Detection of Distributed Denial of Service Attacks Using Statistical Pre-Processor and Unsupervised Neural Networks

Rasool Jalili[1], Fatemeh Imani-Mehr[1], Morteza Amini[1], Hamid Reza Shahriari[1]

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
jalili@sharif.edu, {imani, amini, shahriari}@mehr.sharif.edu

Abstract. Although the prevention of Distributed Denial of Service (DDoS) attacks is not possible, detection of such attacks plays main role in preventing their progress. In the flooding attacks, especially new sophisticated DDoS, the attacker floods the network traffic toward the target computer by sending pseudo-normal packets. Therefore, multi-purpose IDSs do not offer a good performance (and accuracy) in detecting such kinds of attacks. In this paper, a novel method for detection of DDoS attacks has been introduced based on a statistical pre-processor and an unsupervised artificial neural net. In addition, SPUNNID system has been designed based on the proposed method. The statistical pre-processing has been used to extract some statistical features of the traffic, showing the behavior of DDoS attacks. The unsupervised neural net is used to analyze and classify them as either a DDoS attack or normal. Moreover, the method has been more investigated using attacked network traffic, which has been provided from a real environment. The experimental results show that SPUNNID detects DDoS attacks accurately and efficiently.

Index Terms – DDoS Attacks, Intrusion Detection System, Unsupervised Neural Nets, Statistical Pre-Processor

1 Introduction

Generating successful flooding DoS[1] attack on today's powerful computers is not possible using single ordinary computers. One of the solutions to have a succeed attack is to distribute the attack among a group of computers around the network. Moreover, tracing an attack originated from multiple sources is much harder than from single source attacks. Consequently, attackers can generate distributed DoS attacks and sustain any network bandwidth using thousands of computers.

A DDoS attack consists of three main components: master or main attacker, slave computers, and the victim computer. The main attacker initiates the attack from the master computer and tries to find some slave computers to be involved in the attack. A small piece of software is installed on the slave computers to run the attacker

[1] Denial of Service

commands. The attack scenario continued through a command issued from the attacker resides on the master computer toward the slave computers to run their pieces of software. The mission of the piece of software is to send dummy traffic destinated toward the victim. Therefore, the victim will not be able to do anything to prevent this attack. To reduce the network traffic, the victim should detect the attack just in time to be able to block some IP addresses. Although on time detection of an attack has an important role in preventing the progress of the attack, detection of DDoS[2] attacks is not so easy. As DDoS attack generation tools and methods try to increase traffic toward the victim computer using generating normal packets, signature based intrusion detection systems are unable to detect such attacks.

In this paper a new approach to detect distributed DoS attacks using statistical perprocessor and unsupervised neural nets is presented. In this method an unsupervised artificial neural net has been used to analyze and classify extracted statistical features.

The rest of the paper organized as follows: section 2 represents related works. The overall approach is described in section 3. Section 4 describes the base SPUNNID system [1], as the base architecture. Section 5 presents evaluation results of our method. Section 6 draws some conclusions and future works.

The preparation of manuscripts which are to be reproduced by photo-offset requires special care. Papers submitted in a technically unsuitable form will be returned for retyping, or canceled if the volume cannot otherwise be finished on time.

2 Related Work

Flooding attacks create enormous amount of normal packets and create anomalies in the target network traffic. Therefore, most approaches to detect such kinds of attacks, tries to detect these anomalies using semi statistical methods. In this paper, we use statistical methods to construct a Statistical Pre-Processor to extract some features, which demonstrates the behavior of DDoS attacks. Then an unsupervised neural net is used to analyze and classify these features. Accordingly, in this section we overview some research on Detection of DDoS attacks and IDSs based on unsupervised neural nets.

