NETWORK INTRUSION DETECTION AND COUNTERMEASURE SELECTION IN VIRTUAL NETWORK (NIDCS)

James D. Gadze[1] Maxwell Cobbah[2] and Griffith S. Klogo[3]

[1,2]Department of Electrical Engineering, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana
[3]Department of Computer Engineering, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana

ABSTRACT

Intrusion in a network or a system is a problem today as the trend of successful network attacks continue to rise. Intruders can explore vulnerabilities of a network system to gain access in order to deploy some virus or malware such as Denial of Service (DOS) attack. In this work, a frequency-based Intrusion Detection System (IDS) is proposed to detect DOS attack. The frequency data is extracted from the time-series data created by the traffic flow using Discrete Fourier Transform (DFT). An algorithm is developed for anomaly-based intrusion detection with fewer false alarms which further detect known and unknown attack signature in a network. The frequency of the traffic data of the virus or malware would be inconsistent with the frequency of the legitimate traffic data. A Centralized Traffic Analyzer Intrusion Detection System called CTA-IDS is introduced to further detect inside attackers in a network. The strategy is effective in detecting abnormal content in the traffic data during information passing from one node to another and also detects known attack signature and unknown attack. This approach is tested by running the artificial network intrusion data in simulated networks using the Network Simulator2 (NS2) software.

KEYWORDS

Denial of Service (DOS) attack, Intrusion Detection System (IDS), Discrete Fourier Transform (DFT), Virtual Network, Virus or Malware

1. INTRODUCTION

The recent attack trend has posed many security challenges to network administrators in a digital and electronic information hungry society. DOS attack is increasingly becoming a major challenge for network administrators to handle, a prevalent threat and a leading Internet attack today which is easy to launch. DOS can occur in a network system when victim network resources are barraged with high amount of fabricated attacking packets devised from a single or a large number of machines. The aim of the attack is to overload or send an abnormal high volume of requests to the servers that cause the server resources to collapse or to disrupt the network services and render the legitimate user incapable of performing normal transactions. This is done by exploiting essential vulnerabilities in the network and rapidly becoming the weapon of choice for hackers around the globe. DOS attack has been developed from the simplest direct flooding attacks, Distributed Denied of Service (DDOS) attack and to remote controlled Reflexive Distributed Denied of Service (RDDOS) attacks. Although the technique of DOS attacks is relatively simple, it can attack both the Internet and system resources. In February 2014 a new DOS attack type was introduced called Network Time Protocol (NTP) Amplification attack; the biggest so far reaching 180Gbps which means volume of attack packets continue to grow. Such network based attacks are increasing frequently resulting in a huge financial loss to the organizations and causing the network to be paralyzed for several hours [1]. The global

impact of malicious code attacks is estimated to be over US $113 billion annually according to Norton Cybercrime report in 2012. A 2014 report released by Centre for Strategic and International Studies also estimated that cybercrime and cyber espionage are costing the global economy more than US $400 billion per year [2], [3]. Since the extent of financial loses and damage by DOS attacks are increasing, many studies on Intrusion Detection (ID) mechanism have been carried out by many security experts. ID includes a range of security techniques designed to detect and report malicious system and network activity or to record evidence of intrusion. A tremendous effort has also been made by experts to design very efficient and effective Intrusion Detection System (IDS) which is the main security tool leading in the field of cyber defense currently. Though many researches' have been carried out extensively in this area, DOS attacks continue to harm, as the attackers adapt to the newer elusive mechanisms. The existence of system vulnerabilities in the traffic data during information passing from one node to another in a network is unavoidable simply because of human error. As long as humans make mistakes, such as inappropriate system configuration, bugs in program codes and poorly designed network architecture, security violations will continue to exist. In fact, many of these system vulnerabilities are discovered only after an attack.

In order to maintain confidentiality, integrity, control, authenticity, availability, and utility of the network resources, there is the need to introduce an effective and efficient approach for network intrusion detection as an effective countermeasure for various network attacks. The trend of successful network attacks such as DOS attack continues to rise. These attackers can explore vulnerabilities within a network to gain access to deploy sophisticated attacks. Many algorithms have been developed and implemented to achieve intrusion free network. Most of these algorithms use time-based approach which is unable to detect some attacks. It is also difficult for such techniques to calculate the accurate threshold value above which an abnormality is to be considered 'intrusive' and therefore lead to high rate of false alarm

1.1 Intrusion Detection

There are several IDS techniques for host-based and network-based intrusion detection as well as anomaly-based and signature-based intrusion detection techniques available and they all proved to be very efficient and effective to detect intrusions in a network. However, there are some drawbacks despite the extensive research in recent years. The following are some of the drawbacks considered in the existing IDS;

1. The signature-based intrusion detection cannot detect unknown attacks.
2. The anomaly-based intrusion detection can detect both known and unknown attacks but generate high rate of false alarm.

A signature-based IDS technique determines intrusion by comparing packets on the network against a database of signatures or characteristic from known malicious threats [4]. This technique is capable of detecting only known attacks and cannot detect unknown attacks. Anomaly-based (behavior-based) IDS technique references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered. In this technique the false alarm rate is high which makes it unreliable for practical applications. This encourages the use of frequency-based intrusion technique for network intrusion design. The purpose of this paper is to develop a frequency-based Intrusion Detection System (IDS) that can detect Denial of Service (DOS) attack, specifically to develop an intrusion algorithm for anomaly-based detection techniques. A mathematical model would is introduced in order to reduce or eliminate false alarm rate during the detection process. A Centralized Traffic Analyzer Intrusion Detection System called CTA-IDS is introduced. This

CTA-IDS combines three levels of detection mechanism to reduce false alarm rate and also detect known and unknown attacks.

