International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

DDOS Attack Detection using DFT Based Signal Processing Approach

Parneet Kaur[1], Abhinav Bhandari[2]
[1]*M.tech Scholar,* [2]*Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala*

Abstract: Distributed Denial of Service (DDoS) attacks are the perennial upheavals over the Internet. Numerous DDoS attacks defending contraptions have been posited in the liberal arts but yet such assaults are surging year by year. In this paper, we instigate a detection technique that is hinged on DFT (Discrete Fourier Transformation) based signal processing technique. Through flow based assay the various parameters (Meu value, packet size variance and entropy) for each connection of network traffic are scrutinized. If the difference between above parameters and their corresponding mean values exceeds the threshold value, the attacks are recognised. Our detection mechanism analyse both the local and the global data traffic efficiently and effectively with high detection accuracy and no false alarms. Beside these, the last phase of the proposed strategy isolates the malicious nodes.

Keywords: Discrete Fourier Transformation, signal processing, entropy and DDoS attacks

I. INTRODUCTION

The dependence on Internet has been increased with the increasing number of Internet users and the online services. In the last decade due to the rapid growth of network associations and online service receptiveness, network attacks have resulted in huge amount of cost damage [1]. That is why; the security of the network system is a major concern. Pre-eminently, the dilemma of the detection of DDoS attacks is to the fore impedance. Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks knock off the online services inaccessible to the expected users or degrade the quality of service. DDoS attacks make use of a large number of remote machines (bots or zombies) to interrupt network services or to attack on a particular node of the network system [2]. One good example of DDoS attack that stumbled on Moscow stock exchange [3] is a cracking DDoS attack in a blended form (SYN + TCP Connect + HTTP-flood + UDP flood) with its multi-vector nature in coalition with passably low power (3 Gbps). It was said that in order to tackle such complex attacks, the latest DDoS protection channels are needed because the network security agencies are unable to trail the emergence of the attack in a very short duration with high accuracy.

Network attacks site the arbitrary conjured data packs to the victim node (or system) so that its resources are dissipated. Due to the presence of such situations, the network communities have flourished competent detection and traceback schemes. But instead of these protection mechanisms, the DDoS attacks are still escalating year by year [4].

The main contribution of this paper is as follow:

A. We have plied the Discrete Fourier Transformation (DFT) based signal processing technique in NS2 simulator to represent the frequency motifs in order to detect the DDoS attacks with sky-high detection accuracy and no faulty alarms.

B. We have developed a better technique based on three parameters: entropy, average variance and meu value that handle the local and global traffic separately and isolate the affected connections.

C. Our paper gives the identification of the attacker node while the base paper [1] does not.

The rest of the paper consists of the following sections: Section 2 highlights the existing literature in the field of detection of DDoS attacks. Section 3 introduces the proposed the new detection methodology. Section 4 gives a view of simulation environment through experiment setup and results. Finally, section 5 discuss some issues and concludes the paper.

II. RELATED WORK AND BACKGROUND

Basically, the detection approaches are catalogued into two classes: Pattern-based detection and Signature-based detection. The former class refers to the detection procedures in which the attacks patterns are stashed in a database and are likened with the futuristic attack forms. Then the later class mirrors a benign behaviour model in which if the incoming data instances diverge from the predefined threshold, an attack is detected [5]. Our proffer technique plunges into anomaly-based detection system. Most of the

detection methods have used the IP address for detection purpose, but this parameter is not abundant enough. Our approach relies on entropy calculation along with the new parameters like average variance and meu value.

There are some related publications that have proposed the detection techniques with signal processing. Petropulu et al. [6] has enrapt on stirring an advance span of signal processing to scrutinize the network traffic over the Internet. Barford et al. [7] delineate an effectual mode to bare anomalies with the detection procedure that results in high local variance in case of affected IP flow data. Chen and Hwang [8] has proposed a collaborative character-based detection technique that have used DFT hinged autocorrelation function for seeping the ogress DDoS attack flux from normal flows. Nychis et al. [9] ensue a PCA algorithm using entropy based metrics to unmask the network quirks with low false positives, early and high detection accuracy. Wang et al. [10] postulate a clustering based detection mode that reckons the correlative entropy for new specimens to riddle the cynical bouts. Devi and Yogesh [11] instigate an entropy based detection framework in which the HTTP plea rate, page deeming estimates and supplicated a string of entities and their disposition is kept an eye on in order to assess the entropy of arising requests. If the computed entropy overreaches the threshold and the request rate goes up from the presumed tally, the spell is viewed as acrimonious. David et al. [1] discuss the Fast Entropy and flow based analysis mechanism for the detection of DDoS attacks. In this paper, the author shows the significance reduction in computation time and also achieves good detection accuracy using proposed method. The author suggests the IP traceback mechanism that can further improve the detection accuracy as it helps out to find out the attacker in the system. Also, the effective monitoring with dynamic threshold to check the flow rate of packets can further enhance the detection accuracy of the existing system. The proposed work will be implemented using a suitable platform or simulator.

