Denial of service attacks – an updated perspective

Gulshan Kumar
Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India

ABSTRACT
Network security is a specialized field consisting of the provisions and policies to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources as well as ensuring their availability through proper procedures. Many security mechanisms tools are being developed and deployed to defend against network attacks and to make the network computing resources available to the legitimate users. In spite of all these efforts, the organizations around the world continue to suffer security attacks specially called denial of service (DoS) attacks. DoS attacks constitute one of the major threats and among the hard security problems in today’s Internet. These attacks can easily consume computing and communication resources of the victim or disrupt clog availability of resources to the intended users within a short period of time. The problem is a serious concern in today’s network security field. Several defence mechanisms have been proposed to tackle the problem of DoS attacks. This paper highlights a structural way to understand DoS attacks with respect to different layers of the Open System Interconnection (OSI) reference model proposed by International Organization of Standardization. Moreover, various attack vectors, attack tools, and trends in detection and mitigation mechanisms are delineated. The goal of the paper is to communicate an updated perspective of DoS attacks and their detection and mitigation mechanisms for a better understanding of these attacks; consequently more efficient and effective mechanisms to combat these attacks may be developed.

1. Introduction

With the rapid growth of technology, application service providers, network service providers, cloud services and availability of network capable mobile devices, our dependence on the networks is increasing day by day (Kumar, Kumar, & Sachdeva, 2010b; Nsfocus, 2014). For example, we are now more dependent over the networks for online banking, information retrieval, online shopping and many more. This has changed the scenario in terms of business and other information-based systems, but also opened an avenue for network attackers to mount a large number of attacks against network resources and making network service unavailable to the legitimate users. Motives for these attacks appear equally diverse such as personal reasons, the prestige, criminal, commercial, or ideological in nature (Chauhan, Mishra, & Kumar, 2012; Kumar & Kumar, 2014; Kumar, Kumar, & Sachdeva, 2010a; Schneider, 2012; Verizon, 2013).

The main objectives of network security are to ensure availability, integrity and confidentiality of network resources (Kumar et al., 2010b). Denial of service (DoS) attack disrupts the availability of network resources to legitimate users. A DoS attack usually either involve attackers sending messages to exploit certain vulnerabilities leading to the abnormality or paralysis of network-based systems, or sending an enormous amount of regular messages swiftly to a single node to run out the system resources that result in crash of the entire system (Nsfocus, 2014). A DoS attack is called a distributed denial of service (DDoS) attack if it gets originated from multiple distributed sources. In DDoS attacks, a large number of controlled bots (also referred to as zombies) are used from distributed locations to initiate a huge amount of traffic against the victim(s).

DoS attacks have been a significant problem for many years, but remain to be un-resolved. In the recent past, DoS attacks are assumed to be an important issue in the field of network security because these attacks incidents continue to prevail (Alam, 2014). A research survey conducted in the first quarter of 2014 by Prolexic highlighted that there is a 47 % increase in total DDoS attacks in comparison to first quarter of 2013 (Prolexic, 2014a). These attacks can be easily launched by exploiting flaws in Internet protocols such as TCP/IP and UDP. Moreover,
availability of free attack tools such as BackTrack, Metasploit, Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC) and many more also simplifies the attack process. These tools automate the process of creating DoS types of attacks, allowing even non-technical people to quickly and easily threaten their choice of website.

Generally, DoS attackers exploit TCP/IP and UDP protocols for launching these attacks. Either, they direct a huge amount of abnormal network packets towards the victim(s) – which results in overloading of their network resources such as consuming entire bandwidth and memory – or they exploit vulnerabilities in network protocols to fail the functioning of network devices. In both the cases, network resources or services are restricted for or prevented from the intended users. Major difficulty in detecting such attacks is that network traffic consists of a mix of normal or legitimate traffic and abnormal or attack traffic. Moreover, in most of the cases, attack traffic looks like normal traffic.

