will be. An attacker is able to construct a valid certificate corresponding to the hash collision [82].

In various networks there are two types of attacks: passive and active attacks, In DoS, the aim of the attacker is to render the targeted destination unreachable from legitimate nodes. In addition, there are two categories for misbehaving nodes: selfish or harmful. The selfish nodes keep and protect their battery life and the other nodes resources for their private communication without any collaboration within the network. Such an attack is known as a passive one. On the other hand, the harmful node prioritizes harming and damaging the network by using its own resources and by performing several actions, for example: spoofing, modifying and fabricating; this attack type is called an active attack [10]. A passive attack is actually riskier than an active attack because it is difficult to find and notice; besides there are not any changes or alterations to the data. Conversely, an active attack is simple to find and detect because the user be able to notice these alterations, adjustments, or any modifications [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 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].

1.2 Attack Incidents

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 happened 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. [18]

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]

The structure of the remaining part of the paper is as follows. Section 2 explains challenges and drawbacks of WN. Section 3 compares between DoS and DDoS attacks and refers to popular references for both. Section 4 represents SYN flooding DDoS attacks defense methods which is divided into three categories based on the methods they use: Edge router based, Packet flow based and Swarm Intelligence. Section 5 presents the related work of SYN flooding methods, compared the advantages and disadvantages of different methods. Section 6 demonstrate the main requirements of a system to find and mitigate SYN Flooding DDoS attacks in WNs. Section 7 concludes the paper.

II. CHALLENGES AND DRAWBACKS IN WIRELESS NETWORKS

There are Challenges in the WN due to which attacks happen. The various challenges and limitations of WN are due to its nature. WN are more vulnerable to attacks if compared with other networks. These constraints make it difficult to implement security mechanisms on WNs. Some of these limitations/ challenges are as follows

- **Constraints of energy:** This renders the wireless links among nodes undependable.
- **Restrictions of bandwidth**: The connections among nodes are at low capability in comparison to the wireless networks. Wireless networks are susceptible to certain issues, for example, signal influences, interference and external noise.
- **Scalability:** In accordance with the nature of nodes in WNs, the methods used for security detection must be incorporated into the networks with large and small-scales [75]. Bounded power supply: The nodes in WNs have limited power supply, making them susceptible to various problems. In WNs, a node may act in a selfish manner when faced with a limited power supply.
- **Limited Resources:** Wireless Sensor Networks have limited resources which cause difficulty in implementation of security mechanism as they need certain amount of resources for operations.
- **Unreliable Communication:** Security of the network greatly depends on the medium of communication and in case of WN the communication is wireless.
- **Unattended Operations:** The sensor nodes in WN may remain unattended for long time depending upon the application of the particular WN which makes them more vulnerable to attack [76].
- In WN, trust management is difficult. Users in the wireless sensor networks are very keen to realize others personal information, and the communication is over public accessible wireless links, so the data collection is susceptible to attacks that endanger the privacy. The communication of privacy sensitive data over civilian wireless sensor networks is regarded unpractical, without suitable protection of privacy.
- During in-network aggregation, enemies can without difficulty change the intermediate aggregation outcomes and cause the final aggregation result deviate from the true value very much. Without security of data integrity,

the data aggregation consequence is not reliable [71,72].

- Data collection over wireless sensor networks does not trust in dedicated infrastructure. In several situations, the number of nodes responding a question is not distinguished before the data aggregation is directed [74].
- Resource restricted portable devices are not able to provide heavily computation and communication load.
- The necessity on exactness of information collection (i.e., aggregated result) causes the existing randomized privacy-preserving algorithms not appropriate. In addition to the mentioned factors, it is so difficult to secure privacy and integrity of data aggregation at the same time, since of typical privacy-preserving plans disqualify traffic peer monitoring process, which decrease the accessibility of information in a neighborhood to confirm data integrity [73].

Due to these limitations and constraints, the overall WN performance may get degraded. For nodes the constraints are limited energy, memory, storage space and processing power. Due to above written challenges the network will become vulnerable and untrusted, can be managed remotely with no resiliency.

III. 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]. Author of [53] classified DoS attacks divided into the following two general categories

1. **Semantic Attacks:** The first category of attacks exploits system vulnerabilities by employing an attacker to find large numbers of connections to a victim host then it then sends specialized packets with low volumes.

2. **Brute Force Attacks:** The second category of attacks includes brute force-based flooding attacks. These attacks use various concurrent links to a particular host; they send many packets that exceed the host’s ability to handle them. As such, these attacks work by overwhelming the system’s resources. The two categories have approximately the same influence.

The widely known DoS attack is a network kind of attack. Popular defense means to distribute firewalls and interference of the systems of sensing and deterrence. Firewall rules that perform access control and egress filtering deter spoofing attacks that originate on the local network and also prevent incoming traffic from impacting the local network. This weakens/impairs the ability of local computers to participate in DoS attacks [19]. 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.

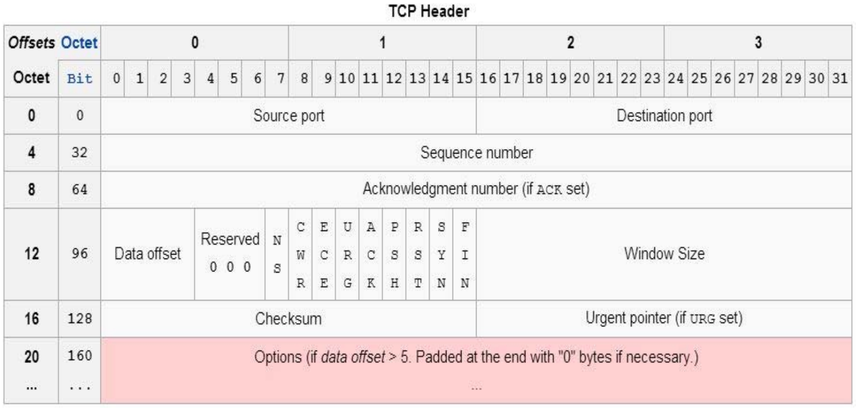
1) Volumetric Attacks: This attack uses the huge amount of traffic which saturate the bandwidth of the target attacked site. These attacks are easy to generate by using simple amplification techniques. The goal of this attack is to fill the bandwidth of the attacked site with the traffic generated by the amplification techniques. The huge amount of the attack traffic completely blocks the access to the resources (website). The common volume based DDoS attacks are the DNS amplification, UDP Flood and TCP Flood. The magnitude of this attack is measured in bits per seconds (Bps) or Packets per second. A massive 200 Gbps Attack detected on DynDNS in October 2006.

2) 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.

3) 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. These attacks establish a connection with the target server and then exhaust the server resources by monopolizing transaction and processes. 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.

2.1 TCP SYN Flooding Attack

The TCP is connection oriented and reliable, in-sequence delivery transport protocol. It provides full duplex stream of data octets and it is the main protocol for the Internet. Most nowadays services on Internet relay on TCP. For example, mail (SMTP, port 25), old insecure virtual terminal service (telnet, port 23), file transport protocol (FTP, port 21) and most important in this case also is the hypertext transfer protocol (HTTP, 80) better known as the world wide web services (WWW). Almost everything uses TCP some way to do their communications over the network - at least the interactive ones.



TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Figure 4 TCP Header

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. Fig. 4 shows the TCP header, which is twenty bytes long without options.

The TCP SYN flooding attack is of interest in this work since it is the most widespread denial of service (DOS) attack and a serious threat to organizations that provide online services. The SYN Flooding is a type of DoS (Denial of Service) attack that attempt to make a machine or network resource unavailable to its intended users or suspend services of a host connected to the Internet. By using multiple attack sources, the DoS attack evolves into a distributed denial of service (DDoS) attack, which amplifies the attack power and detection or defense difficulties. TCP SYN flooding is the most commonly used one and known as one of the most powerful flooding methods. SYN Flood attack exploits the TCP connection establishment procedure. In this, client and server connection should be established first before data transmission. This is called TCP three-way handshake. The SYN flood attack is well-known DoS method which affects hosts that run TCP server processes (the three-way handshake mechanism of TCP connection). Nowadays, despite the original one, a lot of its variations can be seen. Although there are many effective techniques against SYN flood attack, and even RFC4987 is covering some common mitigation techniques against this attack [45], yet there is no single mechanism (schemes) for effective defense.

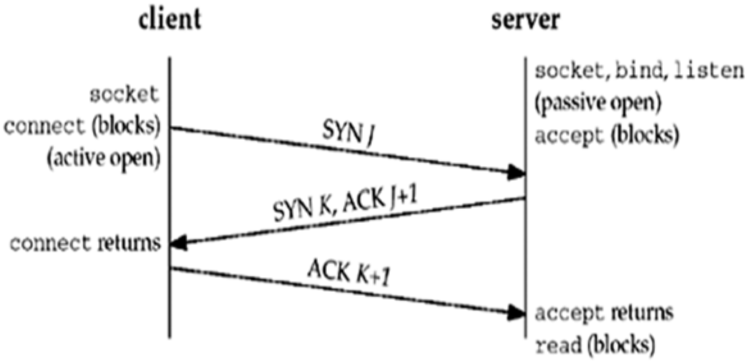


Figure 5 TCP three-way Handshake procedure

The TCP three-way handshake procedure 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 two main causes of SYN flood attacks. The first is the essential asymmetry feature in TCP three-way handshake protocol, which enables an attacker to consume substantial resources at a server, while leaving its own resources. The other is that a server cannot control the packets it receives, especially the SYN packets can easily reach a server without its approval.

There are three types of SYN flooding attacks [19,23,45], 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. This type of SYN flooding attack does not involve directly injecting or spoofing packets below the user level of the operating system of the attacker. One way to perform third type of attack is by simply using many TCP connect () calls [46]. However, the attacker's operation system must not respond to the SYN-ACKs, because any ACKs, RSTs, or ICMP (Internet Control Message Protocol) messages will allow the listener to move the TCB (Transmission Control Block) out of SYN-RECEIVED. In order to prevent its operating system from responding to the SYN-ACKs, the attacker can set some firewall rules which can filter outgoing packets to the listener (allowing only SYNs out), or filter incoming packets so that any SYN-ACKs are discarded before reaching the local TCP processing code. 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 send SYN packets spoofed with the legitimate user source address to victim and then victim will respond with SYN-ACK to the legitimate user. Also During this type of SYN flooding attack instead of merely manipulating local firewall rules, the attacker also needs to be able to form and inject raw IP packets with valid IP and TCP headers. Moreover, the IP address spoofing techniques can be categorized into different types according to what spoofed source addresses are used in the attacking packets. 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.

IV. TCP SYN FLOODING DDOS DEFENSE METHODS

There are different methods available for defense from TCP SYN Flooding attacks and in this paper survey have been done on these methods which comes under the TCP State-Exhaustion attacks category. There are number of methods have been proposed those are listed in this section with brief explanation and with advantages and disadvantages of each.

❖ Backscatter Analysis

Reference [20], presented a new technique, called “backscatter analysis”, that provided an estimate of worldwide denial-of service activity. It used 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 [21]. Nevertheless, the dark addresses are hard to obtain since the IPv4 address space is almost exhausted.

❖ Firewalls

They enhanced 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 used the honeypots based scheme. The results show that 97.5% identification, detection and mitigation using proposed technique. For attack generation, the code is written in c language because it supports both windows and Linux. A three-way counter protocol is proposed in which it will check the Complete ACK packets will meet the three-way handshake procedure successfully and others packet that do not meet three-way handshake. Three tables are created that store IP address that come first time, repeatedly and the IP which have completed the three-way handshake procedure. Some IP do the handshake procedure more than one time that is counted by the table and according to that the classification of attacker and valid user is done based on the threshold. The basic idea here is to use honeypots which attracts the hackers and then it recorded their information and this information is used for classification of attacker and legitimate users. Cloud security is also discussed in this. 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 [33]

❖ WSAND

In reference [22] 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 was designed. Total eight positions are designed. Then algorithm WSAND to detect attack is proposed. They have used SYN/SYN+ACK pair. In this technique traffic is merged at the border because the technique is router based and if the live network has more than one router then there will be different traffic and merging is necessary. For each scenario, a vector is generated and then total number of types of attacks that WSAND can detect is calculated. Calculations of total attacks are made in keeping mind that some attacks can coexists. For flow monitoring, a hash table is made to store the detection metric in each interval. An attack table is made from hash table when one interval is ended. To evaluate the performance WSAND is deployed at 28 main POP’s of CERNET. The advantage of this attack observed when deployed at 28 main POPs of CERNET. Backscatter can also be observed at live border. With the help of detected attacks, internal zombies who use real addresses for the attacks can be identified. Similar to darknets, back scatter can be observed at live networks. It detects attacks targeting inside host and internal Bots.

❖ PSO_SYN

Authors of [27] proposed a technique to defend against SYN Flooding attack using particle swarm optimization. They have taken the problem as an optimization problem and solved it with the particle swarm optimization algorithm. In this method, they optimized two parameters. One is, each connection can be held for the period of time ‘h’ seconds and Other is ‘m’ the number of maximum concurrent half open connection are allowed also the attack request are also categorized as RRBOP, ARBOP, Ploss. These parameters are optimized based on an objective function which is formulated by counting each connection in the buffer space. That is how many are of attack requests; how many are of regular requests and how many are blocked requests. The overall goal of this proposed approach is to minimize the attack request buffer space and Connection loss, maximize the regular requests. Values of h and m plays important role and these values are changed dynamically in this work by using Particle Swarm Optimization. PSO_SYN algorithm moves these h and m towards best defense positions dynamically. Basically, after the initialization phase three basic operations are performed. First, at one point of time the System is checked and Objective function will be computed. Second, by using this Objective function local and global best positions are updated. Third, new values of h and m are computed and set these parameters of the under-attack system. Two Algorithms are implemented one is on the attacker computer simulating SYN Flood attack and other is on server system PSO based defense scheme PSO_SYN. The results of PSO_SYN are compared with the Linux TCP using four scenarios of attack intensity which shows very good results. One limitation of this work is that PSO sometimes get trapped in local best solutions, so for improving this ACO or GA can be hybrid with it for defense against attacks. In future, resource allocation strategy can be changes or investigate the effect of changing buffer size on attacks. Similar approach can be employed on network routers.