III. DESCRIPTION OF PROPOSED METHODOLOGY

The proposed methodology consists of a DFT technique to model an algorithm for DDOS attacks. DFT is used in order to generate frequency pattern which is used to identify attack and decrease the rate of fault alarm. Frequency based method is specially designed for DDOS detection. Network simulator 2 is event driven simulator that is used to study dynamic computer or communication network.

A. Signal Processing

DFT is used to transform the signals between time and frequency, this method is called signal processing. The time and frequency series data are converted into time and frequency domain using DFT.

1) *Definition 1: Meu Value:* The meu value is the threshold which is used for our proposed algorithm to compute the average of number of packets for each connection. This threshold value starts generating an alarm when the value of a connection deviates from its threshold value. This meu value is computed for each node, if this value represents major changes in contrast with other nodes it represents that the attacker has attacked the network. Let n be the number of connection and k be the number of packets for each i^{th} connection. The meu value is represented as:

$$U = \frac{1}{n}\sum_{i=1}^{n} packet\ (k)$$

2) *Definition 2: Average Variance:* Normally, when there is no attack on the network the PDR (Packet Delivery Ratio) is high. This PDR value drops down significantly during attack which is represented by average packet variance. Let the packet size is represented by (k) which varies from 1 to n and the average variance is represented as:

$$Variance_{Avg} = \frac{1}{n}\sum_{i=1}^{n} \sqrt{(packet(k) - U)^2}$$

3) *Definition 3: Entropy:* Entropy demarcates the randomness in the nexus packets. Higher variability steers to high value of entropy. Fast entropy for each flow count is assessed for each network association. In normal data runs, the entropy remnants in a tenacious range but in case of attack flows, the entropy revamps enormously. Let an arbitrary variable $f_{(i,t)}$ depict the flow count of a distinct connection i over a given time span t. The entropy for a peculiar flow count of each link is calibrated as follow:

$$E^{n}_{(i,t)} = -log\ \frac{f_{(i,t)}}{\sum_{i=1}^{n} f_{(i,t)}} + \tau_{(i,t)}$$