Many researchers reviewed exiting DoS attack detection techniques (Carl, Kesidis, Brooks, & Rai, 2006; Modi et al., 2013), and mitigation techniques (Hoffman, Zage, & Nita-Rotaru, 2009; Wu, Chen, Wu, & Cardel, 2007). Peng et al. presented a survey study focused on network-based defence techniques (Peng, Leckie, & Ramamoohanarao, 2007), while Durcekova et al. focused on application-layer-based DoS attacks (Durcekova, Schwartz, & Shahmehri, 2012). Gupta et al. presented their study of DoS attack detection at MAC layer for wireless network (Gupta, Krishnamurthy, & Faloutsos, 2002). Different researchers considered one layer at a time but not all the layers simultaneously. To the best of our knowledge, no comprehensive study exists for DoS attack detection and their mitigation techniques with respect to Open System Interconnection (OSI) reference model for their better understanding at various layers of the model. So, it became a motivation factor for us to present a comprehensive perspective of DoS attacks, attack vectors, attack tools, their detection and mitigation technique with respect to OSI reference model layers. In our previous work, we presented a limited study for understanding DoS attacks using the OSI reference model (Kumar, 2004).

In this paper, we attempt to introduce an updated perspective of DoS attacks by presenting the state of the art in the field through a classification of DDoS attacks with respect to different layers of the OSI reference model and a recent trend in the defense mechanisms that can be used to combat these attacks.

Article overview: following this introduction, Section 2 highlights the adversaries behind the DoS attacks. Section 3 introduces the basic functions of the OSI reference model. Section 4 details the possibilities of DoS attacks with respect to the layers of the OSI reference model. Next section describes the possible DoS attack detection and mitigation mechanisms and their current trends in the field of network security. Finally, the paper concludes with the current scenario of DoS attacks.

2. Who is behind the DoS attacks?

In order to address network threats in a better way and secure network resources thoughtfully, it is essential to know who is most possibly behind the attacks. Various types of opponents are as follows:

- **Extortionists**: They menace to inactivate the web service and then ask for the ransom money to put a stop to an attack.
- **Exfiltrators**: They use a DoS attack to distract interest from their actual aim – stealing data for money in a form of intellectual property or credit card numbers.
- **Hacktivists**: They are different than rest of the opponents. They are irritated and look for making a political announcement or stand out a focus on a cause.
- **Competitors**: Your competitors may cause your site inactive to gain an advantage; or they might screen scratch information on your site, for example, to determine and beat your pricing.

3. Briefs of the OSI reference model

In the recent past, the skyrocketing popularity of network-based information systems and applications has attracted a sudden increase in the numbers, types, magnitudes and costs of attacks that particularly intend their vulnerabilities. Usually, these attacks belong to the following categories:

- DoS attacks,
- Attacks that steal confidential data, such as SQL injection and other command injection attacks.

Recently, there occurred a large number of DoS attack incidents. DoS attacks take many forms, and utilize many attack vectors. The sheer number of DoS attacks makes understanding for better prevention of a challenging task. Many researchers classified DoS attacks based upon different criteria such as degree of automation, random scanning, communication mechanism, exploited vulnerabilities (Mirkovic & Reiher, 2004), attacked protocol level, attack rate dynamics, impact (Doulgeris & Mitrokotsa, 2004) and many more. The detailed classification can be further studied in Doulgeris and Mitrokotsa (2004), Mirkovic and Reiher (2004), and Saafan (2014).
The researchers attempted to present a clear-cut view of DoS attacks and their countermeasures. But still, we believe that a more simplified and effective view of these attacks can help the people think about the attacks, their impact and hence their countermeasures. In order to present a simplified view of attacks, we examined them at a level of various layers of the OSI reference model. Because the OSI reference model details each phase of the process involved to connect a computer to the network and communication of data, most of the researchers, developers and manufacturers use the OSI model as a common platform to improve network communications.

There are seven layers in total, each fulfilling its own purpose in a connected network framework called the OSI model. In a nutshell, the OSI model is separated into seven layers that transport data up and down the chain, from the user all the way to the physical server and back again as depicted in Figure 1 (Miller, 2014). Each layer contains a set of protocols and is responsible for sending/receiving protocol data unit (PDU) to/from its counterpart. These protocols are responsible for carrying out its each layer’s assigned functions. The brief break down of functions of different layers is shown in Figure 2 and described in the following paragraphs:

**Layer 7**: Application layer allows the access to network resources. It is responsible for sending and receiving data from one application to another. The unit of communication (PDU) at this layer is message/data.

**Layer 6**: Presentation layer is responsible to format data for exchange between points of communication like translates, encrypts and compress the data.