❖ Using Swarm Intelligent Water Drop Algorithm

Authors of [28] proposed a solution to mitigate the effect of DDoS attack using Swarm intelligent water drop algorithm. Intelligent water drop is used to get the path from which water drop (packet) can go with less soil(delay). GA’s Crossover is used to get the node with maximum speed in swarm nodes. Comparisons are done of number of connections between network with Swarm and without swarm nodes. Parameter over which comparison is done is PDR. There is swarm network which have number of nodes and when any client needs to connect with server, the request will be sent to the server will reach through that swarm network. A swarm node optimizes the path and secure from attack. One path for the communication in the swarm does not guarantee that next time the path will be same. So, the path is keeps on changing in the swarm network so that attacker could not get the information about the server. Swarm network uses the fast flux hosting therefor high robustness is achieved. 4,00,000 client nodes are communicating with the 10,000 swarm nodes network. DDoS attacks are simulated with 10,000 attacker nodes against the swarm network. With location anonymity, the security of server get increases and it does not allow SSL connections. Moreover, there are factors which are require maintaining the overhead of Swarm network. TTL values are for long period of time for any typical domain name but for fast flux network it is very short and hence disruption in the name server. This problem can be handled by deploying number of name servers in Swarm network but that may require more resources of network.

❖ Game Theoretical Approach

Authors of [29] 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. This algorithm detects the attacker and find the malicious nodes which is sending delayed ACK’s. There are three steps in which the attack and malicious node is detected. First, Monitor the network for number of SYN’s, ACK’s, number of half open connections, number of acknowledgements sent from multimedia sever to the node, number of ack’s sent to the sever by node, number of acknowledgements received and connection establish information. If half open connections are more, then detection procedure is called. Second, detection is carried out by intermediate nodes which verify towards client that the node is malicious by calculating SYN's received, ACK's sent and final ACK's received. Then the Five steps of game Theory are used. Which are, forming the game between the attacker and server, Finding the utility of Attacker and defender, Formulating strategy space for both an attacker and defender, finding the NASH equilibrium, the potential of the attacker to attack and potential of the defender to defend is also calculated. If some node is found which delays the network then it is put into black list. Third, if some attacker is found then all the communication from this node is terminated and some different node is selected for the new path. The quality of algorithm is checked by parameters like PDR, Control Overhead, throughput, End to End Delay, Jitter.

❖ SACK^2

It's an algorithm to detect SYN flood attack which is initiated by attackers having spoofing skills. Spoofing attackers means they always try to evade or bypass the detection policies. For all those attacks this SACK^2 method is implemented. It's an edge router based technique. This algorithm is implemented with limited implementation costs. This algorithm uses the SYN-ACK/CliACK pair to detect the attacker and the TCP port on which the attack happened. It also uses the Space efficient data structure Counting Bloom Filters to identify the CliACK. All the TCP connection information is saved in bloom filters. Information like IP addresses ports, initial sequence numbers of client and server. It first identifies five kinds of spoofs. Some of which uses SYN/FIN pair and other uses SYN/ACK. SACK^2 uses the difference between SYN/ACK and CliACK packets in number. It detects the start and end of SYN Flood attack on any victim server and port. It's impossible for an attacker to bypass this SACK^2 method. It has shortest response time for start and end of attacks. Architecture of SACK2 takes 6 tuple data and by using hash function sand counting bloom fit extract CliACK and port being attacked. Then according to the outputs, it turns into alert state or non-alert state. It is showed that SACK2 is the fastest and accurate detection algorithm than all the other that uses packet pairs. Although it has many advantages but its limitation is that SACK2 is only used for skillful spoofs attacks. [30]

❖ 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 Open Day Light controller. 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. The comparison of SLICOTS is done with the OPERETTA, which is a control plane to defend against SYN Flood attacks. Author have implemented both SLICOTS and OPERETTA on OpenDayLight and compared. The various parameters that are used are HTTP response time, number of Installed entries, attack detection time, CPU utilization. In all the cases SLICOTS performs better than the OPERETTA in SYN Flooding attacks detection and prevention. [31]

❖ Fuzzy Based Systems

It's a Fuzzy logic based network intrusion detection system to predict the Neptune SYN Flooding attack. 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. They have detected SYN Flood denial of service attacks in NSL KDD dataset. This dataset is generated from the KDD99 dataset by removing some redundant instances and reducing the size of dataset. In this the membership values (L_low, M_medium and H_high) of the three attributes and the output in the form of percentage intrusion and their membership functions are defined. Fuzzy rules are generated in the form of IF THEN statements. This was implemented in matlab. The decision tree was constructed in R Studio using the processed training data. For each attribute an average is calculated and these averages are tested with the fuzzy rules to predict the intrusion percentage in the test data. The metrics used are the proportion of the attacks predicted by the two algorithms and the accuracy of prediction. Results shows that the accuracy of decision tree is more than the proposed system [32]

❖ 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 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 signals are mapped according to the computer security. The various signals in immune systems are PAMP, Danger, safe and antigen. The PAMP signal is the ratio of incoming SYN packets and the outgoing SYN_ACK packets (when ratio is higher than median value of data input). The Danger signal is Number of incoming SYN packet. Safe signal is the ratio of incoming SYN packets and the outgoing SYN_ACK packets. (When ratio is lower than median value of data input). Antigen is the IP Address of attacker or user. The main function of this system is to distinguish between the attacker and legitimate user. In first phase Data is collected and in second phase analysis of data is done which distinguish between attacker and legitimate user. In the data collection phase, the dendritic cell collects information from environment which includes signals and antigens. If the costimulation value exceeds the threshold value then this cell is moved to the analysis phase and then MVAC value is calculated. The design of TCP flood DDoS attack using Dendritic Cell Algorithm will be implemented into a simple intrusion detection software using Python programming language and its package. Furthermore, there will be a research about the abnormal threshold of this intrusion detection based on MCAV value. [34]

❖ CNoA

Author of [47] proposed an approach to detect and prevent the TCP SYN Flooding spoofing attack. It detects the spoofed packet with the CNoA method. This Method generates a Challenging number and which is sent with the SYN+ACK packet from server to the client. So that the overall packet becomes SYN + ACK + Challenging Number. If the server received the ACK + challenging number then the client is not spoofed otherwise the packet is dropped because this packet is from spoofed IP. Here the computational overhead of appending the challenging number during the connection establishment is minimized. The spoofed packets are to found in the router itself so that the bandwidth consumed to transfer the malicious data from source to destination can be avoided.

❖ Exponential Weighted Moving Average (EWMA) algorithm

The author of [52] explained and investigated the Exponential Weighted Moving Average (EWMA) algorithm for detection of SYN flooding DDoS attacks in IoT infrastructure. this algorithm shows the tradeoff between detection rate, false alarm and detection delay also it further investigates that how performance is affected by tuning the parameters. This technique described, analyzed and discussed how the EWMA algorithm can be used for detecting DDoS attacks. In the simulation experiments author investigated how the performance of the algorithm is affected by the tuning parameters (α, β and k). These were efforts to find optimal parameter tuning for best EWMA algorithm performance. Author also investigated the trade-off between detection rate and false positive rate; detection rate and average detection delay. Furthermore, the experiments were conducted on real network traffic data with simulations for attack data synthetically generated for various attack intensity, i.e. low rate to high rate attacks. In these experiments it was found that optimal EWMA parameter tuning for this network traffic was: $\alpha = 0.5$, $\beta = 0.98$ and $k = 3$. Furthermore, it was found that the EWMA algorithm performs well for high rate attacks, however its performance collapses for low rate attacks. This further confirms the findings by the authors in [48]. Ongoing research work will include performance comparison of the EWMA with other anomaly detection algorithm, similar to the work of authors in [49-51]. This will also include efforts to improve current anomaly detection and change detection algorithms by developing algorithms that perform well under various characteristics of attacks.

