IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 4 (Mar. - Apr. 2013), PP 50-56
www.iosrjournals.org

Interactive Detection and Classification of DDoS Attacks Using ESVM

[1]S.Elanthiraiyan, [2]Mr.P.Pandiaraja M.E,
[1]PG Scholar(2nd year) [2](PhD) M.E computer science and engineering Asst professor, Dept of CSE Arunai Engineering College Arunai Engineering CollegeTiruvannamalai-606 603 Tiruvannamalai-606 603

Abstract: *Distributed Denial of Service (DDoS) attack is a continuous critical threat to the internet. Application layer DDoS Attack is derived from the lower layers. Application layer based DDoS attacks use legitimate HTTP requests after establishment of TCP three way hand shaking and overwhelms the victim resources, such as sockets, CPU, memory, disk, database bandwidth. Network layer based DDoS attacks sends the SYN, UDP and ICMP requests to the server and exhausts the bandwidth. An anomaly detection mechanism is proposed in this paper to detect DDoS attacks using Enhanced Support Vector Machine (ESVM). The Application layer DDoS Attack such as HTTP Flooding, DNS Spoofing and Network layer DDoS Attack such as Port Scanning, TCP Flooding, UDP Flooding, ICMP Flooding, Land Flooding. Session Flooding are taken as test samples for ESVM. The Normal user access behavior attributes is taken as training samples for ESVM. The traffic from the testing samples and training samples are Cross Validated and the better classification accuracy is obtained. Application and Network layer DDoS attacks are classified with classification accuracy of 99 % with ESVM.*

Keywords— Anomaly detection, DDoS, Enhanced Support VectorMachine (ESVM), Intrusion detection, String kernels.

I. INTRODUCTION

Computer security mainly comprise of confidentiality, integrity and availability. The major threats in security research are breach of confidentiality, failure of authenticity and unauthorized DoS. DDoS attack has caused severe damage to servers and will cause even greater intimidation to the development of new internet services. Traditionally, DDoS attacks are carried out at the network layer, such as ICMP flooding, SYN flooding, and UDP flooding, which are called Network layer DDoS attacks [4]. In Application layer DDoS attacks zombies attack the victim web servers by HTTP GET requests (e.g., HTTP Flooding) and pulling large image files from the victim server in overwhelming numbers. In another instance, attackers run a massive number of queries through the victim's search engine or database query to bring the server down. On the other hand, a new special phenomenon of network traffic called flash crowd has been noticed by researchers during the past several years. On the web, "flash crowd" refers to the situation when a very large number of users simultaneously access a popular web site, which produces a surge in traffic to the web site and might cause the site to be virtually unreachable. Web user behavior is mainly influenced by the structure of web site and the way users access web pages [2]. Application layer DDoS attacks are considered as anomaly browsing behavior and characteristic of web access behavior is used to construct the normal profile which is used for differentiating attack traffic from normal traffic.

The browsing behavior of a web user is related to the structure of a website, which comprises of a huge number of web documents, hyperlinks, and the way the user accesses the WebPages. A typical webpage contains a number of links to other embedded objects, which are referred to as in-line objects [2]. A website can be characterized by the hyperlinks among the web pages and the number of in-line objects in each page. When users click a hyperlink pointing to a page, the browser will send out a number of requests for the page and its several in-line objects. Time taken to display the content of the webpage is called as 'HTTP ON' period. Time spent by the user to understand the content of the page is called 'HTTP OFF'. User may follow a series of hyperlinks provided by the current browsing web page to continue the access. During normal user access 'HTTP ON' period is less than the 'HTTP OFF' period, but during Application layer DDoS attack 'HTTP OFF' period is less than the 'HTTP ON' period.

