Investigation of Network Anomaly Detection Techniques for Distributed Denial of Service Attacks

Shreevyas. H M[a], Dr. Ravikumar, Dr.Dinesha H.A.

ABSTRACT

Distributed Denial of Service (DDoS) attacks are the risk on the Internet which reduce the network bandwidth and increases the zombie resources. DDOS attacks affects in availing the network services and resources which results negatively in business. Many detection and prevention techniques have been proposed and deployed to resist DDOS attacks. But with the evolution of these security techniques, attackers evolve their techniques as well to break the security measures. The existing DDOS security has to advance by novel techniques and innovations. In literature various signature-based and anomaly-based techniques were used for the detection and prevention of DDoS attacks. These techniques need advancement in real-time application for low rate, rare, and novel DDOS attacks. However, to investigate the existing challenges in proposed techniques, we made a survey and presented the same precisely. This paper reports the various existing DDOS attacks, proposed network anomaly detection techniques for DDoS attacks, proposed machine learning and data analytics for DDOS attacks, and the summary of study to realize future research objectives.

KEYWORDS

DDOS Attacks, Data Analytics, Machine learning, Network Anomaly Detection, Security Techniques,

1. Introduction

Due of advancements in internet technologiesand its components variety of network attacks has been increased drastically. It leads to network anomalies, detection and prevention of attacks has become a significant research issue. In spite of remarkable research progress and a huge contribution, there are still many demands and opportunities to propose the stateof- the-art in detecting and preventing network related attacks [1].Many network-based attacks reported in literature, few of the known attacks are described in table 1 with proposed solutions. All the reported attacks were addressed by signature-based intrusion detection and anomaly-based intrusion detection techniques. But many rare and low rate DDOS attacks are difficult to identify with these techniques. DDoS attacks have become a critical problem of today’s Internet. DDoS attacks are intelligent in nature which follows the same techniques as Denial of service (DoS) attacks. It attacks the internet on very higher range through botnets [2]. Botnet is a wide chain of remotely controlled zombies / slave agents.

Table 1: The identified existing network attacks and its correspondence solutions

Sl No	Name of the Attacks	Attack description	Existing proposed solution to address the problem
1.	Backdoor channel attacks	It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. It uses *Zombie* to initiate DDoS attack.	Signature-based intrusion detection and anomaly-based intrusion detection techniques.
2.	Flooding attack	Attacker sends huge number of packets from innocent host to create flood in network. It results into fake usage of resources.	Signature based intrusion detection and anomaly-based intrusion detection techniques
3.	Root attacks	Attacker gets access to the authentic user's account by sniffing password.	Anomaly based intrusion detection techniques
4.	Port Scanning Attack	Attackers can identify the opened ports and can disturb the services which are running on these ports.Also, it can leak/reports thenetwork confidential details such as IP& MAC address, router, gateway filtering, firewall rules and etc.	Signature-based intrusion detection and anomaly-based intrusion detection techniques
5.	Insider attack	Authorized user/ insiders may commit frauds and disclose information to others.	Signature based intrusion detection

The history and basic strategy of DDoS attacks need to be understand to determine the solutions. History says that initially, DDoS attacks were launched in August, 1999 against different organizations and continued attacking the various websites like Yahoo, Amazon, Buy.com, CNN and eBay [2]. In 2009, a DDoS attack triggered which interrupted the entire network services of popular websites such as Facebook, amazon, twitter and etc. [3]. During 2010 -2011, 75,000+ computers among 2500 organizations and 4 million computers among 100 nationshadimpacted by DDoS attacks respectively [4]-[8]. Every day, 7000+ DDoS attacks are created from attackers [9][10]. The average attack volume reached around 48.25Gbps during the first quarter of 2013, which was 718% more as compared to the last quarter of 2012[11]- [13].

At these days, DDoS attacks have become shorten its time duration. According to the highest reported DDoS attacks hadincreased up to 1000% from 2008, from 40 Gbps to 400+ Gbps in 2013. These attacks executed at an average rate of 3000 times per day. According to the review reportof Verisign, there was a growth upto111% in DDoS attacks per year (Verisign) [2]. Verisign reported 85% more DDOS attacks during the fourth quarter of 2015 in compared to fourth quarter report of 2014 (Bisson). In 2015, the biggest attack was around 500 Gbps that interruptedthe whole ISP's network of Kenya (Baraniuk) nation.

DDoS attack was launched against the BBC website to 602 Gbps during the first quarter of 2016 (Khandelwal) [15]-[17]. As per the reports, the highest DDoS attacks in the history was orchestrated during October,2016. As per the estimates of Dyn, the launched DDOS attack had prodigious attack strength of 1.2 terabits (1200 gigabytes) per second and had intricate '100,000 malicious agents'. These were summarized and presented in Figure 1. The DDOS attacks and its variants are presented in section 2.

