A PCA BASED FRAMEWORK FOR DETECTION OF APPLICATION LAYER DDoS ATTACKS

[1] R.Bharathi., [2]Prof. Dr. R. Sukanesh,

[1]AP/ECE Department, University College of Engg., Nagercoil
INDIA

[2] Professor/ECE Department, Thiagarajar College of Engineering, Madurai.
INDIA
E-mail {bharathi_akce@yahoo.co.in , sukanesh@tce.edu }

Abstract- Hackers uses Distributed Denial of Service (DDoS) and leaves hundreds and thousands of bots to overwhelm the victim in terms of bandwidth and reduce the services that are rendering to the users. To initiate an attack against victim, hackers use the internet as their venue. To address this threat various methods were proposed, but all the earlier method identifies the DDoS attack that exists in IP and TCP layers. Attackers, on the other hand, found the vulnerabilities in the application-layer (higher layer) to attack the victim and using DDoS known as (App-DDoS) and makes complexity in finding and handling the attack. In this paper, in order to detect the attack in earlier stage that is targeted for the application layer, we proposed a framework. This framework uses the profiling of user's browsing behavior and network traffic by sequence order independent and Principal Component Analysis (PCA) respectively. These profiles are clustered, and a threshold is used to verify and determine whether a HTTP request from a user is normal or abnormal. If the user request to the victim is normal, then it allows the access otherwise denies the request in the early stage itself. Finally, the proposed method is verified experimentally and confirmed with various types of App-DDoS attacks.

Keywords- *App-DDoS, anomaly detection, user browsing behavior, network traffic, PCA, sequence order independent, clustering.*

1. Introduction

Organizations that depend on the internet for their business, like financial services, online gaming, e-commerce, etc, requires continuous and fast response to their customer request. Internet and other products that depend on the internet are always prone to failure. This failure may be accidental or intentional. One such intentional attack is Distributed Denial of Service (DoS) with the motivation of attacking the target's (victim) computer or any other resources that use internet. Attackers threat companies that use internet for transactions and other client processing through Denial of Service (DOS) by making the network of the victim unavailable to provide services to legitimate users. Nowadays attackers make use of multiple malicious computers to attack the victim server. This way of compromising many malicious computers

and/or packet stream for attacking a target is named as DDoS. It can be categorized into two types [14]: (1) Bandwidth flooding (2) Resource flooding. In case 1, hackers flood the network by massive request thereby creates unwanted traffic and prevents the legitimate user request to reach the network. In case 2, victim resources are engaged by attackers causing the services of victim not available to legitimate users. By either way DDoS degrade or disturb the services/resources that are available to the legitimate user.

DDoS attacks are programmed by hackers and launched from a machine known as Botnet through many controlled computers connected in a network. Small scripting program with specific task [18] is known as "bots", which is automated. Bots are correlated with remote access Trojan Horses and malicious computers (Zombies) for fewer positive purposes like virus and worm propagation, delivery of SPAM emails, spyware installation etc, DDoS attack etc. Figure 1 portrays the DDoS attack.

Since 2001, DDoS attack is growing rapidly till date. Because of the seriousness of DDoS attack in various business fields, many defense mechanisms were developed using statistical methods to defend against this attack. Earlier methods proposed to using statistical method make use of the attributes of the header in a packet such as time-to-live, IP address, etc., are measured and from the analysis of the packet, which are deemed to attack are dropped. This dropping of packets depends on some the characteristics of that are assumed inherently to identify the normal packets from the affected packet. These approaches highly depend on the traffic characteristics. All the statistical based approaches for DDoS attack work well in TCP/IP layers whereas they are not adaptable and also not applicable for some typical as well as special DDoS attacks that are working on the application layer (higher layer).

Detecting App-DDoS has the following challenges:

(1) App-DDoS uses higher layer protocols such as HTTP to pass through the detection system, which are designed for lower layer.

(2) Along with flooding, App-DDoS also consumes resources of the targeted victim server and either trace the average request rate of the legitimate user and uses the same rate for attacking the server or employs large-scale botnet to generate low rate attack flows. This cause the detection system to detect the DDoS attack more complex.

To overcome these issues, this article proposed a new framework. The general flow of the proposed framework is expressed in figure 2.