Authors in [2] introduced MULTOPS data structure to detect DDoS attacks. Using the data structure, they detected DDoS attack by searching for significant asymmetries between packets to and from different subnet. AGURI [2] as a monitoring tool uses the traffic pattern aggregation method, to monitor the traffic in a long term and detect DDoS attacks. In [3] a scheme to detect DDoS attacks by monitoring the increase of new IP addresses was proposed. In addition, it was presented that a sequential change point detection algorithm can identify when an attack has occurred. In [45], efficient adaptive sequential and batch sequential methods for an early detection of DDoS attacks have been developed.

[2] Distributed Denial of Service

In [6], the network traffic, which is expressed in terms of *Tcp flag rates* and *protocol rates,* has been analyzed and it has been shown that when the flooding attacks are in effect, intuitively the two rates can be distinctive and predictive, due to the explosion of TCP flags or specific protocol packets. In [7] an approach to reliably identifying signs of DDOS flood attacks based on LRD (long-range dependence) traffic pattern recognition has been discussed. In [8] the authors introduced an automated methodology for analyzing DoS attacks that is based on ramp-up and spectral analysis to build upon existing approaches of header analysis. This identification framework can be used as part of an automated DDoS detection and response System.

In [9], Feinstein and Schnackenberg, present statistical methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. In [10] the effects of multivariate correlation analysis on the DDoS detection were discussed and a covariance analysis model for detecting SYN flooding attacks was proposed. In [11] a combined data mining approach for modeling the traffic pattern of normal and diverse attacks was proposed. This approach used the automatic feature selection mechanism for selecting the important attributes.

Some early research on IDSs attempted to use neural nets for intrusion detection. Such systems must be used in intrusion detection after initial training on normal or attack behaviors (or hybrid of theses behaviors). Both supervised and unsupervised neural nets have been used in IDSs till now such as MLFF, Recurrent, Adaptive, SOM and ART nets.

In [12] the authors presented a robust neural network detector for Distributed Denial-of-Service (DDoS) attacks in computers providing Internet services. A genetic algorithm was used to select a small number of efficient features from an extended set of 44 statistical features, which are estimated only from the packet headers.

Most supervised neural net architectures require retraining in order to improve analysis capability due to changes in the input data, but unsupervised net offers increased level of adaptability to neural nets and are able to dynamically improve their analysis capability [13].

Most of the network-based systems in unsupervised based IDSs used self-organizing maps (SOMs) neural nets and only a few systems used other types of unsupervised neural nets. In [14], multiple SOMs are used for intrusion detection, where a collection of more specialized maps is used to process network traffic for each protocol separately. Each neural net was trained to recognize the normal activity of a single protocol.

Some of the research in unsupervised neural net based IDSs in recent years, focused on using more than one neural net in a hierarchical structure. Improving the accuracy of classification is the main advantage of this method. In [15], a Hierarchical Intrusion Detection (HIDE) system is introduced which is able to detect network based attacks as anomalies using statistical pre-processing and neural net classification. In [16], a two-level hierarchical SOM is applied for intrusion detection. The system has emphasis on the representation of time and incremental development of a hierarchy. The SOM in this system is able to detect attack patterns over sequence of connections. The system developed in [1617] (named NSOM), uses structured SOM to classify real-time ethernet network data. The system is able to classify DoS attacks graphically as opposed to normal traffic by demonstrating that the clustering of neurons is very different between the two.

Most statistical methods reviewed in this section use some thresholds to detect DDoS attacks. In many cases, such thresholds cannot distinguish the normal behavior from the attack behavior precisely. In this paper, some statistical features showing the behavior of DDoS attacks have been extracted, and using unsupervised neural nets, they have been classified into normal and attack. In application phase of the neural net, this classification is used to detect DDoS attacks.