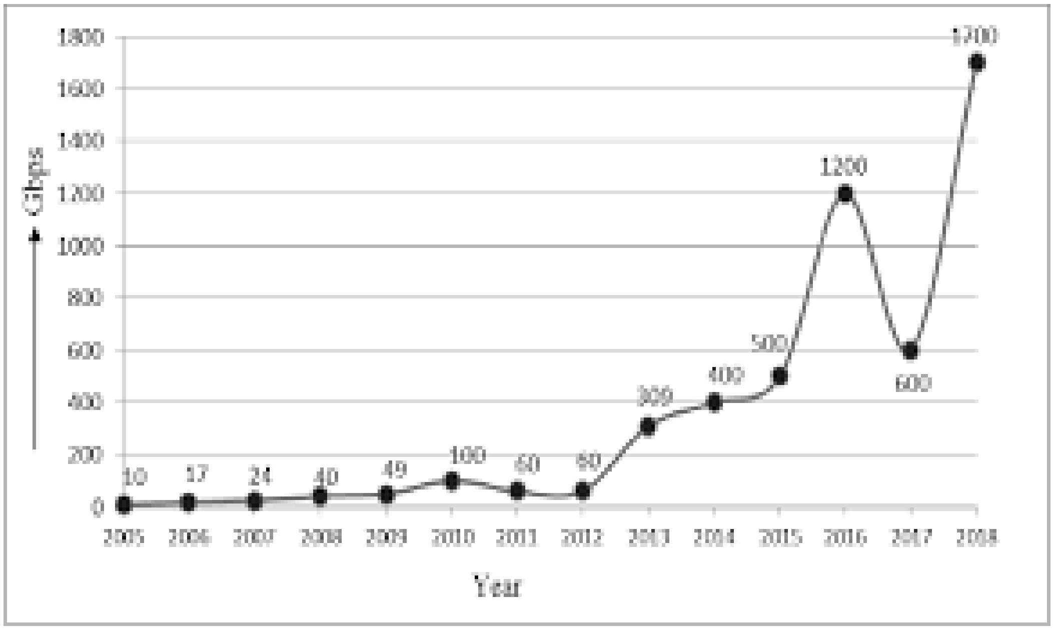


Figure 1: Strength of DDOS attacks in GBPS (Bhandari et.al, 2019)

This paper is organized in following manner; Section 2 describes the study report of different DDOS Attacks. Section 3 describes analysis of existing network anomaly detection techniques. Section 4 presents the review highlights for research outcomes. Finally, Section 5 concludes the paper along with future research directions.

2. DDOS Attacks and its Variants

This section discusses the DDOS attacks and its Variants. DDoS attacks are mainly of two types such as i) flooding attacks and ii) vulnerability attacks. In flooding attacks, the attacker sets a zombie's/compromised systems army to send unwanted packets to the destination in order to raise the traffic to the extent that victim should unable to do its service. The flooding attacks again divided into direct and indirect DDoS attacks based on attack ways. Based on protocol, flooding attacks are grouped into Network/Transport level and Application level DDoS. Figure 2 represents the DDOS attack and its variants. Many DDOS attack and its tyoes with respect to flooding, http protocol, network and complex attacks presented in table 2 , table 3 , table 4 and table 5 relatively.

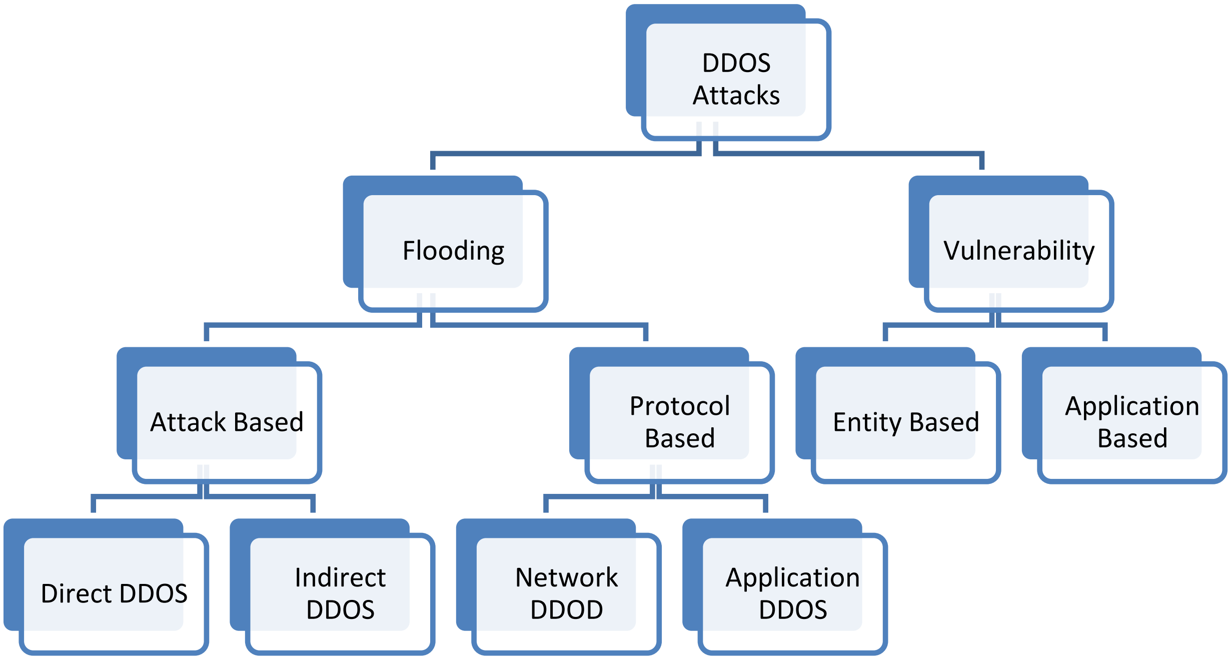
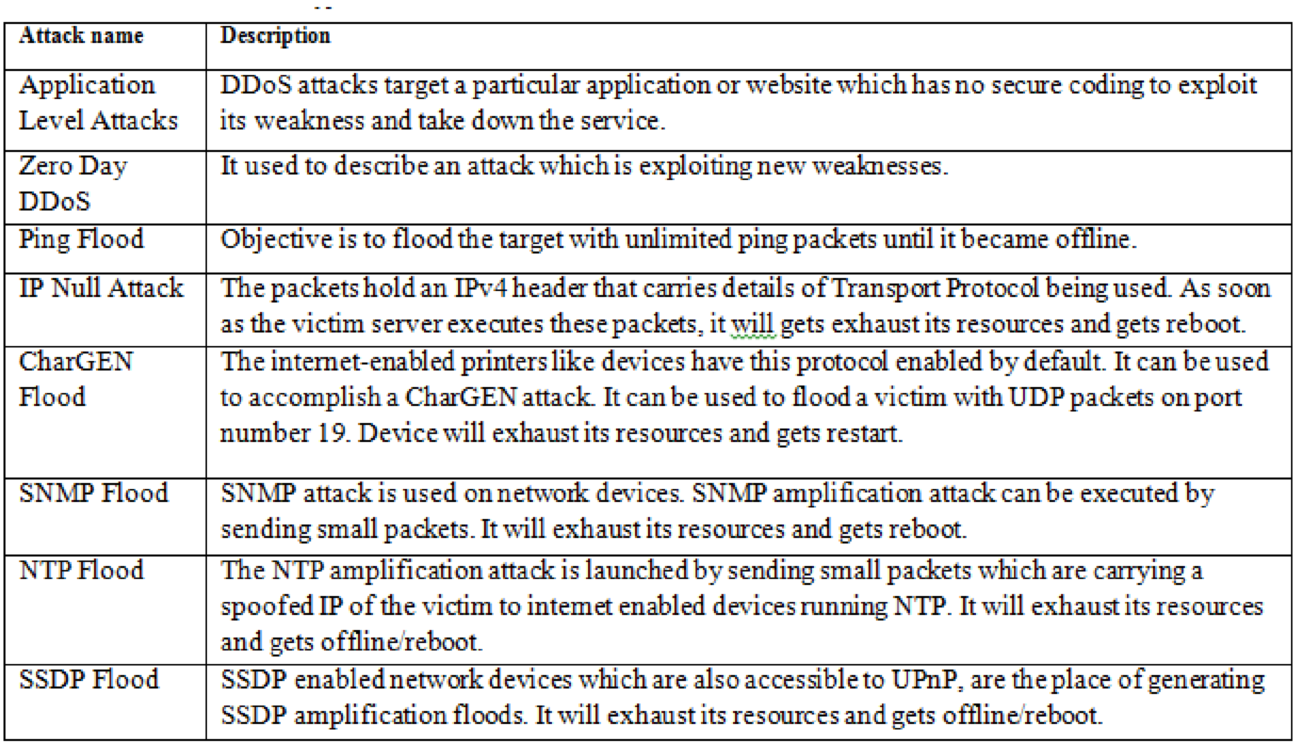