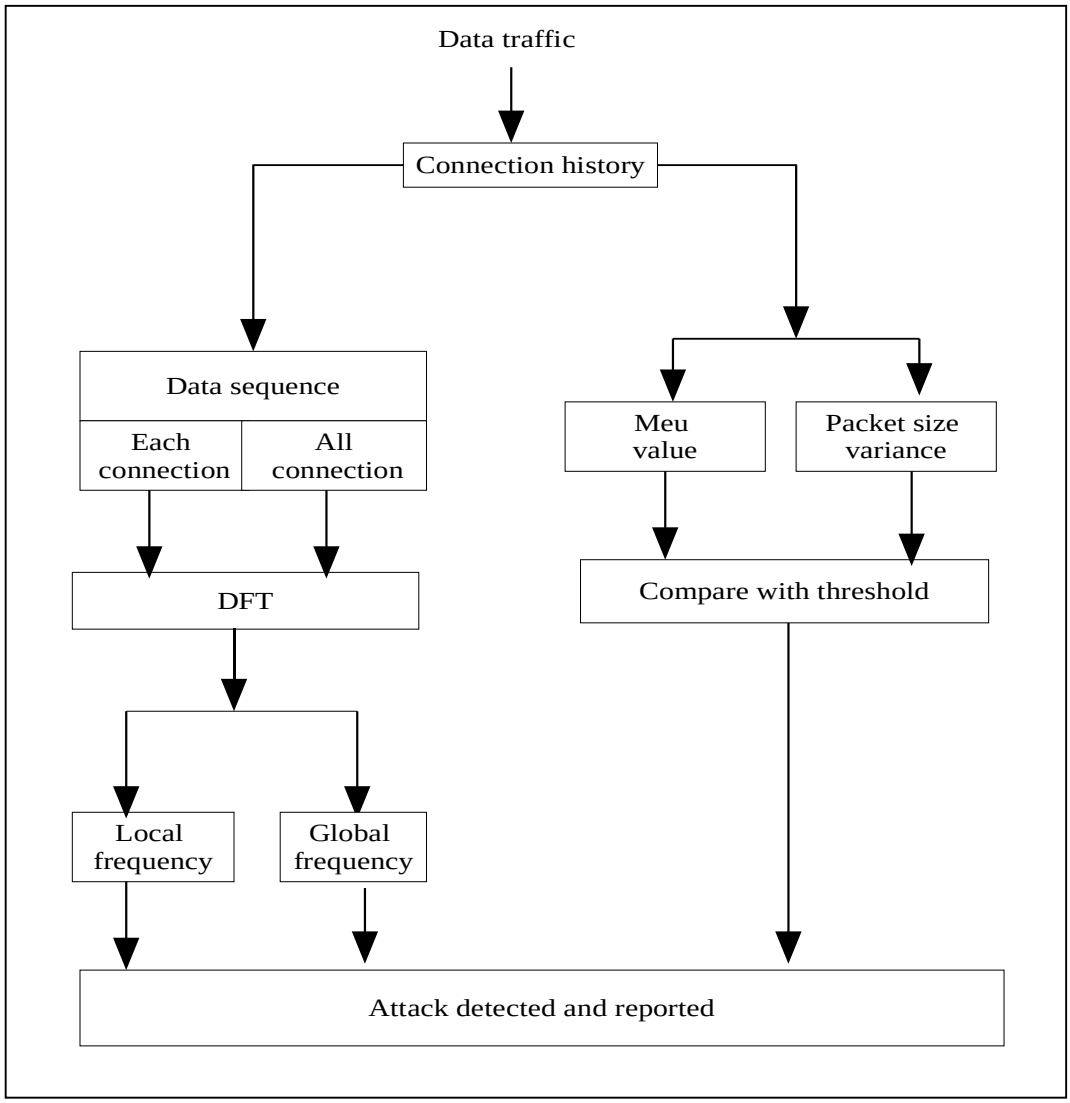
where,

$$\tau_{(i,t)} = \begin{cases} \left| log \frac{f_{(i,t+1)}}{f_{(i,t)}} \right|, & f_{(i,t)} \geq f_{(i,t+1)} \\ \left| log \frac{f_{(i,t)}}{f_{(i,t+1)}} \right|, & f_{(i,t)} < f_{(i,t+1)} \end{cases}$$

t – Time Interval
i – Flow Connection
E – Fast Entropy

B. Detection Method

In first step, the history of connections would be maintained for all new nodes connections that are coming from new IP and the trace back mechanism is used to record the packet size, inter-arrival time and the packets rate per unit time within or among the nodes connection. In second step, considering the abundant amount of data, compressed time-series is used to boost the process of next step analysis. Third, DFT would be applied to the time-series data generated to collect frequency information.



Both local and global frequencies are computed in this step using DFT. Finally, by applying the Fourier analysis to the time-series created by network traffic signal, the periodicity pattern that may exist in the network traffic would be identified.

C. *Network Connection History*

In this work, a network connection has all network traffic (packets) sent between two nodes which has following properties:

1) Two numbers of Source and destination IP addresses.
2) Single or multiple protocols can be used for connections at different time.

In the proposed work, the data traffic is broken down into two different components, local and global data traffic. Then the traffic data is changed into time-series using DFT to compute the data packets variance size and meu value. Then from the different behaviour attack can be detected. In this proposed work a trace file in ns2 is also used to find malicious IP by changing time based series into frequency using DFT. We can also detect attacks coming from multiple connections. These attacks can be prevented by isolating the nodes which are detected by global and local frequency connection history.

The average packet variance is miniature in contrast with ordinary data queue. Before connection set up between two apexes, a packet called Hello Packet is swapped among nodes. This packet has a field called flag. If this flag is not present, the packet arrives from attacker nodes. The malicious nodes are detected by using meu value (*U*) and other factors and no exchange is done with these nodes.

IV. EXPERIMENT AND RESULTS INTRODUCTION

This section evaluates the effectiveness and efficiency of the proposed DDoS detection strategy basen on DFT based signal processing with a traceback mechanism. The new strategy is based on flow based analysis which requires the information as packet size, inter-arrival time and the packets rate per unit time within or among the nodes connection.