**Layer 5**: Session layer is responsible for governing/establishing/terminating sessions over the network.

**Layer 4**: Transport layer is aimed to provide reliable delivery of message/data from one process to another. It ensures error free, in sequence and without duplication of transmission of packets. The unit of communication (PDU) at this layer is a segment, datagram or packet depending upon the protocol used in this layer.

**Layer 3**: Network layer is handling the movement of packets from source to destination. It provides addressing and routing to the packets. The unit of communication (PDU) at this layer is the packet.

**Layer 2**: Data link layer manages the error-free transmission of data over physical media. The unit of communication (PDU) at this layer is a frame.

**Layer 1**: Physical层 deals with transmission of 0s and 1s over transmission media. Its function involves translation of bits into signals. The unit of communication (PDU) at this layer is bit.

### 4. DoS attacks and the OSI reference model

In this paper, we attempt to introduce the DoS attacks by presenting an updated perspective for their classification and recent trends in detection and mitigation mechanisms. DoS attacks are classified with respect to seven layers of the OSI reference model. Such classification will present a simplified and clear view of DoS attacks. It will definitely help us to achieve a better communication and cooperation between researchers and hence better defense mechanisms.

Description of DoS attacks with respect to different layers of the OSI reference model is as shown below:

#### 4.1. Application layer attacks

Application layer DoS attacks are a bit more complicated. They disable specific functions or features as opposed to an entire network. Usually, these attacks are used against financial institutions to divert IT and security administrators from security breaches. As per the report of second quarter 2014 conducted by Prolexic, the most common...
application layer attacks were HTTP GET floods (7.5% of all attacks mitigated in Q2), HTTP POST floods (2.3%), PUSH floods (0.8%) and HEAD floods (0.2%) (Prolexic, 2014b). These kinds of attacks are launched generally for specific targeted purposes, including disrupting transactions and access to databases, and requires comparatively less resources. These attacks are some of the most difficult attacks to extenuate against because they mimic human behaviour as they interact with the user interface.

The application layer of the OSI reference model has two main categories of protocols as follows (Abliz, 2011):

- Protocols that directly service users (e.g. HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH)
- Support protocols that fortify various system functions (e.g. DNS, SNMP, BOOTP/DHCP, TLS/SSL, SIP, RTP, NTP).

Application layer DoS attacks are more worrying than the attacks at other layers because of following reasons (Infosec, 2014):

**High obscurity:** These attacks follow legitimate TCP or UDP connections; so it is very difficult to differentiate them from legitimate users.

**Highly efficient:** These attacks require very less number of connections.

**Affect multiple applications:** They may affect many different applications. Any one of the protocols examined above may be subject to a DDoS attack (Abliz, 2011). Many of them targets HTTP to exhaust a web server’s vitality.

**Highly targeted:** These attacks are highly targeted oriented. Generally, these attacks are tailored to aim a specific application. For example, web servers that run a combination of Java, PHP5 and ASP.NET may be targeted by specially crafted HTTP requests, which may collide with the web servers’ hashing operation when unique requests return non-unique and overlapping responses.

**Simplicity in exploitation:** These attacks may exploit the simplicity in the application layer. For example, a simultaneous refresher of browsers by thousands of users may collapse the server soon or later.

**Multiple effects:** These attacks may affect many victims directly or indirectly. For example, a DNS attack at a single DNS provider may affect all of its customers (Arbor, 2014).

**Requirement of limited resources:** These attacks require limited resources, so limited investment by attackers can result a successful attack.

**Follow normal traffic rules:** Traffic involved in these attacks seems to be legitimate as it follows the protocol rules, rate and complete TCP handshake process. It follows all the basic requirements that a normal traffic flow expects.

Most of application layer DoS attacks exploit the following protocols:

- HTTP page flood,
- HTTP bandwidth consumption,
- DNS query flood,
- SIP INVITE flood and
- Low rate, high impact attacks – e.g. Slowloris, HTTP POST DoS.

Application layer DOS attacks can be divided into following categories (Infosec, 2014):

1. **High-Bandwidth Attacks:** These attacks typically flood resource exhaustive pages with either GET or POST requests. These requests reset the connection over and over to consume the server’s session and memory. On the other hand, it is become more complicated if it contains compute-intensive requests or demand for large files from the website, such as PDFs. Such requests results in consumption of resources that knocks down servers. And these servers are unable to respond to legitimate users. Examples include attacks that: exploit of secure socket layer (SSL), Overwhelm the database, attack a form page, etc.