Figure 2: DDOS attacks and its variants

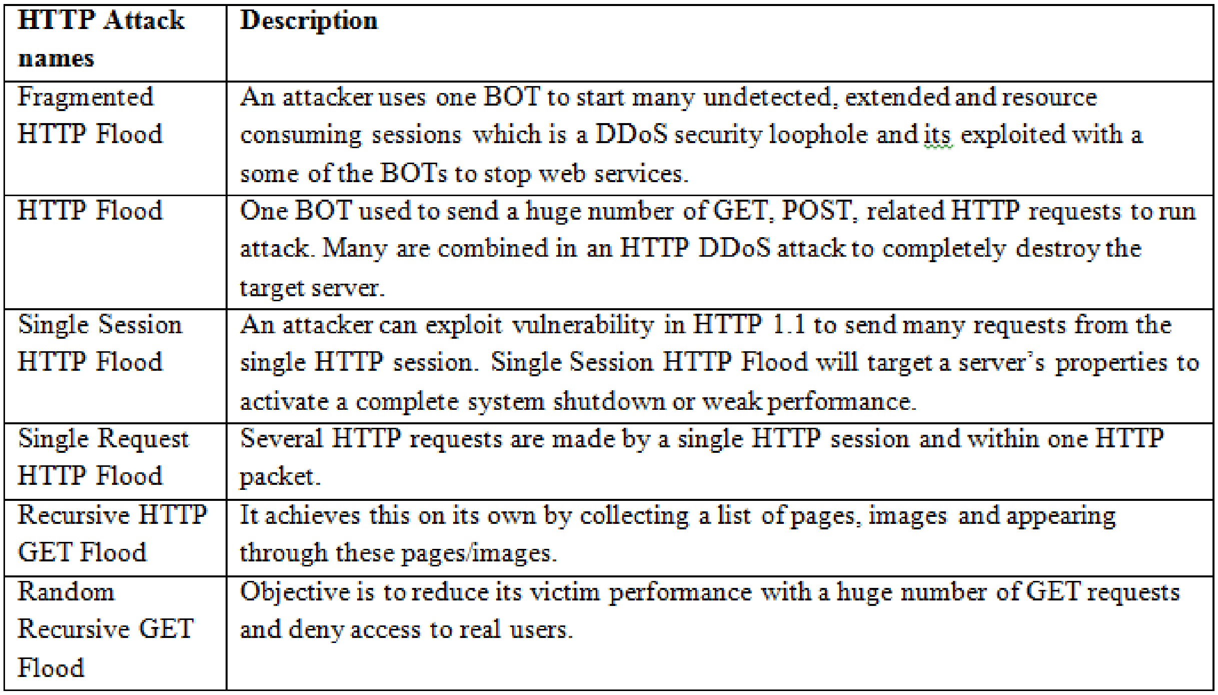
Table 2: Various DDOS Attack types



Attack name	Description
Application Level Attacks	DDoS attacks target a particular application or website which has no secure coding to exploit its weakness and take down the service.
Zero Day DDoS	It used to describe an attack which is exploiting new weaknesses.
Ping Flood	Objective is to flood the target with unlimited ping packets until it became offline.
IP Null Attack	The packets hold an IPv4 header that carries details of Transport Protocol being used. As soon as the victim server executes these packets, it will gets exhaust its resources and gets reboot.
CharGEN Flood	The internet-enabled printers like devices have this protocol enabled by default. It can be used to accomplish a CharGEN attack. It can be used to flood a victim with UDP packets on port number 19. Device will exhaust its resources and gets restart.
SNMP Flood	SNMP attack is used on network devices. SNMP amplification attack can be executed by sending small packets. It will exhaust its resources and gets reboot.
NTP Flood	The NTP amplification attack is launched by sending small packets which are carrying a spoofed IP of the victim to internet enabled devices running NTP. It will exhaust its resources and gets offline/reboot.
SSDP Flood	SSDP enabled network devices which are also accessible to UPnP, are the place of generating SSDP amplification floods. It will exhaust its resources and gets offline/reboot.

Table 2 summarizes the different DDOS attacks such as application level, zero-day, ping flood, IP null, SNMP Flood, NTP Flood, and SSDP Flood. With this we clearly understand the many DDOS attacks can be done in different ways to interrupt the services. Hyper Text Transfer protocol (HTTP) is more vulnerable to security attacks since the execution takes place at application layer, presentation layer cryptographic approach would not be incorporated. Hence security cannot be provided as service. So the various attacks such as fragmented HTTP Flood, HTTP Flood, Single session HTTP Flood, Sinle request HTTP Flood, Recursive HTTP GET Flood and Random recursive GET Flood are possible. Summary of these attacks along with description presented in the table 3.

