Integrated Hidden Markov Model and Bayes Packet Classifier for effective Mitigation of Application DDoS attacks

S.Prabha[1] and Dr. R. Anitha[2]

[1]Research Scholar, Research and Development Centre, Bharathiar University – Coimbatore.

[2]Professor & Head, Department of M.C.A., KSR college of Technology, Tiruchengode

Abstract

Resisting distributed denial of service (DDoS) attacks become more challenging with the availability of resources and techniques to attackers. The application-layer-based DDoS attacks utilize legitimate HTTP requests to overwhelm victim resources are more undetectable and are protocol compliant and non-intrusive. Focusing on the detection for application layer DDoS attacks, the existing scheme provide an access matrix which capture the spatial-temporal patterns of a normal flash crowd on non stationary object. The access matrix captures the spatial-temporal patterns of the normal flash crowd and the anomaly detector based on hidden Markov model (HMM) described the dynamics of Access Matrix (AM) to detect the application DDoS attacks. However current application layer attacks have high influence on the stationary object as well. In addition the detection threshold for non stationary object should be reevaluated to improve the performance of false positive rate and detection rate of the DDoS attacks.

The integrated HMM and Bayes packet classifier with Gaussian distribution factor introduced in this paper, improves the resistance scheme to have better detection rate even for method in terms of collateral damage. Rule sets are used to resist an attack which is pre calculated before an attack takes place. Experimental simulations are conducted on ISP network traffic data to demonstrate the effectiveness of the false positive rate with NS-2. Numerical results based on real Web traffic data shows that the effectiveness of minimizing asymmetric attack on the server resources.

Integrated HMM and Bayes Classifier Model (IHBCM) improves the attack resistance rate of legitimate clients against application DDoS attack to 26% compared to that of simple HMM model. In addition IHBCM increases the throughput of the legal users of the ISP network data to nearly 18% referring to simple HMM model.

Keywords: Application DDoS attacks, Gaussian Distribution, Bayes packet classifier, HMM

1. Introduction

Distributed denial of service (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 Net-DDoS attacks in this paper. The intent of these attacks is to consume the network bandwidth and deny service to legitimate users of the victim systems. Since many studies have noticed this type of attack and have proposed different schemes (e.g., network measure or anomaly detection) to protect the network and equipment from bandwidth attacks, it is not as easy as in the past for attackers to launch the DDoS attacks based on network layer.[1]

When the simple Net-DDoS attacks fail, attackers shift their offensive strategies to application-layer attacks and establish a more sophisticated type of DDoS attacks. To circumvent detection, they 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. Such attacks are called as application-layer DDoS (App-DDoS) attacks.

Special phenomenon of network traffic called flash crowd has been noticed by researchers during the past several years [2]. On the Web, flash crowd refers to the situation when a very large number of users simultaneously access a popular Website, which produces a surge in traffic to the website and might cause the site to be virtually unreachable. Because burst traffic and high volume are the common characteristics of App-DDoS attacks and flash crowds, it is not easy for current techniques to distinguish them merely by statistical characteristics of traffic [3].

Therefore, App-DDoS attacks may be stealthier and more dangerous for the popular websites than the general Net-DDoS attacks when they mimic (or hide in) the normal flash crowd. Few existing papers focus on the detection of App-DDoS attacks during the flash crowd event. This work presents a scheme to capture the spatial-temporal patterns of a normal flash crowd event and to implement the App-DDoS attacks detection.[4] Since the traffic characteristics of low layers are not enough to distinguish the App-DDoS attacks from the normal flash crowd event, the objective of this work is to find an effective method to identify whether the surge in traffic is caused by App-DDoS attackers or by normal Web surfers.

Simple App-DDoS attacks (e.g., Flood)[6] can be monitored by improving existing methods designed for Net-DDoS attacks, e.g., can apply the HTTP request rate, HTTP session rate, and duration of user's access for detecting. The second characteristic of App-DDoS attacks is that the attackers aiming at some special popular Websites are increasingly moving away from pure bandwidth flooding to more surreptitious attacks that masquerade as (or hide in) normal flash crowds of the Websites. Since such Websites become more and more for the increasing demands of information broadcast and electronic commerce, network security has to face new challenges. The proposal in this work present an integrated HMM[5] and Bayes Packet Classifier based Gaussian distribution factor to detect and respond to the App-DDoS attacks if they occur during a flash crowd event for both dynamic and stationary objects.