2. **Low-Bandwidth Attacks:** such attacks are mounted by hackers by applying their knowledge about the application. They exploit weaknesses of the application. Such attacks require few attack nodes and low bandwidth. Traffic during these attacks seems to be legitimate. Differentiation of attack traffic and normal traffic is very difficult and requires expertise in the field. Examples of such attack include: Slowloris, Slow HTTP POST and Slow READ.

3. **Attacks that Steal Data:** Such attacks are particularly designed for the purpose of stealing the data. These attacks exploit the weaknesses of the applications. Traffic generated during such attacks looks like legitimate traffic. Examples of such attacks include: command injection attacks, i.e. SQL injection attack, remote file inclusion and local file inclusion.

Although HTTP is the most under attack protocol, other protocols are attacked as well, such as DNS dictionary attacks consisting of registrar hijacking, and redirection cache poisoning, VoIP (SIP INVITE Flood Attack), SMTP buffer overflow attacks (Arbor, 2014) as described in Table 1.
Table 1. Most commonly exploited protocols at application layer.

| Protocol | Attack method |
|----------|---------------|
| HTTP     | HTTP Malformed Attacks, HTTP Request Attacks and HTTP Idle Attacks |
| DNS      | DNS Query/Answer Malformed Packet, DNS Query-Length Buffer Overflow, DNS Query Buffer Overflow, Man-in-the-Middle, DNS Cache Poisoning Attacks, DNS Amplification Attacks and DNS Dictionary Attacks |
| VoIP     | SIP INVITE Flood Attacks, SIP Call Setup Request Attacks, SIP Malformed Packet Attacks, Real-Time Transport Protocol (RTP) and Flood/Quality of Service (QoS) Attacks |
| SMTP     | SMTP Error DoS, Mailbox DoS Attack (Excessive Email Size), SMTP Mail Flooding attacks and SMTP Buffer Overflow Attacks: Different SMTP commands can cause the SMTP server to crash or execute arbitrary |

Figure 3. Most common protocols targeted for application layer attacks.

Table 2. Most common tools used for DoS attacks at application layer.

| Tool                | Attack method                               |
|---------------------|---------------------------------------------|
| LOIC                | UDP, TCP or HTTP (HTTP GET method)          |
| R.U.D.Y (R U Dead Yet?) | HTTP POST                                  |
| Slowloris           | HTTP GET                                   |
| Dirt Jumper         | HTTP flood, SYN flood, POST flood          |
| Tor’s Hammer        | Slow POST                                  |
| Nuclear DDoSer      | Slowloris, Slow POST                       |
| Railgun             | Slowloris or Slow POST                     |

As per the report of Arbor’s network, most commonly protocols targeted for application layer attacks are depicted in Figure 3 (Arbor, 2014).

A huge number of tools are available over the Internet for launching DoS attacks at the application layer. The most commonly used tools and their attack methods are summarized in Table 2.

4.2. Presentation layer attacks

The presentation layer DoS attack involves malformed SSL requests. SSL provides security in web services like banking, online shopping, etc. Because of the security features, most of the well-liked organizations are migrating to SSL for providing improved security in their services (Arbor, 2014). Nowadays, most of the transactions are protected by SSL. But it has also attracted more attention of the attackers. The TCP protocol – TCP handshake is a common victim of a DoS attack. After finishing the TCP handshake, there is a session of the network layer for SSL handshake. During an SSL handshake, there is an exchange of messages to validate the authenticity of both communicating entities. They establish the encryption key and options for the secure communication afterwards.

There are several attacks which exploit the SSL handshake to exhaust server resources. The Pushdo botnet carry out this simply by sending garbage data to a target SSL server. The SSL protocol is computationally expensive and it generates extra workload on the server to process garbage data as a legitimate handshake. In this process, the server may stop accepting SSL connections or it may restart them. A device such as Firewalls fails in this scenario because both the entities have successfully finished the TCP handshake. And now they are sending traffic to an authorized service. Generally, attackers use SSL to tunnel HTTP-based DoS attacks.
DoS attacks at SSL may be classified into two categories:

**Protocol misuse attacks:** These attacks take advantage of the protocol being used. They can mount a DoS attack without completing the creation of secure connection. They do not require secure keys. For example, THC-SSL-DOS, which can be used to create repeating ‘renegotiation’ in the same connection, though never completing the creation of a secure channel. Simple mitigation techniques such as IPS signatures can help us to detect such attacks.