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 elaborates on the designing procedure for the proposed system. Section 4 reports the simulation results of the proposed IDS, and illustrates how to detect DOS attacks by extracting the frequency patterns and the threshold values generated by the algorithm through our Centralized Traffic Analyzer (CTA). Finally, Section 5 describes results conclusion and future work of this paper.

2. RELATED WORK

This section reviews the related work in the area of data mining approach to intrusion detection. Data mining has been used for host-based and network-based intrusion detection as well as anomaly-based and misuse-based intrusion detection. In this section, the focus will be on the data mining applications on network-based IDS. Lee et al [5], [6] explored application of different data mining techniques in intrusion detection system. The main contribution of their work [5] is that they used multiple data mining techniques with classification, frequent episodes and association rules in order to build a framework for intrusion detection. A practical feature construction system for the classification was also introduced, which categorized the connection based features into low-cost and high-cost features in terms of their computation time. Therefore, different features according to the time requirement would be chosen based on the classification model.

The classification methods are fundamentally rule-based algorithm such as RIPPER. Lee and Solfo further extended their previous work in [6], where they applied association rules and frequent episodes to network connection record to obtain additional features, and then the classification algorithm, RIPPER, was applied on the labeled attack traffic to learn the intrusion pattern. They also extended their cost-sensitive model by explicitly defining three cost levels for features; the rule-sets that are formed by these features are also “cost-sensitive”.

Barbara et al [7] applied association rules and classification for anomaly detection. Their system, ADAM, first built a normal profile by mining on the attack free data, then use the entire training data to look for the suspicious patterns that are not found in normal profiles. Finally, a classifier is trained to identify if the suspicious pattern belongs to known attack, unknown attack or normal event. An alternative classification approaches that use fuzzy association rules is from [8].

Bridges and Vaughn used traditional rule-based expert system for misuse detection and made contribution to anomaly detection by using fuzzy logic and genetic algorithms. They created fuzzy association rules from the normal data set, and also built a set of fuzzy association rules from the new unknown data set, and then compared the similarity between the two groups of rules. If the similarity is low, it indicates a possible intrusion in the new data set.

The genetic algorithm (GA) is used for tuning the membership function of the fuzzy sets and to select the most relevant features. Basically, GA is used to give rewards to a high similarity of normal data and reference data and penalize a high similarity of intrusion data and reference data. By doing so, the similarity between fuzzy rules set of the normal dataset and the reference data set is going to slowly evolve to more, and the similarity between fuzzy rules set of the intrusion data set and the reference data set is going to evolve to less.

Decision tree is another classification technique that applied to intrusion detection [9], [10]. For instance, Sinclair et al use genetic algorithm and decision trees for intrusion detection. The decision tree is constructed by applying the IDS [11] algorithm on the organized data information, such as the tabular form of connection features and the related label of whether they are intrusive.

The constructed tree and genetic algorithms are then used to generate rules for classifying the network connections.

Other data mining approaches such as neural network [12], [13] and Bayesian classifiers are also exploited for the intrusion detection. The major challenge in the anomaly-based detection method is the occurrence of high false alarms.

3. DETECTION MECHANISM

The primary focus of this section is to use DFT to model an algorithm for IDS to generate frequency pattern in order to detect network intrusions and also reduce false alarm rate during the detection process. In this paper, three different levels of detection mechanism would be used in order to reduce the false alarm rate during the detection process. The following are the three levels of detection mechanism that would be used in this work.

- The frequency-based approach which is specifically designed for intrusion pattern analysis on DOS, Probe and password guessing attacks.
- The μ value which is the threshold values (i.e. the average number of packets in each node set by the system by some amount).
- The third one is the average variance of packets sizes within a connection.

This detection mechanism is evaluated using a virtual network in NS2 simulator.

3.1. Intrusion Detection Using Frequency Strategy

A technique introduced in signal processing on time-series data would be used for the frequency based intrusion detection. A time-series consists of a sequence of numbers each representing a data value at some point in time such as traffic throughput of networks. In this paper, consideration would be extended to three different kinds of time-series on network traffic. The first one is the time-series of packets throughput per unit time. The second is the time-series of inter-arrival time of the packets. The last one is the time-series of packet payload size. Our observation is that the attacks generated by coded scripts to flood a network with large amount of traffic such as DOS, probes, and guessing of passwords, may cause some regular patterns in the traffic data. These types of attacks often use fabricated constant sized payloads. The intrusion detection algorithm would be designed based on the observations above and it is expected to capture anomalous traffic behaviors, known attack signature as well as unknown attack signature. There are four steps for this approach. First, the connection history would be constructed for all those connections that are coming from new IPs and trace the traffic features including the packet size, the inter-arrival between packets and the packets throughput per unit time within or among the connections. Second, considering the possible huge amount of data, compressed time-series would be used to speed up the next step's analysis. In the third step, DFT would be applied to the time-series data generated and collect the resulting frequency information. Both the global frequency patterns for all connections in the connection history and local frequency patterns for each single connection would be computed using DFT. Finally, by applying Fourier analysis to the time-series created by network traffic signal, the periodicity pattern that may exist in the network traffic would be identified. Figure 3.1 shows the Flow Chart for proposed Intrusion System. The detail and the whole strategy would be given at the following subsections.