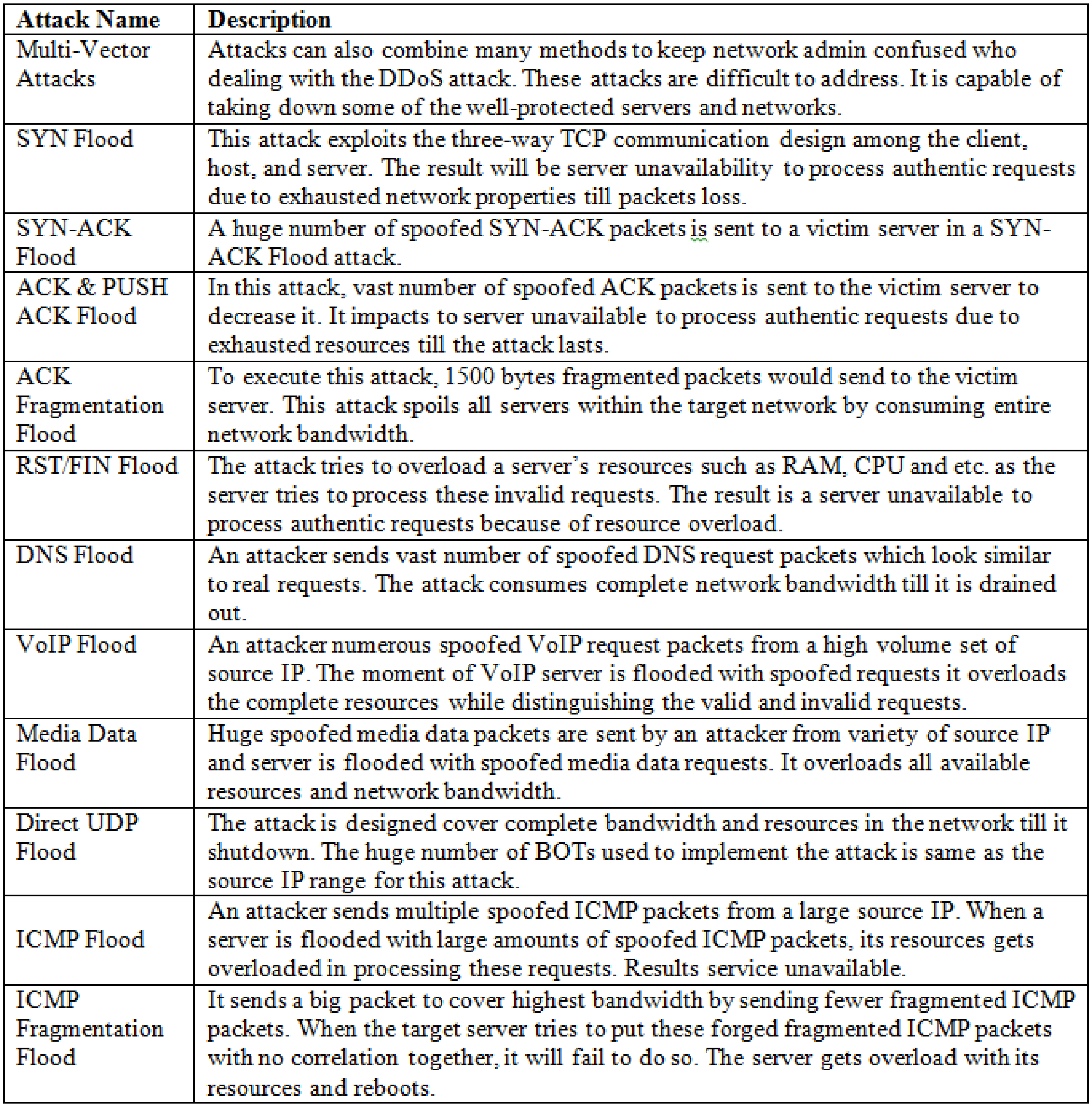
Table 3: Various DDOS Attack typesrelated to HTTP



HTTP Attack names	**Description**
Fragmented HTTP Flood	An attacker uses one BOT to start many undetected, extended and resource consuming sessions which is a DDoS security loophole and its exploited with a some of the BOTs to stop web services.
HTTP Flood	One BOT used to send a huge number of GET, POST, related HTTP requests to run attack. Many are combined in an HTTP DDoS attack to completely destroy the target server.
Single Session HTTP Flood	An attacker can exploit vulnerability in HTTP 1.1 to send many requests from the single HTTP session. Single Session HTTP Flood will target a server's properties to activate a complete system shutdown or weak performance.
Single Request HTTP Flood	Several HTTP requests are made by a single HTTP session and within one HTTP packet.
Recursive HTTP GET Flood	It achieves this on its own by collecting a list of pages, images and appearing through these pages/images.
Random Recursive GET Flood	Objective is to reduce its victim performance with a huge number of GET requests and deny access to real users.

Many DDOS complex attacks have been listed in literature which was summarized in table 4. Literature reported many attacks such as Multi-Vector, SYN Flood, SYN-ACK Flood, ACK & PUSH ACK, ACK Fragmentation Flood, RST/FIN Flood, DNS Flood, and VoIP Flood etc. are major noted attacks listed in table 4 along with description.