3 IDS for DDoS Attacks

General network based intrusion detection systems are either packet based or connection based. These systems attempt to detect attacks through analyzing packet or connection templates correspondingly. In DDoS attacks, the attacker floods the network traffic toward the target computer by sending semi normal packets. Therefore, multi purpose IDSs do not have a good performance (and accuracy) in detecting such kinds of attacks. The DDoS victim, which is encountered with a vast number of normal packets, is overloaded, cannot provide services to its legitimate network users and denies them. The attacker tries to flood target network traffic with semi normal packets, but some statistical features on target network traffic will change under DDoS attack such that it becomes different from (and more complicated that) normal ones. Extraction of these features and analyze them is helpful to detect DDoS attacks. The normal network traffic of each computer depends on its user services. In addition, relatives to user services of the computer, it may be different during the day and night. Therefore, the value of some statistical features on DDoS attack generated network traffic, usually is different from values of the features on normal network traffic of the target computer.

In this paper, statistical features in a minor time interval have been extracted from network traffic, and it is shown that these features in attack network traffic differ from those in normal network traffic. Using such exploited result, it is possible to detect DDoS attacks more precisely. Due to the extend of network traffic in the target computer, regardless of the type of traffic in different times, the area of our extracted statistical features is extensive. Because of high clustering power, it seems that unsupervised artificial neural net is a more suitable tool for this purpose.

In this paper, provided normal and attack network traffic is divided into minor time intervals, denoted as *T*. The time interval *T* includes all packets that their timestamps agree with that interval. Then we extract our statistical features from these time intervals. These features form the training vector of neural net. A typical time interval T can be labeled as “Normal” or “DDoS Attack” relative to its attack packets rate. Neural net processes these vectors and automatically clusters them as “Normal” or “DDoS Attack” as well as belonging of them to special belong to their variety.

In the application phase of neural net, packets belonging to the time interval *T* have been captured and statistical features have been extracted. The unsupervised neural net uses these features as input vector, clusters them, and detects their type as "normal" or "DDoS Attack".

In our previous research on IDSs, we introduced an Unsupervised Neural Net based Intrusion Detector (UNNID) system [1], which was network based. That system could detect attack through analyzing packets or connections signature. We promote UNNID system by adding the statistical pre-processor to detect DDoS attacks; yield in a new system called Statistical Pre-Processor & Unsupervised Neural Net based Intrusion Detector (SPUNNID). The architecture of SPUNNID system is presented in the next session.

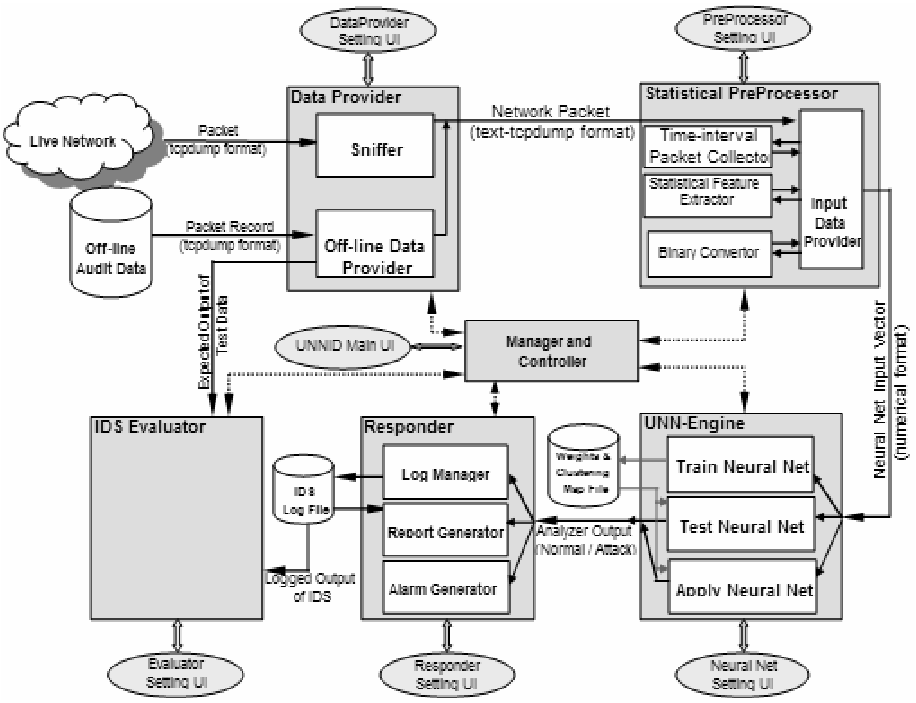

Fig. 1. Statistical Pre-Processor and Unsupervised Neural Net based Intrusion Detector (SPUNNID) System Architecture.