3.2. General Flow Chart

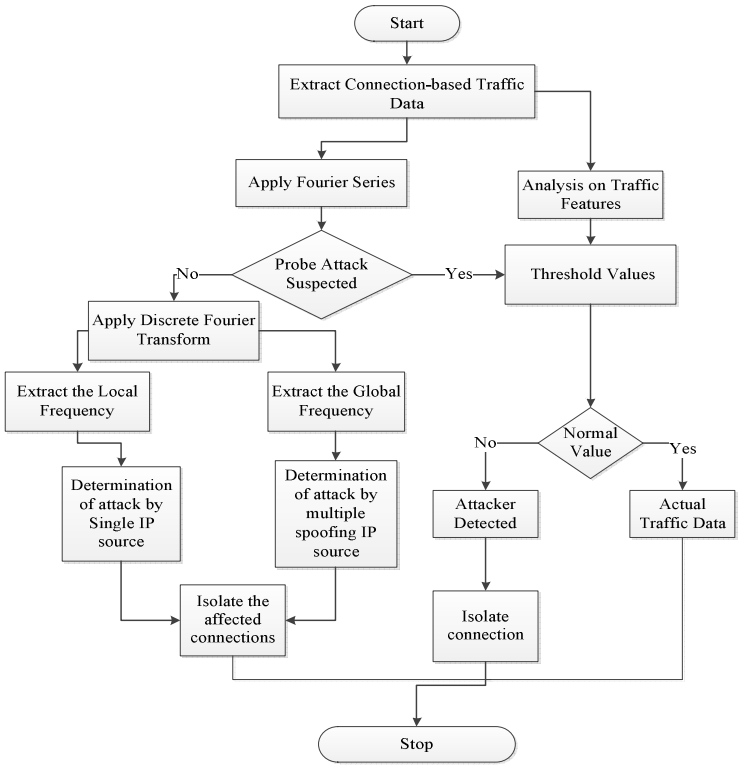

Figure 4.4: Flowchart of Algorithm

The In this work, traffic can be broken down into two distinct components, local data traffic and global data traffic. The IDS program executes as follows:

In the first step, various connection-based traffic data are extracted from the firewall in the given network. Now, the traffic data is converted into time-series using Fourier series and the average variance of packet sizes and the μ values is computed. From the different behavior of the Fourier series, probe attack can be detected during the initial stage. The Discrete Fourier Transform (DFT) is applied on the series of Local Data Traffic and Global Data Traffic. The application of DFT on the traffic extracts the frequency content available in both traffics and finally generates the Local and Global Frequency Patterns. In this work, the trace files are used to find the Suspicious IP by converting the time-based data series into frequency-base using DFT. The Local Frequency Patterns are used to find the attacks coming from a single IP source. Similarly, Global Frequency Pattern is used to find the attacks in multiple spoofing IP source line. In this system, we can find attacks coming from multiple connections. We can also prevent the attacks (from both single and multiple connections) by isolating the affected connections that were detected using Global and local frequency pattern through the connection history. This way, we can make the network free from attacks. Similarly, once the conversion takes place from the time domain into frequency patterns, the Frequency pattern (1) and Frequency pattern (2) are plotted and if the result showing is having a different frequency range from that of the normal frequency range set by the system for all nodes, then it means Suspicious attack is in either connection pattern 1 or 2 or both.

3.3. Application of DFT to Time-Series Sequence of Packet

Author Discrete value representing the time is expressed as *d(n)* for a given data sequence where $n \geq 0$. So the Discrete Fourier Transform (DFT) is chosen and applied to compute the frequency information. The DFT takes the original time series in the time domain, and transforms them into the associated frequency data in the frequency domain. Applying the DFT for the above time-series sequence, we get [14], [15]

$$F(k) = \sum_{n=0}^{N-1} d(n) W_N^{kn} \tag{3.1}$$

where

$$W_N = Exp(-j2\pi / N) \quad \text{For} \quad 0 \leq k \leq (N-1) \tag{3.2}$$

Hence

$$F(k) = \sum_{n=0}^{N-1} d(n) e^{-j2\pi kn / N} \tag{3.3}$$

Expanding the right hand side of equation (3.3), we have

$$F(k) = \sum_{n=0}^{N-1} d(n) \cos(2\pi kn / N) - j \sum_{n=0}^{N-1} d(n) \sin(2\pi kn / N) \tag{3.4}$$

where *N* is the total length of *d(n)*

However, applying equation (3.4) is time consuming for *N* samples of discrete values. Therefore, Fast Fourier Transform (FFT) procedure would be used to compute the frequency data *F(k)* in *O(n log n)* time. Which means FFT algorithm will speed up the computation process when frequency patterns are extracted from all incoming data traffic.

3.4. μ Value

The μ value is the threshold value set by the proposed algorithm to determine the average number of packets in each node. The threshold algorithms activate an alarm when a value deviates from its normal (expected) threshold value set by the system by some amount. This μ value is calculated each and every time for all nodes in the system. If the μvalue of a node is found to be abnormal, comparing to the other nodes in the network then it means an intruder has entered the network.

Let the packet size of the data be represented by *pack (j)* where '*j*' varies from 1 to *n*, and '*n*' is the number of packets within a connection. Then the μ value is considered as

$$\mu = \frac{1}{n} \sum_{i=1}^{n} pack(j) \tag{3.5}$$

Normally, if no attacker node is found in a network packet, delivery rate is high. If any intruder exists in the network, then the network will not allow forwarding packets to it. This brings down the packet delivery ratio automatically.