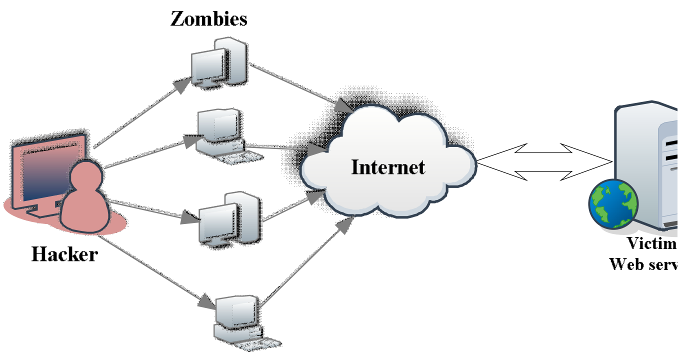

Figure 1 A typical DDoS attack

We detect the DDoS attack through the anonymous behavior of the user. We collect the user and network details and create a log file containing the attributes of all the users such as data, time, website details, hyperlink details, IP address, etc. Using the log file we create a matrix named behavior matrix using sequence order independent. To derive the browsing patterns of various users we use Principal Component Analysis (PCA), which is used to remove the unwanted information and reduces the dimension that are needed to explain a given data. The browsing patterns, which are retrieved using the PCA, are clustered using k-means algorithm. Using k-means algorithm we can frame any number of cluster as we required. The important properties of k-means clustering algorithm are (1) it will not overlap (2) all the members of a cluster are very closer to that cluster than to other clusters. For these properties, we have chosen k-means algorithm. A data matrix is constructed from which a threshold value is set. The threshold value act as the decided factor for the given request whether to accept or to deny.

Rest of this article is structured as follows. In section II describes the works that are related to our research. In section III, we describe our proposed framework in detail. The frame is validated in Section IV. Finally, in section V, we conclude our work with fine points for future enhancement.

2. Related works

A large amount research was carried in order to detect DDoS attacks. This section provides a brief discussion of detecting mechanism used earlier by different authors.

DDoS attacks were the major threat to large scale network in order to detect the threat present in the network authors of [1] uses the technique by computing the entropy and frequency sorted distributions of packet attributes that were selected. The experimental study showed that the affected packets showed the anomaly characteristics in the attributes that were selected for the analysis of a packet. For experimental analysis live traffic traces are taken from many networks setting sources were used. Similarly [2] discussed the impact of multivariate correlation for detecting the DDoS also proposed a covariance analysis model to detect the DDoS attack, which are simulated through the SYN flooding. Analysis of this model expressed that the covariance model significantly detects the attacked and normal traffic.

Statistical method along with filtering technique was used in [3] for detection of DDoS that were effectively applicable in the areas such as ISP, enterprise, etc. For detection it used traffic matrix, which represents the traffic state. The process of detection DDoS in [3] consisted of two step. In step one, a filter named Kalman filter was used to filter normal traffic through the comparison of traffic matrix states of both the future prediction and actual state. The filtered states were examined for anomalies. Authors also explained how the DDoS detection (anomaly) can be viewed as a trouble in statistical testing. A collaborative defense mechanism was proposed in [9] using statistical method to identify attacks and false alarm rate. This effectively uses duplicate detection window scheme for identifying various dynamic attacks at early stage.

Authors of [12] also used the traffic matrix and weighted moving average to detect the spoofed DDoS attack. Also, explained the concept of dispersible characteristics of DDoS attack like, DDoS traffic rate and duration, intensity etc. The proposed work in [12] had not taken the fine points of traffic matrix such as a threshold value of variance, time based window size, and the size of the traffic. To deal with the above issues, [16] optimized the parameters of the traffic matrix through genetic algorithm, which helps to increase the detection rate. Furthermore time based window was replaced by packet based window. Experimental study shows that the detection of DDoS attack was increased in a considerable amount. A well known classification method, artificial neural net was used in [4] to analyze and classify the request as normal or DDoS affected. The classification and analysis steps were preceded by a statistical pre-processing in order to extract the traffic features statistically. New direction for detection of DDoS attack was attended in [5] and [11] to detect the DDoS in a network by machine learning algorithm. Genetic algorithm and support vector machine (SVM) were incorporated in [5] for anomaly detection. Features were selected using genetic algorithm and to classify the request packet depending on normal and affected packets authors used SVM technique. Apart from the detection of DDoS, some existing methods wrongly classified the normal request as the affected packet. In order to cope with this [11] proposed a new machine learning method named wavelet support vector machine (WSVM), which is a combination of SVM and wavelet kernel function theory to detect DDoS and for the validation of the detection regarding false positive.