**SSL Traffic Floods:** Such attacks pass huge traffic over the created secure channel, resulting in consumption of bandwidth and/or other resources. Without further information, these magnificent mitigation devices cannot distinguish between valid connections to malicious connections. They cannot even issue web challenge in an attempt to try and assess source legitimacy. So you are stuck with either nothing or some rate–limited protection – prone to false actions.

The most commonly used tool for launching attacks at this layer is THC-SSL-DOS.

### 4.3. Session layer attacks

Session layer manages the establishment, termination and synchronization of sessions within an operating system over a network system. The attackers exploit log-on and log-off protocols for mounting DoS attacks in the session layer. For example, Telnet DoS attack. The Telnet application allows a terminal to remotely communicate with the counterpart. Telnet with IP network sends and receives the data remotely using port 23. Telnet attacks can be categories into three classes as follows (Popes-kic, 2011):

**Telnet communication sniffing:** The most critical issue in Telnet protocol is the lack of encryption. Every transmission between communicating parties over the network is sent in plain text. Of course, it is a vulnerability in the protocol and being exploited by the attackers for frame sniffing. The attacker can easily sniff the plain information flowing over the network.

**Telnet brute force attack:** Telnet protocol Brute force password attack begins with the attacker using a list of commonly used passwords and a program designed to try to establish a Telnet session using each word on the dictionary list.

**Telnet DoS:** Telnet DoS attacks in general are simply a way to disrupt the communication of two network devices by using all the bandwidth that their connection has to offer. To do so, an attacker sends many not useful and irrelevant data frames and in this manner suffocate the connection. The genuine communication will not be able to get across this connection and will not function. This sort of attack can be also used to prevent network administrators to Telnet into their devices.

### 4.4. Transport layer attacks

Transport layer DoS attacks are generally volume-based attacks on a network infrastructure. As per the report of Prolexic, 89% of Q2 2014 DDoS attacks targeted the infrastructure layer; the remaining 11% were application attacks (Prolexic, 2014b). The most common infrastructure attacks included SYN floods (26% of all attacks mitigated in Q2), UDP floods (25%), NTP (7.4%) and ICMP (6.6%).

| Tools          | Description                                                                 | Attacks               |
|----------------|-----------------------------------------------------------------------------|-----------------------|
| Macof Dsniff   | Macof is a tool that can flood a switched LAN with random MAC addresses. Macof is also included in Dsniff. | MAC Attacks           |
| Linux Bridges  | A project to develop Ethernet bridges using Linux. Source codes are available. | STP Attacks           |
| Stp.c          | A source code in C language that can generate BPDU frames. The code can be used as a framework to write STP attacking tools. | STP Attacks           |
| IRPAS          | Internetwork Routing Protocol Attack Suite (IRPAS) is a suite of tools developed for attacking routers. A tool called CDP attack is also included. | CDP Attacks           |
| Ettercap       | Ettercap is a multifunction sniffer for switched LAN. It can be used for password capturing, packet filtering and dropping, passive OS fingerprinting, and connection killing. It also supports plugins that can launch STP and ARP attacks. | STP Attacks, ARP Attacks and MAC Attacks |
| Libdnet        | Libdnet is a testing program that can be used to change a network’s configuration by generating ARP request packets. | ARP Attacks           |
| VLAN Attacks   | VLAN attacks. Gobbler is a tool that can launch DHCP attacks. Gobbler can gobble all available IP addresses in a network and can perform man-in-the-middle attacks. | DHCP Attacks          |
| Gobbler        | IRPAS Internetwork Routing Protocol Attack Suite (IRPAS) is a suite of tools developed for attacking routers. A tool called CDP attack is also included. | DHCP Attacks          |
| SToP           | SToP is an utility that can modify any relevant field in the BPDU messages. It can generate enough packets to flood a network. | STP Attacks           |
These attacks are dependent upon generation and transmission of a huge volume of network traffic to disrupt or completely block the availability of network services/resource for legitimate users. Such attacks generally involve exploitation of TCP and UDP protocols for saturating network resources. For example, the TCP/IP protocol uses a system of requests and acknowledgments to handle transmission of messages. For establishing a connection, the client sends Requests to server, and the server acknowledges the client’s request. After a successful exchange of request and acknowledgements, a connection gets established for the transmission of data over it. Transport layer keeps track of exchange of requests and acknowledgements and holds the connection open till a corresponding acknowledgement is not received. This point is exploited by the attackers in DDoS attack classed SYN attack. On SYN attack, a large number of bogus requests are sent towards the victim server, resulting in consumption of the victim’s memory for handling half-opened connections. Until the bogus requests time out, the victim server is unavailable to the intended users.