3.5. Average variance of packet size (Var_{avg})

The average variance, Var_{avg} of the packet size *pack* (*j*), for this work is given as follows:

$$\mathrm{Var}_{\mathrm{avg}} = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(\mathrm{pack(j)} - \mu)^2} \qquad (3.6)$$

Where, $1 \leq j \leq n$, and '*n*' is the number of packets within a connection.

The average variance of packet size Var_{avg} of an attacker packet is very small as compared to that of the normal traffic. This is because the goal of an attacker is to consume the network resources of the victim or to probe the information, and the payload of each packet is of a similar size since it is fabricated. This factor is used to detect the anomalies in the network.

Before communication can be established between two nodes a packet called control packet would be passed between the two nodes with the help of the hub. The control packet has a field called "Flag". If the "Flag" packet is missing in the received packets of this proposed centralized network, then an intruder has entered the network.

Once the system identifies an attacker node(s) in the network through our CTA-IDS the system automatically isolates the node(s) with the attacker packet by informing the nearby nodes with the help of the hub through the control packets. The system again will not allow the intruders to come inside the network.

3.6. Implementing the Intrusion Detection Strategy

Intrusion detection strategy is required for the implementation of this system. First, firewall is placed on the central device (Hub) to capture the network traffic data. The firewall has the database table of the recent connections within a specified time window. Each table entry contains an IP address that has been connected to the protected computer at least once within the time window. The traffic data of each connection is converted to a time series; the average variance of the packet sizes and the μ values are computed and recorded by the firewall. In addition, information about port connections are recorded which will be useful in detecting probe attacks. Finally, the firewall will report the suspicious IPs based on the observed frequency patterns, average variance of packet sizes and μ values. In the next section, we will describe the intrusion simulation framework using NS2, and report the simulation results evaluating the frequency-based intrusion detection strategies.

4. NS2 SIMULATION RESULTS

The following subsections are the simulated results for various network nodes. The results and analysis are as follows. The results indicate the traffic visualization and connection-based activities analysis of various network nodes in the form of frequency patterns. It is necessary to note that, the simulations in this work are implemented using NS2 version 2.35. DFT introduced in signal processing technique forms the basis of the algorithm for this simulation.

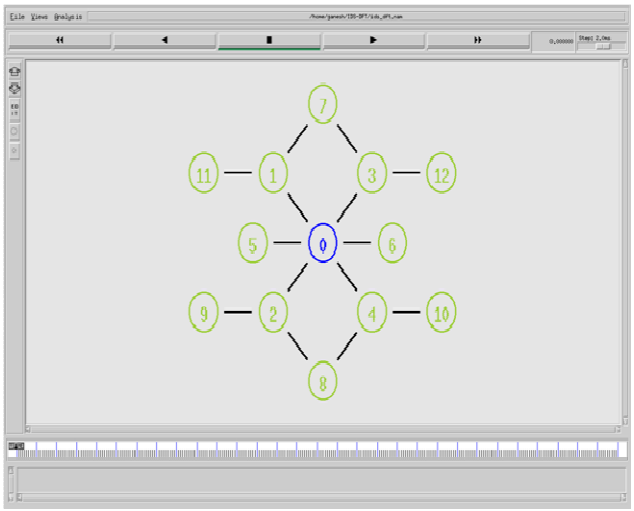

Figure 4.2: Formation of Network with Nodes

Here the 0th node is a HUB and the remaining nodes are addressable nodes that are used to assist the hub to transfer data in the network. A firewall and an intrusion detection algorithm are implemented inside the hub where network traffic would be monitored for suspicious activities

.

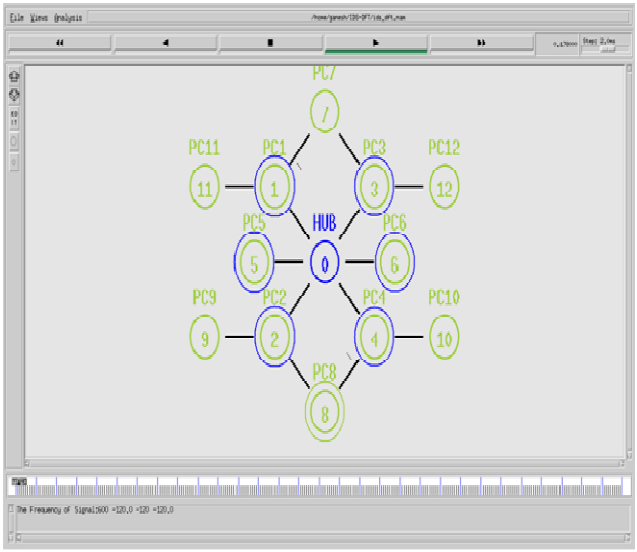

Figure 4.3: Data Transfer from the hub

The blue circles around nodes (1, 2, 3, 4, 5, and 6) indicate that frequency signal is generated during data transfer from the hub to the nodes as shown in Figure 4.3. From this signal, frequency pattern is generated.

Applying Discrete Time Series method, traffic data is converted to time-series data using the information at the connection history. Also DFT is applied to a time series data to create frequency data at the connection history and the frequency information for each node is then used for the frequency patterns.