II. Related Work

Yi Xie and Shun-Zheng Yu have conducted the experiment on Application layer DDoS attack [4] which utilizes legitimate HTTP requests to overwhelm victim resources. A scheme based on document popularity is introduced in this paper. An access matrix is defined to capture the spatial temporal patterns of a normal flash crowd. Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are applied to abstract the multidimensional access matrix. A novel anomaly detector based on Hidden semi-Markov Model

(HsMM) is proposed and high classification accuracy is achieved and also proposed a mechanism to construct browsing behavior [3] from HTTP request rate, and access matrix using Hidden semi-Markov Model.

Yi Xie and Shun-Zheng Yu have investigated the Application layer DDoS [2] attacks, in this type of attack HTTP requests from legitimately connected network machines to overwhelm web server. Detection mechanism is proposed based on web user browsing behavior to protect the servers from these attacks. Hidden semi-Markov Model is used to describe web browsing behaviors of web users.

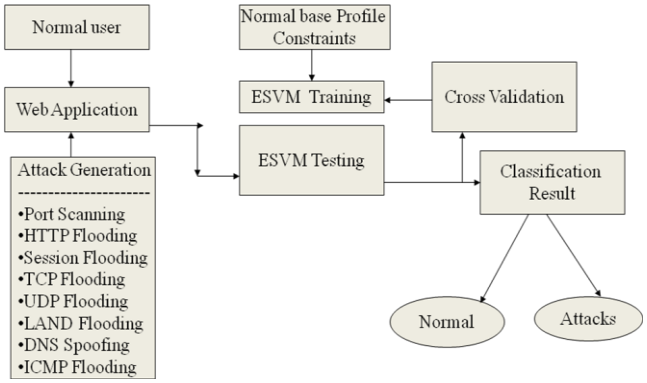

Fig. 1 Classification Of DDoS Attack Architecture diagram

Jie Yu, Zhoujun Li, et. al. have investigated the attack model and characterizes Application layer [1] attacks into three classes: session flooding attacks, request flooding attacks and asymmetric attacks. Mechanism named as DOW (Defense and Offense Wall) is proposed, which defends against layer-7 attacks using combination of detection technology and currency technology.

Yoohwan Kim, et. al. have introduced DDoS [5] defense scheme that supports automated online attack characterizations and accurate attack packet discarding based on statistical processing. The key idea is to prioritize a packet based on a scores are calculated from packet size, Time-tolive (TTL), protocol-type values and source IP prefixes, TCP flag patterns and server port numbers. Once the score of a packet is computed, this scheme performs score based selective packet discarding where the dropping threshold is dynamically adjusted based on the score distribution of recent incoming packets and the current value of system overload and tabulated the percentage of false positive and false negative.

Amey Shevtekar and Nirwan Ansari, proposed a new stealthy[6] DDoS attack model referred to as the"quiet" attack. Mostly attack traffic consists of TCP traffic only and short-lived TCP flows can be intentionally misused. Demonstrated the inability of representative defense schemes such as adaptive queue management and aggregate congestion control to detect the quiet attack and proposed a mechanism to detect short-lived TCP flows using variations in TTL field in the TCP header field.

Thing et.al. have proposed[7] a method to determine entry and exit points or paths of DDoS attack traffic flows into and out of network domains is proposed. Anomalies route are detected by determining which routers have been used for unknown source addresses, to construct the attack paths. Mirkovic et.al. have proposed[8] the D-WARD, a source-end DDoS defense system that achieves autonomous attack detection and surgically accurate response, D-WARD has been extensively evaluated in a controlled testbed environment and in real network operation. Selected tests results are presented in the paper.

Chonka et.al. have [9] used the theory of network selfsimilarity to differentiate DDoS flooding attack traffic from legitimate self-similar traffic in the network and observed that DDoS traffic causes a strange attractor to develop in the pattern of network traffic. From this observation, neural network detector trained by our DDoS prediction algorithm has developed.

Velarde-Alvarado et.al. have used the [10] Method of Remaining Elements (MRE) to detect anomalies based on the characterization of traffic features through a proportional uncertainty measure. MRE has the functionality and performance to detect abnormal behavior and serve as the foundation for next generation network intrusion detection systems.

