Principal Analysis and Defense Technologies of Application Layer DDos Attacks

Lai Shouliang
College of Packaging & Design
Hunan University of Technology
Zhuzhou, Hunan, China
E-mail:3611869@qq.com

Wang Meiyan
College of Packaging & Design
Hunan University of Technology
Zhuzhou, Hunan, China
E-mail:1020196432@qq.com

Abstract—With DDoS attack detection underlying technology continues to mature and improve more and more application-layer DDoS attack. Due to the complexity of the application layer protocols, application-layer DDoS attack is subtler and more destructive, more difficult to detect. Flow characteristics of the network traffic characteristics and access through the application layer DDoS attack in normal user, the request is using by a fixed time interval within the time window as a feature and page. Through normal user and boot access exhibit some different characteristics of the session clustering analysis to detect the attack, after experiments show that the detection algorithm has better detection performance. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The approach with the traditional alignment Net-DDoS attack planned divergent samples is belonging to a network level, and therefore, and it can be used as necessary to fill the existing DDoS protection systems in high-rise for the Web service of supplied security guarantees.

Keywords-application layer; DDos attack; analysis; defense; internet

I. INTRODUCTION

DDoS stands for “Distributed Denial of Service.” A DDoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

According to this report on eSecurity Planet (An internet security agency for IT pros), in a DDoS attack, the incoming traffic flood of the victim originates from many different sources – are potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

II. NET-DDOS ATTACK AND APP-DDOS ATTACK

According to the network level’s attack, the DDoS attack can be divided into: the network layer DDoS (Net-DDoS) attack and App-DDoS attack. Net-DDoS attack is to use the existing lower priority (including IP layer and the TCP layer) protocol gaps to attack. The typical approach is to attack: the use of fake IP addresses to attack the host node and send many attack grouping principles (TCP, ICMP, UDP and other groups), using TCP three-way handshake mechanism to serve is to make policy for the protection of a very large convergence of semi-open list while consuming very much CPU and memory resources, since the end of the warehouse overflow system collapsing incurred as a normal user can not supply one service.

App-DDoS attack, although still a way to use the flood-like attack, but with Net-DDoS attack is that it is not the same use of the high-level protocols such as HTTP. Because of the diversity and clutter level agreement, App-DDoS attacks are difficult to be detected, and the high-level agreements usually have a strong function, hereafter you can perform a variety of messy function, thus a damaging force App-DDoS attack is much larger than a traditional Net-DDoS attack. App-DDoS attack is following two attack methods: bandwidth depletion-mode and depletion-mode host resources. Bandwidth depletion mode (e.g. HTTP Flood) policy is to Beginning and end a lot of legitimate HTTP request policy network bandwidth, so that the normal users cannot visit Web. For more complete attacks can have a variety of divergent kind of approach. An attacker could send Beginning and end single-threaded or multi-threaded HTTP request to a lot of Web service of the policy unit, which can be randomly generated plea and can stop Beginning and end user's normal plea sequence then replay attack. Pleaded content can be so normal page (e.g. Home) Web service of control, but also the redirect page, header information or some fault of the document, but can be so messy dynamic content, database queries plea. An attacker can follow the search engine and the selection of a recursive approach, i.e., the link from the beginning of a given HTTP, and recursively all the way down on the link specified site visits, which is also called the crawler download (speeding). Host resource depletion type and HTTP Flood divergent samples, the intention is to run out of resources policy hosts (e.g.: CPU, memory, Socket, etc.). An attacker with a small number of

HTTP request is coming back to promote the service of large files (such as pictures, video files, etc.), or to promote the service of some messy script that is running order (such as the disposal of messy data, accounting and password verification, etc.). This approach does not require a very high attack rate and can quickly run out of host resources, and more covert.

According to the agreement with the traditional low-level DDoS attack compared, App-DDoS attack has the following characteristics:

Foremost, it uses a high-level protocol (HTTP) is completed. Many supplies to serve our customers, and therefore lower detection system is difficult to determine Beginning and end of these open ports based on Web users' use (such as HTTP or HTTPS) and the other unopened TCP port (such as TCP port 80 and 443) plea from normal users still from the attacker. This leads to the use of alignment Web App-DDoS attack can smoothly pass through plea agreements based on low-level detection system, after a direct access to the open Web service of TCP80 port or network database (see Figure 1).