A framework for detection of attack was proposed in [6] named DefCOM, which takes the strength of earlier method and organized them into a collaborative overlay. Profile-based algorithm [7] was proposed to find the short and long lived, also low intensity anomalies. This algorithm put the technique of random projection and multi-resolution non-Gaussian distribution modeling together for reducing the dimension of data and to extract anomalies at various levels of aggregation. The random projection technique was also used in recognition of IP address of source and destination that are associated with the anomalies detection. Cluster based analysis was introduced at [10] for the detection of DDoS attack. This system carefully noticed the procedures of DDoS attack and set the features for capturing the anonymous behavior, which are then clustered for effective detection of DDoS. A multi stage detection mechanism was proposed in [17], it also construct a model for determining the factors that had severe impact on the deviation on traffic features. In [8], hidden Markov models and cooperative reinforcement learning methods were introduced for implementing distributed multiple detectors, which helped to increase the accuracy without any modifications in the communication information among detectors.

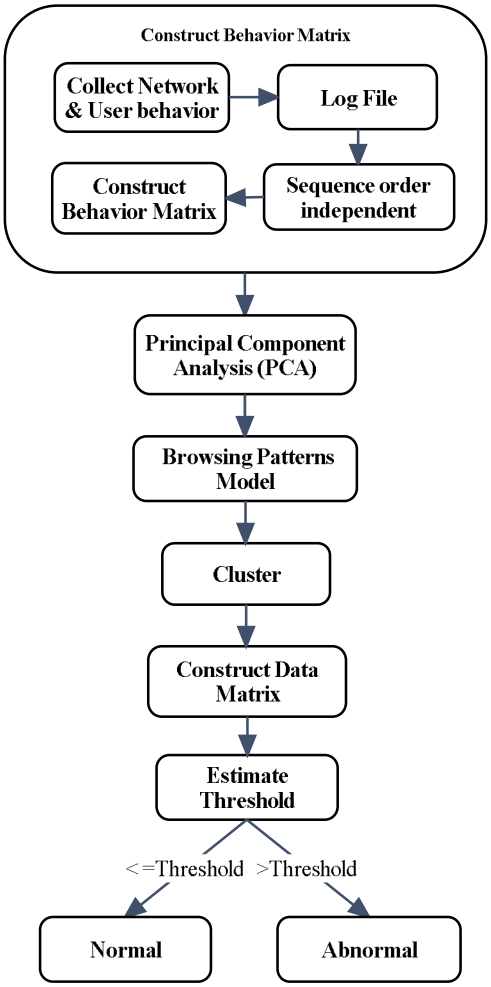
Construct Behavior Matrix
Collect Network & User behavior
Log File
Sequence order independent
Construct Behavior Matrix
Principal Component Analysis (PCA)
Browsing Patterns Model
Cluster
Construct Data Matrix
Estimate Threshold
<=Threshold
>Threshold
Normal
Abnormal

Figure 2 Overall Flow of Proposed Framework

A survey and study was carried by the authors of [14] and [18], which explains the application level DDoS and their impact on the network respectively. Like traffic matrix, access matrix can also be utilized for detecting the DDoS attack. Access matrix [13] along with document popularity is used to find imprison of patterns of normal crowd. To become aware of attacks, a detector was constructed using semi-Markov model, which describes the dynamic Access matrix. Entropy of document popularity was used in the revealing the potential DDoS attacks in application-layer. For the detection of DDoS efficiently in the application-layer [15] designed HTTP and FTP based architectures. The architecture used the extended form of hidden semi-Markov model for collecting the behavior of web surfers. M-algorithm based forward algorithm was proposed to reduce the computational overhead.

3. Proposed Methodology

In this section, we proposed a defensive framework used for detecting the App-DDoS attack. Web browsing behaviors are taken as an alternative of web page request sequence. Sequence-order-independent is used for representation of web browsing behaviors. To model the web browsing behavior, we used PCA. The behavior pattern derived is clustered using k-means algorithm. Browsing behaviors that are clustered is analyzed by a threshold values to differentiate the normal from the anomaly detection.

3.1 Construct Behavior as Attribute vector Matrix

User details such as user ID, web site address, time and date, hyperlink details are retrieved for all the users. These details are framed into a matrix through representing the each request in a vector form. Consider, T_{WP} web pages of a web server 'S' are viewed by T_{User}. Here, T_{WP} and T_{User} denotes the total number of web pages and total users of the server.