2. Literature work

Literature survey indicates that researchers attempt to detect DDoS attacks from three different layers i.e., IP layer, TCP layer, and application layer. From all of these perspectives, researchers are investigating various approaches to distinguish normal traffic from the attack one. Most DDoS-related research has focused on the IP layer.[7] These mechanisms attempt to detect attacks by analyzing specific features, e.g., arrival rate or header information. For example, [12] used the management information base (MIB) data which include parameters that indicate different packet and routing statistics from routers to achieve the early detection.

In [13] used the cross-correlation analysis to capture the traffic patterns and then to decide where and when a DDoS attack possibly arises. A DDoS attack can be characterized as a simultaneous network attack on a victim (e.g., a web server or a router) from a large number of compromised hosts, which may be distributed widely among different, independent networks. By simply exploiting the tremendous asymmetry existing between network-wide resources and local capacities of a victim, a flooding-based DDoS attack can build up an intended congestion very quickly at an attacked target.

The Internet routing infrastructure, which is stateless and based mainly on destination addresses, appears extremely vulnerable to such large-scale, coordinated attacks. DDoS attacks cannot be detected and stopped easily because forged source addresses and other sophisticated techniques are used to conceal attack sources. DDoS flooding attacks can take a victim network off the Internet even without exploiting particular vulnerabilities in network protocols or weaknesses in system design, implementation, or configuration. While applying security patches may avert attacks against protocol or system vulnerabilities, principal components[10] of congestion-inducing DDoS attacks exploit an inherent weakness in the Internet design, and thus present a serious threat to Internet stability.[9]

In [14], asymmetry of two-way packet rates is used to identify attacks in edge routers. A flash crowd is a surge in traffic to a particular web site that causes the site to be virtually unreachable. The proposal in this paper, present a method for the detection of DDoS attack by classifying the network status of the general DDoS framework. The proposal describes the two fold DDoS architecture, the control stage and the attack stage. It analyzes the procedures of DDoS attacks to select feature variables that are important in recognizing DDoS attacks. The feature of network data traffic may get abnormally changed whenever the attack happens. To overcome this, apply Bayes packet classifier method to classify the status of networks data traffic for each phase of the DDoS attack With this HMM [8] is improvised to eliminate the unwanted features for the DDoS application attack resistance. It provides a mapping element to the ISp data traffic which describes the period of packet transfer in a network. The simulation result has shown that the phases of the attack have been classified well and DDoS attacks could be detected in the early stage, with efficiency. The Gaussian distribution factor is

applied to resists gradually changing anomaly DDoS attack with flexible adjustment of feature variables.

3. Integrated HMM and Bayes Packet Classifier with Gaussian Factor

The distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system by one or more web servers. These systems are compromised by attackers using a variety of methods. Malware can carry DDoS attack mechanisms, one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hard coding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents. These collections of systems compromisers are known as botnets. DDoS tools like stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. The proposal in this work of Gaussian factor for detecting attacks with integrated HMM and Bayes Classifier model is explained below.

The proposal of this work develops an integrated mode to capture the spatial-temporal patterns of a normal flash crowd event and to implement the App-DDoS attacks detection. Since the traffic characteristics of low layers are not enough to distinguish the App-DDoS attacks from the normal flash crowd event, the objective of this paper is to find an effective method to identify whether the surge in traffic is caused by App-DDoS attackers or by normal Web surfers. Web user behavior is mainly influenced by the structure of Website (e.g., the Web documents and hyperlink) and the way users access web pages. The proposed monitoring scheme considers the App-DDoS attack as anomaly browsing behavior. Investigate the characteristic of Web access behavior plots the HTTP request number and the user number per 5s during the burst Web workload. From the maximum correlation coefficient 0.9986, between the series of request numbers and that of the user numbers, identify the normal flash crowd is mainly caused by the sudden increment of user traffic data.