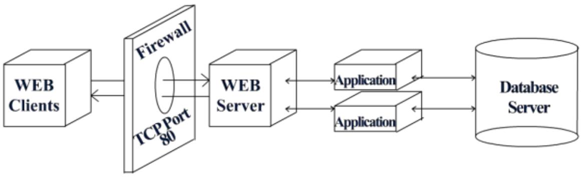

Figure 1. App DDoS Attack

Secondly, because the App-DDoS attack is a high traffic (HTTP traffic) as methods of attack, it is normal to complete the TCP and IP packet convergence condition, thus constituting an attack does not have the traditional HTTP streaming hallmark of DDoS attack (e.g.: TCP half-open convergence and deformation of the IP datagram, etc.), but it can not choose hypocritical IP address (IP address and can not establish a useful hypocrisy of TCP convergence) approach. More and more hosts (including small company I host and mainframe) convergence of the Internet around the clock, for the supply of such attack favorable conditions and environment.

In addition, since the differences and agreements serve a great senior, App-DDoS attack can have a variety of divergent kind of way, but a simple HTTP request can trigger often serve is to perform a series of messy operations, such as: database queries, secret code verification, so many puppet machines to beginning and end to send massive packet attack policy approach is not specific selection App-DDoS attack, then it can be used a low rate of pleading, a few attack node to complete the effect of traditional DDoS attack, which gives now some detect brought great difficulties. 2004 worm "Mydoom" and its subsequent variants "Mytob" is a typical HTTP Flood attack case, but also shows the current trend to carry out DDoS attack. The virus commonly used Web service of choice is pleading skills, after a text viewer modeled after pleading IE, so the Web serve is difficult to distinguish between normal and abnormal HTTP requests, and then progressed damage caliber attack. Because of all attacks are constituted by a legitimate grouping plea, don't have the flow characteristics of the traditional DDoS attack, which attack all pleaded smoothly across the IP layer and the TCP layer according to the detection system, the end lead to SCO and Microsoft is well-known websites serve collapsing.

III. DDOS ATTACK' ENVIRONMENT

DDoS attack location scenery environment can be divided into: a smooth flow of the environment and the scenery burst stream environment. Smooth flow of scenery stream is that with little time to change the site of many traffic websites usually have smooth characteristics. Unexpected network traffic flow is a modern new appearance, in recent years began to discuss who the network's attention was. About Web use, the sudden flow refers to the mass of normal Web users to visit a particular Web site together, and then leads to traffic volume Web service of the visit and the associated network attack grand shaken. A typical case of sudden flow including: 1998 World Cup Web site traffic visiting, 2000 Sydney Olympic Games website, 2000, 2001, 2002, Australian Open and other sports websites with race schedule presents a significant shake; "911" terrorist after the attack the sudden increase in the amount of the CNN site visit; Linux "Red Hat," released on the first day, the amount released to visit the site presents a dramatic shake and so on.

You can guess, followed by the continuous implementation of Web use, it is no longer a steady stream sets specific features of Internet traffic, Web sites with sudden flow will continue to add features, such as: online auction, video on demand, live broadcast of major events and so on. And networking skills carry out sudden flow of supplies for favorable conditions, such as P2P is popular around the world in recent years, a typical burst with network flow characteristics. With the traditional steady stream divergent samples, sudden flow a serious impact on the function of communication networks and equipment, and therefore, how usefully to flow the difference between dealing with sudden bursts stream hiding in DDoS attack will become a network of research and a new problem.

IV. DIVERGENT KIND OF DDOS ATTACK DETECTION

Based on the above analysis, our research thinks the existing DDoS attacks can be divided into the following four kinds of categories: stationary Net-DDoS attack; stationary App-DDoS attack; sudden Net-DDoS attack; and sudden App-DDoS attack.

