IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 11 November, 2016

NEW TECHNIQUE TO DETECT DDoS ATTACK

Author: V.PRAVEENA[1];S.SRIKAMALESH[2];S.SRUTHI[3];R PRIYANGA[4]
SNS college of Technology, Coimbatore, Tamilnadu.
veenasri158@gmail.com,srikamalesh05@gmail.com

ABSTRACT

Internet and Computers have evolved into indispensable implements for our personal, convivial lives and professional. As the result of growing simplicity and availability in this systems has become a concern. In this concern exponential are increases when considering systems such as public utility accommodations and keenly intellective power grids. Consequently, research should be conducted to develop efficacious ways of detecting system anomalies. Denial of Service(DOS) accommodation assailment's are a most consequential difficulty for a communication systems. Novel DDoS detection approach: Cusum Entropy is utilized along with the client puzzle technique in the ingress side router which reduces the network traffic. It performs additional signal processing on the entropy of the packet header field to increase our detection efficiency. We tested our approach without using jeopardizing operation network. In our result showed gives high deduction and low false positive rates. The main advantage of the proposed system is that network traffic is reduced which in turn reduces the network overhead.

Keywords: DDoS,Entropy,Cusum, VoIP,Tcp

1. INTRODUCTION

Denial of Service (DOS) assailments are a most consequential quandary for a communication systems. A DDoS attack incapacitates network accommodations for legitimate users. The number of flooding DDoS attacks in . 10 Gbps range have increase significantly and highest bandwidth are observed for a single attack has reached 300 Gbps.

Physically, damaging consuming resources and network components. It performed by altering the configuration files of compromised nodes. It used generally two categories; susceptibility attacks and flooding attack. In this assailment mainly perform, zombies send dummy traffic/requests to the victim at the assailants command. CUSUM algorithm on entropy for used observe network traffic after a pre-filtering stage by utilizing a wavelet filter. CUSUM and wavelet filtering are amend the detection performance.

2. LITERATURE SURVEY

When a particular message or an image is sent from the client, the image is sent automatically to the client browser and then the user want to decode them, it decodes and send a request and image to the server that has been requested. It takes long process to arrange the images. It is used to solve at

difficult levels. The user must want to solve the image and want to arrange to form a complete image. Its takes long time process. So, the user cannot send the multiple request to servers. While the client puzzle protocol is placed in between it avoids the continuous requests from the client and hence the server failure will not occur and hence it increases the efficiency. In these time, server cannot be down by sending multiple requests. Bandwidth of server can be increased.Once the client accessed the puzzle the Cusum entropy will collect all the information of the puzzle and wavelet will filter the request sent by the attacker.

A INFORMATION-THEORETIC MEASURES FOR ANOMALY DETECTION

Anomaly detection is an essential component of the bulwark mechanisms against novel attacks. These can be divide entropy several methods. Anomaly it utilizes information-theoretic measures, namely, entropy, conditional entropy, relative conditional entropy, information gain, and information cost for anomaly detection among them condition entropy is used. The condition entropy method is used to describethe characteristics information about observed data. In this anomaly observe that on Unix system call data, BSM data, and network TCP dump data to illustrate the utilities of these quantifications.

B TRAFFIC ANOMALY DIAGNOSIS IN INTERNET BACKBONE NETWORKS:

This paper we investigated that the current state of the art of DDoS attack within the network anomaly diagnosis domain for Internet data backbone networks. It used to dehydrate the overall anomaly diagnosis detection problem spectrum divided into four main dimensions, namely, processing costs, diagnosis granularity, theoretical methodologies and traffic features. The anomaly diagnosis area is structured further and an overview of the most pertinent research is provided by individually reviewing each component of the quandary spectrum and proposed solutions with a deeper fixate on methodologies and features. Therefore, we additionally present a review seminal pieces of work. Which are considered key for the detection of anomaly diagnosis in the research domain. These is used to collect information about false information.

C EARLY DOS/DDOS DETECTION METHOD USING SHORT-TERM STATISTICS

Early DoS/DDoS detection method is used to predicate the short-term entropy fixating on the early DDoS detection attacks. In these we have to calculate the window width size to identify the false data. These can be used to give details about types of attacks. And, they generated pseudo attacking packets. The window width is generated by elapsed time. Here it engendered the pseudo assailing packets under a mundane condition to calculate the entropy and carry out a test of paramount. When the number of assailing packets is is equal to the number of arriving packets the high detection results with Erroneous-negative.

D OPEN FLOW: ENABLING INNOVATION IN CAMPUS NETWORKS

Open Flow is predicated on an Ethernet switch with an internal flow-table.it gives a standardized interface to integrate and abstract flow ingressions. Network administrator can be used to partition traffic into production and research purposes. It

helps the researchers to run experiments on heterogeneous switches (Ethernet switch) in a uniform way at line-rate and with high port-density. But vendors do not require to expose the internal workings of their switches

III EXISTING SYSTEM

In Subsisting system, Web application form an ecumenical podium for network accommodations. Dos detection can be divided into two different categories types: signature detection and anomaly detection. Signature detection compares network traffic and Anomaly detection the detector use network traffic by statistical feature such as entropy of incoming packet source IP addresses. Anomaly detectors have a higher mendacious positive rate than signature detectors.