The entropy of the aggregate access behavior against our model does not change much during the flash crowd event, which implies that both the main access behavior profile of normal users and the structure of Website do not have obvious varieties during the flash crowd event and its vicinity area. The users' access behavior profile can be used to detect the abnormal varieties of users' browsing process during the flash crowd. Since the document popularity has been widely used to characterize the user behavior and improve the performance of Web server and Internet cache

3.1 HMM and Access Matrix

3.1.1 Access Matrix

The access matrix model is the policy for user authentication, and has several implementations such as access control lists (ACLs) and capabilities. It is used to describe which users have access to what objects. The access matrix model consists of four major parts a list of objects, a list of subjects, a function T which returns an object's type and the matrix itself, with the objects making the columns and the subjects making the rows. In the cells where a subject and object meet lie the rights the subject has on that object. Access restrictions such as access control lists and capabilities sometimes are not enough. In some cases, information needs to be tightened further, sometimes by an authority higher than the owner of the information. For example, the owner of a top secret document in a government office might deem the information available to many users, but his manager might know the information should be restricted further than that. In this case, the flow of information needs to be controlled secure information cannot low to a less secure user.

3.1.2 Hidden Markov Model

The hidden Markov model (HMM) is a statistical model in which the detection system being modeled is assumed to be a Markov process with unobserved state. The HMM is considered as the simplest dynamic Bayesian network. In a regular Markov model, the state is directly visible to the observer, and therefore the state transition probabilities are the only parameters. In a hidden Markov model, the state is not directly visible, but output dependent on the state is visible. Each state has a probability distribution over the possible output tokens. Therefore the sequence of tokens generated by an HMM gives some information about the sequence of states. The adjective 'hidden' refers to the state sequence through which the model passes, not to the parameters of the model. Even if the model parameters are known exactly, the model is still hidden. Hidden Markov models are especially known for their application in temporal pattern recognition such as application layer DDoS attack mitigation, bio informatic, speech recognition etc.,

3.2 Gaussian Distribution

Uni-Variate-Gaussian distribution of network is utilized to separate data points characterizing network utilization across the traffic of the ISP server. Estimation of network utilization for the gaussian distribution model is presented with feature vector includes time of day (as a fraction of

the total day), the ratios of each of the packet counts to the total number of packets, and overall network utilization. The proposal analyzes the collected data with the Bayes Packet Classifier with underlying Gaussian distribution factor leading to good detection results.

Before the Gaussian scheme is applied to detection, some parameters have to be preset, which includes the time unit of observed data, the length of the observed vector sequence, the number of the remaining principal components, and the detection threshold of entropy for anomaly detection in HMM. discuss each of them as follows. The time unit and the length of the observed vector sequence can be set according to the computation ability and memory of the detection system. In this paper, set the time unit to be 5 s and the length of one observed sequence to be 1 min. Although the small scale of the time unit may bring us high precision, the length of sequence can not be set too short because it may not contain sufficient attack signals for reliable detection.

3.3 Bayes Packet Classifier

Bayes classifier a probabilistic classifier based on applying Bayes' theorem with strong independence assumptions. Independent feature model for the anonym packets. Bayes classifier assumes that the presence (or absence) of a anonymn packet feature of a class is unrelated to the presence (or absence) of any other packet feature. Depending on the precise nature of the probability model, Bayes optimal classifiers can be trained very efficiently in a supervised learning setting. In our case, parameter estimation for Bayes models uses the method of maximum likelihood

Arrange the attack sources to simultaneously launch constant rate App-DDoS attack and to generate requests at full rate. This help to easily identify attack intensity. As shown in, use to denote the parameters of the constant rate attack. The notation is listed. Three parameters are set randomly by each attack node before it launches the attacks. The entropy varying with the time, are measured as two events where one event represents the normal flash crowd's entropy and other event represents the entropy of flash crowd mixed with constant rate App-DDoS attacks. An abrupt change in traffic volume is the important signal to initiate anomaly detection. The attacker uses the gradually increasing rate. The state change in the victim network could be so gradual that services degrade slowly over a long period, delaying detection of the attack.

The attackers inject vicious requests into the flash crowd traffic, the original popularity distribution of documents is changed, which causes the entropy series lower than the normal level. Therefore detect the potential App-DDoS attacks by the entropy of document popularity fitting to the proposed model. Bayes classifer based Gaussian Distribution, found the normal user's access behavior and the Website structure exhibit hours-long stability regardless of whether or not there are flash crowd events occurring during the period. The popularity of documents is mainly affected by the daily life of the users or information update of the Web pages. Therefore, the model parameters of document popularity change in the period of ten minutes or hours. Model parameters are be updated by the bayes packet classifier implementation in a

period of few minutes. The way of implementing off-line or asynchronous attack will not affect the online detection.