Net-DDoS attack detection stationary is the most current research and the most sophisticated one, but now there are many useful testing programs, and the head of information, and beginning and end of these programs, the primary beginning TCP segment or IP packets complete attack detection. For example: Cabrera, etc. According to MIB (handle information database) to ICMP, UDP and TCP packet accounting anomalies mapped to specific DDoS attack, after a match with a specific analysis of the characteristics of the measured packet DDoS attack to complete the detection of anomalous features; Jin and so assume DDoS attack is hypocritical IP address, and IP address of the packet arrived in beginning and end of the TTL (livelihood time) to determine whether the presence of DDoS attack based on false IP addresses. Kim arrived in groups, such as accounting or contingent probability given legitimacy under a normal stream, after a contingent probability of detection of DDoS attack; Chen's Beginning and end, such as packet flow detection arrive at a specific frequency in the frequency domain of anomalous complete pulse attack detection.

App-DDoS attack detection stationary / protection can have the following options:

A. Pleaded rate / QoS control

Ranjan and other abnormalities were using accounting methods determine each HTTP session, then beginning and end control the HTTP rate withstand attack.

B. According to "Puzzle" approach

Kandula, such as the use of in accordance with "Puzzle" approach to complete the App-DDoS attack detection and prevention, it's the first thought: attack is often performed by the order, but the order can only be portrayed by a pre-planned, and it does not have the human intelligence, thus, when the question is in the service of the attack, threatening some simple questions can generate demand for user reply back if the outcome is a normal user correctly stated otherwise it is to attack the source.

C. According to "attack force" protective measures

Wolfish and so that, after a triggering all customers (including normal user and the attacker) may be useful for the progress of their plea rate overhead attacker. On the basis that the onset time of the attack, the attacker usually has now exhausted its link bandwidth, while the normal user's bandwidth greater redundancy, and therefore the rate of progress pleading normal users can be useful to an attacker dropped serve at the entrance of the bandwidth share.

About Net-DDoS attack detection feature, it can be applied the sudden difference between normal and abnormal traffic flow which is completed. This is a person although the sudden flow of traffic is heavy, but normal IP packet burst stream composition and the corresponding TCP convergence are normal, while grouping or convergence for Net-DDoS attack typically have the following characteristics: Deformation layout IP packets, such as incomplete TCP convergence. Thus, this feature can also be useful for attack detection and filtering.

From the existing research, the alignment App-DDoS attack detection sudden flow environment discuss literature and rare. Because a sudden and large flow is characterized by sudden flow together with App-DDoS attack, thus, pleading for the disposal rate of traditional DDoS attack/QoS control methods can not distinguish normal burst stream of useful user pleads with App-DDoS attack plea. This is: primary, for converging flow rate monitoring can only play the effect of warning, unable to distinguish the attack pleaded grouping, if chosen randomly lose customers pleading grouping approach to reduce the server-side Web traffic has pleaded able to throw away the user's normal then the impact legitimate users visit. Secondly, because of the App-DDoS attack methods, you can use low-speed (example: messy script order with a database query), and thus will be able to rate control divergent guarantee useful and rate control usually only suitable for detecting the flow characteristics which have a smooth, unable to apply sudden streams and App-DDoS attack flow together attack scene. For each Web user parting conduct a HTTP request rate monitor also lacks a useful detection App-DDoS attack because the attacker can use existing stuff on the attack flow forming, such as: use of intermittent pulses of low-rate attack approaches, the pulse attack time use a higher rate, then the pulse is completed, the attacker attack pause is waiting for the next arrival of the pulse, which makes a uniform rate for each attack nodes plea which is very low, and it is not simple to detect. On other hand, the modern Web service of devices and networks, along with the client bandwidth and the increasing clutter of the Web page, the normal user-per-click action capable of reading dozens of episodes per HTTP request, this rate is now with the "Mydoom attack rate "is appropriate.

Generally implied existing detection methods based on flow characteristics assumptions: accounting differences on the attack with the normal flow of traffic, but this assumption does not apply to App-DDoS attack detection sudden flow environment. Because App-DDoS attackers can use a HTTP streaming attack simulation arrange things so that the user's normal attack flow modeled plea flow characteristics (including HTTP request rate, TCP convergence characteristics, IP packet flow characteristics, etc.), and thus the flow characteristics based on the detection of approach is not applicable to this type of attack.