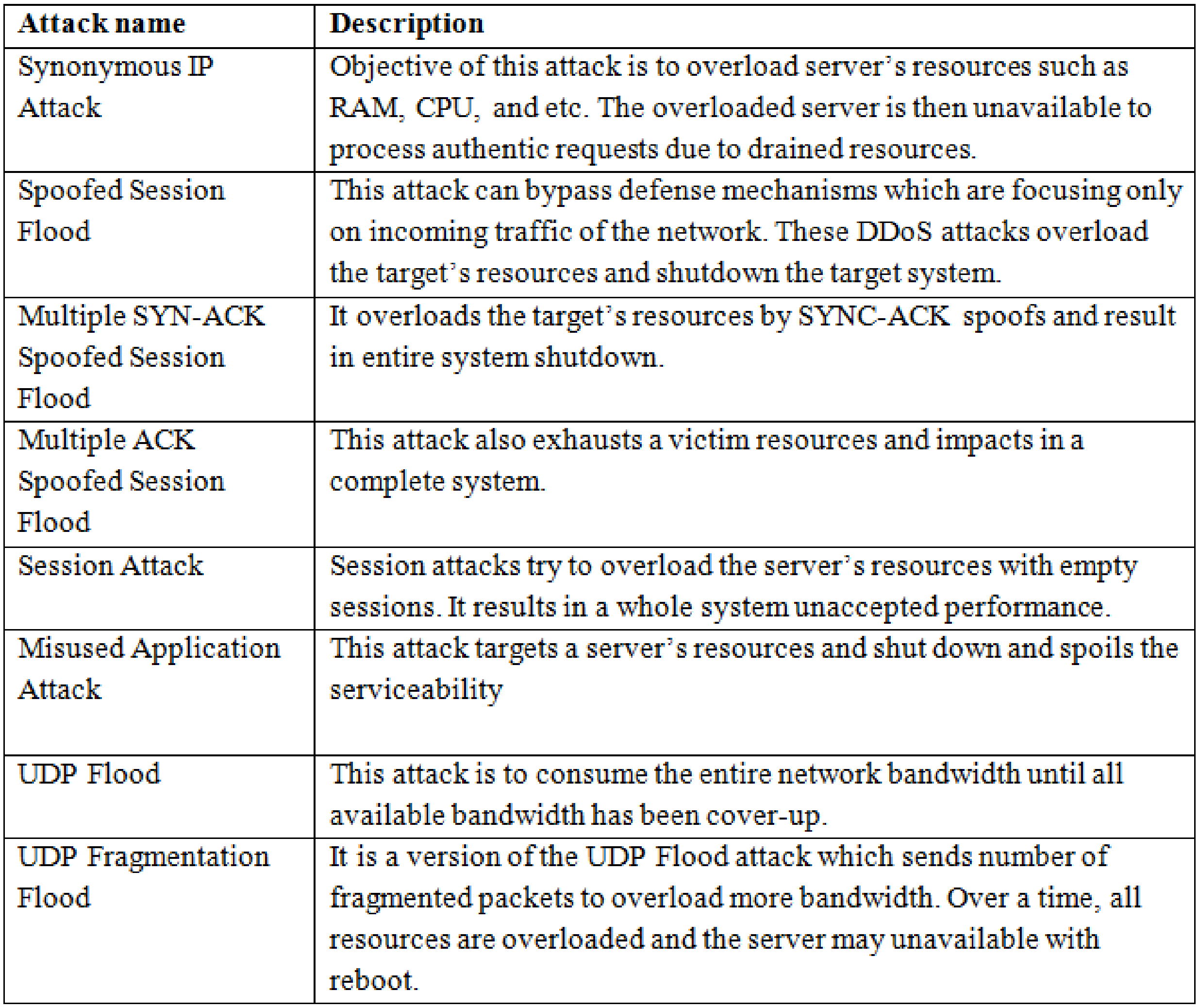
Table 4: DDOS Complex Attacks and its varieties



Attack Name	Description
Multi-Vector Attacks	Attacks can also combine many methods to keep network admin confused who dealing with the DDoS attack. These attacks are difficult to address. It is capable of taking down some of the well-protected servers and networks.
SYN Flood	This attack exploits the three-way TCP communication design among the client, host, and server. The result will be server unavailability to process authentic requests due to exhausted network properties till packets loss.
SYN-ACK Flood	A huge number of spoofed SYN-ACK packets is sent to a victim server in a SYN-ACK Flood attack.
ACK & PUSH ACK Flood	In this attack, vast number of spoofed ACK packets is sent to the victim server to decrease it. It impacts to server unavailable to process authentic requests due to exhausted resources till the attack lasts.
ACK Fragmentation Flood	To execute this attack, 1500 bytes fragmented packets would send to the victim server. This attack spoils all servers within the target network by consuming entire network bandwidth.
RST/FIN Flood	The attack tries to overload a server's resources such as RAM, CPU and etc. as the server tries to process these invalid requests. The result is a server unavailable to process authentic requests because of resource overload.
DNS Flood	An attacker sends vast number of spoofed DNS request packets which look similar to real requests. The attack consumes complete network bandwidth till it is drained out.
VoIP Flood	An attacker numerous spoofed VoIP request packets from a high volume set of source IP. The moment of VoIP server is flooded with spoofed requests it overloads the complete resources while distinguishing the valid and invalid requests.
Media Data Flood	Huge spoofed media data packets are sent by an attacker from variety of source IP and server is flooded with spoofed media data requests. It overloads all available resources and network bandwidth.
Direct UDP Flood	The attack is designed cover complete bandwidth and resources in the network till it shutdown. The huge number of BOTs used to implement the attack is same as the source IP range for this attack.
ICMP Flood	An attacker sends multiple spoofed ICMP packets from a large source IP. When a server is flooded with large amounts of spoofed ICMP packets, its resources gets overloaded in processing these requests. Results service unavailable.
ICMP Fragmentation Flood	It sends a big packet to cover highest bandwidth by sending fewer fragmented ICMP packets. When the target server tries to put these forged fragmented ICMP packets with no correlation together, it will fail to do so. The server gets overload with its resources and reboots.

All amplified attacks use the same strategy described above for CHARGEN, NTP, etc. Other UDP protocols that have been identified as possible tools for carrying out amplification flood attacks U.S. CERT are:SNMPv2, NetBIOS, QOTD, BitTorrent, Kad, Quake Network Protocol, Steam Protocol. Next section describes the network anomaly detection techniques which are proposed against DDOS attacks. DDOS attack in networks are possible, many of varieties such as synonymous IP , Spoofed Session Flood, Multiple SYN-ACK spoofed session, UDP and Misused applications are highlighted along with its description in table 5.