TABLE 1: Definition of Attack Parameter

Notation	Description
H	Intensity (request rate) of the attack
t_s	Presetting start time of attack
t_e	Presetting terminative time of attack
Δt	Difference between the real start time of attack and t_s
L	Duration of the attack
l_1	Duration of the gradually increasing rate
l_2	Duration of the gradually descending rate
T	Attack period of stochastic pulsing attacks

For these considerations, suggest the time unit is selected in between [5 s, 20 s] and the length of sequence is selected in between [1 min, 5 min]. The number of remaining PCs can be decided by the cumulative variance. select the largest PCs whose cumulative variance is over 80% in our experiments, which actually resulted in ten PCs in the experiments. The PCs can be selected by a higher cumulative variance, but this may require more computational capacity and memory amount. In contrast to most current work that decides the detection threshold by subjectivism or empiricism, use Gaussian distribution to provide a universal and reasonable method for the detection threshold. The Central Limit Theorem (CLT) has us that given a distribution with a mean and variance, the sampling distribution approaches a Gaussian distribution. Then describe the entropy distribution of training data by Gaussian distribution. From the rational of Gaussian distribution, know error level could give us a confidence interval of 99.7% which is good enough even in high precision detection scenarios. Table I lists attack parameters for DDoS application services. The detection threshold setting and their corresponding FPR and DR of our experiments (the mean and variance) are evaluated.

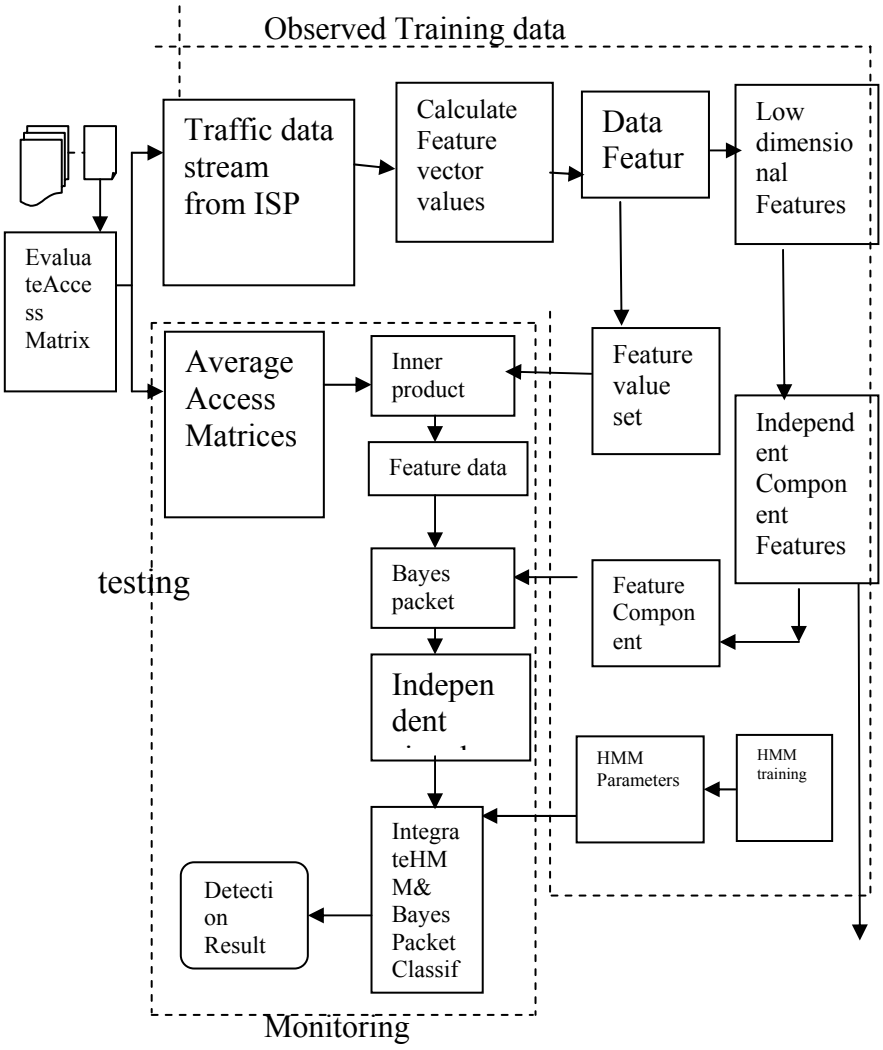

Figure1: Integrated HMM based Bayes classifier for resisting Application DDoS Attack