❖ Scheduling based Highest Residence Time Ejection (HRTE) algorithm

This algorithm is a preemptive two-phase scheduling algorithm. This algorithm is useful for scenarios in which the service time of requests is unknown. According to this scheduling algorithm, while input queue is not full, HRTE is in its first phase and acts exactly like round robin algorithm. But upon queue becomes full and arriving requests are blocked, HRTE switches to its second phase during which ejects the job with the highest residence time and assigns the released capacity to the arriving requests. HRTE remains in this phase until a free capacity is available in the wafting queue. In other words, it has some similarities with SRTF, but when remaining time is unknown SRTF cannot be used. In this situation it is assumed that those requests that have the longest duration in the past will have longest remaining time as well, and hence will be rejected. When a connection request arrives at a TCP-based server, receives a buffer space of the backlog queue upon finding an inactive buffer space and is blocked otherwise. Now, consider a server under the SYN flooding attacks. Assume that in this computer each half-open connection is held for at most a period of holding time (h), and at most a number of maximum half-open connections (m) are allowed. It is assumed that a half-open connection for a regular request packet is held for a chance time which is exponentially distributed with parameter μ. The arrivals of the regular request packets and the attack packets are both Poisson processes with rates $\lambda 1$ and $\lambda 2$, respectively. The two arrival processes are independent. It is believed that the defense against this attack can be considered as a queue scheduling algorithm that differentiates attack requests from regular requests and then ejects the attack requests. This defense scheme, called HRT_SYN, tries to block attack connections and to prevent the system from allocating buffer space to attack connections. the proposed scheduling algorithm and keeps attack request from occupying system resources for a long time. According to this approach while there is free capacity for coming connection requests they will be accepted and inserted in the queue. But, when a connection arrives and faces with a full queue, then the HRTE scheduling algorithm is invoked and ejects the connection with the highest residence time. The ejected connection is likely an attack request that leaves the system to make the capacity free. This scheduling algorithm remove the half open connection running from longest time when the number of half open connection exceeds the limit and this proposed scheme behaves extremely better than the Linux TCP [60]

V. RELATED WORK: TCP SYN FLOODING ATTACKS DEFENSE MECHANISMS

Over the past years several methods have been proposed to detect the SYN Flooding attack [23]-[26]. They have used the characteristics of the attack and normal conditions to detect the attacks and they also focused on the characteristics of TCP packets. According to above, these works can be roughly classified as

1. In [23]- [24] 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 [25], is a detection algorithm that uses the difference between the number of outgoing SYN and incoming SYN+ACK packets.
3. In reference [26] the key is to match the SYN packets and CliACK packets. CliACK packets are ACK which client sent in the TCP handshake process.

In software defined networks various countermeasures of SYN Flooding attack are proposed [54]- [56]. In [54] A collaborative technique for SYN flooding attack detection and containment is proposed. They have developed some new components such as monitors and correlators in SDN architecture for mitigating DDOS attacks. The monitor continuously listens to ongoing traffic for detecting the SYN packets with different source IP addresses which denotes IP spoofing. When the monitor detects an attack, it informs the correlator by sending an alert message which contains a number of source IP addresses found in SYN packets. Upon receiving the alert message, the correlator issues a query of the switch flow table which the origin of the malicious traffic connected to it. If the correlator finds that the IP address in the alert message originated from a port that has had a different IP address in the original database, it concludes that the traffic is malicious. As a result, the correlator informs the controller and the controller blocks the malicious host. As [54] have mentioned, proposed technique works only for SYN flooding attack in which the attackers use spoofed IP addresses. Furthermore, this method requires connecting a monitor to each switch in the network which is not possible in general case it is the disadvantage of this attack. SPHINX [55] is a framework which has been proposed to detect security attacks in SDN. SPHINX is implemented on the control plane and can detect SYN flooding attack by investigating the rate of packet-in messages which correspond to the new SYN requests. If the rate of new SYN request is above the administrator-specific threshold, SPHINX raises an alarm. However, setting a control threshold for detecting SYN flooding attack is a static solution and would likely generate false alarms [56]. The reason is that SPHINX does not investigate the SYN requests to distinguish the legitimates from illegitimate requests and only strictly controls SYN packets with a predetermined threshold. Learning Automata algorithm is used for detection of SYN flooding attack [57]. This method gave a self-managing approach, in which host defends by dynamically optimizing its two parameters that is m (maximum no of half open connections) and h (hold time of each open connection). Simple queuing model is used to show network parameters of the system under attack. By merging Packet filtering technique with this algorithm will give perfect results for future. Author of [59] proposed a method to detect SYN flood attacks in File transfer protocol by checking the TCP header and IP header using the payload. In this method they performed packet filtering that focused on payload where the whole payload in the TCP header and IP Header was investigated. Every packet was analyzed by comparing normal of these two headers to infected ones. They also performed traffic monitoring in terms of the usage of the CPU for attack free network and attacked network and the history of the network in receiving data during the normal situation, downloading file and downloading a file during attacked situation. The CPU utilization showed an increase in usage for TCP SYN flood infected network as compared to normal network. There was a radical increase in the amount of data received and the downloading time when downloading file during attacked situation as compare to when there was file downloading only and normal situation. However, the authors did not report on any performance metric used to evaluate the packet filtering algorithm's performance. Therefore, it had not known that how well it could detect this attack.

4.1 Classification of TCP SYN Flooding DDoS defense methods

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

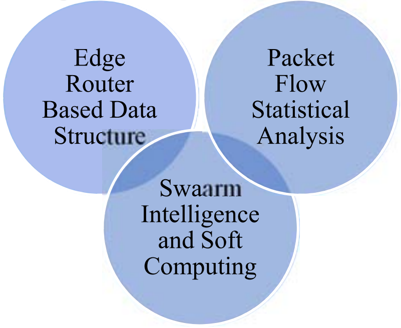

Edge Router Based Data Structure
Packet Flow Statistical Analysis
Swaarm Intelligence and Soft Computing

Figure 6 Classes of DDoS SYN flooding defense methods [65]

1. Edge Router Based Data Structure -Bloom Filter based Methods
2. Packet Flow Statistical Analysis based Methods
3. Swarm Intelligence and Soft Computing Based Methods

1. Edge Router Data Structure Based Defense Methods

A bloom filter is a space-efficient data structure used in router for pattern matching in many network communications. It is used to inspect packets and detect malicious packets based on many algorithms [61] [62].