4.1 Mew values and average variance of packet sizes for various connections

Connection	μ Values	Average Variance of Packet Sizes
Node 1	6	1.3656854249492381
Node 2	4	1.3120955864630133
Node 3	7	1.7191508225450298
Node 4	5	1.2292528739883946
Node 5	6	1.3656854249492381
Node 6	7	1.7191508225450298
Node 7	4038	0.3186765101345355
Node 8	3972	0.4375681123928461

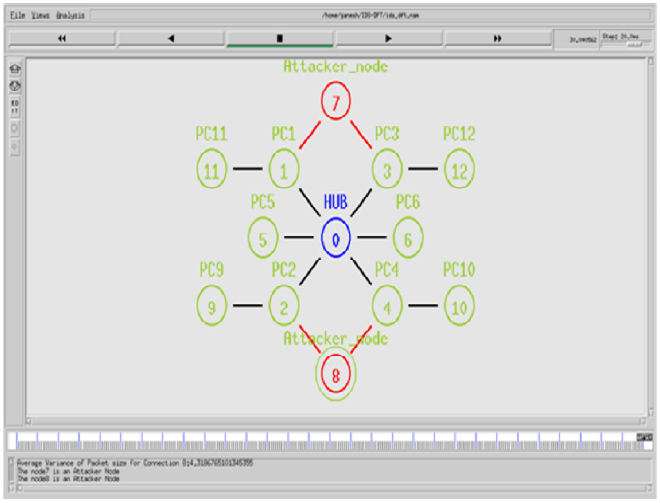

Figure 4.4: Identification of Attackers

While passing data from node 1 or 3 to node 7 and from node 2 or 4 to 8, attacker nodes were identified, indicated as red in Figure 4.4. The attacker nodes are found by using the μ values set by this system and the average variance of packet size for each node at the connection history. The mew value is a threshold value set for each node at some point in time in the system. These values can be seen in Table 4.1 below. From the connection history, node 7 and node 8 records mew values of 4038 and 3972 respectively and these are very large and above the normal threshold values of this system as seen in Table 4.1. The average variance of packet sizes for both nodes 7 and 8 are very small, and this can be considered as automated DOS attack.

Table 4.1 illustrates the μ values and average variance of packet sizes for the eight network connections scanned by the NS2 simulator with the proposed algorithm introduced in this work. Nodes 7 and 8 are identified as attacker nodes and disconnected by the algorithm. From the above table, it is clear that the mew values of connection 7 and 8 are abnormal and also the average variance of the packet size for both nodes is small enough to be considered as suspicious. Thus, connections 7 and 8 are likely to be automated attack traffic and these attack type is DOS attack.

4.2. Analysis of NS2 Simulation Results

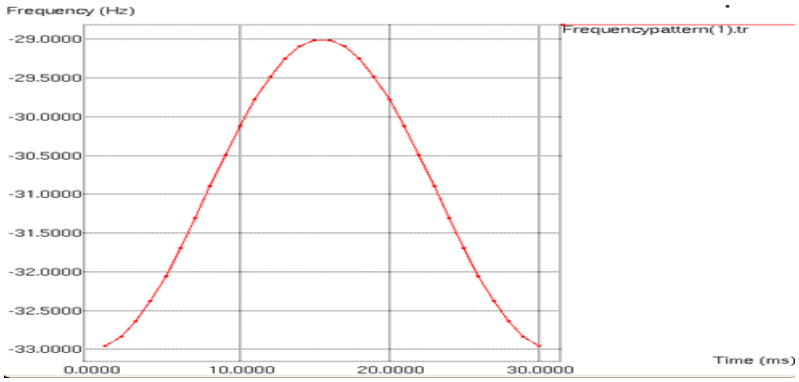

Figure 4.5: Frequency Pattern I

The frequency pattern for connection one is plotted in Figure 4.5. In this graph, there is a clear frequency pattern generated without any distortion. From the time 1.0 to 15.0, the frequency values are gradually increased from -33.0000 to -29.0000. From the time 15.0 to 16.0, we have a constant frequency value of -29.0000 and from the time 16.0 to 30.0, the frequency values are gradually decreased from -29.0000 to -33.0000. The normal frequency range set by this system as a reference for all nodes is between -45.0000 and -17.0000. Hence, since this graph is generated within the normal range as shown in the Y-axis, it means that there is no attacker packet in this node. This can be confirmed by comparing the μ value and the average variance of packet size of node 1 to that of nodes 7 and 8 which have the abnormal values as shown in Table 4.1 above. The concept of the negative frequency on this graph at the Y-axis is used for mathematical calculation only and it gives the frequency spectra in the negative domain which helps to analyze real signal using a complex number framework. A complex number can only be real if added to its conjugate [16], hence the negative frequency comes from a representation using the sum of complex exponential values for the DFT variables.