4. Experimentation of Gaussian distribution factor for resisting application DDoS attacks

The experimental evaluation was carried to implement the proposed algorithm in the NS2 simulator. The network topology is generated by NS2. The simulation includes 1000 client nodes each of which replays one user's trace collected from synthetic data sources. The ratio of randomly selected attack nodes to whole nodes is 10%. Furthermore, assume the attackers can intercept some of the request segment of normal surfers and replay this segment or hot pages to launch the App-DDoS attacks to the victim Web server.

Thus, when the attack begins, each potential attack node replays a snippet of another historical flash crowd trace. The interval between two consecutive attack requests is decided by three patterns including constant rate attacks, increasing rate attacks and random pulsing attacks. use the size of requested document to estimate the victim node's processing time (delay) of each request, i.e., if the requested document is larger, the corresponding processing time will be longer. By this way, simulate the victim's resource (e.g., CPU) cost by client's requests. The simulation topology is generated with the following parameters

a. Three level hierarchy: transit domain, stub domain and nodes
b. 2 transit domains; each transit domain has (on average) five nodes, each transit mode connects (on average) twenty nodes
c. each sub domain has (on average) twenty nodes
d. 10 Mps link for domain, 5 Mbp for stub domain, 2 Mps for nodes
e. Attack coverage is 10% of the nodes except the 10 transit nodes, ie., 100 nodes are potential attack nodes.

Among the variables and are preset by each attack node randomly before it is going to fire the next pulsing attack, which makes the different attack nodes have different attack parameters and the same attack node have different attack parameters in different attack periods. Thus, the attacks exhibit a fluctuating rate oscillating between different and zero, appearing as a stochastic ON/OFF process. Such stochastic pulses are very difficult to be detected by the existing methods that are based on traffic volume analysis, because the average rate of the attacks is not remarkably higher than that of a normal user. The fact that the entropy series is stable shows that the document popularity is stable. Although the attackers can inject vicious requests into the flash crowd traffic, the original popularity distribution of documents is changed, which causes the entropy series lower than the normal level. Therefore, the proposed model detects the potential App-DDoS attacks by the entropy of document popularity fitting to the model.

5. Performance Evaluation of DDoS Attack Resistance

The integrated HMM and Bayes Packet Classifier performance is evaluated, based on the entropy outputted to detect the anomaly caused by the App-DDoS attack on both stationary and dynamic data traffic. There exist significant differences in entropy distributions between two

groups, the normal Web traffic's entropies are larger than 6, but most entropies of the traffic containing attacks are less than 8. The statistical results of the entropy of normal training data and emulated App-DDoS attacks are identified. Because the number of the remaining principal components will affect the precision of detection, use the contribution ratio to decide the first principal components (PCs). Then the evaluation compared the performance of the proposed scheme with the moving average in implementing anomaly detection.

The length of moving average is 40 samples, step of moving average is 8 samples, the cosine distance between the observed vector and the average vector of training data is used as the detection criterion. The proposed method is remarkably better than the moving average in the detection rate given the false positive rate. The variance versus number of users is evaluated to find the variance is mainly contributed by the first ten users whose cumulative ratio is about 70%. This means can keep the first ten users at the effect of losing 20% information.