Shui Yu et.al. [11] have observed that the zombies use controlled function(s) to pump attack packages to the victim, therefore, the attack flows to the victim are always share some properties, e.g. packages distribution behaviors, which are not possessed by legitimate flows in a short time period.

III. PROPOSED INTERACTIVE ANOMALY DETECTION AND CLASSIFICATION OF DDOS ATTACKS SYSTEM ARCHITECTURE

The Application layer DDoS Attack such as HTTP Flooding, DNS Spoofing and Network layer DDoS Attack such as Port Scanning, TCP Flooding, UDP Flooding, ICMP Flooding, Session Flooding are taken as test samples for ESVM. The Normal user access behavior attributes is taken as training samples for ESVM. The traffic from the testing samples and training samples are Cross Validated and the better classification accuracy is obtained. The Application Layer DDoS Attack and Network Layer DDoS Attack are designed in web application. The cross validation of ESVM testing sample and ESVM training sample are design to obtain the classification results.

Uniqueness of the research

In this paper both Network and Application layer DDoS attacks are addressed. ESVM with string kernels are used to classify the attack traffic from normal traffic which shows effective results in classification. Since the count of packets is used as the major parameter of detection, this is best suitable for DDoS which is mainly based on the number of packets.

The phases of attack classification system is listed as

A. Network Layer Attack Generation
B. Application Layer Attack Generation
C. Normal base Profile Constraints
D. Traffic Analysis
E .Classification Results

A. Network Layer Attack Generation

The network layer attack generation module includes the network layer DDoS attacks such as Port Scanning, TCP Flooding, UDP Flooding, ICMP Flooding, Session Flooding. Here,

A Port Scanning: is a software application designed to probe a server or host for open ports. A Port scan helps the attacker find which ports is available i.e. what service might be listing to a port. Essentially, a port scan consists of sending a message to each port, one at a time.

*TCP Flooding***:** Attackers request connections to the server so attackers create half open connection with the server.

*UDP Flooding***:** Attackers sends the UDP packets continuously without receive UDP packets.

*ICMP Flooding***:** Attackers send the ping requests in high rate.

*Session Flooding***:** Attackers request more No.of.Connections to the server. So, Sockets are completely utilized by the attackers. So normal user will face the service unavailability.

*LAND Flooding***:** Attackers spoof the source IP Address as the destination IP Address. So, that the server crashes out.

B.Application Layer Attack Generation

Application layer DDoS attacks are generated to the web application. Attacking scripts are created using traffic generation program. The application layer attack generation module includes the application layer DDoS attacks such as HTTP Flooding, DNS Spoofing. Here,

HTTP Flooding: There will be more number of requests for the inline objects like number of pages.

DNS Spoofing: Spoofing of destination address as a source address.

C Normal Base Profile constraints

The Normal Base Profile Constraints module has the parameters like HTTP Requester rate, Session rate, Number of TCP packets, Number of UDP packets, Number of ICMP packets.

*HTTP Request rate***:** It is the number of HTTP request form client to server within particular time duration.

*Session Rate***:** Number of sessions established from client to server within particular time duration.

*Number of TCP Packets***:** Total no. of TCP packets received by the server for the particular flow.

*Number of UDP Packets***:** Total number of UDP packets received by the server for a particular flow.

*Number of ICMP Packets***:** Total number of ICMP packets received by the server for a particular flow.

*Number of Land Packets***:** Total no of land packets received by the server for a particular flow.

D. Traffic Analysis

The traffic of the normal flows of all attribute like *HTTP Requester Rate, Session Rate, Number of TCP Packets, Number of UDP Packets, Number of ICMP Packets* are taken as ESVM training samples. The attack generation from the web application is taken as ESVM Testing and these two traffics are analyzed.

Traffic to the web application is raw packets. These packets are captured and attributes are derived such as HTTP rate, session rate, page viewing time, number of TCP packets, number of UDP packets, number of ICMP packets, number of land packets, and protocol. After establish the connection attacker requests the web page.