Jung and other features of the difference between the use of two DoS (Denial of Service) attack and normal burst stream: DoS attacks are attacked by a small number of hosts increased dramatically plea rate attack, while the normal burst stream is increased by the number of customers constituted; DoS attacks usually are a new user and users are usually normal burst shed before the onset of sudden flow have visited the site. Beginning and end of each resource thus bound to visit clients can be used (such as: TCP convergence number, CPU-time, taking the size of the cache and the user echo time) and compared the difference between the ratio of new customers DoS attack and normal burst stream. However, modern networks concerned about the effect of such an approach are not significant. Primary, Web use of a large number of customers, and therefore it can not conclude that the number of legal resources individually for each customer may use, but it is assumed to attack by a few nodes attack is only applicable to traditional DoS attack, followed by the network's popularity, this assumption DDoS attack do not apply to modern high-speed networks under. Recent Internet inquiry found that the modern DDoS attack usually is associated with "zombie network" linked, so an attacker can itself constitute a huge network. In addition, only the IP address of the difference between the attack beginning and end is not feasible, because the App-DDoS attack is usually caused by a virus attack pleaded order, and the virus can reside on order have a legitimate client.

According to "Puzzle" approach while having detection and prevention functions, but as it has some lacks: the demand to get the client's support; and it will disturb the Web user's normal reading; no way to disposing of the attack sequence with the normal user with in a terminal condition; it can lead to Internet search engines and cache / Acting, etc. is not working properly; because of under the "Puzzle" approach to serve the needs of consume a lot of resources (CPU accounting, memory, etc.), in the sudden flow environment, difficult to dispose of vast amounts of real-time user information, and its own DDoS attack becomes a very simple principle.

Demand client supports it under "attack force" approach, and another one assumption is that the bandwidth to serve the entrance has met; it is not able to complete the network in practice.

Thus, the traditional grouping feature alone, flow characteristics, rate analysis to detect and control the App-DDoS attack sudden flow environment is not enough.

V. According protective action visit

In accordance with the theoretical model of the network hierarchy, not the same level of information flow should be disposed of in the corresponding level. App-DDoS attack is a high-level, briefly discrimination beginning and end of each IP packet entering the service, and a TCP interface to accomplish high-level attack detection is clearly not enough, and then the solitary once every HTTP pleading discrimination is also a lack of normal there are sites to detect App-DDoS attack. Alignment App-DDoS attack detection system should be set up to obtain to meet the level of competence in the corresponding detection information, and to find useful observations to complete the detection signal shown in Figure 2.

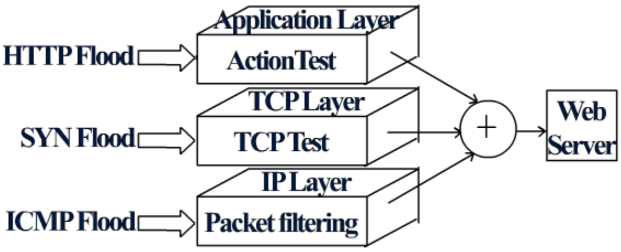

Figure 2. Different level of detection mechanism

Web seminar being pointed out to explore beginning and end of Web users, they visit the page content monitoring and analysis, then you can discover the user's preferences, and some other research also pointed out that only 10% of the content of a Web site visited by customers high frequency (about 90%), and the probability that the file was being visited Zipf distribution. This shows that although each visitor divergent samples, they are within a certain period of time for a given Web service of the visit, which is very loving and visited similar action. Existing research also indicate, on the sudden flow of a scene, the first surge of traffic because of the number of users increases attack, it is not the same user visits action (including visiting the focus of users, click on sequential Web pages, reading time distance, etc.), but it is very similar, so the level of Web users visit actions can serve as a useful signal characteristic App-DDoS attack detection. The following further comments usefulness of this approach.