4 System Architecture

The architecture and main components of our SPUNNID system is shown in figure 1. The system is designed firstly to facilitate training, testing, tuning and evaluating different types of unsupervised neural nets for intrusion detection, and secondly to apply them for analyzing network traffic in on-line and off-line mode in order to classify classifying network traffic into normal and attack.

In SPUNNID, *Data Provider* collects packets from network audited data file (off-line mode) or live network (on-line mode) and send data in the text form to the *Statistical*

Pre-Processor component. *Statistical Pre-Processor* extracts some features from packets of the specified time interval using statistical techniques. *The component* converts extracted feature vector into the numerical form and if needed converts numerical data into binary or normalized form, and send them to Unsupervised *Neural Net based Engine*. The *UNN-Engine* uses data either for training and testing its neural net or for analyzing and detecting denial of service attacks. The analyzer output (normal or DoS attack type) is given to *Responder* for recording in the system log file and generating alarm in case an attack is detected. The *IDS Evaluator* component provides a facility for reporting true detection rate, false positive detection rate, false negative detection rate, and other criteria to evaluate our system in detecting denial of service attacks. This component calculates these criteria by comparing the output of IDS and expected output of the system, which is determined by labels on records of test data. The criteria are:

- Exact True Type Detection Rate (detecting normal traffic from attack and recognizing the known attack type);
- True Detection Rate (only separating normal traffic from attack);
- False Positive Detection Rate (miss-detecting attack);
- False Negative Detection Rate (failing to detect attack when it is occurs);

Finally the *Manager & Controller* component in this system manages and directs other components to work in one of the possible modes (e.g. training, testing, and detecting) based on the command and parameters delivered from the operator.

4-1 UNN-Engine

One of the main components of UNNID is UNN-Engine, which has the role of analyzing the network traffic and detecting denial of service attacks using one of the convenient unsupervised neural nets named Adaptive Resonance Theory (ART) nets. In unsupervised ART nets, input patterns may be presented several times and in any order. Each time a pattern is presented, an appropriate cluster unit is chosen and related cluster weights are adjusted to let the cluster unit learn the pattern. In these nets, choosing a cluster is based on the relative similarity of an input pattern to the weight vector for a cluster unit, rather than the absolute difference between the vectors (that is used in SOM nets). As in the most cases of clustering nets, the weights on a cluster unit may be considered an exemplar (or code vector) for the patterns placed on that cluster. ART nets are designed to allow the user to control the degree of similarity of patterns placed on the same cluster that can be done by tuning the *vigilance parameter* in these nets. In ART nets, the number of clusters is not required to be determined in advance, so the vigilance parameter can be used to determine the proper number of clusters to decrement probability of merging different types of clusters to the same cluster. Moreover, ART nets have two other main characteristics. First is *stability* which means a pattern not oscillating among different cluster units at different stages of training, and second is *plasticity* which means the ability of net to learn a new pattern equally well at any stages of learning.

Stability and plasticity of ART nets and the capability of clustering input patterns based on the user controlled similarity between them, made these nets more appropriate for using in IDSs, rather than most of other types of unsupervised nets (such as SOM) for classifying network traffic into normal and intrusive/ attack. For this purpose, we used a type of unsupervised ART nets, named ART-1. ART-1 is the first type of ART nets, which designed for clustering binary inputs.