A user *x* who browsed the server S may surf any number of web pages. His/her request sequence can be expressed as $RS_{wp,x}$ represents the total number of times the user *x* surfed the web page *wp* of the server S. From this value we can derive total number of request for a user to the server S. This is obtained through the equation 1.

$$T_{Req_x} = \sum_{wp=1}^{T_{WP}} RS_{wp,x} \qquad (1)$$

In the above equation, T_{Req_x} denotes the total number of request given by the user *x* to the web server S. The average number of the request of a user *x* can be determined through dividing the total request of user *x* by total number of users accessed the server over time. This average value can be mathematically represented as in equation 2.

$$\overline{T_{Req}} = \sum_{x=1}^{T_{User}} \frac{T_{Req_x}}{T_{User}} \qquad (2)$$

With the above basic values we can frame sequence-order-independent attributes, which are used to capture the DDoS attacks on the application layer. Following attributes that are defined can be used for clear representation of lively user *x*. The attribute γ_x, is presented to express the ratio between the total request of user *x* and their average value. Mathematically the ratio attribute can be denoted as in equation 3.

$$\gamma_x = \frac{T_{Req_x}}{\overline{T_{Req}}} \qquad (3)$$

In addition to ratio attribute we introduced another attribute whose arithmetical representation is as given in the equation 4.

$$I_{wp,x} = \frac{RS_{wp,x}}{T_{Req_x}} \qquad (4)$$

$I_{wp,x}$, reveals the fraction of page wp among pages requested by user x. This attribute represents how much the user x is fascinated in the page wp of S.

In order to detect the incoming request from a user as a normal or showing any resemblance of DDoS attack two more subsidiary attributes are introduced along with the above two basic attributes. Two attributes are expressed to mention the browsing patterns of a user x on S. First of the subsidiary attribute is defined as the fraction of all pages in the server requested by user x. This value can be symbolized as shown in equation 5.

$$\alpha_x = \sum_{wp=1}^{T_{WP}} \frac{breath_{wp,x}}{T_{WP}} \qquad (5)$$

Here, the $breath_{wp,x}$ is the value equals one when the $RS_{wp,x}$ is > □ otherwise zero. □ is the value that is set depending on the total number of pages and users in the network. This value is not constant it various with respect to the server it is being implemented. Second subsidiary attribute represents the greatest intensity of attraction for a particular web page of a user x, which can be depicted in equation 6.

$$F_{wp_x} = \max \_arg_x\{RS_{wp,x}\} \qquad (6)$$

It denotes that most repeatedly requested web page wp of S by user x.

Intensity of a user's interest for a page can be personified as in equation 7.

$$\partial_x = \frac{RS_{wp,x}}{T_{Req_x}} \qquad (7)$$

This delineate the ratio of the total number of request for the page wp of greatest interest by the user x and the total number of pages request hit S.

From the two basic attribute and two subsidiary attribute we can frame the vectors as $v_x = [I_x, \alpha_x, \gamma_x, F_{wp_x}]^T$ where $I_x = [I_{1,x}, I_{2,x} \ldots\ldots I_{T_{WP},x}]^T$. From these vectors we can frame the behavior matrix as $V = [v_1 \ldots\ldots.. v_{T_{User}}]$.

3.2 Model for Browsing behavior

Transforming number of correlated values into uncorrelated values is said to be the principal component, a mathematical procedure. Here, in this section we use PCA for converting the given raw data into new coordinates through eliminating the unwanted and comparably less important components. As a result it reduces the number of dimensions required to elucidate the given data. The reduced attribute set can be efficiently expressed in a least-squares sense. Therefore, browsing details can be framed as a model using PCA in an efficient way. The browsing data can be denotes as below.

$\beta_0 = \frac{\left(\sum_{x=1}^{T_{User}} v_x\right)}{T_{User}}$ and $CM = \frac{YY^T}{T_{User}}$ where β_0 is the mean vector and CM denotes the covariance matrix, $Y = [Y_x \ldots\ldots\ldots Y_{T_{User}}]$, $Y_x = v_x - \beta_0$ and $X = 1, \ldots\ldots, T_{User}$. We then compute the eigen vector and values through singular value decomposition to CM.

For example if $Z_j$is the most significant principal eigenvector of CM, then the significant principal components can be expressed as $\tilde{Q} = [Q_1 \ldots\ldots. Q_p]$, here p delineates the number of significant principal components. Therefore, the remaining eigenvectors such as $\left[Q_{p+1} \ldots\ldots. Q_{T_{wp}+3}\right]$, are considered the less significant one. Then, these can be removed and without significant loss. Using PCA we can represent the attribute of web user x as below:

$b_i = \widetilde{Q_{x_i}}^T$, i=1, ……..$T_{User}$. This denotes the effectiveness of the PCA contribution in representing the given attributes.

