Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Received on: 6-05-2015
Accepted on: 10-05-2015
Published on: 30-05-2015

Sumit Pote, Ashish Nikalaje,Rahul Bhalerao, Prashant Gade, Kunal halkandar
Dept. of Computer Engineering DYPCOE, Akurdi, Pune
sumitpote92@gmail.com
kunalhalkandar@gmail.com
prashantgade07@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared

Low Rate DoS Attack Detection Mechanisms

Sumit Pote, Ashish Nikalaje,Rahul Bhalerao, Prashant Gade, Kunal halkandar
Dept.of Computer Engineering DYPCOE, Akurdi, Pune.

Abstract: As opposed to the conventional DoS attacks, Low rate DOS Attacker injects a short burst of traffic periodically to fill up the bottleneck buffers right before the expiration of the sender's RTO. This forces the sender's TCP connections to timeout with very low throughput. These attacks are hard to detect and prevent, as most of the DoS attack detection systems are triggered by high-rate traffic. This paper presents the survey of techniques available for detecting Low rate Do'S attacks and compares them using various parameters.

Keywords: DoS attack, LDoS attack, RTO exploitation, a apriori algorithm, naïve bayesian

Cite this article as:
SumitPote, AshishNikalaje,RahulBhalerao, PrashantGade, Kunalhalkandar,Low Rate DoS Attack Detection MechanismsAsian Journal of Engineering and Technology Innovation 03 (06); 2015; 60-64.

INTRODUCTION

A DoS attack is any event that diminishes or eliminates a networks capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. DoS attacks with single host are seldom successful in casting a massive damage. Mostly, attackers scan for vulnerable loop holes to add more hosts to their attacking army. These innocent hosts join the attacker and aid in strengthening the attack unwillingly and unknowingly. DoS against Domain Name Servers (DNS) could be even more disastrous as the entire Internet infrastructure is built on it. DNS servers are responsible for translating the website addresses into respective IP formats which is then directed to its destination. When corrupt packets are sent or when the DNS server is flooded, IP translations will not be successful thus stopping legitimate requests. Every DNS server in the internet backbone is fed with the IP addresses of root server. When a particular webpage is requested by a web page, the corresponding IP address is fetched by the DNS server and directs it to the corresponding root server. The root server then forwards this request to the specific server to which the IP belongs. Thus the effect of DoS attacks could be dreadful when it is targeted towards DNS servers.

A Denial of Service (DoS) attack is an event in which a legitimate users or clients are deprived from certain services which they are authorized to have. The attackers injects maliciously designed packets in to the network to flood the network or the server and deplete some or all of its resources. A Distributed Denial of Service (DDoS) is a type of DoS attack which uses multiple sources to attack on a network or a server. The power of DDoS attack is based on the massive number of attack sources instead of the vulnerabilities of one particular protocol. DDoS attack aims at flooding a target server with an immense volume of useless traffic from distributed and coordinated attack sources which pose to be an immense threat to the stability of the internet.

The most recent proposal in the field of DoS attack was made by Aleksandra Kuzmanovic and Edward W. Knightly, they proposed a kind of DoS attack called by them as Shrew attack at Rice University, and pointed out that just sending a short pulse periodically may cause TCP flow to decline seriously [1]. Afterwards Luo X Chang et al proposed another kind of DoS named LDoS (Low Rate Denial of Service) upon the basis of thorough research on the shrew attack. In 2005, the LDoS attack was found on the Internet2 Abilene backbone network and hence the LDoS attack became the reality [9].

In LDoS attack attacker periodically sends a short burst of packets to overflow the router's queue which leads to packet loss of legitimate users. The source can retransmit the packets to recover from the congestion problems only after one Retransmission Timeout (RTO). If the attacker is wise enough to again flood the router with malicious packets after timeout then no legitimate traffic will pass through the router thus completely denying the access to the legitimate users. LDoS attack aims at self-adaptive mechanisms of network such as the Congestion Control Mechanism, Active Queue Management (AQM) and Retransmission Timeout (RTO) mechanisms on routers. This feature of LDoS of periodic attack keeps the average rate of attack flow relatively low than other types of DoS which makes it difficult to detect and prevent. Most of the DoS detection implementations are triggered by high rate of constant traffic but as the traffic generated by the LDoS is very much similar to the normal burst of traffic LDoS disguises itself and fails from getting detected[10].