In *SPUNNID*, *Statistical Pre-Processor* feeds binary input vector to ART-1 net. In the training phase, the input vectors are clustered through ART-1 net regardless of their nature (normal or intrusive). Following the training phase, system must determine the neurons of each type of cluster and assign name to each cluster using the label of each time interval records (in train data). Each cluster has the same name as its units. Each unit is named based on the type of the majority of input data that the unit represent the winning or best matching for. This reduces to constructing a *Clustering Map*. In the map, units are clustered together to indicate either the normal traffic, known trained attacks, or possibly a new DoS attack. New attacks may appear in abnormal traffic, which is neither a normal traffic nor a known DoS attack.

4-2 Statistical Feature selection

The attacker uses flooding attacks such as UDP flood, Syn flood, ICMP flood, and ICMP Smurf to generate DDoS attacks and finally floods the target network. When the DDoS attack is being initiated, the number of packets in the network increases instantly. The number of packets may also be increased in normal network traffic. Increasing the number of packets in normal heavy network traffic and attacked network traffic cannot be distinguished easily. Analyzing the DDoS attack and the normal network traffic shows that packet rates are a better criterion for deciding about happening of the attack. Tcp flags rates and protocol rates in normal network traffic change slowly. Flooding packets, which are used by the attacker, specify the behavior of the DDoS attack and the effect of this attack in changing the statistical features. In attacked network traffic, depends on its behavior, these rates change and become different from the normal traffic. Therefore, we extracted the features that shown these rates in a typical time interval *T*.

These features are:

- N_{ICMP}: the percent of *ICMP* packets.
- N_{UDP}: the percent of *UDP* packets.
- N_{TCP}: the percent of *TCP* packets.
- N_{TCPSYN}: the percent of *SYN* packets in *TCP* packets.
- $N_{TCPSYNACK}$: the percent of *SYN+ACK* packets in *TCP* Packets.
- N_{TCPACK}: the percent of *ACK* packets in *TCP* packets.
- $A_{Packet\ Header\ Sizes}$: The packet header sizes average.
- $A_{Packet\ Data\ Sizes}$: The packet data sizes average.

After extracting these features, the neural net input vector is constructed.

The operation of *Statistical Pre-Processor* is similar to an operation of the Bus Station system. The packets, which have been come from Data Provider, wait for coming of a bus. The bus comes to the station every T seconds (the length of time interval), and takes captured packets to the Statistical Features Extractor component. This component processes the coming packets, extracts selected features and converts these features to binary or normalized form in order to feed neural net sensors in UNN-Engine component.

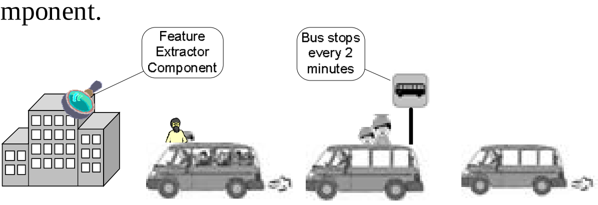

Fig. 2. Statistical pre-processor is similar to bus station system.

5 Evaluation

Providing proper data (including attack and normal network traffic) play main role to get a high performance in detection of DDoS attacks. If the data covers normal traffic (during day and night) and all types of DDoS attacks, the training phase of the neural net will be done better and thus having a better performance for the net. In the following subsection, a method of gathering suitable data, for training and testing phase of the neural net, will be explained and then evaluation results will be shown.

5-1 Data Gathering

Generating DDoS attacks on a real environment and gathering normal and attack data are so costly. Meanwhile it has been tried to maintain the gathered data comparable with the real one.