3.3 Cluster Formation

Given refined data are partitioned into different clusters using the k-means clustering algorithms. This is a well-known algorithm, which are well placed in unsupervised clustering. We reduce the dimension of the attributes on the b_i values of the PCA. These values are used due to the reason that if v_i is used, then we contain huge amount of spare data. The spare data is presented because a particular attribute frequently contains zero, which represents the particular web pages of S is not viewed by the user for a long time. If a cluster contains the sparse data, then it is hard to cluster those data into a cluster using k-clustering methods.

After removing the less significant attributes, we obtain an effective set of attribute, these values are taken and the "Time" attribute is used to cluster the user behavior. That is the users who view in a particular time interval are clustered into one group. Once the k-clusters are framed, then the original attribute vector v_x is reconstructed. Depending on the requirement we can frame k number of clusters. The clusters framed in this set are used for the detection of anomaly.

4. Anomaly Detection Policy

Detection policy is carried out by using the behavior matrix and the cluster we framed. The detector lies between the internet and the web server (victim). The detector accepts the request and checks the HTTP request and analyzes the request. If the detector finds that it is affected by the DDoS attack, then the detector drops the packet. Otherwise, it accepts the request and forwards it to the server for further processing. An example, of the detector is as shown in the figure 3. As web browsing behavior is dynamic and short-term stable it is necessary to change the detecting policy as a dynamic one. The detection policy that we applied also exists only for short period. The policy for detection is changed depending on time and requirement.

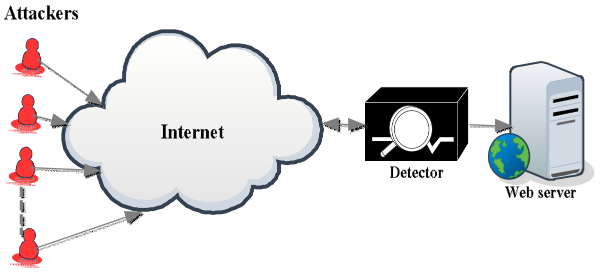

Fig. 3 Detector based on behavior

To detect the anomaly behavior, we used the clusters that are framed earlier and compute a threshold value for those clusters. For a single user, the PCA b_i at the time $\sigma_t$is multiplied with the total number of users in the cluster T_{CUser}. This product value of a user is divided by the constant value 2. This process is carried out for all the users in the clusters. The Summation of all the values obtained for each user in a cluster as above is computed. The summation value that we obtained is the threshold for a cluster. Similarly, for all the clusters the values are computed. The division is carried out to obtain optimal value for threshold. The threshold is computed from the equation 8.

$$Threshold = \sum_{x\in T_{CUser}} \frac{\sigma_t(b_i,1)*T_{CUser}}{2} \qquad (8)$$

User's b_i value is compared with the threshold that we obtained from equation 8. If b_i of a user is lesser or equal to the threshold, then it is threshold, then we conclude that the user is normal user. Otherwise, the user is an anomaly and his/her requests are dropped by the detector.

5. Experimental Results

To validate our proposed frame work for detecting the App-DDoS attack, we have taken web-log data sets from real website such as (1) Entertainment website, (2) Educational website. In entertainment web site, users surf for the movie, game and song links and their hyperlinks. Students and research person are the maximum users of the educational website, where they surf the web sites that are related to specific domain oriented. From these data set of web logs we extracted the IP address of the host, requested web site and time, hyperlink chosen. The characteristics of the data set chosen are as show in the table 1.

Table 1 Dataset and their Characteristics

Type of Site	Sequence	Characteristics
Entertainment	70490	A group of people search for specific data
Educational	20345	Domain specific websites are requested mostly

Repeated experiments are carried out in order to get the reliable and accurate results.

In our experiment we considered the attacks that mimic the normal behavior. The random page attacks are not considered in our experiment since they deviate from the normal behavior therefore, it can be easily detected. The more complex type of attack is the one that are the same as normal behavior.

We initially analyzed the overall interest rate ∂_x of the user with and without attack. Figure 3 represents the interest rate of the user in browsing the web pages of the server without attack.

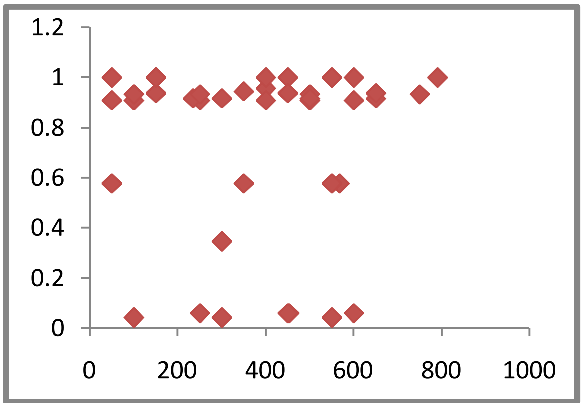

Fig. 3 Overall interest rate without attack

Figure 4 express the rate of overall interest with attack.