E. Classification Result

` The classification result is obtained from the cross validation of ESVM training samples and ESVM Testing. The result will be obtained as two differentiated classes as normal users and attackers.

Thus the DDoS attacks in application and network layer such as HTTP flooding, DNS spoofing and TCPflooding, UDP flooding, ICMP flooding, LAND flooding, session flooding are classified from the normal users through ESVM.

Input: Network traffic
Output: Classified instances

1. **Begin**
2. Collect traffic from server
3. For each flow
   Get patterns (HTTP request rate, Session rate,
   Page viewing time, Number of TCP packets,
   Number of UDP packets, Number of ICMP
   packets, Number of land packets)
4. Get Nomal Base profile constraints in ESVM
   training samples
5. Get Attack Generation Traffic flows in ESVM testing
   Samples
6. Classify attack flows and normal flows by ESVM.
7. ***End***

Fig. 2 Classification Algorithm using ESVM

Attack traffic is used for testing the ESVM. HTTP flooding, DNS spoofing and TCPflooding, UDP flooding, ICMP flooding, LAND flooding, session flooding are included in ESVM testing.

HTTP request rate, Session rate, Time spent on the link, number of TCP packets, number of UDP packets, number of ICMP packets, number of land packets, are given as input to the ESVM training and classification is done between ESVM testing and ESVM training.

IV. EXPERIMENTAL RESULTS

Application and Network layer detection are experimented in this paper. During normal user access HTTP ON period is less than the HTTP OFF period. During attack HTTP OFF period is less than the HTTP ON period. This condition is used to drive the time spent on link in normal profile ESVM classification result is tabulated in this section. ESVM with string kernels produce the better classification result.

A. ***Performance of Application layer Attack Detection***

` Numbers of user Vs number of requests are used to detect the Application layer HTTP flooding attacks. During normal access user and requests in particular time unit increase gradually. During attack number of user will not increase, request rate will increase drastically. This condition is used to drive the HTTP request rate in normal profile.

HTTP flooding can be detected by comparing the number of users and number of requests during particular time unit. During normal user access number of users and number of requests increase gradually but during attack number of users will not increase and requests only increase because same number of attackers only requests the page repeatedly, as shown in Figure. 3. Numbers of user Vs number of sessions are used to detect the Application layer DDoS attacks such as session attack. During normal access user and session will increase gradually but during attack number of user will not increase, but session rate will increase drastically.

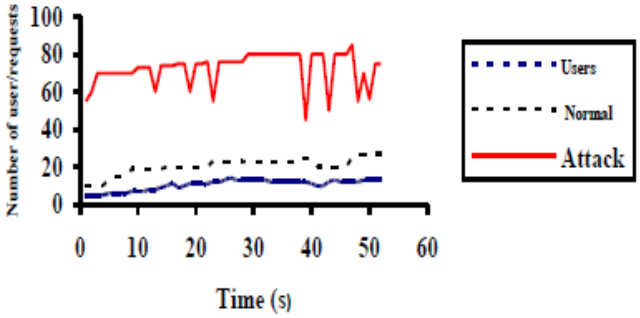

Fig. 3 Time Vs User and Request

This condition is used to drive the session rate in normal profile. During attack noticeable change happen in these three parameters. These three parameters are used to detect the attack. Two files are created for ESVM training and testing. Normal profile data is used to create training file and attack traffic is used to create testing file. Testing file can be varied to test the performance during different time intervals.