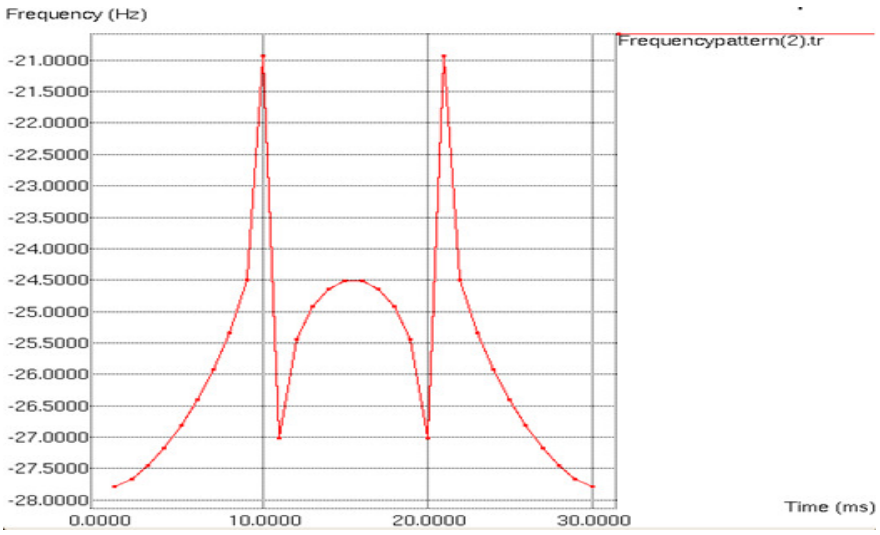

Figure 4.6: Frequency Pattern II

Figure 4.6 shows the frequency pattern for node 2 in the connection history. It can be seen that the frequency pattern of this graph looks different as compared to the graph in Figure 4.5 and the reason being that, activities at the various network nodes differ from each other and this generate different patterns. In this graph, the frequency range is set between -28.0000 and -21.0000 as illustrated in the Y-axis. This frequency range falls within the normal range and therefore concludes that node 2 does not have any malicious packets. Table 4.1 provides the μ value and the average variance of packet size for connection two as 4 and 1.3120955864630133 respectively.

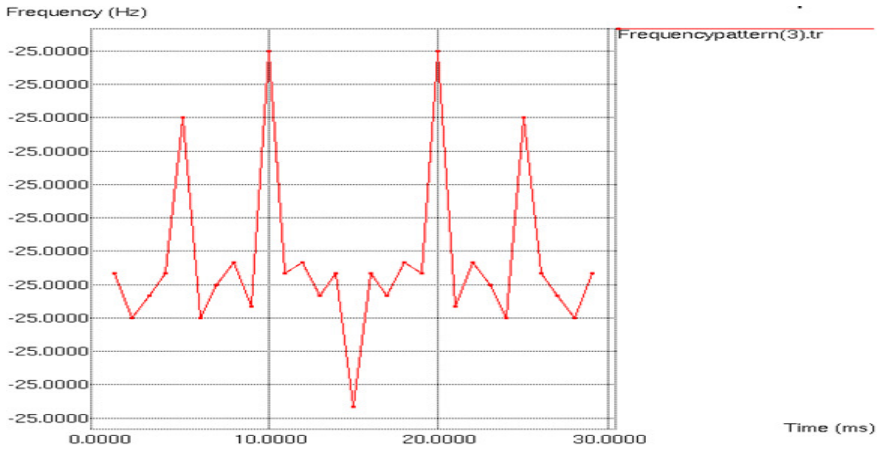

Figure 4.7: Frequency Pattern III

The third frequency pattern for node 3 is plotted in Figure 4.7. It has a distinctive frequency pattern but the frequency range is set between -25.0000 and -24.9999. The frequency range seems to be very close but in the data file (which is not showing in this report) for the graph, the frequency values are different at each point. The frequency values are in the form of fifteen decimal places which cannot be exhibited at the Y-axis of the graph hence rounded off. This format generated by the simulation helps the accuracy and precision in order to eliminate false alarm rate during detection process. The frequency range has created frequency pattern with similar frequencies in legitimate traffic due to traffic data broadcast to lists of its subnet machines periodically. The μ value recorded at the connection history is 7 and the average variance of packet size is 1.7191508225450298. This shows that node 3 is not having any malicious content.

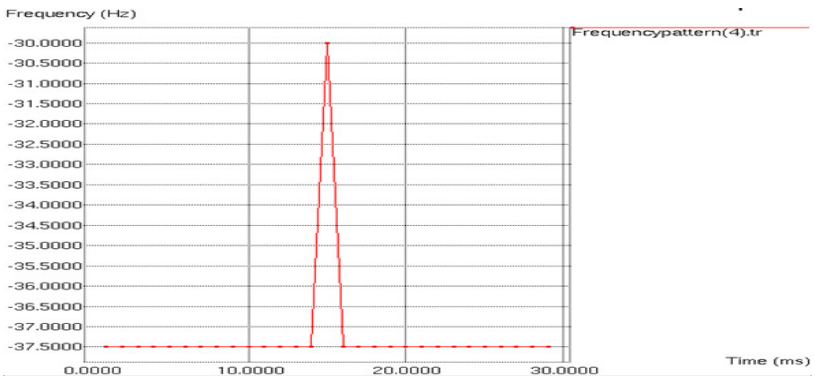

Figure 4.8: Frequency Pattern IV

The fourth frequency pattern for node 4 is plotted in Figure 4.8. From the time 1.0 to 14.0, we have a constant frequency value of -37.5000. From the time 14.0 to 16.0, the frequency values are gradually increased and decreased from -37.5000 to -30.0000 and from the time 16.0 to 30.0, we have a constant frequency value of -37.5000. The frequency range of this graph is -37.5000 and -30.0000 and this range is considered to be in a normal range. The μ value and the average variance of packet size for node 4 in the connection history are 5 and 1.2292528739883946 respectively as seen in Table 4.1.This node is having only legitimate data and does not have any attacker packets.