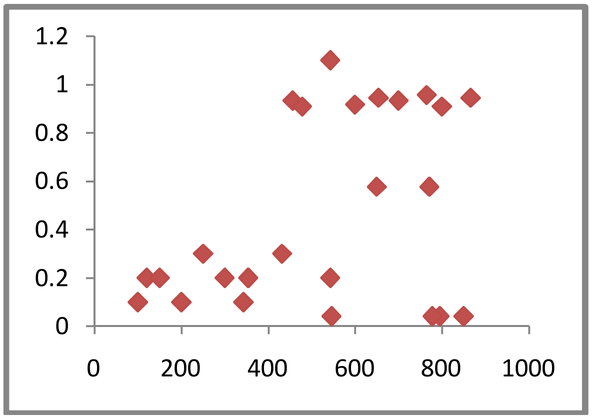

Fig. 4 Overall interest rate with attack

Individual page intensity $I_{wp,x}$ attribute's decision efficiency is portrayed in the following figures. Figure 5 and 6 denotes the intensity rate without and with attack respectively. These attributes are tested in order to check their efficiency in the detection mechanisms.

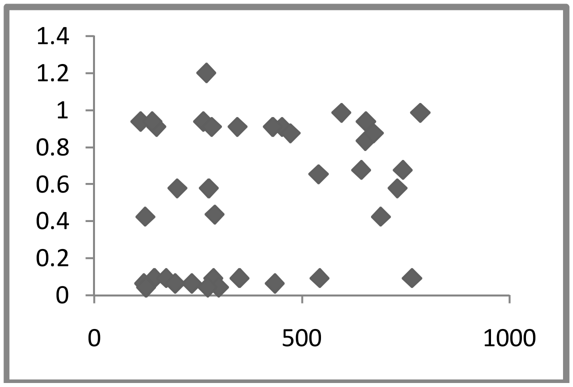

Fig. 5 Individual page intensity without attack

For evaluation of our proposed work's efficiency we compared the accuracy and execution time of our proposed work with [15].

The accuracy of our detecting mechanism is pictured in the figure 7. This depicts that the accuracy of our proposed framework in the detection of App-DDoS is greater than the existing method proposed in [15]. Our proposed framework accurately identifies 94.4% of App-DDoS attacks; whereas the existing method that uses HsMM for detection of DDoS attacks in the application layer discriminates on 80.4% of given data set that are trained. Our proposed method outperforms the existing by 14% in finding the application layer DDoS attack.