TABLE 2: Gaussian Distribution Detection Threshold

Detection level	Detection Threshold	FPR	DR
$\eta \pm \sigma$	[-3.44,-23.55]	0.18	0.95
$\eta \pm 1.35\ \sigma$	[-3.66,-3.52]	0.07	0.92
$\eta \pm 1.65\ \sigma$	[-3.47,-3.42]	0.06	0.91
$\eta \pm 2\ \sigma$	[-4.43,-3.16]	0.02	0.90
$\eta \pm 2.29\ \sigma$	[-4.25,-2.61]	0.01	0.91

Mean --- η and variance --- σ,

In contrast to existing attack detection methods, the stationary properties of Gaussian distribution factor with Bayes packet classifier can best describe the self-similarity or long range dependence of network traffic that has been proved by vast observations (Table 2). As shown in table 2, the detection level could be reasonably selected to be, and this choice ensures us with FPR smaller than 1.5% and DR larger than 93%. This shows that the detection threshold determined by the CLT can achieve pretty high accuracy in detection. Based on our experiment, found the normal user's access behavior and the Website structure exhibit hours-long stability regardless of whether or not there are flash crowd events occurring during the period, i.e., the popularity of traffic data is mainly affected by the daily life of the users or information update of the Web pages. Therefore, the model parameters of document popularity change in the period of ten minutes or hours. The model parameters can be updated by the IHBCM implementation in a period of ten minutes of simulation, have higher attack resistance rate compared to the existing simple HMM for dynamic traffic as shown in figure 2. Figure 2 depicts that as dynamic traffic increases the detection rate is also increased for both the methods. However the detection rate for the IHBCM model has nearly 26% of improved detection rate compared to simple HMM.

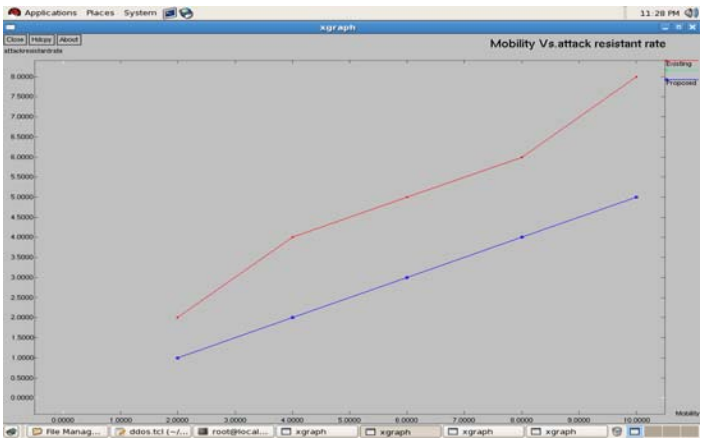

Figure 2: Performance of IHBCM of dynamic traffic data in terms of attack resistance rate.

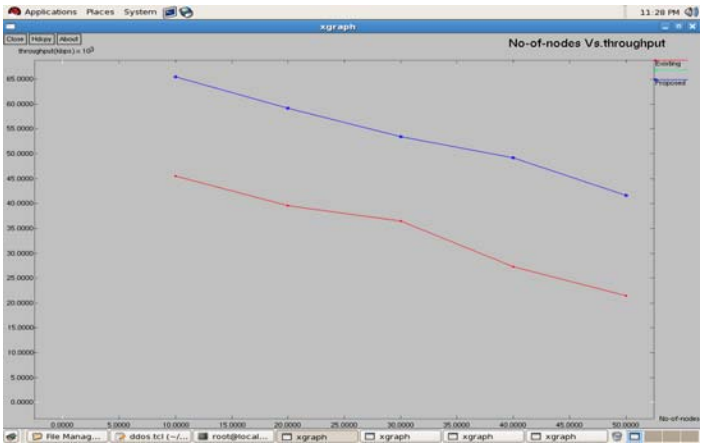

Figure 3: Throughput performance of IHBCM in stationary traffic data of ISP Server

The small scale of the time unit may bring us high precision, the length of sequence can not be set too short because it may not contain sufficient attack signals for reliable detection. For these considerations, suggest the time unit is selected in between [5 s, 20 s] and the length of sequence is selected in between [1 min, 5 min]. The number of remaining users data is decided by the cumulative variance. Select the largest user data whose cumulative variance is over 80% in our experiments, which actually resulted for ten users data. The user traffic data is selected by a higher cumulative variance, but this may require more computational capacity and memory amount. In contrast to most current work that decides the detection threshold by subjectivism or empiricism, use Gaussian distribution to provide a universal and reasonable method for the detection threshold. With this, Figure 3 shows that throughput of the IHBCM model obtained from the simulation results, is better than the simple HMM model (improved by 18%) for stationary traffic data.