The most commonly exploited protocols at transport layer include TCP-SYN attack, CHARGEN-UDP. Common tools used for launching such attacks are highlighted in Table 3.

### Table 4. Summary of DoS attacks.

| OSI layer       | Functions                                                                 | Protocol(s)                                                                 | DoS attack method                  | Impact of DoS attack                    | Attack tools                                                                 |
|-----------------|---------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------|----------------------------------------|----------------------------------------------------------------------------|
| Application Layer | It supports application and end-user processes by identifying communication partners, ensuring quality of service, providing user authentication and privacy. It interacts with the application such as file transfers, e-mail and other network software services | Telnet, FTP, SMTP, HTTP                                                      | HTTP GET request, HTTP POST request, DNS malformed packets, VOIP and SMTP | Resource starvation                                                           | LOIC, RUDY, Slowloris, Dirt Jumper, Tor’s Hammer, Nuclear DDoSer and Railgun |
| Presentation layer | It helps in providing uniformity in data representation (e.g. encryption) by translating from application to network format, and vice versa. It transforms data into the format that the application layer can accept. The layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems | SSL                                                                         | Malformed SSL request                | Resource starvation                                                           | THC-SSL-DOS                                                                 |
| Session layer   | It is responsible for establishing, managing and terminating connections between applications. The layer sets up, coordinates, and terminates sessions, exchanges, and dialogues between the applications at each end. It deals with session coordination | Telnet                                                                      | Deny remote login services          | Unavailability of Telnet services for remote administration                  | –                                                                          |
| Transport layer | It provides end-to-end transmission of data between hosts. It ensures end-to-end error recovery and flow control. It is responsible for the complete data transfer | TCP, UDP                                                                   | SYN attacks, Smurf attacks          | Consume resources like bandwidth, connections, causes unavailability of services | Trinoo, Brobot, Tribe Flood Network, TFN2K and Stacheldraht                  |
| Network layer   | It is responsible for switching and routing of packets, through virtual connections, for transmitting data from node to node. Other functions of this layer include addressing, internetworking, error handling, congestion control, and packet sequencing | IP                                                                          | Flooding-based attacks              | Causes unavailability of bandwidth and other services                        | –                                                                          |
| Data link layer | At this layer, data packets are encoded and decoded into bits. It handles errors in the physical layer, flow control and frame synchronization | IEEE 802                                                                   | MAC flooding attacks                | Interrupt normal flow of traffic between sender and receiver                 | Macof /Dsniff, Linux Bridges, Stp.c, IRPAS, Ettercap, Libdnet, VLANand Gobbler, STOP |
| Physical layer  | It transfers the bit stream—electrical impulse, light or radio signal – through the network at the electrical and mechanical level. It interfaces the hardware for sending and receiving data on a carrier, including defining cables, cards and physical aspects | Ethernet, RJ45, etc.                                                       | Destruction, obstruction, and manipulation of media                         | Interruption in communication through physical media                        | –                                                                          |
4.5. Network Layer attacks

Network layer DoS attacks involve injecting a victim network with a traffic more than it can handle. As a result of additional network traffic, the victim network starts responding slow or it drops some packets. The loss of packets may cause a flood of retransmitted requests, which further increase the network traffic. Increased network traffic saturates the network and it becomes unavailable for the intended users. For example, in Ping flood attack, ICMP data flood the network and consumes the whole bandwidth. The network starts denying the services. Other examples of network attacks include Smurf attack, ping of death, DNS amplification attacks, ACK attacks, reflection attacks, etc. As per report conducted by Prolexic in Q2 of 2014, the most common reflection attack vectors included NTP (7.35%), CHARGEN (4.54%) DNS (4.00%) and SNMP (3.03%) (Prolexic, 2014b). During the attack at this layer, network bandwidth is generally saturated by imposing an extra load. As a result, bandwidth becomes unavailable for the intended users.