Table 5: DDOS Attacks in networks and its varieties



Attack name	Description
Synonymous IP Attack	Objective of this attack is to overload server's resources such as RAM, CPU, and etc. The overloaded server is then unavailable to process authentic requests due to drained resources.
Spoofed Session Flood	This attack can bypass defense mechanisms which are focusing only on incoming traffic of the network. These DDoS attacks overload the target's resources and shutdown the target system.
Multiple SYN-ACK Spoofed Session Flood	It overloads the target's resources by SYNC-ACK spoofs and result in entire system shutdown.
Multiple ACK Spoofed Session Flood	This attack also exhausts a victim resources and impacts in a complete system.
Session Attack	Session attacks try to overload the server's resources with empty sessions. It results in a whole system unaccepted performance.
Misused Application Attack	This attack targets a server's resources and shut down and spoils the serviceability
UDP Flood	This attack is to consume the entire network bandwidth until all available bandwidth has been cover-up.
UDP Fragmentation Flood	It is a version of the UDP Flood attack which sends number of fragmented packets to overload more bandwidth. Over a time, all resources are overloaded and the server may unavailable with reboot.

The above table2 to Table 5 has clearly represented the existing various DDOS attacks with respect to HTTP, Network, application, protocol and etc. Hence these investigation recommends to do research for identifying network anomaly detection techniques which are described in section 3.

3. Network Anomaly Detection Techniques

This section discusses the network anomaly detection techniques proposed to address the DDOS attacks. In DDOS detection has two broad categories such as offline and online .Offline DDOS detection again sub divided into anomaly and specific. Which is presented in fig.3

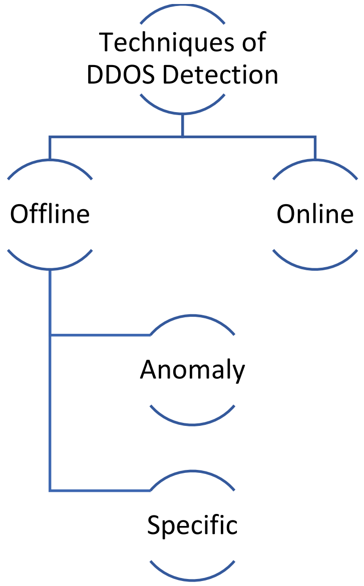


Figure 3. Techniques to detect DDOS attacks

Figure 4 represents the Classification of network anomaly detection methods. Table 6 represents the Anomaly based detection approaches. Figure 5 summarizes the DDOS detection approaches

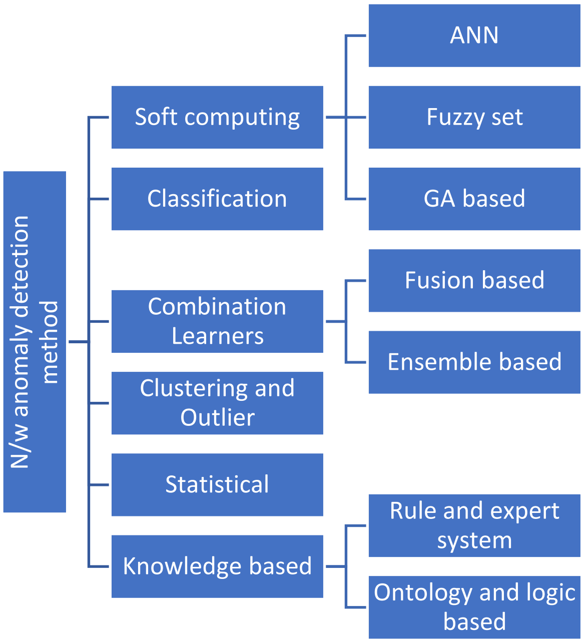


Figure 4: Classification of network anomaly detection methods [3]

The DOS attack detection can be done in following way such as signature based, anomaly based and hybrid based etc. Inturn each of these has several ways to detect the dos attack. Figure 5 represents the DDOS detection approaches in different ways. Signature based again classified into state transition analysis, expert systems, petri-nets, description scripts and adopt system. Anomaly based detection again divided as point anomaly-based detection, contextual anomaly based and collective anomaly based detections. The point anomaly based detection are classified as statistical methods, artificial intelligence, information theoretic and nearest neighbor. Many approaches have been highlighted with its pros and cons. The approaches are statisticalmethods-based anomaly detection, data mining based, information theoretic based, nearest neighbor based and artificial intelligence based etc. has been presented with it pros and cons in table 6.