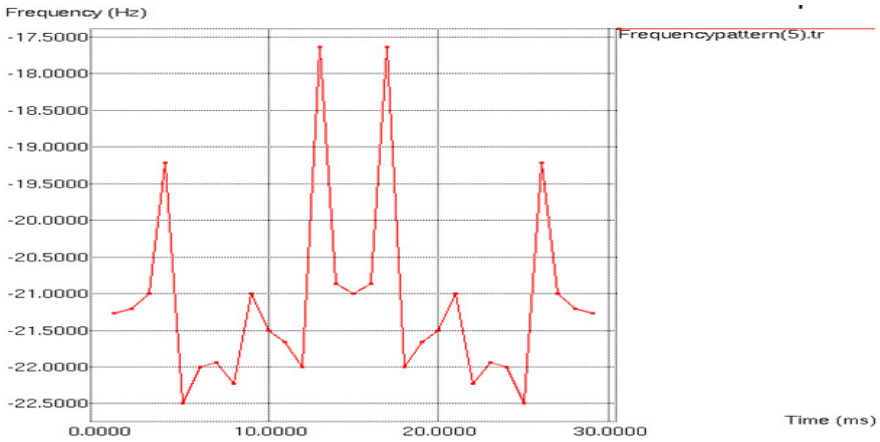

Figure 4.9: Frequency Pattern V

Figure 4.9 illustrates the frequency pattern for node 5 in the connection history. Here the frequency pattern is distinct from the one in Figure 4.8 but its frequencies are in the range between -22.5000 and -17.5000, which falls within the acceptable range. The μ value and the average variance of packet size for connection five is shown in Table 4.1 and when these values are compared to the abnormal values of nodes 7 and 8 we can conclude that node 5does not have any malicious content to collapse the network.

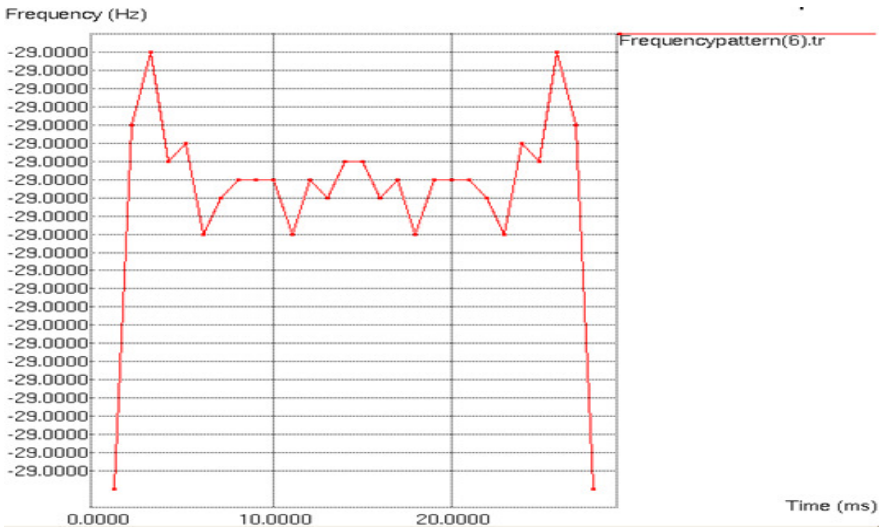

Figure 4.10: Frequency Pattern VI

The frequency pattern for node 6 in Figure 4.10 is also different from the other frequency patterns in the above Figures. In this node traffic data is broadcast to lists of its subnet machines periodically similar to the one in Figure 4.7. The frequency range of this graph is between -29.0000 and -28.9999 and it falls within the reference frequency range which declares node 6 to be free from attacker packets. This is confirmed by considering the mew value and the average variance of packet size in Table 4.1.

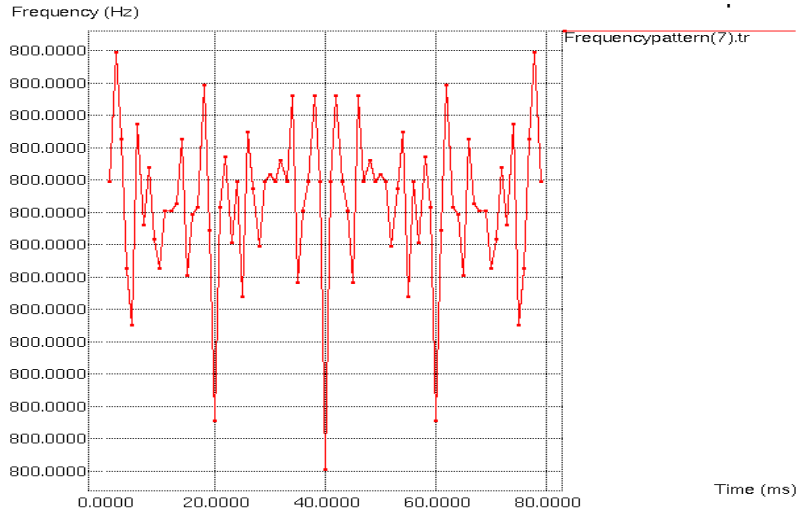

Figure 4.11: Frequency Pattern VII

In this connection, it is observed that the frequency pattern and the frequency range shown in Figure 4.11 are distinct from all the above graphs. The frequency range for this node is between -800.0000and -799.0000 and it is out of the normal frequency range for this system which is between -45.0000 and -17.0000. Again, the μ value for node 7 in the connection history is 4038 and is above the normal threshold values set by the system by some amount. This mew value is abnormal as compared to the μ values of node 1 to node 6 as shown in Table 4.1. The average variance of packet size is 0.3186765101345355 which is too small and satisfies the condition of attacker packet for DOS attack. This can be considered as an automated and scripted attack demonstrates the occurrence of an intruder.