4.6. Data link layer attacks

The data link layer is responsible for establishing/ maintaining and deciding how to transfer data over the physical layer. PDU used here in this layer is frame. IEEE 802 standards are used as protocols for communication at this layer. Attacks at this layer can vary from Address Resolution Protocol (ARP) cache poisoning for wired clients to de-authentication of wireless clients.

The most critical attacks at the data link layer involve Content Address Table (CAM) exhaustion, ARP spoofing, DHCP starvation attacks, MAC address spoofing, VLAN attacks and many more. These attacks generally disrupt the normal traffic flow from sender to receiver. Tools used to mount DoS attacks at the data link layer are summarized in Table 3 (Yeung, Fung, & Wong, 2008).

4.7. Physical layer attacks

The physical layer is concerned with media, i.e. cable to transfer bits from source to receiver. The layer uses 100 Base-T and 100 Base-X protocols, and hub, patch panels, and R45 jack as devices to transfer data. Attacks on physical layer include physical destruction, obstruction, manipulation and malfunctioning of physical media, which leads to its unavailability to the intended users. It requires the repair to make the physical media resources available.

The DDoS attack described in above-cited section can be summarized in Table 4.

5. DoS threat detection mechanism and tools

A large number of detection and mitigation mechanisms have been proposed for DoS attacks. Most of the organizations use multiple threat detection mechanism and tools for detecting DoS attacks. As per the report of Arbor network 2014, NetFlow analyzers, firewall logs and SNMP-based tools are the most successful and most commonly deployed threat detection tools (Arbor, 2014). Proportions of other tools used for threat detection are as depicted in Figure 4. Most commonly used tools for DoS detection include NetFlow analyzer, Firewall logs and SNMP-based tools.

The effectiveness of these tools is depicted in Figure 5. It can be observed from the results that NetFlow analyzers and SNMP-based tools are the most commonly used and most effective tool for DoS threat detection.
6. DoS threat mitigation mechanism and tools

A vast variety of mechanism and tools are used for DoS attack mitigation. The mechanisms involve mitigation using access control list (ACL), Rate Limiting or combination of both (Rao and Rao, 2011). The proportions of mitigation tools for DoS attacks are depicted in Figure 6.

The Intelligent DDoS Mitigation Systems (IDMSs) and ACL are the most effective mechanisms and commonly used mitigation mechanism (Arbor, 2014). It is also believed that IDMSs provide more intelligent, surgical capabilities for DoS attack mitigation. Firewall usage is at the third place after IDMS and ACL. Other possible DoS attack mitigation techniques include SYN proxy, connection limiting, aggressive ageing, source rate limiting, dynamic filtering, active verification, anomaly recognition, granular rate limiting, white list-black list, and dark address prevention (Jain, 2008).

7. Conclusions

Certainly, DoS attacks pose a severe problem on the Internet and challenge its rate of growth. In this paper, we attempted to attain a clear view of the DoS attack problem, and presented an updated perspective of the problem in respect to different layers of the OSI reference model. Having, this view of the problem, our understanding about the problem is clarified and this way we can discover more effective solutions to the problem of DoS attacks. This paper also presented various attack vectors, attack tools, trends in detection and mitigation mechanisms.

One big benefit of the development of DoS attack classification is that it helps for an effective communication and cooperation between researchers. The effective communication and cooperation can result to identify additional weaknesses of the DoS attack problem. This classification necessitate be constantly updating and
extending as new threats are being discovered and hence their defense mechanism. Their value in achieving further research and discussion is definitely great. DoS attacks remain at the top of operational threats nowadays, whereas DoS attacks against infrastructure and sophisticated attacks against applications remain the top concern for the recent past. DoS attacks and their variety remain a key issue; so most of the organizations demands for DoS detection/mitigation mechanisms/tools for their customers.

However, we believe that no single technology-based solution alone can be effective in providing defense against a variety of DoS attacks. The comprehensive protection of an organization’s from DoS attack requires a multi-faceted security strategy.

**Disclosure statement**

No potential conflict of interest was reported by the author.

**References**

Abliz, M. (2011). *Internet denial of service attacks and defense mechanisms* (Tech. Rep. TR-11-178), Pittsburgh: University of Pittsburgh.