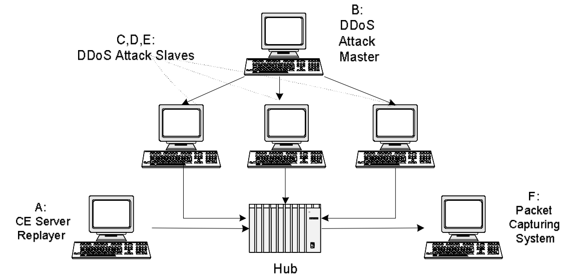

Fig. 3. Topology of Data Gathering Network For Evaluation

The network topology, shown in figure 3, is used to generate data in our evaluation. In this topology, the captured network traffic on the real environment has been replayed using the computer A. This computer plays the role of the real Computer CE[3]. The computer B is considered as the DDoS attack master. To generate an attack, B orders the DDoS attack slave computers including C, D and E to initialize the attack. These computers initialize the attack through sending flooding packets into the network. These packets are compounded with the CE computer network traffic and form the traffic under DDoS attack, captured by the computer F. If DDoS attack does not flow in the network, F captures the CE normal network traffic. Finally the captured network traffic by F includes both normal and attack network traffic.

The traffic of CE was captured as normal network traffic for the training and testing phase. Using the network topology, the traffic was replayed, and DDoS attack traffic was generated at once. Regarding this scenario, flooding attacks for the training data include UDP Flood, SYN Flood, ICMP Flood, ICMP SMURF, and mixture of these flooding attacks, each flowing for a period of 15 minutes. So the generated training traffic includes normal and attack network traffic. The traffic for the testing phase was generated using this method. This traffic contains the network traffic under the DDoS attack, trough 15 minutes.

5-2 Evaluation Results

Evaluation is achieved using the network topology described above. Parameters considered in the evaluation phase are:

- The number of clusters in ART1 neural net.
- The number of epochs in the training phase of ART1 neural net.
- The vigilance parameter of ART1 neural net.
- The length of the time intervals.
- The vigilance parameters value in the application phase of SPUNNID.

The effect of these parameters has been evaluated based on the Exact True Type detection Rate (ETTR), True Detection Rate (TR), False Positive detection Rate (FPR) and False Negative detection Rate (FNR).

The number of clusters in ART1 neural net

Specifying the number of clusters depends on the variation of training data. Furthermore, the volume of training data and its variations depends on the length of time intervals in the introduced method. So changing the length of time intervals, results in changing the number of clustered neural net clusters. Generally, the number of clusters must cover the selected data of the training phase.

The number of epochs in the training phase of ART1 neural net

The next parameter, which can affect on our experimental results, is the number of epochs or iterations in neural net training phase. Our experiments show that, 100 is a good option in this regard.

[3] The server in Department of Computer Engineering, Sharif University of technology.

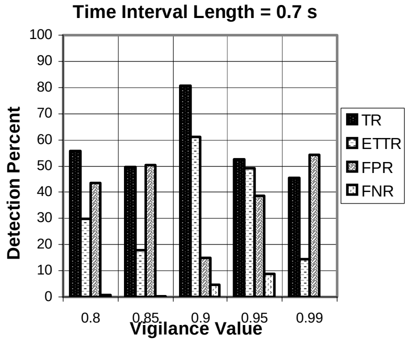

Fig. 4. The effect of changing the Vigilance value on *SPUNNID* detection performance.

The vigilance parameter of ART1 neural net

The vigilance parameter is the most important parameter that can affect on ART1 clustering and classification quality. This parameter specifies the degree of similarity of patterns placed on the same cluster. Neither high value nor low value for this parameter is suitable for our system. To specify the appropriate value of vigilance parameter and its effect on the system performance, the system was trained with different vigilance values and ETTR, TR, FPR, and FNR criteria were evaluated. Results of the experiments are presented in figure 4. The results show that ART1 with vigilance value of 0.9 offers the best level of detection performance.

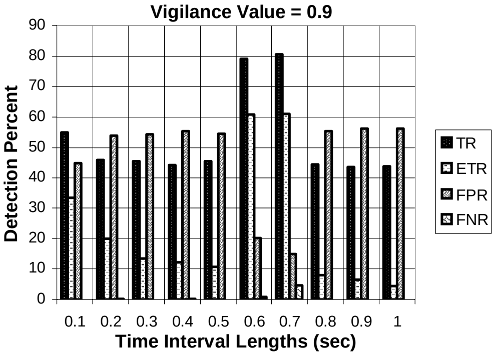

Fig. 5. The effect of changing the length of Time Interval on SPUNNID detection performance.