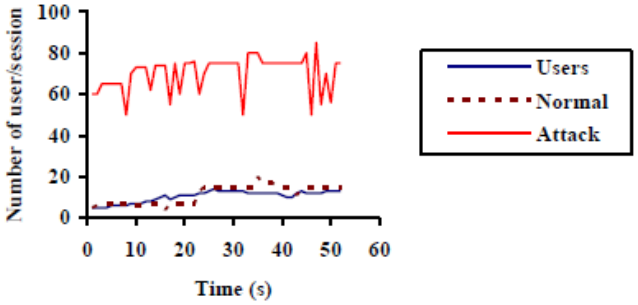

Fig. 4 Time Vs User and Session

Session flooding can be detected by comparing the number of users and number of Session during particular time unit. During normal user access number of users and number of session will increase gradually, but during attack number of users will not increase and session rate only will increase because same number of attackers only create session repeatedly its illustrated Figure 4.

B. ***Performance of Network layer Attack Detection***

Normal client server communication takes place through TCP packets. In TCP flooding attacker sends the number SYN requests, number of TCP packets received during attack is deviated from the number of TCP packets during normal access as shown in Figure 5.

In UDP flooding attacker sends the number of UDP packets without receive any UDP packets as illustrated in Figure 6. Server sends the error message to the server based on the server replay UDP flooding attack will be detected.

In ICMP flooding attacker sends the ping flooding to the server which is deviated from the normal ping request which is illustrated in Figure 7. In land flooding attack attacker spoof the source IP as the destination IP so victim sends the replay packets to itself.

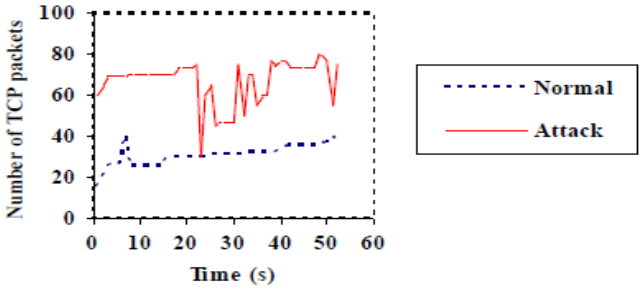

Fig. 5 Time Vs Number of TCP packets

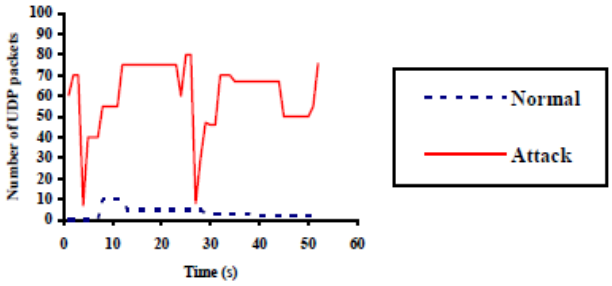

Fig. 6 Time Vs Number of UDP packets

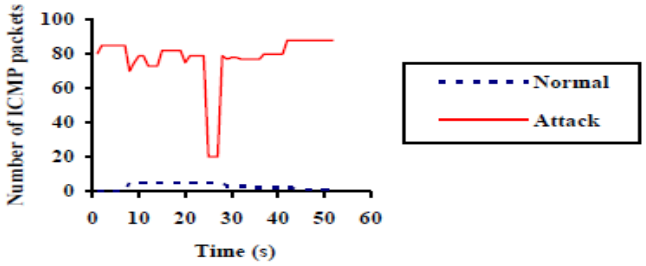

Fig. 7 Time Vs Number of ICMP packets

C. ***Performance of ESVM***

Training Result is shown in Table. 1 nSV and nBSV are number of support vectors and bounded support vectors. Optimal values of obj, rho is fixed for the kernels using trial and error process.

TABLE I
ESVM TRAINING RESULT

S.No	Kernel Name	nSV	nBSV
1	Linear	6	2
2	Polynomial	2	0
3	Radial Basis	6	2
4	String kernel	3	0

Testing results are linear, polynomial, and radial basis functions and string kernels are showed in Table 2 ESVM with string kernels shows the better classification result as compared to other kernel functions.