As the number of node users increased the throughput gets decreased due to the load-balance effect of the ISP server.

With Central Limit Theorem (CLT), any given a distribution with a mean and variance, the sampling distribution approaches Gaussian distribution to better detection rate on anomaly identification of the sample space data set (user traffic data). Thus, entropy distribution of training data by Gaussian distribution in our IHBCM model shows that know error level. It gives a confidence interval of 99.7% of traffic data monitoring the ISP serve, which is highly appreciable in high precision application DDoS attack detection scenarios.

5. Conclusion

Resisting measure for application DDoS attacks, requires monitoring dynamic and static objects of the network activities to obtain timely and signification information. The proposed IHBCM model with Gaussian distribution factor introduced in the detection architecture monitor Web traffic in order to reveal dynamic shifts in normal burst traffic.

It indicates the onset of App-DDoS attacks during the flash crowd event. Bayesian factor reveals early attacks merely depending on the document popularity obtained from the server log.

The simulation experiment is conducted with different App-DDoS attack modes (i.e., constant rate attacks, increasing rate attacks and stochastic pulsing attack) during a flash crowd event collected from a network data traffic trace from an ISP. Our simulation results show that IHBCM model capture shift of Web traffic caused by attacks under flash crowd. The entropy of the observed data fitting to the Bayesian distribution factor is used as the measure of abnormality. In our experiments, when the detection threshold of entropy is set 4.82, the DR is 93% and the FPR is 0.78%. It also demonstrates the proposed IHBCM is expected to be practical in monitoring App-DDoS attacks and in triggering more dedicated detection on victim network.

References

[1] Yi Xie and Shun-Zheng Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites" IEEE/ACM Transactions on networking, vol. 17, no. 1, February 2009

[2] S. Kandula, D. Katabi, M. Jacob, and A. W. Berger, "Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds,"MIT, Tech. Rep. TR-969, 2004.

[3] I. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. E. Long, "Modeling, Analysis and Simulation of Flash Crowds on the Internet,"Storage Systems Research Center Jack Baskin School of Engineering University of California, Santa Cruz Santa Cruz, CA, ech. Rep. UCSC-CRL-03-15, Feb. 28, 2004 http://ssrc.cse.ucsc.edu/, 95064

[4] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in Proc. 11th IEEE Int. World Wide Web Conf., May 2002,pp. 252–262.

[5] Y. Xie and S. Yu, "A detection approach of user behaviors based on HsMM," in Proc. 19th Int. Teletraffic Congress (ITC19), Beijing, China, Aug. 29–Sep. 2 2005, pp. 451–460

[6] Y. Xie and S. Yu, "A novel model for detecting application layer DDoS attacks," in Proc. 1st IEEE Int. Multi-Symp. Comput. Computat. Sci. (IMSCCS|06), Hangzhou, China, Jun. 20–24, 2006, vol. 2, pp. 56–63.

[7] T. Peng and K. R. M. C. Leckie, "Protection from distributed denial of service attacks using history-based IP filtering," in Proc. IEEE Int. Conf. Commun., May 2003, vol. 1, pp. 482–486

[8] S.-Z. Yu and H. Kobayashi, "An efficient forward-backward algorithm for an explicit duration hidden Markov model," IEEE Signal Process. Lett., vol. 10, no. 1, pp. 11–14, Jan. 2003.

[9] L. I. Smith, A Tutorial on Principal Components Analysis [EB/OL], 2003 [Online]. Available: http://www.snl.salk.edu/~shlens/pub/ notes/ pca.pdf

[10] A. Hyvärinen, "Survey on independent component analysis," Neural Comput. Surveys, vol. 2, pp. 94–128, 1999

[11] A. Hyvärinen, "Fast and robust fixed-point algorithms for independent component analysis," IEEE Trans. Neural Netw., vol. 10, no. 3, pp. 626–634, Jun. 1999

[12] J. B. D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, and R. K. Mehra, "Proactive detection of distributed denial of service attacks using MIB traffic variables a feasibility study," in Proc. IEEE/IFIP Int. Symp. Integr. Netw. Manag., May 2001, pp. 609–622.

[13] J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, pp. 324–335, Oct.-Dec. 2005.

[14] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in Proc. Int. Conf. Network Protocols, 2002, pp. 312–321.