# A Study on Application-layer Attacks in Communications Network

**Arindam Giri[1], Piyu Sarcar[2], Mrutyunjay Rout[2]**
*[1]Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, INDIA ari.giri11@gmai.com*
*[2]Department of Electronics and Communication Engineering, National Institute of Technology, Jamshedpur,INDIA*

**ABSTRACT**
Distributed Denial of Service(DDoS) attacks are now a threat to Internet. Though traditionally DDoS attacks stuck at network layer, recently an increasing number of DDoS attacks occur at application layer. They target specific web applications. These attacks appear as legitimate traffic, because of their low and slow rate. In this paper, we introduce DDoS attacks along with taxonomy and method to detect application layer DDoS(App-DDoS) attacks. Recent research trends in application-layer attack detection are also included.

**Keywords** Distributed Denial-of-Service attacks, application layer attacks

## I. Introduction

Denial-of-Service(DoS) attacks have been proved the most challenging among many network attacks[1]. They rely on overwhelming the network to deny services to the legitimate users. Distributed Denial-of-Service(DDoS) attack is kind of DoS attack which applies a large number of computers to launch attacks. DDoS attacks consume large bandwidth. Recent development of DDoS attacks involves low bandwidth appearing to be normal traffic. The new class of DDoS attacks, called application layer DDoS(App-DDoS) attacks target application layer. App-DDoS attacks are harder to detect and mitigate because they appear like legitimate traffic. Traditional DDoS attack detection methods[4] are not enough to defend App-DDoS attacks. Although a number of researches[6,7,8,11,12,13] is carried on detection and mitigation of App-DDoS attacks, none of these is of wide use. Information theoretic metrics are being used recently to detect such attacks efficiently.

Section 2 starts with the introduction to different attacks. Section 3 discusses the DoS attack. Section 4 illustrates the application-layer attacks. Related works in application-layer attacks are given in Section 5. Information theoretic approach to detect App-DDoS attack is given in Section 6. Finally, conclusion is made in Section 6.

## 2. Different Classes of Attacks

An attack is an activity access unauthorized use of information, alteration of information to make the system unreliable. All attacks can be broadly classified as external and internal. External attacks are made by unauthorized intruders external to the computer system while the internal attacks are made by authorized users having not enough privileges for the root or superuser mode. There are many types of attacks available in the literature. A taxonomy of such attacks can be found in [3,5]. It includes attacks ranging from virus to Denial-of-Service(DoS). There are various classes of attacks[2] available in the literature such as virus, worm, Trojan, buffer overflow, password attack, social engineering attack, User-to-Root, Remote-to-Local

## 3. DDoS Attack

Denial of Service or distributed Denial of Service attacks[15] are the form of DoS attacks which uses a botnet to launch attack. DoS attacks consumes bandwidth, hold on computing resources of a victim system. The categories of DDoS attacks can be found in Table 1.

3.1 Bandwidth Depletion Attacks

These attacks flood the network with spurious packets to exhaust the bandwidth and routing capacity of the network. Such attacks operate at network layer(layer 3) and transport layer(layer 4).

**Flood Attacks:** Flood attacks send the large volumes of IP traffic to a victim system. UDP and ICMP packets are used to launch bandwidth depletion attacks.

Table 1
DDoSattack taxonomy

| | | | |
|---|---|---|---|
| Bandwidth Depletion Attacks | Flood attack | UDP | Random Port |
| | | | Same Port |
| | | ICMP | |
| | Amplification attack | Smurf | |
| | | Fraggle | Direct |
| | | | Loop |
| Resource Depletion Attacks | Protocol Exploit attack | TCP SYN | |
| | | PUSH+ACK | |
| | Malformed Packet attack | IP Address | |
| | | IP Packet Options | |

**Amplification Attacks:**Amplification attacks send messages to a broadcast IP address. On receiving the packet, the router replicates it and sends it to all hosts under the router, eventually amplifying the traffic in network. Attackers can send the broadcast the messages directly or use agents. Amplification attacks can be launched by smurf and fraggle attacks.

3.2 Resource Depletion Attacks

Resource depletion attacks exploit the vulnerabilities of an application. These attacks operate at application layer(layer 7) and consume low bandwidth. Attackers tie up the critical resources of network such as DNS server, router. These attacks can be launched in two ways: sending packets by exploiting protocol vulnerabilities or malformed packets.