The length of time intervals

Defining the best value for the length of time interval is a tradeoff between the load of captured network traffic for training phase of ART1 neural net, the existence of enough processing power, and the expected efficiency. Neither high value nor low value for this time interval length is suitable for our system. Increasing or decreasing the length of time intervals resulted in increment or decrement of the number of neural net input data. Also in a short time interval, the number of data variation is less than the longer time interval. Thereby, the selection of longer time intervals is more efficient, if the number of training data of neural net is big sufficiently, and there is enough processing power for training of neural net. In this case, the variation and the number of clustering data become greater, thus the training power of neural net will increase.

Generally, the response time of the introduced method corresponds to the selected time interval length. If the length of time intervals is selected very long, the response time will increase. However, the increasing of response time is not so impressive for computer network administrators. In addition, the length of time intervals should not exceed from the length of happened DDoS attacks time. It seems that the length of time intervals cannot exceed from 2 minutes.

If the training data is not very high, selection of shorter time interval can produce suitable results. The minimum length of time intervals is a value in which the effect of DDoS attacks can be represented using the selected features. For example, assume a time interval, which contains only two packets. The type of these packets cannot effect on our features so as they can use to suitable DDoS attack detection. Furthermore, these two packets cannot create a sufficient variation of selected features. Therefore, the good selection of time interval lengths is tradeoff between the load of captured network traffic for training phase, the existence of enough processing power, and the expected efficiency.

Figure 5 shows the best time interval length, which determines the appropriate value for time interval length in our gathered data.

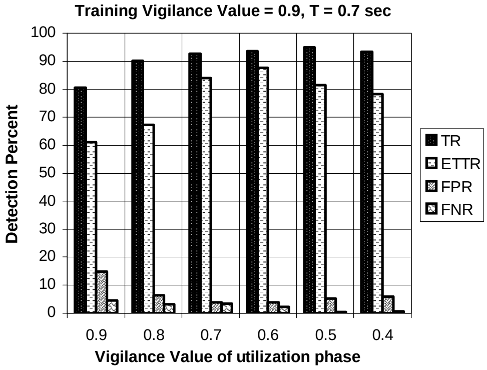

Fig. 6. The effect of changing the vigilance value in testing phase on SPUNNID detection performance.

The vigilance value in application phase of ART1 neural net

One of the main disadvantages of many commercial and expert system based IDSs are their weakness in detecting changed known attacks and also new attacks. So for enhancing our system flexibility and generality we decreased system sensitivity in clustering input patterns by changing in vigilance parameter in application phase of SPUNNID system. It has been shown that the selection of the smaller value for vigilance parameter in application phase can decrease the sensitiveness of clustering in unsupervised neural net based engine. Therefore in many cases, if the value of vigilance parameter decreases, the number of “Can Not Cluster” messages decreases too. Figure 6 shows this obtained result for this purpose.

6 Conclusion and Feature works

In this paper, we introduced a new approach for detection of DDoS attacks, using unsupervised neural nets and statistical methods. In this approach, the statistical features showing the behavior of these attacks along a minor time interval, have been extracted. The ART1 net has been used to analyze and classify these features. Evaluation results show that the approach in 94.9 percent of times is able to recognize the attacked traffic from the normal one. In addition, the introduced approach detects DDoS attack in less than a second (0.7 second in best case).

One of the neural net advantages, specially unsupervised neural nets, is that it can classify the input data automatically without human intervention. Therefore, extraction of proper features to train neural nets (statistical or non-statistical) which can show the effect of a typical attack can be useful to promote detection performance.