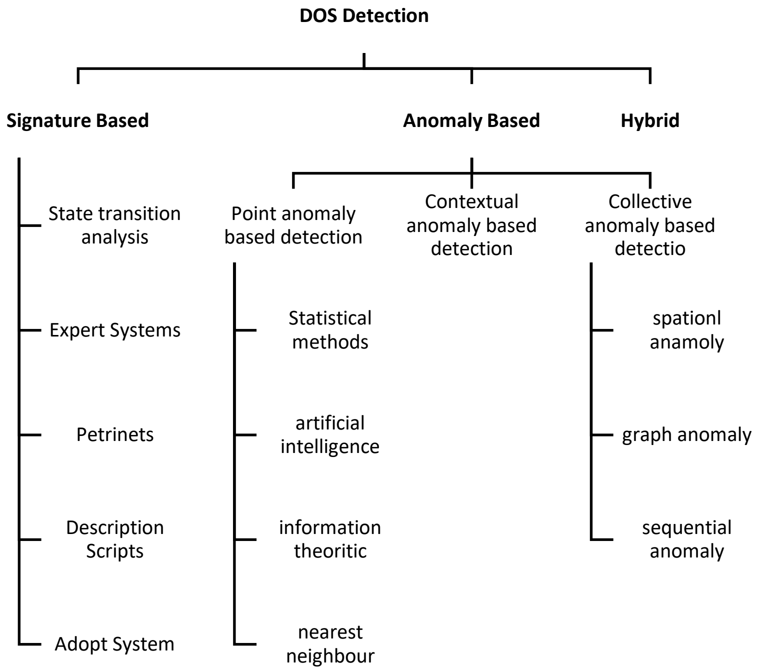
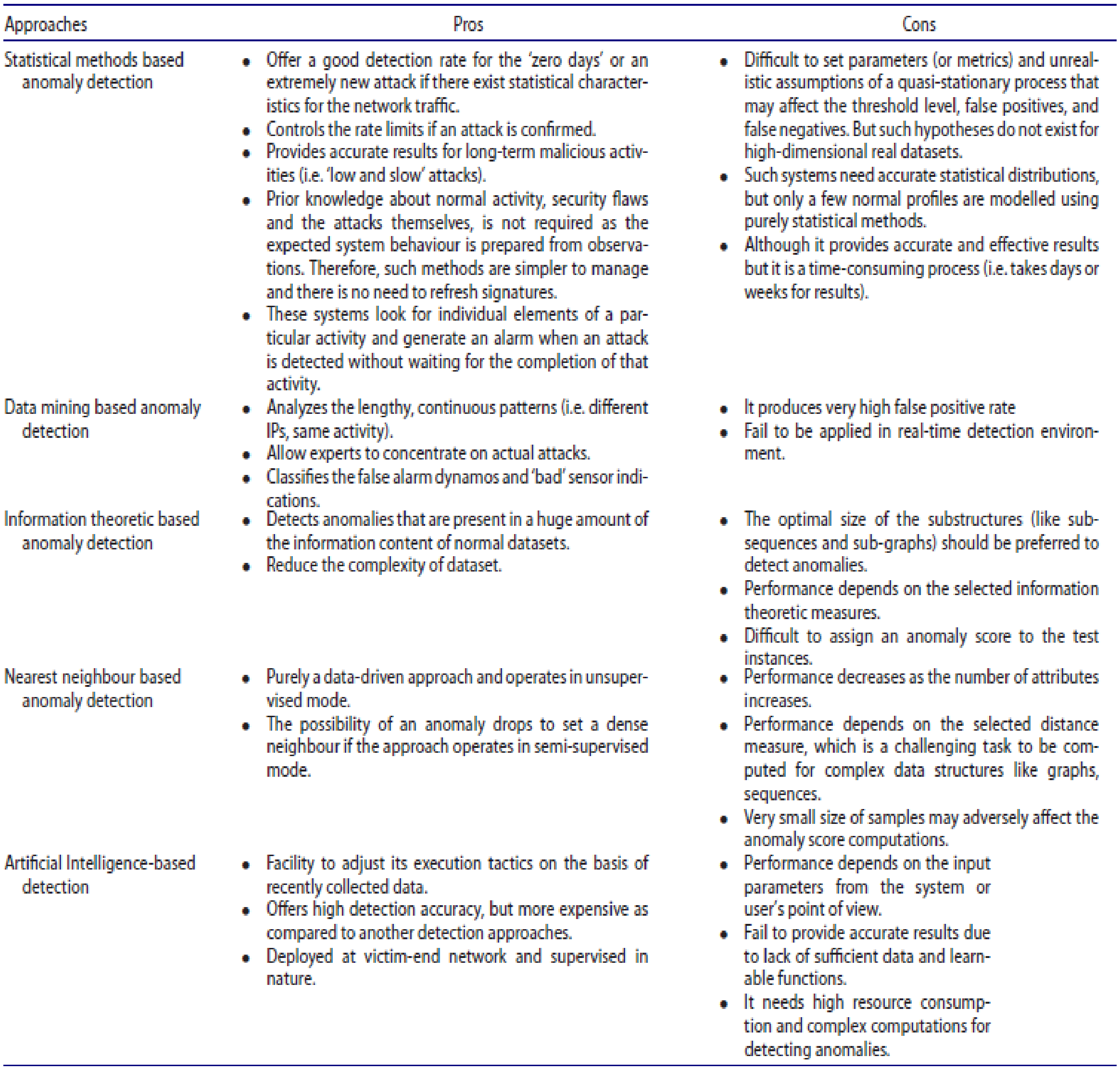


Figure 5: DDOS detection approaches [2]



Approaches	Pros	Cons
Statistical methods based anomaly detection	• Offer a good detection rate for the 'zero days' or an extremely new attack if there exist statistical characteristics for the network traffic. • Controls the rate limits if an attack is confirmed. • Provides accurate results for long-term malicious activities (i.e. 'low and slow' attacks). • Prior knowledge about normal activity, security flaws and the attacks themselves, is not required as the expected system behaviour is prepared from observations. Therefore, such methods are simpler to manage and there is no need to refresh signatures. • These systems look for individual elements of a particular activity and generate an alarm when an attack is detected without waiting for the completion of that activity.	• Difficult to set parameters (or metrics) and unrealistic assumptions of a quasi-stationary process that may affect the threshold level, false positives, and false negatives. But such hypotheses do not exist for high-dimensional real datasets. • Such systems need accurate statistical distributions, but only a few normal profiles are modelled using purely statistical methods. • Although it provides accurate and effective results but it is a time-consuming process (i.e. takes days or weeks for results).
Data mining based anomaly detection	• Analyzes the lengthy, continuous patterns (i.e. different IPs, same activity). • Allow experts to concentrate on actual attacks. • Classifies the false alarm dynamos and 'bad' sensor indications.	• It produces very high false positive rate • Fail to be applied in real-time detection environment.
Information theoretic based anomaly detection	• Detects anomalies that are present in a huge amount of the information content of normal datasets. • Reduce the complexity of dataset.	• The optimal size of the substructures (like subsequences and sub-graphs) should be preferred to detect anomalies. • Performance depends on the selected information theoretic measures. • Difficult to assign an anomaly score to the test instances.
Nearest neighbour based anomaly detection	• Purely a data-driven approach and operates in unsupervised mode. • The possibility of an anomaly drops to set a dense neighbour if the approach operates in semi-supervised mode.	• Performance decreases as the number of attributes increases. • Performance depends on the selected distance measure, which is a challenging task to be computed for complex data structures like graphs, sequences. • Very small size of samples may adversely affect the anomaly score computations.
Artificial Intelligence-based detection	• Facility to adjust its execution tactics on the basis of recently collected data. • Offers high detection accuracy, but more expensive as compared to another detection approaches. • Deployed at victim-end network and supervised in nature.	• Performance depends on the input parameters from the system or user's point of view. • Fail to provide accurate results due to lack of sufficient data and learnable functions. • It needs high resource consumption and complex computations for detecting anomalies.