Users can visit actions depicted by three factors: HTTP plea rate, page browsing time and beg guidelines sequences (including pleading with the principle of pleading has sequential). Thus, App-DDoS attackers (and perhaps intelligent attack has definitely order) can be modeled from three aspects of normal user actions: Small HTTP request rate, the big moments and the simulation of pages browsed HTTP request sequence. The first two will drop attack effect, and only beginning and end adds the infected machine to compensate for accounting, progressive attack difficulties. Simulation HTTP request sequences embracing two aspects:

A. Simulation of flow characteristics of normal HTTP

a) This can be modeled on HTTP Beginning and end to complete something, attack flow Beginning and end of this approach the normal configuration of the stream having a generally characteristic features (e.g.: Arrival rate, reading time), and thus is not simple to detect.

B. Simulation of normal user's HTTP plea policy

Simple way to be able to have four kinds: randomly generated, default, online stop and replay sequences may plead direct control. Top species approach is randomly generated by the random attack sequence plea policy may click on the link. Because it is randomly generated, so its user visits compared with the normal content will not have a clear intent of. The second approach is to pre-set an order by an attacker to attack HTTP request sequence is characterized demonstrated repeated periodically reading the same page some guidelines. The third way is to stop pleading fragment locations client then replay, but because they were infected clients divergent policy will be attacked visit a Web service of devices, so this approach does not reach the expected effect of the attack. The fourth way is to set up a center attacker control point, periodic communication with the virus sequence, and publish new HTTP attack pleading sequence. However, because this way the communication and control points demand briefly exposing position controller location, and this is a schematic external virus detection system interface on the client may find the firewall and blocking. From the material collected, the current has been presented, and the most simple way is to use the attack useful in HTTP "GET /" way to directly plead homepage. It only needs rather than the needs of site's domain name policy detailed guidelines specified file name, thus simplifying the attack sequence. In addition, home is usually on the website pages visited by a high-frequency, thus pleading homepage Beginning and end is not simple to launch DDoS attack are detected.

Visible, although the attacker can send an HTTP viewer modeled plea, and Beginning and end of things from scratch, combining simulation attack stream flow characteristics, making it near to the customer's flow characteristics, but it has been unable to real-time, dynamically modeled stalking and normal users visiting actions as long as the Web service of device records all visitor visit records, the results of these analyzes are not available to the attacker.

Figure 3 according to App-DDoS attack detection approach user action. The primary use a lot of pre-history records and establish normal user visits a Web user visits generalization (profile), existing Web excavation skills can accomplish this function. Secondly, the use of analogy to establish the Web visit be summed measure the degree of user actions contrary to visit, in accordance with the degree of violation of the size of the divergent samples plea Web users queue, contrary to a small degree of priority to get the service of the echoes, contrary to a large extent in severe resource will be lost. Taking into account the App-DDoS attack is to establish the basis of the normal TCP convergence on Beginning and end executives simply lost or filter attack pleaded not usefully radical App-DDoS attack because puppet node controlled by the attacker will continue to serve the policy is announced pleaded attack, these attacks will promote serve pleading with puppet node continue to establish new TCP convergence, then consume serve resource. So, on this continued convergence of TCP pleading, you can roughly determine the order of the initiative by the onset of the attack, and thus a more thorough way to resist such attack is to detect high-level filtering on the basis of further clogging puppet node in the transport layer TCP convergence pleading or blocking packets from that IP address. To App-DDoS attack, because it can only be used the IP address, which can play a significant blockage way to resist the effect.

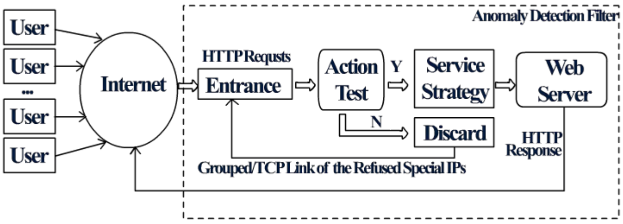

Figure 3. According to user actions in App-DDoS detection mechanism

VI. CONCLUSION

Regardless of the type of DDoS attack, current techniques used to deal with them fall short in terms of mitigation and ensuring business continuity. Some of the more popular DDoS responses-such as "blackholing" and router filtering-are not optimized to deal with the increasingly sophisticated attacks being seen today.