Alam, M. F. (2014). *Application layer Ddos a practical approach & mitigation techniques*. Retrieved from https://conference.apnic.net/data/37/1/ddos_apricot_1_1393257782.pdf.

Arbor, N. (2014). *Worldwide infrastructure security report*, volume ix. Retrieved from pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf.

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *Internet Computing, IEEE*, 10(1), 82–89.

Chauhan, A., Mishra, G., & Kumar, G. (2012). Survey on data mining techniques in intrusion detection. Saarbrücken, Germany: Lap Lambert Academic Publishing.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks, 44*(5), 643–666.

Durcerekova, V., Schwartz, L., & Shahmehri, N. (2012). Sophisticated denial of service attacks aimed at application layer. ELEKTRO, Rajec Teplice, Slovakia (pp. 55–60). IEEE.

Gupta, V., Krishnamurthy, S., & Faloutsos, M. (2002). Denial of service attacks at the mac layer in wireless ad hoc networks. *MILCOM 2002. Proceedings, Vol. 2, Anaheim, CA* (pp. 1118–1123). IEEE.

Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR)*, 42(1), 1–34.

Infosec. (2014). *Layer seven DDoS attacks*. Retrieved August 20, 2014, from http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

Jain, H. (2008). *10-ddos-mitigation-techniques*. Retrieved from http://www.slideshare.net/intruguard/10-ddos-mitigation-techniques-presentation

Kumar, G. (2004). Understanding denial of service (DoS) attacks using OSI reference model. *International Journal of Education and Science Research*, 1(5), 10–17.

Kumar, G., & Kumar, K. (2014). Network security - an updated perspective. *Systems Science & Control Engineering: An Open Access Journal*, 2(1), 325–334. doi:10.1080/21642583.2014.895969

Kumar, G., Kumar, K., & Sachdeva, M. (2010a). An empirical comparative analysis of feature reduction methods for intrusion detection. *International Journal of Information and Telecommunication Technology*, 7(1), 44–51.

Kumar, G., Kumar, K., & Sachdeva, M. (2010b). The use of artificial intelligence based techniques for intrusion detection: a review. *Artificial Intelligence Review*, 34(4), 369–387.

Miller, A. (2014). *What is a layer 7 DDoS attack?*. Retrieved from http://ddosattackprotection.org/blog/layer-7-ddos-attack/

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39–53.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1), 42–57.

Nsfocus. (2014). *Introduction to DDoS Attack*. Retrieved July 28, 2014, from en.nsfocus.com/.../DDoS%20FAQ/What%20is-%20DDoS%20Attack.pdf

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the dos and ddos problems. *ACM Computing Surveys (CSUR)*, 39(1), 1–42.

Popeskić, V. (2011). Telnet attacks ways to compromise remote connections. Retrieved July 28, 2014, from http://howdowseinternetnetwork.com/2011/telnet-attacks

Prolexic: Q1 2014 global ddos attack report (2014a). Retrieved July 28, 2014, from www.prolexic.com/knowledge-center-ddos-attack-report-2014-q1.html

Prolexic: Q2 2014 global ddos attack report (2014b). Retrieved July 28, 2014, from http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html

Rao, S., & Rao, S. (2011). Denial of service attacks and mitigation techniques: Real time implementation with detailed analysis. *SANS Institute Infosec Reading Room Sep*, 11.

Saafan, A. (2014). *Distributed denial of service attacks: Explanation, classification and suggested solutions*. Retrieved July 28, 2014, from http://www.intelligentexploit.com/articles/DDoS-Attacks-explanation-classification-and-suggested-solutions.pdf

Schneider, D. (2012). The state of network security. *Network Security*, 2012(2), 14–20.

Verizon: The 2013 Data Breach Investigations Report (2013). Retrieved September 23, 2013, from www.verizonenterprise.com/resources/reports/rp_data_breach-investigations-report-2013_en_xg.pdf

Wu, B., Chen, J., Wu, J., & Cardel, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Y. Xiao, X. S. Shen, & D.-Z. Du (Eds.), *Wireless Network Security* (pp. 103–135). New York, NY: Springer.

Yeung, K. H., Fung, D., & Wong, K. Y. (2008). *Tools for attacking layer 2 network infrastructure*. Proceedings of the international multiconference of engineers and computer scientists, Vol. 2, Hong Kong (pp. 1–6). Citeseer.