Table 6: Anomaly based DDOS detection approaches [1]-[4]

4. Review outcomes for research objectives

Section 2 describes all variety of DDOS attacks and its impacts. Section 3 represents the existing network anomaly detection techniques, approaches, and methods of DDOS attacks. Based on the above study of network traffic anomaly detection of DDoS attacks, some of the review outcomes of research objectives are listed below:

- With the evolving nature of networking technology and with the constant effort of attackers to launch newer attacks, How to detect novel attacks?
- How to generate real-life network traffic intrusion dataset for effectively testing the NIDS?

- With the rapid/tremendous growth in network traffic and the periodic changes in traffic patterns as well as the presence of noise in the data, building a normal profile or signature for legitimate traffic remain a challenging question?
- How to update online signature database dynamically?
- Techniques holds good for the identification of normal attack may not be successful in identifying attacks which occurs very rarely?

Following are some of the research objectives we have derived from the review.

- To develop and test various Machine learning models for the effective detection of network anomalies in DDoS attacks by analyzing its network traffic behavior.
- To achieve high detection accuracy and Low False Positive (FP) rate.
- Early stage detection and detection of low DDoS attacks
- To model the Network based on its Behavioral Analysis for the detection of network anomalies.
- To propose an approach for minimum disruption of network and its resources during the detection of DDoS attack
- Testing on various datasets and Comparative analysis of proposed approaches.

5. Conclusion and Future Enhancements

In this study report, we studied many DDoS attacks and its varieties. Several DDOS network anomaly detection approaches. Signature-based detection techniques can disclose only known attacks and results in high detection accuracy with the low false notifications. Anomaly-based detection techniques has been widely used to detect the Net-DDoS and App-DDoS attacks. As a part of survey, many DDOS attacks approaches, methods and techniques has been described. Many available network anomaly detection techniques, approaches, and methods have been presented and summarized. The key challenges for these techniquesare online analysis, manipulating large amount of data. And also spreading false signal ratio because of uncertainty data presence. From the above review, we have concluded that the researchers have proposed many defense mechanisms against the DDoS attacks. Because of lack of benchmarks against the performance of defense tools may be compared, the best approaches and solutions for defending against those attacks are questionable.

In future we have decided to focus on research objectives such as i) To develop and test various Machine learning models for the effective detection of network anomalies in DDoS attacks by analyzing its network traffic behavior. Ii) To achieve high detection accuracy and Low False Positive (FP) rate. and Iii) Early stage detection and detection of low DDoS attacks

Acknowledgement

Our sincere thanks to Dr Surendra Pal, Vice Chancellor, DIAT (DU) and SmtManimozhi Theodore, Director, CAIR, Bangalore, for their constant encouragement.

References

1. Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, Network Anomaly Detection: Methods, Systems and Tools, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014, P.P. 303-337.
2. ParneetKaur, Manish Kumar & Abhinav Bhandari, A review of detection approaches for distributed denial of service attacks, Taylor &Fransic, Systems Science & Control Engineering,20 Jul 2017.
3. Acohido, B., & Swartz, J. (2009). Hacker attack takes down Twitter, Facebook, LiveJournal. Hacker attack takes down Twitter, Facebook, Live Journal, ed.
4. Agarwal, B., & Mittal, N. (2012). Hybrid approach for detection of anomaly network traffic using data mining techniques. Procedia Technology, 6, 996–1003.
5. Aggarwal, A., & Gupta, A. (2015). Survey on data mining and IP traceback technique in DDoS attack. International Journal of Engineering and Computer Science ISSN:2319-7242, 4(6), 12595–12598.
6. Alenezi, M., & Reed, M. J. (2012). Methodologies for detecting DoS/DDoS attacks against network servers. Proceedings of the seventh international conference on systems and networks communications—ICSNC, November 18–23, Lisbon, Portugal. pp. 92–98. IARIA.
7. Androulidakis, G., Chatzigiannakis, V., &Papavassiliou, S. (2009). Network anomaly detection and classification via opportunistic sampling. IEEE Network, 23(1), 6–12.
8. Asosheh, A., &Ramezani, N. (2008). A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers, 7(7),281–290.
9. Baraniuk, C. Retrieved from http://www.bbc.com/news/technology-35376327
10. Barbara, D., Couto, J., Jajodia, S., & Wu, N. (2001). ADAM: A testbed for exploring the use of data mining in intrusion detection. ACM Sigmod Record, 30(4), 15–24.
11. Barbara, D., Wu, N., &Jajodia, S. (2001). Detecting novel network intrusions using Bayes estimators. SIAM, 1–17.doi:10.1137/1.9781611972719.28
12. Bhandari, A., Sangal, A., & Kumar, K. (2015). Destination address entropy-based detection and traceback approach against distributed denial of service attacks. International Journal of Computer Network and Information Security, 7(8),9–20.
13. Bhandari, A., Sangal, A. L., & Kumar, K. (2016). Characterizingflash events and distributed denial-of-service attacks:An empirical investigation. Security and Communication Networks,9(13), 2222–2239.
14. Bhatia, S., Mohay, G., Tickle, A., & Ahmed, E. (2011). Parametric differences between a real-world distributed denial-ofservice attack and a flash event. IEEE, 210–217. doi:10.1109/ARES.2011.39
15. Bhuyan, M. H., &Kalita, J. K. (2012). Network anomaly detection:methods, systems and tools.
16. Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., &Kalita, J. K.(2014). Detecting distributed denial of service attacks: Methods,tools and future directions. The Computer Journal, 57(4),537–556.
17. Bisson, D. Retrieved from http://www.tripwire.com/stateof-security/risk-based-security-for-executives/risk-management/report-ddos-attacks-grew-in-number-size-and-sophistication-in-q4-2015/

***