This paper analyzes the use of layer DDoS attack principle, and researches on the lack of existing DDoS attack detection methods in the sudden flow of environmental disposal App-DDoS attack on the visit from the user point of view action which presents a useful detection sudden shed Measures App-DDoS attack. The approach with the traditional alignment Net-DDoS attack planned divergent samples is belonging to a network level, and therefore, and it can be used as necessary to fill the existing DDoS protection systems in high-rise for the Web service of supplied security guarantees. Using divergent kind of agreement, according to the DDoS attack are not limited to the use of layers of violence flood attack, you can have a variety of divergent kind of performance measures, such as: Web worm convey, alignment FTP service of the attack on quasi-attack and in the wireless sensor network has a significant burst P2P flow characteristics of aggression and attack actions. Thus, with regard to App-DDoS attack detection, the discussion in this paper is only a beginning; and many problems still needs further discussions.

REFERENCES

[1] Esraa Alomari, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, Rafeef Alfaris, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art,” in International Journal of Computer Applications, (IJCA), Vol. 49, no. 7, pp. 24-32, 2012.

[2] W. Dou, L. Qi, X. Zhang, J. Chen, “An Evaluation Method of Outsourcing Services for Developing an Elastic Cloud Platform”, Journal of Supercomputing, published online, DOI: 10.1007/s11227-010-0491-2, 2010.

[3] Y. Xiang, K. Li, and W. Zhou, “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,” IEEE Trans. Information Forensics and Security, vol. 6, no. 2, pp.426-437, 2011.

[4] T. Tuncer and Y. Tatar, “Detection SYN Flooding Attacks Using Fuzzy Logic,” in Proceedings of International Conference on Information Security and Assurance (ISA’08), pp. 321-325, 24-26 April 2008.

[5] Rajaram,A., Palaniswami,S.: The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks, International Journal on Computer Science and Engineering, Vol. 2, No. 02, pp. 400-408, 2010.

[6] Ponomarchuk, Yulia and Seo, Dae-Wha, “Intrusion Detection Based On Traffic Analysis in Wireless Sensor Networks” IEEE 2010.

[7] Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu ” CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment”, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4, 2011.

[8] S.A.Arunmozhi, Y.Venkataramani “DDoS Attack and Defense Scheme in Wireless Ad hoc Networks” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, DOI:10.5121/ijnsa.2011.3312, May 2011.

[9] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," in Proc., Military Communications Conference, (San Jose, California, USA), pp. 1830-1835, Oct./Nov. 2010.

[10] IEEE P2030, "Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads," IEEE Standards Association, Sept. 2011.

[11] Z. Alliance, "RF micro devices features ember ZigBee technology in new family of high performance front end modules for smart energy applications," Mar. 2010.

[12] K. Sikes, T. Gross, Z. Lin, J. Sullivan, T. Cleary, and J. Ward, U.S. Dept. Energy, “Plug-in hybrid electric vehicle market introduction study: Final report,” Washington, DC, Tech. Rep. DE2010-972306, 2010.

[13] M. Ahmed, X. Yang, and S. Ali, "Above the Trust and Security in Cloud Computing: A Notion Towards Innovation," in Embedded and Ubiquitous Computing (EUC), IEEE/IFIP 8th International Conference, pp. 723-730, 2010.

[14] R.hangsman and mark spenson, ―advanced security concepts on data management, technology, vol, 326, pp. 1076-1128, Apr. 2009.

[15] B. B. Gupta, R. C. Joshi, Manoj Misra, “ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack,” International Journal of Network Security (IJNS), vol. 14, no. 1, ISSN 1816-3548, pp. 36-45, 2012.

[16] Y. Xiang, K. Li, and W. Zhou, “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,” in IEEE Trans. Information Forensics and Security, vol. 6, no. 2, pp.426-437, 2011.

[17] Anupama Mishra, B. B. Gupta, R. C. Joshi, “A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques,” in the proceedings of 2011 European Intelligence and Security Informatics Conference (EISIC 2011), DOI: 10.1109/EISIC.2011.15, Athens, Greece, September 12-14, 2011.