## 4. Application Layer DDoSAttacks and Classification

The growing threat of Application layer DoS (App-DoS) attacks[15] becomes a nightmare of the security personnel. App-DoS attacks target the vulnerabilities of the specific web applications running on the server to tie up the resources of the victim server such as CPU time, memory, operating system. The App-DoS attacks are seen in a variety of categories[16,14] as shown in Fig.1. The App-DoS attacks are classified into four classes: request flooding, asymmetric flooding, hybrid flooding and exploit-based flooding attacks.

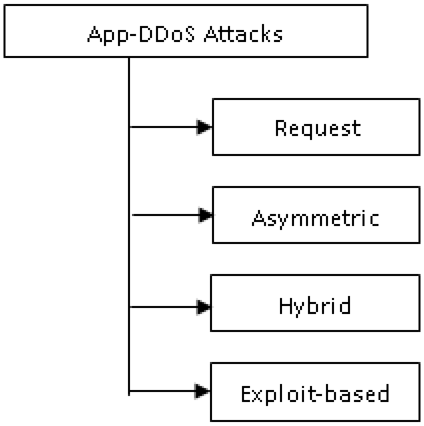

Fig. 1 App-DDoS attack types.

## 5. Related Works

App-DoS attacks mimic the legitimate traffic. A few researches are done on detecting App-DoS attacks. The detection methods for App-DoS attacks are divided into three categories as shown in Fig.2. Application-based approach the behavior of particular web applications is analyzed to detect App-DoS attacks. Rate-limiting acts as the primary defense mechanism here.In puzzle-based approach puzzles such as CAPTCHApuzzle[17] are offered to solve the ability of user at the IP address to solve the puzzle DoS attacks are getdetected.In network traffic characteristics-based approach[8], the characteristics of network traffic is monitored to differentiate App-DoS attack traffic from legitimate traffic.

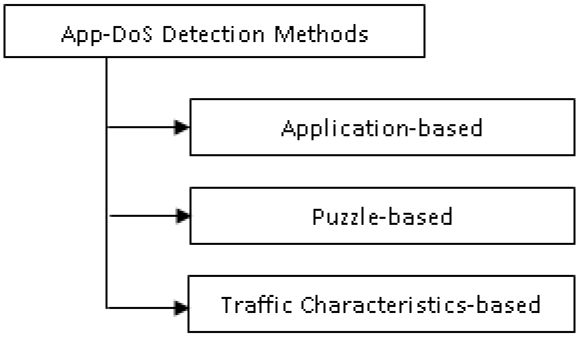

Fig. 2 App-DDoS detection methods.

## 6. Information Theory in App-DDoS Attack Detection

Recently, information theory based metrics are being used by researchers. In information theory, the entropy is the measurement of uncertainty associated with a random variable. The more random the variable is the larger the entropy is. Many such information metrics[18,19] are proposed. Entropy metric is used to measure the difference between probability distributions of normal traffic and DDoS attack traffic.

Let$r_{ij}$ be the request in a session, where i, j $\in$I, a set of positive integers, 'i' denotes the request number in session 'j'. Let |(rj,t)| denotes the number of requests per session j, at a giventime t. It can be expressed as:

$$\left|r_j, t\right| = \sum_{i=1}^{\infty} \mathrm{r_{ij}} \tag{1}$$

For a given interval _t, the variation in the number of requests per session j is given as follows:

$$N_j\left(r_j, t + \Delta t\right) = \left|r_j, t + \Delta t\right| - |(r_j, t)| \tag{2}$$

The probability of the requests per session j, is given by:

$$P_j\left(r_j\right) = N_j\left(r_j, t + \Delta t\right) / \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} N_j\left(r_j, t + \Delta t\right) \tag{3}$$

Let R be the random variable of the number of requests per session during the interval Δt. Therefore, the entropy of requests per session is given as:

$$H(R) = -\sum_j P_j(r_j) \log \mathrm{P_j}(r_j) \tag{4}$$

The range of entropy H(R) is now:

$$0 \leq \mathrm{H(R)} \leq \log \mathrm{N} \tag{5}$$

where N is the number of requests.

Let C be the maximum capacity of the session,t be the threshold and if :

$$|\mathrm{H(R)} - \mathrm{C}| > \mathrm{t}$$

Then, the network is under App-DDoS attack.