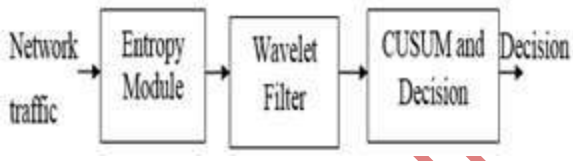

Fig 1: Overview of Existing System

A CUSUM – ENTROPY

Entropy measures the amount of disorder information in the observed data in the DDoS. Entropies of packet header fields; such as source/destination IP address, and protocol type would have been changed during DDoS attacks. The entropy change during an attack varies based on observed packet header field. While the entropy of the source IP addresses increases during a DDoS attack, it causes destination IP address entropy to decrement.

B WAVELET

The wavelet transform analyzes an input signal simultaneously in the time and frequency domains. Haar wavelet coefficients are calculated by averaging and differencing two data values. Averaging gives about the low-pass, and differencing provides the high-pass signal characteristics. Additionally, the coefficient obtained by differencing represents the average amount of signal change between two samples Wavelet Decomposition Level (WDL). Wavelet to filter out the long term variations of the observed entropy values to reduce the number of mendacious alarms. Then the filtered signal is alimented into a CUSUM algorithm for detection.

C CUMULATIVE SUM

The cusum algorithm is utilized to detect extreme increases obnubilated in bursty background data. Their method calculates the difference between the current and long-term average of the observations. If the current average increases more expeditious than long-term average, the cusum coefficient additionally increases. The cusum coefficient goes back to zero when the distinction between two averages is minute. When the cusum coefficient exceeds the called threshold, it denotes an entropy increase which may be caused by a DDoS attack.

D CUSUM ENTROPY- ALGORITHM

The entropy module calculates the entropy of a packet header field from the packets in an observation window. To calculate entropy of the source IP address; unique source IP addresses and number of occurrence of these IP addresses in the

observation window are resolute. The probability of observing a source IP address in the observation window is calculated by dividing the number of times the source IP address was observed by the total number of observations. After calculating all unique source IP address probabilities, we calculated the entropy of the observation window utilizing and normalized entropy utilizing. Wavelet filter is utilized to filter out long term trends of entropy data, which leads to a very impecunious performance of CUSUM algorithm. The entropy data is decomposed into its high-pass and low-pass components. Then the signal was reconstructed to get filtered entropy data. An entropy time-series with three DDoS attack afore and after the wavelet filter is utilized.

IV PROPOSED METHODOLOGY

In anomaly DDoS detection, detectors calculate the deviation of the observed statistical features from background traffic statistics to infer anomalies. Ergo, we have increases the performance of the detection approach utilizing operational background traffic and performing DDoS attacks without jeopardizing the pristine network. We observed the entropy of source IP address in non-overlapping time windows. These observations are preserved with timestamps to engender source IP address time entropy series.

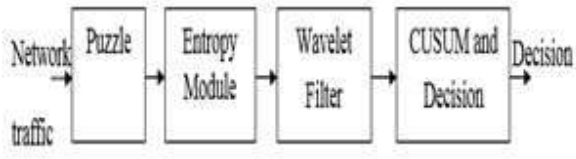

Fig 2: Client Puzzle Protocols

In the Client Server architecture, a client puzzle protocol is set as a middleware between them for the purpose of sending the client request to the server, when the continuous requests are sent from client to server it reduces the server response because of the too many request from the client. The server will send puzzle, attacker must want to encode the puzzle provided by server. The server will decode the puzzle submitted by the attacker.

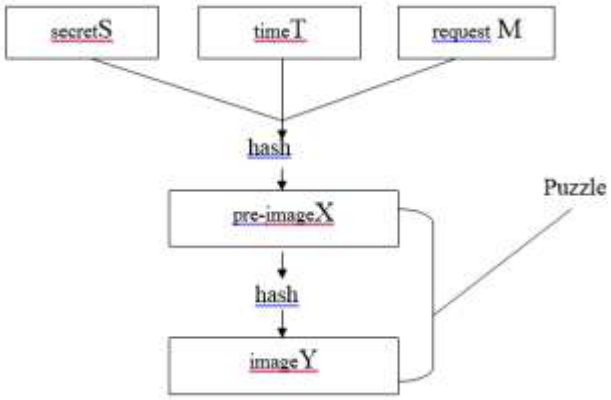

Fig 3. Encoding and decoding of client puzzle protocol

V. Evaluation and results

In this section, using NS2 simulator, the performance results of the proposed PIT-QA is compared with the existing PIT. The parameters and the simulation settings of the proposed method are summarized in the given table 1.