As shown in Figure: the connections C7, C8, C9 and C10 have the large meu value than the normal value of other connections. Here Instead of analysing single parameter, we have

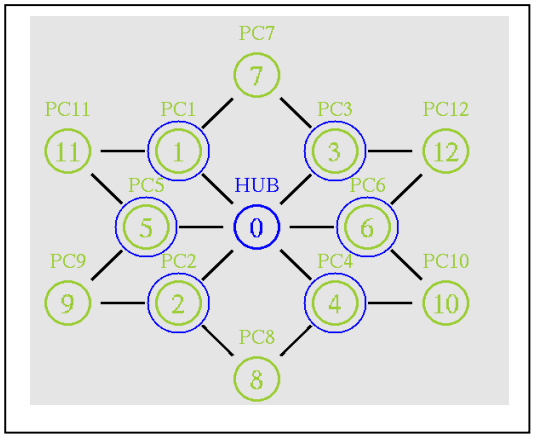


Figure 2: Network topology used for simulation

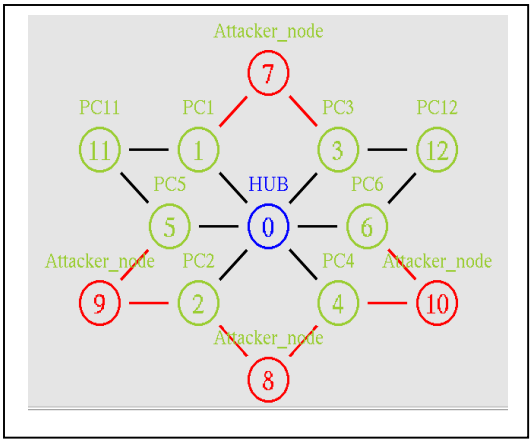


Figure 3: Detection and traceback mechanism

evaluated the experiment for three different parameters. Therefore, there is a significant change in the packets size variance and the entropy value of the attack nodes form the normal connection node. The use of accumulated parameters rather than a single parameter increase the detection accuracy and decrease the chances of fault alarms. At last a traceback mechanism is used for detection of attack node. In the above experiment, node 7, node 8, node 9 and node 10 are detected as malicious node.

Table 1 The values of different parameters for each connection

Connection	Mue value	Average Variance of Packet size for each connection	Entropy
C1	6	1.3656854249492381	0.362134
C2	7	1.7191508225450298	0.346574

C3	4	1.3120955864630133	0.362134
C4	5	1.2292528739883946	0.360599
C5	6	1.3656854249492381	0.362134
C6	4	1.3120955864630133	0.359030
C7	4038	4.3186765101345355	0.054196
C8	4038	4.3186765101345355	0.048428
C9	4038	4.3186765101345355	0.046459
C10	4038	4.3186765101345355	0.040704

V. DISCUSSION AND CONCLUSION

We proffer a coherent DDoS attack detection tack wielding DFT based signal processing technique. The meu value, packet size variance and entropy are figured for each connection at specific time span. From the consideration, it is evident that these variables are illustriously tweaked for discrete point connection at distinct interims. DDoS attack is revealed, when the difference between the above criterion and their mean values overreach the threshold value. Moreover, the dearth of Hello packet assists to the handiness of espying the assailant vertices of the network. Hence, our propounded stratagem has stated a DDoS detection procedure along with traceback efficiency with high detection accuracy and no false alarm rate. It is a better technique with local and global detection and for the isolation of malicious nodes.

REFERENCES

[1] J. David and C. Thomas, "DDoS attack detection using fast entropy approach on flow-based network traffic," *Procedia Computer Science*, vol. 50, pp. 30-36, 2015.
[2] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, 2016.
[3] Khalimonenko and O. Kupreev, 11 May 2017. [Online]. Available: https://securelist.com/ddos-attacks-in-q1-2017/78285/. [Accessed 10 July 2017].
[4] A. Bhandari, A. Sangal and K. Kumar, "Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks," *International Journal of Computer Network and Information Security*, vol. 7, no. 8, p. 9, 2015.
[5] M. Alenezi and M. J. Reed, "Methodologies for detecting DoS/DDoS attacks against network servers," 2012.
[6] A. Petropulu and R. Nowak, "Signal processing for networking [Guest Editorial]," *IEEE Signal Processing Magazine*, vol. 19, no. 3, pp. 12-13, 2002.
[7] P. Barford, J. Kline, D. Plonka and A. Ron, "A signal analysis of network traffic anomalies," in *ACM*, 2002
[8] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1137-1151, 2006.
[9] G. Nychis, V. Sekar, D. G. Andersen, H. Kim and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *ACM*, 2008.
[10] J. Wang, R. C.-W. Phan, J. N. Whitley and D. J. Parish, "Augmented attack tree modeling of distributed denial of services and tree based attack detection method," in *IEEE*, 2010.
[11] S. R. Devi and P. Yogesh, "Detection of application layer DDoS attacks using information theory based metrics," *CS & IT-CSCP*, vol. 10, 2012.