Reference [63] focused on the low-rate agent and present a router-based detection scheme for it. The low rate DoS agent exploits the TCP's slow time scale of Retransmission Time Out (RTO) to reduce TCP throughput. In this case, the DoS attacker can cause a TCP flow in RTO state by sending high rate requests for short-duration bursts. Therefore, The TCP throughput at the victim side will be reduced during the attacking time on low-rate DoS agent. The proposed scheme is based on the TCP SYN-SYN/ACK protocol pairs with the consideration of packet header information (both sequence and Ack. Numbers). The Counting Bloom Filter (CBF) is used to avoid the effect of ACK retransmission, and the change point detection method is applied to avoid the dependence of detection on sites and access patterns. (see Fig 7)

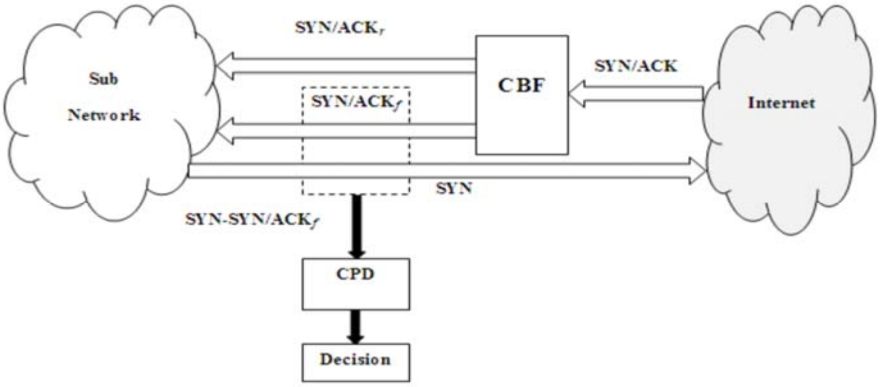


Figure 7 Router Based Bloom Filter Scheme [65]

Traceback based Bloom Filter (TBF) was adopted to record the TCP session statistics Internet Protocol Time To Live (IP-TTL) of SYN packets. As the attacks start, the SYN packets and IPTTL statistics were matched to differentiate the attacks' packets and record IP-TTL, because SYN-flooding attacks, are too time-expensive and consume the resources such as the memory. For instance, when SYN-flooding started, victim servers have to call for a lot of memory, usually more than 500MB, to store the attack packets [36].

The main advantages and disadvantages for each scheme are summarized in Tables below. For the router based detection scheme, the main advantages and disadvantages of important methods are critically examined in Table 1.

2. Packet Flow Statistical Analysis based Methods

Many efforts have been undertaken in using the packet flow of statistics to detect DoS attacks [38]- [41].

[38] presented a statistical scheme to detect the SYN-flooding accuracy on network anomalies using flow statistics obtained through packet sampling. The network anomalies generate huge number of small flows, such as network scans or SYN-flooding. Due to this reason, it is hard to detect SYN-flooding when performing packet sampling because the network flow may be either bursty (non-linear) or under the normal flow rate. Their model is based on

two steps: the first step, analytical model was developed to quantitatively evaluate the effect of packet sampling on the detection accuracy and then investigated why detection accuracy worsens when the packet sampling rate decreases. In addition, it is shown that, even with a low sampling rate, the detection accuracy was increased because the monitored traffic was partitioned into groups. The results show that the proposed mechanism is demonstrated to have the capability of detecting SYN-flooding attack accurately.

According to [39], a new detection method for DoS attack traffic based on the statistical test has been adopted. Investigation of the statistics of the SYN arrival rate revealed that the SYN arrival rate can be modeled by a normal distribution. A threshold for maximum arrival rate to detect SYN-flooding traffic has been established. In addition, the threshold for incomplete three-way handshaking packet ratio to detect possible DoS traffic also has been determined. This mechanism was shown to be effective in detecting SYN-flooding attack, but for the normal traffic threshold, the value is not accurate for the whole packet flow, especially during the attacking time.

For statistical analysis, the main advantages and disadvantages of important methods are critically examined in Table 1.

3. Swarm Intelligence and Soft Computing Based Methods

Swarm Intelligence and Soft Computing Methods (Fuzzy and Neural network) [42,27,28] are used for defense against the SYN Flooding attacks. [27] used the particle swarm optimization algorithm for tuning parameters to best defense positions led to mitigate the effect of SYN flooding attack on server. Author of [28] proposed an Intelligent Water Drop Algorithm with fast flux swarm network to defend from the TCP SYN Flooding attack. A fuzzy logic based system for detecting SYN-flooding attacks has been adopted. Fuzzy logic helps solving the systems which have elements of uncertainly. Fuzzy logic is appropriate for approaching the nonlinear systems

Author of [42] proposed a system represented by two blocks shown in figure 8. The first one is the packet classification block which classifies incoming network traffic packets, where the header of each captured packet is checked to see if it is a TCP SYN packet; if the fragment offset value in the header is zero, then it is a TCP packet. If the SYN flag of the flag bits in this TCP packet is one, then it is a SYN packet (attack possibility). The packet classification block collects the TCP SYN packets for a predetermined t time and gives them to the fuzzy logic system, which is the second block of the proposed system. The t in this work was 5 seconds, while the second block of the proposed system is a fuzzy logic system. This block is responsible for SYN-flooding attack detection. The detection accuracy of the proposed system was compared with Cumulative Sum (CUSUM) for five attacks and showed a high accuracy and low false-negative rate and generate an earlier alarm than CUSUM algorithm which it is an ideal algorithm for identifying DoS attacks based on the measurement for the mean in traffic before, and after they detect comparing with the threshold value.

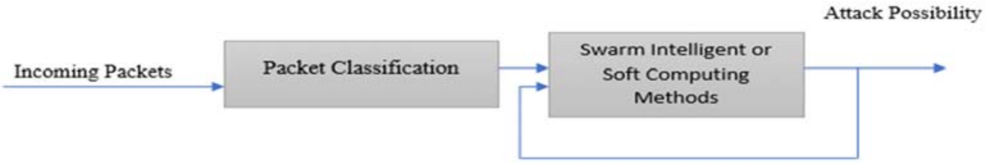


Figure 8 System Based on the Swarm Intelligence and Soft Computing Methods

In the Figure 8 shown above, Incoming packets are classified into attack packets and regular packets and then Swarm Intelligent or Soft computing techniques is used, it can be Fuzzy logic. Particular algorithm is used and this algorithm is used for defense against the TCP SYN flooding DDoS attacks.

On the other hand, [64], adopted a hierarchical off-line anomaly network intrusion detection system based on Distributed Time-Delay Artificial Neural Network(DTDANN).

The work aims to solve a hierarchical multi class problem in which the type of attack (DoS) detected by a dynamic neural network. Actually, the data set used by this method is old data and does not reflect the current behavior of attack packets. For fuzzy logic and neural network detection techniques under the carter gory of artificial intelligence, the main advantages and disadvantages of important methods are critically examined in Table 1

In this section a comparison and their advantages and disadvantages with the technique of each method 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. [35]	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.	The main advantages of this technique is that it uses the Change Point Detection method based on nonparametric Cumulative Sum (CUSUM) that is used for avoidance of discrepancy in TCP and resending of SYN packets.	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 [36]	Edge Router Based Data Structure	It records the TCP sessions statistics (IPTTL) of SYN packets with Bloom Filters and compare it with SYN packets to detect the Attacker's packet.	1.Records the TTL from statistical measurement with bloom filter data Structure. 2. Shows great results when packets sent based on groups.	False Positive cause the difficulty to measure the detection accuracy. False positive Results have been seen in using bloom filter data structure in multiple packets' case. The false positive occurs when the detection method Mistakenly flags a normal traffic as being attacked.