In our future investigation, we intend to use a FIFO queue of extracted statistical feature vector as the neural net input vector. When DDoS attack happens, the correlation between our statistical parameters in some neighbor time intervals decreases. Using the queue of statistical features of the neighbor time intervals as a neural net input vector shows the change of this correlation better than considering single time interval.

References

1. M. Amini, and R. Jalili, *"Network-Based Intrusion Detection Using Unsupervised Adaptive Resonance Theory (ART)"*, Proceedings of the 4th Conference on Engineering of Intelligent Systems (EIS 2004), Madeira, Portugal, 2004.
2. T. M. Gil and M. Poletter. *"Multops: a data-structure for bandwidth attack detection"*, In Proceedings of USENIX Security Symposium'2001, 2001.
3. R. Kaizaki, K. Cho, O. Nakamura, *"Detection Denial of Service Attacks Using AGURI"*, International Conference Telecommunications, Beijing China, June 2002.
4. T. Peng, C. Leckie and R. Kotagiri. *"Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring"*, In Proceedings of the Third International IFIP-TC6 Networking Conference (Networking 2004), Athens, Greece, 2004.
5. R. Bazek, H. Kim, B. Rozovskii, and A. Tartakovsky, *"A novel approach to detection of enial-of-service attacks via adaptive sequential and batch-sequential change-point methods*", IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2001.
6. Sanguk Noh , Cheolho Lee ,Gihyun Jung, Kyunghee Choi, “Using Inductive Learning for the Detection of Distributed Denial of Service Attacks”, International Conference on Advances in Infrastructure for Electronic Business, Education, Science, Medicine and Mobile Technologies on the Internet, 2003.

7. L. Ming Li, *"An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition"*, Computers & Security, Vol. 23, Issue 7, Elsevier, ISSN 0167-4048, April 2004.
8. A. Hussain, J. Heidemann, and C. Papadopoulos. *"A Framework for Classifying Denial of Service Attacks"*. In Proceedings of the ACM SIGCOMM Conference, pp. 99-110, Karlsruhe, Germany, August 2003.
9. L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred, *"Statistical Approaches to DDoS Attack Detection and Response*", DARPA Information Survivability Conference and Exposition, 2003.
10. Shuyuan Jin, Daniel S. Yeung, "*A Covariance Analysis Model for DDoS Attack Detection*", IEEE Communications Society, 2004.
11. K. Mihui, N. Hyunjung, C. Kijoon, B. Hyochan, and N. Jungchan, "A Combined Data Mining Approach for DDoS Attack Detection", Information Networking: Networking Technologies for Broadband and Mobile Networks International Conference (ICOIN 2004), Busan, Korea, February 2004.
12. D. Gavrilis, I. Tsoulos, E. Dermatas, *"Feature selection for robust detection of distributed Denial-of-Service attacks using genetic algorithm"*, Methods and Applications of Artificial Intelligence: Third Hellenic Conference on AI (SETN 2004), Samos, Greece, May 2004.
13. J. Cannady, *"Artificial Neural Networks for Misuse Detection"*, In Proceedings of National Information Systems Security Conference, 1998.
14. B.C. Rhodes, J.A. Mahaffey, and J. D. Cannady, *"Multiple Self-Organizing Maps for Intrusion Detection"*, In Proceedings of 23rd National Information Systems Security Conference, 2000.
15. Z. Zhang, J. Li, C. N. Manikopoulos, J. Jorgenson, and J. Ucles, "HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification", *In Proceedings of the 2nd Annual IEEE Systems, Mans, Cybernetics Information Assurance Workshop*, West Point, NY, June 2001.
16. P. Lichodzijewski, A. N. Zincir-Heywood, and M. I. Heywood, *"Dynamic Intrusion Detection Using Self-Organizing Maps"*, The 14th Annual Canadian Information Technology Security Symposium, CITSS, 2002.
17. K. Labib, and R. Vemuri, *"NSOM: A Real-Time Network-Based Intrusion Detection System Using Self-Organizing Maps"*, Networks and Security, 2002.