LITERATURE REVIEW

How to thwart DLDoS attacks is another hot issue, analyzing aggregated attack flows time domain characteristics or frequency domain characteristics are the cutting-edge methods, some of them can detect the attack precisely, but most of them have the shortage of inaccuracy and low efficiency .Furthermore, discovering attack hosts in our new pattern of Shrew attacks are even impossible using these methods because the flow shapes as constant background traffic. QOS method and remedy of BGP or TCP protocol are also possible, but they are not practical in large network. Preventing aggregated attack flows in short term and detecting botnets in the long-term coordinately are the solution to defend this kind of attacks, although they'll cost much more effort than the attacker. Some of the techniques suggests use of trace back method in which the ip or set of ips from which the LDoS attack was launched can be tracked. But this method has also proved to be in vain because of ease of ip masking tricks which can be achieved with a very little or no efforts. Existing mechanisms for Low Rate DDoS attack detection demands modifications in routers and protocols which seems to be highly impractical. Kai Chen et al. [2] proposed a real time LDoS attack detection method based on Shewhart Control Chart Theory and devices detection criterions based on abundant experiments. It is a probabilistic method which is not efficient against novel LDoS attacks. The mechanism proposed by Yang Xiang et al. [3] uses information metrics to quantify the differences of the network traffic with various probability distributions. They have presented concept of

inculcating these metrics for detection of LDoS attacks viz.Generalized entropy metric and the information distance metric. In this type of detection mechanism an information metric is maintained to keep track of IPs and uses a trace back algorithm to prevent LDoS attack. But masking of IP's is possible thus this method is not precise. Zhu Lina and Zhu dongzao [4] presented that edge routers must be assigned additional functionalities, in this technique comparison of features of the current traffic and features of LDoS attack flow is done to detect the attack. But modification in the functionalities of all the edge routers is not feasible if the size of the network is huge. Neha Tewari and Akash Bharadwaj introduced an entropy based scheme is used for effective detection of both low rate and high rate DDoS attacks [5]. It is a simulation based system so it is not been tested on real datasets. Gautam Thatte et al. [6] proposed a mechanism which uses IP to hop-count mapping table for identification and removal of spoofed IP packets. Petros Efstathopoulos presented a new way of LDoS attack detection with the help of randomization of retransmission timeout [7]. LDoS takes the advantage that most of the systems has RTO as 1sec. If this RTO is set to any random values after every certain period of time then it would be almost impossible for the attacker to guess the accurate RTO. RTO randomization along with proper flow monitoring helps to detect the problems with the packet and thus can lead us to successful LDoS attack detection. Rejo Mathew and Vijay Katkar proposed a lightweight software based approach for LDoS detection which can be easily integrated with existing IDS without any memory overheads [8]. The solution is a formula based solution and if the attributes for the solution are not chosen correctly, the accuracy is compromised.

PROPOSED SYSTEM

LDoS is an active type of attack which targets the buffer capacity of the server thus bogging down the network considerably. During an LDoS attack the attacker fills the buffer of the server instantaneously and remains latent for a certain amount of time till the buffer inputs are processed by the server, and this mechanism is carried out in a loop till the attacker wishes to keep the server engaged. Following steps were carried out in given sequence:

- Server was implemented which provides files to client when requested
- Legitimate application was implemented which genuinely asks the server for a file.
- A slow attacking client application was implemented which asks for a file but sends the acknowledgement of the reception of packets at a slow rate that is with a delay, thus keeping a connection open for a long time.
- An application that keeps the record of all the processes running in the resident machine and saves them in the database was created.
- A Trojan was implemented which attacks the file server with garbage packets and resides in the zombie machine.

Data mining is a process of analyzing data from different sources and summarizing it into useful information. It is a process of converting data into information. Data are facts and information is processed data. Data mining is process of finding correlations or patterns among a large dataset. The proposed mechanism uses data mining algorithms for classification of dataset.

A. NAIVE BAYESIAN CLASSIFIER

Bayesian classifier are called as statistical classifiers. Bayesian classifiers can predict class membership functions i.e. probability that the given tuple belongs to a certain class. Naïve Bayesian classifiers are probabilistic classifiers which work on Bayesian classifier along with naïve assumptions. It works on posterior probability. Naive Bayesian assumes that the absence or presence of attributes is related with every attribute which may be present or absent in the dataset. Naïve Bayesian classifiers are able to work on small amount of training dataset and classify a testing dataset of a considerably large size.