Reference	Category	Technique Used	Advantages	Disadvantages
N. N. P. Mkuzangwe et. al. [58]	Edge Router Based Data Structure	It detects the TCP SYN flooding attack by implementing the adaptive threshold and CUCUM algorithm then combine them using OR operator.	Logic OR operator outperformed better results than the two algorithms in terms of detection accuracy and detection delay.	This method gives high False alarm ratio which needs to be less.
L. Yun et al. [37]	Edge Router Based Data Structure	The proposed method is Detection of validity of outgoing SYN and incoming SYN-ACK in edge router which connects end hosts to the internet. Hash table is maintained that shows the mapping process by checking SYN and SYN-ACK packets.	1. The new method guarantees that each packet sent by the client is valid by two parts storage module and inspection module. 2.Use of Hash table is efficient to store IP addresses. 3. Proposed method accurately detects the SYN-Flooding attack based on the mapping.	In case of congestion of network flow the process of storing the source and destination IP addresses is difficult which results incorrect values in the mapping table.
Miao, L et. al. [22]	Edge Router Based Data Structure	Eight attack scenarios are introduced and they propose a Netflow based SYN Flooding attack detection algorithm at live network borders.	1. Darknets are usually fixed and can be known by attackers. Therefore, attackers might evade them to avoid detection. Live networks on the contrary are hard to avoid and thus stand a better chance to observe certain attacks. 2. It detects attacks targeting inside hosts and then measures can be taken to protect them. 3 It detects attacks internal participants and the detection	A differential threshold configuration mechanism is not there which might be useful for the popular and regular hosts. Also, overhead of maintaining the live networks.

Reference	Category	Technique Used	Advantages	Disadvantages
			results can be utilized to understand botnet activities.	
R. Kawahara, et al. [38]	Packet Flow Statistical Analysis	To detect the effect of packet sampling on the detection accuracy, an analytical model was developed.	Uses a threshold value to find the problems in the flow rate which is resolved based on natural traffic Statistics. Moreover, the traffic has been partitioned into batches to increase the Detection accuracy of Network problems.	1.The new proposed analytical model is not detecting the SYN-flooding at low sample rate. 2.In addition, the statistical analysis limits the performance of network communication as the overhead for real time packets sampling is high.
C. L. Chen [39]	Packet Flow Statistical Analysis	In this method there is statistical test for SYN arrival rate. Moreover, experiments were done to find the threshold value. This value is checked against the SYN-Flooding threshold value to detect the attack.	1.In this control is done with the threshold value makes it more advantageous. 2. It reflects the nature of packets flow and measurement of False positive and False negative values.	1.To determine the normal traffic there is not any threshold of SYN and SYN-ACK packets and it's difficult to find that value due to False Positive and Negative. .

Reference	Category	Technique Used	Advantages	Disadvantages
C. Chin-Ling [40]	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.
M. Dhawan, et. al. [55]	Packet Flow Statistical Analysis	It can detect SYN flooding attack by investigating the rate of packet-in messages which correspond to the new SYN requests. If the rate of new SYN request is above the administrator-specific threshold, SPHINX raises an alarm.	It strictly controls SYN requests with a predefined threshold.	1. Using a control threshold for detecting SYN flooding attack is a static solution and would likely generate false alarms 2. SPHINX does not investigate the SYN requests to distinguish the legitimates from illegitimate requests

Reference	Category	Technique Used	Advantages	Disadvantages
G. Kanwal, &Rshma, C [41]	Packet Flow Statistical Analysis	1. The methodology is to deploy the real-time detection system at the leaf router to detect and monitor the Dos attack. 2.At the leaf router, system analyse and detect the attack efficiently in normal operation. 3. Samples the traffic from each IP to make the traffic synchronization.	1. System can detect the attacker, victim, normal user by a quick identification method. 2. This method checks the differences between the request and response. 3. Results verify that this system can detect the real-time attacks of SYN-Flooding type.	This technique takes the CPU time and Consumes memory
T. Tuncer and Y. Tatar [42]	Swarm Intelligence and Soft Computing	Fuzzy logic membership functions are used in this method to defend from the DoS attack.	This method gives the best results as compared to the CUSUM algorithm especially in False Positive and Negative at low rate flow of packets.	Due to linear and burst property of flow it is difficult to model the traffic before and after the attack. Also, this technique depends on offset in a TCP packet.
S. Jamali and V. Shaker [27]	Swarm Intelligence and Soft Computing	(PSO_SYN) Particle Swarm optimization algorithm is used to mitigate the effect of SYN Flooding attack	This method shows good results i.e. it reduces the effect of SYN flooding attack.	Algorithm sometimes trapped in local best solutions.
Ruiping Lua and Kin Choong Yow [28]	Swarm Intelligence and Soft Computing	Intelligent Water Drop algorithm is used to mitigate the DDoS attack with Swarm nodes.	This method provides location anonymity, the security of server gets increases. And attacker will not get the location of the server which led to secured server from the DDoS attacks	Overhead of maintaining so much swarm nodes.

4.2 Comparison based on General Parameters

Different methods use different parameters so general parameters have been taken. 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. Comparison based on these parameters are summarized in the Table 2

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. [35]	Edge Router	Flexible	Flexible	R	Yes	Yes	High	Very good	No
H. Tang, et al [36]	Edge Router	Low	Low	R	Yes	Yes	High	Good	Good
N. N. P. Mkuzangwe et. al. [58]	Edge Router	High	Flexible	N	N	No	High	Good	Fair
L. Yun et al. [37]	Edge Router	Flexible	Flexible	R	No	No	High	Very good	Fair
Miao, L et. al. [22]	Edge Router	High	Flexible	R	Yes	Yes	Low	Good	Good
R. Kawahara, et al. [38]	Packet Flow	High	High	R	No	No	High	Good	No
C. L. Chen [39]	Packet Flow	High	High	R	Yes	Yes	High	Good	No
C. Chin-Ling [40]	Packet Flow	NA	NA	N	No	No	High	Good	No
M. Dhawan, et. al. [55]	Packet Flow	Flexible	Flexible	R	No	Yes	High	NA	NA
G. Kanwal, &Rshma, C [41]	Packet Flow	High	High	R	Yes	Yes	NA	Good	NA
T. Tuncer and Y.	SI and SC	Flexible	Flexible	R	Yes	No	High	Good	No

Reference	Category	CPU Time	Memory Required	R/ N`	Scalability	Unknown attack detection	False Positive	Accuracy Detection	
								High traffic rate	Low traffic rate
Tatar [42]									
S. Jamali and V. Shaker [27]	SI and SC	Flexible	Flexible	R	Yes	NA	NA	Good	Good
Ruiping Lua et al. [28]	SI and SC	High	High	R	Yes	NA	NA	Good	Good

VI. IMPORTANT REQUIREMENTS OF THE SYSTEM TO DETECT AND MITIGATE THE TCP SYN FLOODING ATTACKS

As section 3 and 4 discussed about various defense methods of TCP SYN Flooding DDoS. The advantages and disadvantages of all these methods had also been discussed. However, there are still limitations present in the system which prohibit the detection and mitigation of attack, the System can be wireless(WN). This section will list various important requirements of the WN system to detect and mitigate the SYN flooding attacks.