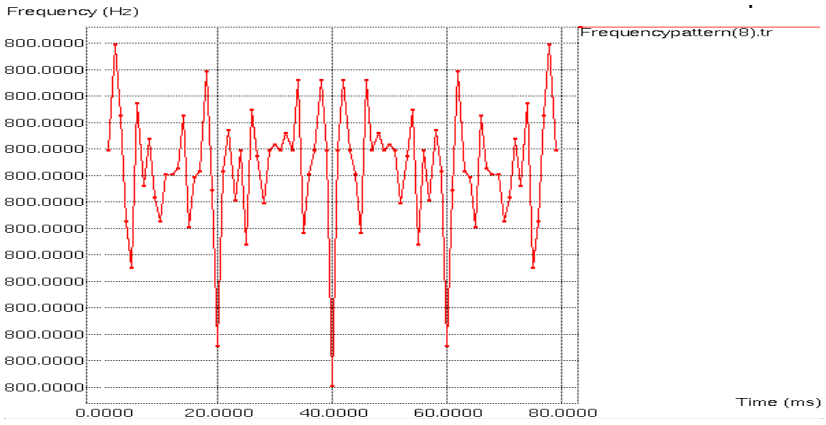

Figure 4.12: Frequency Pattern VIII

Connection eight is also having almost the same abnormalities as connection seven and it is identified as an attacker node. Figure 4.12 demonstrates the frequency pattern of node 8 and the frequency range for this node is between -800.0000 and -799.0000 as shown in the Y-axis of the above graph. It is observed that frequency range for node 8 is out of the normal frequency range for this system. The μ value and the average variance of packet size of connection eight is 3972 and 0.4375681123928461 respectively and these values are considered as anomalous.

3. CONCLUSIONS AND FUTURE WORKS

This paper focused on frequency-based intrusion detection approach to detect Denied of Service (DOS) attack in a virtual network system setup in NS2 simulator. The frequency-based approach looks for periodicity patterns in the time-series created by the traffic flow using Discrete Fourier Transform (DFT). A Centralized Traffic Analyzer Intrusion Detection System called CTA-IDS was introduced to further detect the intrusion accurately inside a network with fewer false alarm due to accurate threshold values set by the system. The strategy is able to detect abnormal content in the traffic data, known attack signature and unknown attack. This approach is tested by running the artificial network intrusion data in simulated networks using the Network Simulator2 (NS2) software.

The experimental results demonstrated that the nodes with malicious packets were out of the normal frequency range set for this system. The idea behind this frequency pattern analysis is that the traffic with constant Inter-arrival time is generated by the coded automated DOS attacks which need many packets to finish a subtask in a repeated attack process.

The three levels of detection mechanisms; the frequency pattern, the μ value, and the average variance of packet size reduce or eliminate the false alarm rate during detection process.
This frequency-based detection algorithm is recommended for DOS and Probe attacks only. The future work will be extended to other types of intrusion attacks and finally be tested on a real environment to confirm the effectiveness of this technique.

REFERENCES

[1] Incasula 2013-2014 DDOS Threat Landscape Report, http://www.imperva.com/docs/RPT_2013-2014_ddos_threat_ landscape.pdf, accessed on 17 September2014 @ 3:05pm

[2] The Global Initiative Against Transnational Organized Crime, “Cybercrime and the Private Sector” http://www.globalinitiative.net/programs/cybercrime/ cybercrime-and-the-private-sector/, accessed on 10 July 2014 @ 11:34pm GMT

[3] S. Durbin, “The CIO's Secret Weapon: Stakeholder Pressure”, http://www .cioinsight.com/it-management/expert-voices/the-cios-secret-weapon-stakeholder-pressure.html, accessed on 13 December 2014 @ 6:42pm GMT

[4] S. Kumar, “Survey of Current Network Intrusion Detection Techniques”, http://www.cse.wustl.edu/~jain/cse571-07/ftp/ids.pdf, accessed on 11thDecember 2014

[5] W. Lee, S. J. Stolfo, K. W. Mok, “Mining in a Data-flow Environment: Experience in Network Intrusion Detection”, Proceedings of the Fifth International Conference on Knowledge Discovery and Data Mining (KDD), ACM 1999.

[6] W. Lee, S. Stolfo, “Adaptive Intrusion Detection: a Data Mining Approach”, Artificial Intelligence Review, 2000.

[7] D. Barbara, et al., “ADAM: A testbed for exploring the Use of Data Mining in Intrusion Detection”, SIGMOD Record 2001.

[8] S. Bridges, R. Vaughn, “Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection”, NISSC 2000.

[9] C. Sinclair, L. Pierce, S.Marzner, “An Application of Machine learning to Network Intrusion Detection”, Proceedings of the 15th Annual Computer Security Applications Conference 1999

[10] X. Li, N. Ye, "Decision tree classifiers for computer intrusion detection", Real-time system security, ACM 2003.
[11] J. Ross Quinlan. C4.5 Programs for Machine Learning Morgan Kaufmann Publishers, San Mateo, CA 1993
[12] A. K. Ghosh, A. Schwartzbard, "A Study in Using Neural networks for Anomaly and Misuse Detection", Ghosh, 1999.
[13] J. Ryan, M. Lin, "Intrusion Detection with Neural networks", NIPS, 1998
[14] K. Kawagoe and Tomohiro Ueda, "A similarity search method of Time series data with combination of Fourier and wavelet Transforms", IEEE TIME'02, 2002.
[15] S. Sharma, "Digital Signal Processing" for 6th Semester B. Tech Students of Punjab Technical University, Jalandhar, 2008
[16] http://www.researchgate.net/post/Can_anyone_explain_the_concept_of_ negative_frequency, accessed on 11February 2015 @ 1:21pm GMT