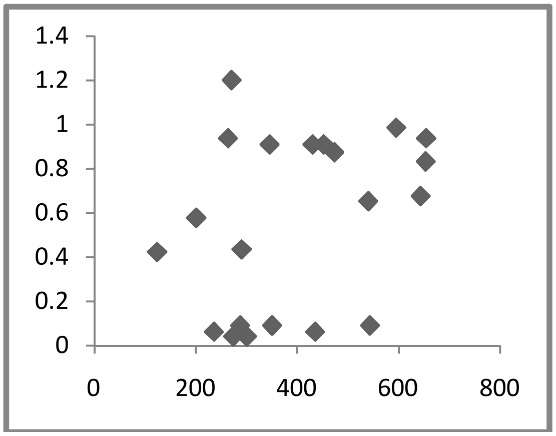

Fig. 6 Individual page intensity with attack

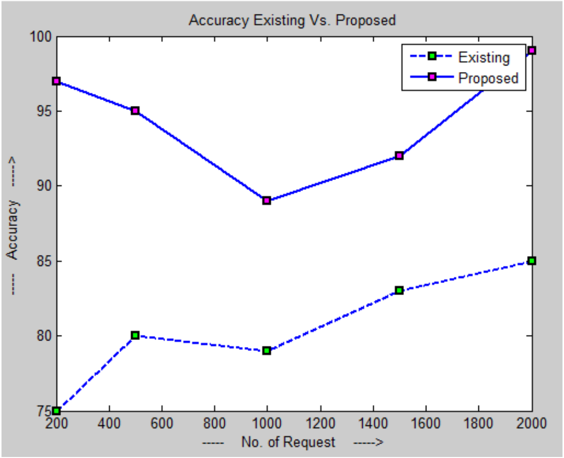

Fig. 7 Accuracy of Existing Vs. Proposed

Similarly, time requirement of the detection mechanism can be compared. Time factor for evaluation of our proposed method is determined since they play a vital role. If the detection mechanism itself consumes more time, then processing the user request is delayed. Therefore, this affects the process and efficiency of the web server by increasing the time requires for replying the request. Figure 8 portrays the required time for both the existing and proposed frameworks. It also specifies that if the number of request increases, then the time required for both the proposed and existing increases. However, our proposed method requires 0.368 seconds as an average detection rate of the application layer DDoS. This rate is 0.126 seconds higher than the existing method as an average.

Therefore, our proposed framework also helps in the further processing of server. It explicitly shows that our framework consumes less time than the existing method in [15].

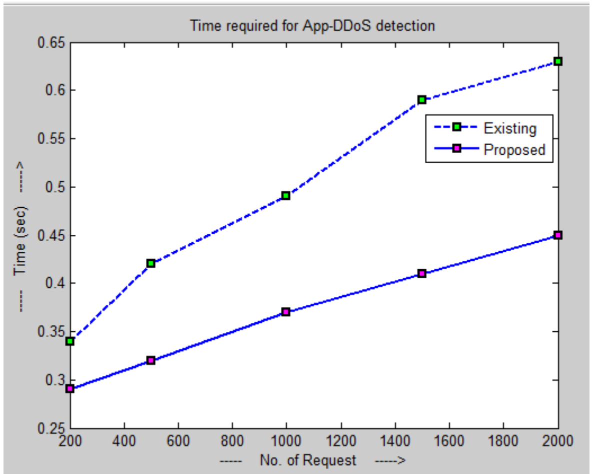

Fig. 8 Required Time for execution of detection mechanism

6. Conclusion

This article focused on the detection of DDoS attack in the application layer. We proposed a framework for determining the abnormal behavior of the user in order to find the DDoS attack. The detection framework uses sequence order independence's two basic and subsidiary attributes rather than the sequence order of web page to construct behavior based attribute vector matrix. To model the browsing pattern, we use PCA, which also reduces the spare data. Depending on the time interval attribute we cluster the browsing pattern using k-means clustering algorithm. Removal of spares data will improve the clustering speed. Threshold value of the clusters is used to find the deviation in behavior of the user as a normal or attacker. The experimental results in section 4 are evident that our proposed framework more efficiently detects the anomaly behavior than the earlier method. In future we extend our proposed framework to discriminate App-DDoS attacks from flash crowds.

REFERENCES

1. Feinstein L, Schnackenberg D, Balupari R, and Kindred D, "Statistical approach to DDoS attack detection and response," In the proceedings of DARPA Information Survivability Conference and Exposition, vol. 1, pp. 303-314, 22-24 Apr. 2003.
2. Shuyuan Jin, and Yeung D.S., "A covariance analysis model for DDoS attack detection," In the IEEE International Conference on Communications, vol. 4, pp. 1882-186, 20-24 Jun 2004
3. Augustin Soule, Kave Salamatian, and Nina Taft, "Combining filtering and statistical methods for anomaly detection," In the proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, pp. 31-31, 2005.
4. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, and Hamid Reza Shahriari, "Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Networks," Lecture Notes in Computer Science, vol. 3439, pp. 192-203, 2005
5. Taeshilk Shon, Yongdae Kim, Cheolwon, and Jongsub Moon, "A machine learning framework for network anomaly detection using SVM and GA," In the proceeding of 6th Annual IEEE SMC Information Assurance Workshop, pp. 176-183, 15-17 June 2005
6. George Oikonomou, Jelena Mirkovic, Peter Reiher and Max Robinson, "A Framework for a collaborative DDoS Defense," In ACSAC 22nd Annual Computer Security Application Conference, pp.33-42, Dec 2006
7. Guilaume Dewaele, Kensuke Fukuda, Pierre Borgnat, Patrice Abry, and Kenjiro Cho, "Extracting hidden anomalies using sketch and non Gaussian multiresolution statistical detection procedures," in the proceedings of the workshop on Large scale attack defense, pp. 145-152, 2007, doi. 10.1145/1352664.1352675
8. Xin Xu, Yongqiang Sun and Zunguo Huang, "Defending DDoS Attack Using Hidden Markov Models and Cooperative Reinforcement Learning," in the Lecture Notes in Computer Science, vol. 4430, pp. 196-207, 2007
9. ByungHak S, Joon H, and Choong Seon H, "Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks," in the proceedings of IEICE transactions on Communication, vol. E90-B, no. 10, Oct 2007

10. Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggo Han, and Sehun Kim, "DDoS attack detection method using cluster analysis," in the proceedings of Expert Systems with Applications, vol. 34, issue 3, pp. 1659-1665, Apr 2008
11. Ming-hui Y, and Ru-chuan W, "DDoS detection based on wavelet kernel support vector machine," in the proceedings of The Journal of China Universities of Posts and Telecommunications, vol. 15, issue 3, pp. 59-63, Sep. 2008
12. Tae Hwan Kim, Dong Seong Kim, Sang Min Lee, and Jong Sou Park, "Detecting DDoS Attacks Using Dispersible Traffic Matrix and Weighted Moving Average," in the proceedings of 3rd International Conference and Workshops on Advances in Information Security and Assurance, pp. 290-300, 2009, doi. 10.1007/987-3-642-02617-1 30
13. Venkata Ramana V, Shilpa Choudary V and Maya B. Dhone, "Analysis & Study of Application Layer Distributed Denial of Service Attacks for Popular Websites," In the proceedings of International Journal of Computer Science and Telecommunications, vol. 2, issue 8, pp. 88-92, Nov. 2011
14. Anuja R. Zade, and Suhas .H. Patil, "A Survey On Various Defense Mechanisms Against Application Layer Distributed Denial Of Service Attack," in the proceedings International Journal on Computer Science and Engineering, vol. 3, No. 11, pp. 3558-3568, Nov. 2011
15. Sanjay B Ankali, and Ashoka D V, "Detection Architecture of Application Layer DDoS Attack for Internet," in the Proceedings of International Journal of Advanced Networking and Applications, vol. 3, issue 1, pp. 984-990, 2011
16. Sang Min Lee, Dong Seong Kim, Ja Hak Lee, and Jong Sou Park, "Detection of DDoS attacks using optimized traffic matrix," in the proceedings of computer and Mathematics with Applications, col. 63, issue 2, pp. 501-510, Jan 2012
17. Fei Wang, Hailong Wang, Xiaofeng Wang, and Jinshu Su, "A new multistage approach to detect subtle DDoS attacks," in the proceedings of Mathematical and Computer Modelling, vol. 55, issue 1-2, pp.198-213, Jan 2012
18. Esraa Alomari, Selvakumar Manickam, Gupta BB, Shankar Karuppaya, and Rafeef Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," in the proceedings of International Journal of Computer Applications, vol. 49, No. 7, pp. 24-32, Jul. 2012

R.**Bharathi** received B.E degree in the year 1998 and M.E degree in the year 2006.Currently she is pursuing Ph.D Degree in Anna University, Trichy, India. She is presently a Assistant Professor with Anna University College of Engineering ,Nagercoil, India. Her current research interests include network and security, secure communication, and secure e-commerce.

Dr. R. Sukanesh, senior professor in Biomedical Engineering received her B.E. Degree (ECE) from Government College of Technology, Coimbatore in 1982. She obtained her M.E. (Communication Systems) degree from P.S.G. Technology, Coimbatore in 1985 and Ph.D. in Bio Medical Engineering from Madurai Kamaraj University, Madurai in 1999. Since 1985 she is a faculty in the Department of ECE at Thiagarajar College of Engineering, Madurai and presently she is professor of ECE and Head of the Medical Electronics Division in the same college. Her main research areas include Biomedical Instrumentation, Neural Networks, Bio-Signal processing and Mobile Communication. She isguiding twelve Ph.D. thesis in the mentioned areas. She has published 30 papers in referred journals and around eighty papers in International and National conferences conducted both in India and aboard. She has delivered a number of invited lectures in various universities. She has a Diploma in Higher Learning and has co-authored a book on Gandhian thoughts. She is a reviewer for International Journal of Biomedical Sciences and International journal of signal processing. She is an editorial member for journal of Engineering students. She contributed a chapter titled, "Impact of Information Technology in Business" in the book, "Future Organization strategies and Business" edited by Professor Biswajeet Pattanayak. She is the recipient of the outstanding paper award at the 12th International conference on Biomedical Engineering at untec city, Singapore in the year 2005. She also received The President of India's Prize (English) 2006, The Jawaharlal Nehru Memorial prize-2006 and Woman engineer award from IE (India).

She is a fellow of Institution of Engineers (India) and a life member of biomedical society of India, Indian Association of Biomedical Scientist and ISTE.

.