$P(X|Ci)=\Pi Pnk=1(Xk|Ci)$……(1)

P(X|Ci)=P(X1|C1)*P(X2|C2)*…* P(Xn|Cn)……..(2)

Given data sets with many attributes, it would be extremely computationally expensive to compute $P(\boldsymbol{X}|Ci)$. In order to reduce computation in evaluating $P(\boldsymbol{X}|Ci)$, the naive assumption of class conditional independence is made. This presumes that the values of the attributes are conditionally independent of one another, given the class label of the tuple. The probabilities can be easily estimated $P(X1|Ci)$, $P(X2|Ci)$, : : : , $P(Xn|Ci)$ from the training tuples.

B. APRIORI ALGORITHM

Apriori is used to generate probabilistic rules based on the frequent item set discovered in the dataset and provide information using "if-then "statements. It uses Support and Confidence for generation of association rules.

Support(X)= no of transactions which contains the item set X / total no of transactions

Confidence(X->Y) = Support(X U Y)/ Support (X)

Normal apriori requires k+1 database scans where k is the size of largest frequent item set but one pass.

Apriori requires 1 database scan. Large frequent item set are discovered just by a single pass of database in one pass apriori.

RESULT

The training dataset consisted of 23,327 records and the testing dataset consisted of 10,000 records. Naïve Bayesian classifier and apriori algorithm was used for deducing the classification accuracy of the system. After applying naïve Bayesian algorithm the accuracy achieved was 97.79% and results for apriori algorithm is 96.62%.

Naïve Bayesian results analysis

Dataset Types	Total Records	Classified Records	Unclassified Records	Accuracy %
Attack	4000	3980	20	99.5
Legitimate client	3000	2862	138	95.4
Slow client	3000	2937	73	97.9
Total	10000	9779	221	97.79

Apriori results analysis

Dataset Types	Total Records	Classified Records	Unclassified Records	Accuracy %
Attack	4000	3944	56	98.6
Legitimate client	3000	2871	129	95.9
Slow client	3000	2847	153	94.9
Total	10000	9662	338	96.62

ADVANTAGES

1. Low or No start-up costs
2. Great flexibility in relation to fast up and down scaling of resource needs.
3. It is very useful to easily detect low rate DDoS attack.
4. It's Time Complexity is Lower.

CONCLUSIOON

This system proposed a software based solution to detect LDoS attack. This software can be installed on a server which will continuously monitor the network data flow incoming to the server and write the data records in a file. Data mining algorithms like naïve Bayesian and apriority are applied on the preprocessed the records & detect L DoS threats. Serious challenges arise when IPv6 needs to be established globally & transition from version 4 to version 6 has to be done. Actual network current capacity is changeable & complex, so just one way to detection & prevention does not really work & it is better to combine a variety of means to deal with LDoS.

REFERENCES

1. AmeyShevtekar, KarunakarAnantharam, and Nirwan Ansari, "Low Rate TCP Denial-of- Service Attack DetectionatEdgeRouters", IEEE COMMUNICATIONS LETTERS, VOL.9, NO. 4 (2005)
2. Gabriel Macia-Fernandez, Jesus E.Diaz- Verdejoand Pedro García-Teodoro, "Evaluation of a low-rate DoS attack against iterative servers", Department of Signal Theory,University ofGranada, c/Daniel Saucedo Aranda, s/n, 18071 Granada, Spain (2006)
3. A.Kuzmanovic and E. Knightly, "Low-Rate TCP Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)", Proc. ACM SIGCOMM pp. 75-86(2003)
4. Wuhan, Hubei,"Detection of Low-rate DDoS Attack Based on Self-Similarity", China in 2010 Second International Workshop on Education Technology and Computer Science (March 06-March 07)
5. GautamThatte,Urbashi Mitra and John Heidemann,"Detection of Low-Rate Attacks in Computer Networks", University of Southern California IEEE (2005)
6. AdityaAkella, AshwinBharambe, Mike Reiter, SrinivasanSeshan, "Detecting DDoS Attacks on ISP Networks", Carnegie Mellon University
7. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants In: Proceedings of the 2003 conference on Applications, technologies, architectures, And protocols for computer communications Pages: 75 –86 Year of Publication: ISBN: 1-58113-735-4 (2003)
8. Haibin Sun, John C.S. Lui, David K.Y. Yau, "Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection", Proceedings of the 12th IEEE International Conference on Network Protocols (2004)

9. Zenghui Liu, LiguoGua, "Attack simulation and signature extraction of low-rate DoS." 3rd International Symposium on Intelligent Information Technology and Security Informatics IEEE 2010 Computer Society (2010)
10. SandeepSarat and Andreas Terz, "On the Effect of Router Buffer Sizes on Low-Rate Denial of Service