## 7. Conclusion

In this research we have introduced the recent trends of application-layer DoS attacks. These attacks are low and slow, and mimic the normal traffic. So, App-DoS attacks remain invisible to the traditional DoS attack detection methods. Recently, information theory-based metrics are being used effectively to trace such attacks. More research is required on the detection and mitigation of such attacks at an early stage.

## References

1. J. P. Anderson, “Computer Security Threat Monitoring and Surveillance”, James P Anderson Co, Fort Washington, Pennsylvania, Tech. Rep., April 1980.
2. Colon E. Pelaez and John Bowles, “Computer Viruses”, System Theory, *Proc. Twenty-Third Southeastern Symposium on System Theory*, pp. 513-517, 1991.
3. Simon Hansman, “A Taxonomy of Network and Computer Attack Methodologies”, University of Canterbury, Christchurch, New Zealand, 2002.
4. Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, “Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions”, *The Computer Journal*, doi: 10.1093/comjnl/bxt031, 2013.
5. Stephen M. Specht, Ruby B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures”, *International Conference on Parallel and Distributed Computing Systems*, pp. 543-550, 2004.
6. Macia-Fernandez, G., J. Diaz-Verdejo, and P. Garcia-Teodoro, “Mathematical model for low-rate dos attacks against application servers”, *IEEE Transactions* on *Information Forensics and Security* , Vol. 4, no. 3, pp. 519–529, 2009.
7. Maciá-Fernández, G., R. A. Rodríguez-Gómez, and J. E. Díaz-Verdejo, “Defense techniques forlow-ratedos attacks against application servers”, *Computer Networks,* vol.54 no.15, pp. 2711–2727, 2010.
8. Jung, J., B. Krishnamurthy, and M. Rabinovich, “Flash crowds and denial of service attacks: characterization and implications for cdns and web sites”, *in Proc. 11th international conference on WorldWide Web*, New York, USA: ACM 2002, pp. 293–304.
9. P. Chwalinski, R. Belavkin, and X. Cheng, "Detection Of Http-Get Attack With Clustering And Information Theoretic Measurements", *Foundations And Practice Of Security,* Vol. 7743, Pp. 45-61, 2013.
10. Arbor Networks, "The Growing Threat Of Application-Layer Ddos Attacks," 2012.
11. S. Mcgregory, "Preparing For The Next Ddos Attack", *Network Security*, Vol. 2013, pp. 5-6, 2013.
12. S. Renuka Devi and P. Yogesh, "Detection of Application layer DDoS Attacks using Information Theory based Metrics", *CS & IT-CSCP* , pp. 217–223, 2012.
13. D. Das, U. Sharma and D. K. Bhattacharyya, "Detection Of Http Flooding Attacks In Multiple Scenarios", *Proc. International Conference On Communication, Computing&Security*(ICCCS), Orisa, India, pp. 517-522
14. FuiFui Wong and Cheng Xiang Tan, “A survey of trends in massive ddos attacks, and cloud-based mitigations”, *Intl’ Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.3, 2014

15. S. Heron, "Denial Of Service: Motivations And Trends," *Network Security*, Vol. 2010, pp. 10-12, Issue 5, 2010.
16. Maciá-Fernández, G., J. E. Díaz-Verdejo, and P. García-Teodoro, “Assessment of a vulnerability in iterative servers enabling low-rate dos attacks”, *in Proc. of 11th Europe*an *conference on Research in Computer Security*, Berlin, Heidelberg: Springer-Verlag, pp. 512–526, 2006..
17. Mehra, M., M. Agarwal, R. Pawar, and D. Shah, “Mitigating denial of service attack using captcha mechanism*”, in Proc. International Conference &Workshopon Emerging Trends in Technology*, New York, USA: ACM 2011, pp. 284–287.
18. A.Chonka,J.Singh,W.Zhou,Chaos theory based detection against network mimicking DDoS attacks,IEEECommun.Lett.13(2009)717-719,doi:10.1109/LCOMM.2009.090615.
19. J.Francois,I.Aib,R.Boutaba,FireCol:acollaborativeprotectionnetworkforthedetectionoffloodingDDoSattacks,IEEE/ACMTrans.Networking20(2012)1828–1841,doi:10.1109/TNET.2012.2194508.