Parameter	Value
No of Nodes	100
Mac Type	802.11
Queue Type	Priority Queue
Coverage Area	250m
Topology Area	1000x1000

Antenna Type	Omnidirectional
Simulation time	200s
Interval	0.1, 0.2, 0.3, 0.4, 0.5
Packet size	2000bytes
Initial energy	100J
TxPower	0.2watts
RxPower	0.1watts
Number of ddos attackers	1,2,3,4,5

Table 1: Parameter of detection rate

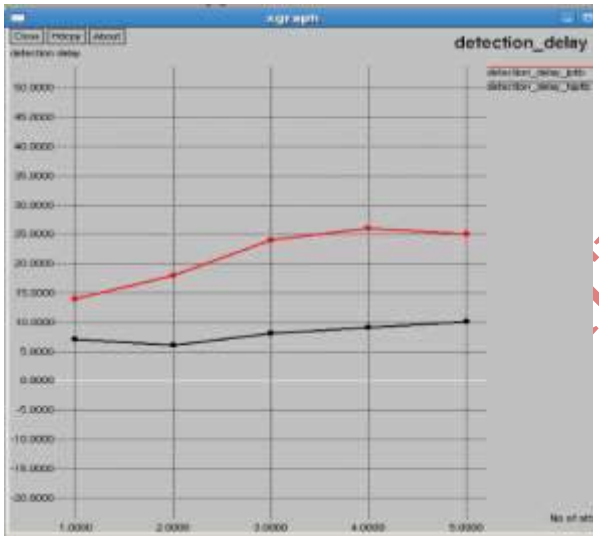

Fig 1: comparison of detection rate entropy with client puzzle protocols

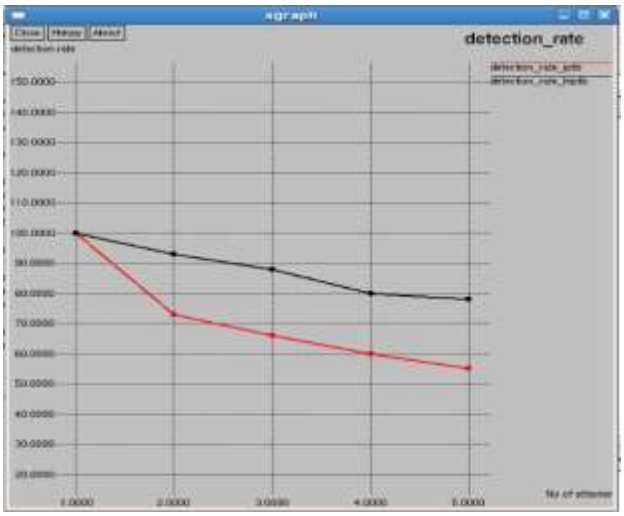

Fig 2: Comparison of detection delay entropy with client puzzle protocol

VI CONCLUSION AND FUTURE WORK

Computers and networks were the critical part of the control and coordination part of crucial infrastructures environment. As a result of this growing dependence, we require a better understanding of these systems and their reactions under unexpected conditions. Ergo there is a definite desideratum for research and development of methods to analyze and forfend these systems. Researchers proposed many DDoS detection approaches to address this issue. Client puzzle protocol plays major role for obviation of DDoS attacks. The assailer must want to solve the client puzzles, which is difficult to solve. Entropy predicated detection is one of the prevalent approaches studied in the past decade. In this, we proposed a DDoS detection method: Cusum – Entropy and client puzzle protocols. In the additionally signal processing we applied on observed entropy data amends detection efficiency.

Our results show that attacker is difficult to send request using puzzle protocol. Cusum - Entropy approach detects attacks with high detection and low false positive rates. Additionally Cusum Entropy approach gives better detection efficiency than a detection approach utilizing entropy of packet header field without further processing. We used entropy of source IP address, but this approach can be generalized to entropy of other packet header fields.

Reference

[1]Information-Theoretic easures for Anomaly DetectionWenke Lee Computer Science Department North Carolina State University Raleigh, NC 27695-7534 wenke@csc.ncsu.edu

[2] D. Kushner, "The real story of stuxnet." This is an electronic document. Available: "http:/ /spectrum.ieee.org /telecom /security /the-real-storyof-stuxnet". Date of publication: [February 26, 2013]. Date retrieved: February 4, 2016.

[3] R.R. Brooks. Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks. CRC Press, 2005.

[4] Random. Stacheldrahtv4. This is an electronic document.Available:http://packetstormsecurity.org/distributed/stachel.tgzDateof publication: [February 8,2011]. Date retrieved: September 6, 2012.

[5]A. M. Batishchev. Low orbit ion cannon (loic). This is an electronic document. Available: "http://sourceforge.net/projects/loic/". Date of publication: [January 29,2012]. Date retrieved: September 6, 2012.

[6] A. Network. Worldwide infrastructure security report, 2012. Available: "http://ddos.arbornetworks.com/report/", Published: February 7, 2012; Accessed: October 31, 2012.

[7] Denial of service attacks. This is an electronic document.Available:"http://www.cert.org/tech tips/denial of service.html". Date of publication: [October,1997]. Date retrieved: June 26, 2012.

[8] G. Carl, G. Kesidis, R. Brooks, and S. Rai. Denial-ofserviceattackdetection techniques. Internet Computing, IEEE, 10(1):82 – 89, Jan.-Feb. 2006.