TABLE II
ESVM TESTING RESULT

S.No	Kernel Name	Classification Accuracy
1	Linear	93.00
2	Polynomial	96.45
3	Radial basis	97.15
4	String kernel	99.32

D. Comparison with existing approaches

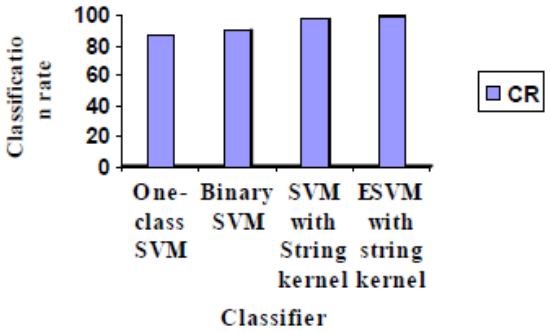

Fig. 8 ESVM Vs existing mechanism

Figure. 8 shows the comparison of ESVM with other existing SVM used in the DDoS detection. ESVM results the better classification result as compared to other SVM.

E. Outcomes of the research

- Application and Network layer DDoS attacks are detected using derived attributes in real time.
- Interactive classification system has proposed to classify attack classes and normal using ESVM with string kernels.

V. Conclusion

Application and Network layer DDoS attacks are successfully generated and detected by proposed Interactive anomaly detection system designed using ESVM . Classification system classifies the incoming flows as attack or normal flow by using ESVM. To prevent the malicious process such as spoofing, flooding, monitoring from the normal traffic flows, the first stage is the classification of attacks traffic from normal traffic. In Future different types of DDoS attacks can be employed for classification like Eves dropping, Sniffing.

References

[1] " Real Time Detection and Classification of DDoS Attacks using Enhanced SVM with String Kernels", A.Ramamoorthi,Subbulakshmi Dr.S.Mercy Shalinie, Department of Computer Science and Engineering, Thiyagarajar College of Engineering, Madurai, TamilNadu, India.

[2] Jie Yu and Zhoujun Li, "A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks" *IEEE Third International Conference on Networking and Services*, pp.54 – 54, 2007.

[3] Yi Xie and Shun-Zheng Yu, "A Novel Model for Detecting Application Layer DDoS Attacks", *IEEE Proc. of the First International Multi- Symposiums on Computer and Computational Science*, pp.56-63, 2008.

[4] Yi Xie, and Shun-Zheng YU, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors", IEEE/*ACM Trans.on networking*, Vol. 17, No.1, pp. 54-65, 2009.

[5] Yi Xie, and Shun-Zheng, "Monitoring the Application layer DDoS Attacks for Popular Websites", *IEEE/ACM Trans. on networking*, Vol. 17, No. 1,pp. 15-25, 2009.

[6] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and Jonatan Chao"Packet Score: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks", IEEE Trans.

[7] Amey Shevtekar and Nirwan Ansari,"Is It Congestion or a DDoS Attack?" , transaction IEEE communications letters.

[8] Thing, V.L.L. Sloman, M. Dulay, N. "Locating network domain entry and exit point/path for DDoS attack traffic" , IEEE Trans. Network and Service Management, Vol. 6, No.3, pp. 163-170, 2009.

[9] Mirkovic, J. Reiher, P. "D-WARD: a source-end defense againstflooding denial-of-service attacks", IEEE Trans. On Dependable and Secure Computing, Vol. 2, No. 3, pp. 216-225, 2005.

[10] Chonka, A.Singh, J.Wanlei Zhou, " Chaos theory based detection against network mimicking DDoS attacks", IEEE Trans. On Communications Letters, Vol. 13, No. 9, pp. 717-721, 2009.

[11] Velarde-Alvarado, P. Vargas-Rosales, C. Torres-Roman, D. Martinez- Herrera, A." Detecting anomalies in network traffic using the method of remaining elements", IEEE Trans. On Communications Letters.

[12] Shui Yu Wanlei Zhou Doss, R., "Information theory based detection against network behavior mimicking DDoS attacks", IEEE Trans.