In defending from the SYN Flooding attacks the system should have following features

a. Differentiation and recognition between regular and attack traffic must exist within the network. Firewalls, for example, cannot differentiate between normal and malicious or anomalous traffic [77]. Also, some firewalls consider congestion, which is normal in any network, as DoS traffic.
b. It is very important to detect a DoS attack as rapidly as possible before it achieves its aim. DEMEM, as per [78], illustrate its ability to watch up to a one-hop neighbor node. Messages are used to interchange the data between nodes and to detect the intrusion. There is one disadvantage of this technique: it cannot find and perceive combined attacks, such as the attacks of wormhole as both the attacking nodes falsely show that they are actual neighbors.
c. To know and identify the origin of the attack between the nodes, traceback must be performed. An attacker spoofed the network's real IP address. The Hello packet is used in the method established by [79] to find and perceive SYN Flooding DDoS attacks, where the Hello packet ensures that the regular node will be applied. Unfortunately, there is no obvious trace-back procedure to determine the source of the attack, which is the only disadvantage. As mentioned before, WN have few restrictions, such as limited power. Thus, it is unreasonable to say that a node is harmful only because it does not respond to the other node.
d. Also, as a result of the power restrictions of WN, the detection method should not contain large amounts of information. Unfortunately, the exchange of data results in massive loads, which are unsuitable for WNs.
e. There needs to be a distinction among various categories of nodes, such as regular, harmful, and selfish nodes; there must be a difference between a selfish and a harmful node. Selfish nodes are the nodes that refuse to collaborate with the rest of the nodes within the network to run network services and perform actions. Malicious nodes are defined as nodes that apply attacks to

decrease the network's performance. Many works have focused on identifying misbehaving nodes in WN as selfish nodes. Abstractly, the defense scheme used to detect DoS attacks must have the ability to perceive the entire categories of misbehavior, including both harmful and selfish nodes.

f. Every node should transmit and deliver the wanted packet to its ultimate endpoint. The route that is the least jammed, rather than the shortest route, should be used by the node. These points highlight the value of collaboration among nodes. A reputation encompasses visions or views that humans keep in mind concerning a person or a thing. Thus, this approach selects a route that depends on the reputation of a given node; this reputation is obtained by interchanging and comparing data among nodes.

g. Each node is primarily able to identify the neighbor’s position as regular, harmful, or selfish. There are various factors that must be taken into account in WN, including the active topology, movement, stable infrastructure, and constraints on power and bandwidth. In this way, a node would not depend only on its own views, rather it is supposed to consider the visions of the other nodes.

h. It is necessary to isolate the misbehaving nodes from future transmission and services in the network for a particular amount of time. As such, there must be an examination to assess whether the nodes are still being harmful, or if they are back to their regular status. Thus, it would minimize the network’s performance. The notion of restoration might be applied to the harmful nodes to drastically enhance the network. Rehabilitation involves returning the network to a secure state.

i. Because of the nature of WN, particularly given its mobile and active topology, trust among nodes is not transitive. Trust is the solid belief that an individual is secure, trustworthy, truthful, and well-mannered. Also, the same individual would not hurt you in any circumstances. In addition, because of the nature of WNs, transitive trust among nodes is not possible, and trust in WNs encompasses various elements that denote the reliability of the nodes. Therefore, the position and category of a given node would aid in bypassing vulnerable nodes in some transmissions. Mainly, the node’s position status must be examined periodically due to not being constant. The method in [79] uses the trust and reputation of each node; trust in a node is related to the value of its reputation. In their work, there were three types of trust: trustworthy=1, untrustworthy=–1, and trustworthy undecided=0. The meaning of trustworthiness as it pertains to nodes means a particular node behaves appropriately and depends on the reputation value afforded by remaining nodes. An untrustworthy node is a harmful node and must be bypassed in the process of evaluation of the distributed IDS. A node with undecided trustworthiness is normally a new node in the network, and should pay attention through the IDS evaluation process. There is one drawback associated with this particular method which is, other factors should be used to identify a node’s level of trustworthiness, rather than the value of reputation provided by other nodes.

VII. CONCLUSION

This paper presented the DoS and DDoS SYN Flooding attacks with WN and their trends over the past with attack incidents worldwide. 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, is also discussed. Limitations of Wireless Sensor Networks are also presented**.** Some of New Defense Methods of SYN Flooding attack are also summarized in related work with advantages and disadvantages of each. These methods can be categorized based on the methods they are using to defend from attack, which are Edge router based data structure methods, Packet Flow Statistical analysis based method, Soft computing and Swarm Intelligence based methods. This paper has listed various important requirements a system should have in order to defend from the SYN Flooding attacks. 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 schemes 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 security report (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/ITU-D/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] Parker Donn. Toward a New Framework for Information Security, Computer Security Handbook, 4th ed., edited by Seymour Bosworth and M. E. Kabey. New York: John Wiley & Sons, 2002.

[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] E. Bertino, D. Leggieri, and E. Terzi, “Securing DBMS: Characterizing and Detecting Query Flood,” Proc. Ninth Information Security Conf. (ISC ’04), Sept. 2004.

[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] A. Networks, “The 11th annual worldwide infrastructure security report (wisr),” https://www.arbornetworks.com/insight-into-the-global-threat-landscape/

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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

[28] 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

[29] 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

[30] 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

[31] 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

[32] 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

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

[34] 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

[35] 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.

[36] 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.

[37] 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.

[38] R. Kawahara, *et al.*, "Detection accuracy of network anomalies using sampled flow statistics," *International Journal of Network Management,* pp. 1959-1964, 2007.

[39] L. Chen, "Detecting distributed denial-of-service attack traffic by statistical test," in *Third International Conference on Communications and Networking*, China, 2008, pp. 1253-1257

[40] 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.

[41] 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.

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

[43] Singh, Karan, and Rama Shankar Yadav. "A Review Paper on Ad Hoc Network Security" International Journal of Computer Science and Security (IJCSS) 1, no. 1 (2007): 52.

[44] Nawneet Raj; Priyanka Bharti; Sanjeev Thakur," Vulnerabilities, Challenges and Threats in Securing Mobile Ad-hoc Network ", Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference, pp. 771 - 775, 2015.

[45] W. M. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007. [Online]. Available: http://tools.ietf.org/html/rfc4987.

[46] W. Eddy, "Defenses Against TCP SYN Flooding Attacks", Cisco Internet Protocol Journal Volume 9, Number 4, December 2006,

[47] Kavisankar, L., and C. Chellappan. "CNoA: Challenging Number Approach for uncovering TCP SYN flooding using SYN spoofing attack." *arXiv preprint arXiv:1110.1753* (2011).

[48] V. A. Siris and F. Papagalou. Application of anomaly detection algorithms for detecting SYN flooding attacks. Comput. Commun. 29(9), pp. 1433-1442. 2006.

[49] P. Machaka, A. McDonald, F. Nelwamondo and A. Bagula. Using the cumulative sum algorithm against distributed denial of service attacks in internet of things. Presented at International Conference on Context-Aware Systems and Applications. 2015, .

[50] P. Machaka and A. Bagula. "An investigation of scalable anomaly detection techniques for a large network of wi-fi hotspots," in Scalable Information Systems 2014, .

[51] P. Machaka. "Drought monitoring: A performance investigation of three machine learning techniques," in Context-Aware Systems and Applications 2014.

[52] Machaka, P., Bagula, A., & Nelwamondo, F. (2016, November). Using exponentially weighted moving average algorithm to defend against DDoS attacks. In *Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech), 2016* (pp. 1-6). IEEE

[53] A. K. Pandey and C. Pandu Rangan, "Mitigating denial of service attack using proof of work and Token Bucket Algorithm," in Proc. IEEE Stmnvxudents' Technology Symp. (TechSym), 2011, pp. 43–47 IEEE, 2015, pp. 659–664.

[54] T. Chin, X. Mountrouidou, X. Li, and K. Xiong, "Selective packet inspection to detect dos flooding using software defined networking (sdn)," in 2015 IEEE 35th

International Conference on Distributed Computing Systems Workshops. IEEE, 2015, pp. 95–99.

[55] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, “Sphinx: Detecting security attacks in software-defined networks.” in NDSS, 2015.

[56] T. Chin, X. Mountrouidou, X. Li, and K. Xiong, “An sdn-supported collaborative approach for ddos flooding detection and containment,” in Military Communications Conference, MILCOM 2015-2015 IEEE.

[57] Bekravi, M., S. Jamali, and G. Shaker, Defense against SYN-Flood denial of service attacks based on learning automata. arXiv preprint arXiv:1208.5037, 2012.

[58] N. N. P. Mkuzangwe, A. McDonald and F. V. Nelwamondo, "Implementation of anomaly detection algorithms for detecting Transmission Control Protocol Synchronized flooding attacks," *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, Zhangjiajie, 2015, pp. 2137-2141.

[59] Haris, S. H. C., Ahmad, R. B. and Ghani, M. A. H. A. "Detecting TCP SYN flood attack based on anomaly detection." *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*. IEEE, 2010.

[60] Jamali, shahram, and gholam shaker. "defense against syn flooding attacks: a scheduling approach." (2014): 55-61.

[61] C. E. R. Mikko Sarela, *et al.*, "BloomCasting: Security in Bloom filter based multicast," in *Aalto University, Espoo, Finland*, Finland, 2010.

[62] F. S. Tabataba and M. R. Hashemi, "Improving False Positive In Bloom Filter," *IEEE,* pp. 1-5, 2011.

[63] D. Nashat, *et al.*, "Router based detection for low-rate agents of DDoS attack," in *International Conference on High Performance Switching and Routing*, Tohoku, 2008, pp. 177-182.

[64] 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.

[65] Manna, Mehdi Ebady, and Angela Amphawan. "Review of syn-flooding attack detection mechanism." *arXiv preprint arXiv:1202.1761* (2012).

[66] T. Kaur, K. K. Saluja and A. K. Sharma, "DDOS attack in WN: A survey," *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*,Jaipur, 2016, pp. 1-5.

[67] Kumari, J.; Prachi, "A comprehensive survey of routing protocols in wireless sensor networks," in Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, vol., no., pp.325-330, 11-13 March 2015

[68] Yun Zhou; Yuguang Fang; Yanchao Zhang, "Securing wireless sensor networks: a survey," in Communications Surveys & Tutorials, IEEE , vol.10, no.3, pp.6-28, Third Quarter 2008.

[69] Sedef Gunduz, Bilgehan Arslan, Mehmet Demirci, "A Review of Machine Learning Solutions to Denial-of-Services Attacks in Wireless Sensor Networks", *Machine Learning and Applications (ICMLA) 2015 IEEE 14th International Conference on*, pp. 150-155, 2015.

[70] R. Anderson and M. Kuhn, "Tamper Resistance - a Cautionary Note," in *The Second USENIX Workshop on Electronic Commerce*, Oakland, California, USA, 1996, pp. 1-11.

[71] I. F. Akyildiz. and I. H. Kasimoglu. "Wireless sensor and actor networks: research challenges." Ad hoc networks 2(4) , 351 367, 2004.

[72] I. F. Akyildiz T. Melodia, et al. "A survey on wireless multimedia sensor networks." Computer Networks 51(4). 2007, 921-960.

[73] M. Hefeeda, and M. Bagheri. "Forest fire modeling and early detection using wireless sensor networks." Ad Hoc &

Sensor Wireless Networks 7, 169-224, 2009.

[74] K. Sunitha, and H. Chandrakanth. "A Survey on Security Attacks in Wireless Sensor Network." International Journal of Engineering Research and Applications (IJERA) 2(4), pp.1684-1691, 2012.

[75] Goyal, Priyanka, VintiParmar, and Rahul Rishi. "MANET:Vulnerabil of Computational Engineering & Management 11 (2011): 32-37.

[76] Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala, "*Security in Wirelesss Sensor Network : Issues and Challenges"*, IEEE int. Conf. on Space Science and Communication (IconSpace), 2013.

[77] Gupta, B. B., Joshi, R. C. &Misra, M. (2012). Distributed Denial of Service Prevention Techniques. arXiv preprint arXiv:1208.3557.

[78] Tseng, Chinyang Henry, et al. "DEMEM: Distributed evidence-driven message exchange intrusion detection model for MANET." Recent Advances in Intrusion Detection.Springer Berlin Heidelberg, 2006.

[79] Chhabra, Meghna, Brij Gupta, and Ammar Almomani. "A Novel Solution to Handle DDOS Attack in MANET." Journal of Information Security 4.3 (2013).

[80] E. Darra and S. K. Katsikas, "Attack detection capabilities of intrusion detection systems for Wireless Sensor Networks," *IISA 2013*, Piraeus, 2013, pp. 1-7.

[81] D.G. Padmavathi, M. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009

[82] T.G. Lupu, "Main Types of Attacks in Wireless Sensor Networks", Recent Advances in Signals and Systems, International Conference in Recent Advances in Signals and Systems, 2009.

[83] K. Sharma, M.K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks (MANETs), 2010

[84] M.S.I. Mamun, A.F.M. Sultanul Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network", International Journal of Network Security & Its Applications (IJNSA) 2(3), 2010

[85] H.C. Chaudhari, L.U. Kadam, "Wireless Sensor Networks: Security, Attacks and Challenges", International Journal of Networking, Vol. 1, Issue 1, pp-04-16, 2011.

[86] Celia Li, Zhuang Wang, Cungang Yang, "Secure Routing for Wireless Mesh Networks", International Journal of Network Security, Vol.13, No.2, pp.109–120, 2011.

[87] M.R. Ahmed, X. Huang, D. Sharma, "A Taxonomy of Internal Attacks in Wireless Sensor Network", International conference on information systems, 2012.

[88] R. Dubey, V. Jain, R.S. Thakur, S.D. Choubey, "Attacks in Wireless Sensor Networks", International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, 2012.