International Journal of Soft Computing 10 (4): 247-253, 2015
ISSN: 1816-9503

Cluster Based Detection Mechanisms for Distributed Denial of Services (DDoS) Attacks

K. Saravanan, R. Asokan and K. Venkatachalam
Department of Computer Science and Engineering,
Erode Sengunthar Engineering College, Thudupathi, 638057 Erode, Tamilnadu, India

Abstract: Denial of service attack restricts indented requests from accessing required resources. DoS attacks synchronized by a group of attackers will lead to distributed DoS. This can be tackled by the Cluster Model which will produce anomaly in generated data packet clusters. The attack packets can be detected by proposing a fuzzy based cluster formation which can be applied on both wired and wireless networks. DDoS alert aggregation scheme along with statistical technique is used to generate meta alerts and detect anomalies. Statistical techniques are used to classify packets followed by cluster formation which helps in improving proposed system performance.

Key words: DDoS (Distributed Denial of Service Attack), DoS, cluster aggregation, anomalie, meta alerts

INTRODUCTION

Resource consumption attacks, the most common type of network DoS seek to exhaust a server's resources, thus, rendering the server incapable of providing its services to legitimate clients. Connection depletion attacks, a type of resource consumption attack, overwhelm a server by initiating a large number of connections and leaving them unresolved. The server then lacks the resources to service legitimate connection requests. Connection depletion attacks do not usually require special privileges because they exploit properties of the communication protocol itself. TCP SYN flood attack is a well-known example of this type of attack that takes advantage of a weakness in the TCP protocol that leaves connections unresolved. Normally, a TCP connection is established through a three-way handshake. A client initiates a connection by sending a SYN packet to the server. The server acknowledges the request by sending a SYN ACK packet back to the client and allocating space for the connection in a buffer. The client then replies with an ACK packet and the connection is completely established. In the TCP SYN flood attack (Kumarasamy, 2011), an attacker initiates many connections in which the SYN and SYN ACK packets are exchanged as usual but the final ACK message is never sent to the server. Thus, the connection is never completely established and the server is left with buffer space allocated for all the incomplete connections. If the attack succeeds, the server fills up its buffer with incomplete connections, leaving no space for non-malicious connection requests and thus preventing the server from establishing connections with legitimate (non-malicious) clients.

According to the computer incident advisory capability, the first DDoS attack occurred in the Summer of 1999. In February 2000, one of the first major DDoS attacks was waged against Yahoo.com. This attack kept Yahoo off the internet for about 2 h and cost Yahoo a significant loss in advertising revenue. Another recent DDoS attack occurred on October 20, 2002 against the 13 root servers that provide the Domain Name System (DNS) service to internet users around the world.

COLLECTION OF TRAFFIC ANOMALY DDOS ATTACK

DDoS Detection Systems are a very popular network security tool that allows network administrators to identify and react to hostile traffic aimed at or generating from their network. Two common DDoS Detection algorithms are behavior or traffic anomaly based detection where an attack is deduced from unusual traffic patterns without examining the contents of this traffic (Yau *et al*., 2005). Another one is knowledge or signature based where the content of data packets is examined for known malicious content, e.g., Trojan code. One very desirable feature of advanced detection method is to be capable of learning and generalizing from known patterns of system, process or user suspicious behavior. This ensures that

Corresponding Author: K. Saravanan, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Thudupathi, 638057 Erode, Tamilnadu, India

given any novel attack, it is identified as such and any normal behavior that deviates from known normal behavior is not flagged as anomalous. This requirement applies to all DDoS attack detection but is clearly best met by traffic anomaly based schemes.

Traffic anomalies are characterized by unusual and significant changes in a network traffic behavior. They can be malicious or unintentional. Malicious traffic anomalies can be caused by attacks, abusive network usage and worms or virus propagations. However, unintentional ones can be caused by failures, flash crowds or router misconfigurations. In the fast growing internet commercial transaction base, attacks on internet infrastructure, anomaly DDoS traffic attacks combined with traditional network intruders have become one of the most serious threats to the network security (Kumarasamy and Asokan, 2011).

The traffic anomaly DDoS Detection Method is carried out on the principle traces of non intrusive packet header data obtained from the internet server traffic basement. Traffic is monitored at regular intervals to obtain a signal that can be analyzed through statistical techniques and compared to historical norms to detect anomalies. The anomaly DDoS traffic detection envisions statistical non intrusive wavelet transform mechanisms for real-time data source extracted from NetCon server over a period of 3 months at various time intervals. The experimental results suggest that address spoofing by attackers which imply that such attacks will be invisible to indirect backscatter measurement techniques. Further, at the detailed packet-level characterization (e.g., attack destination ports), there are significant differences between anomaly and traditional DDoS attack measurements. Thus, there is tremendous value in moving towards direct observations to better understand recent DDoS attacks (Ioannidis and Bellovin, 2002).

Traffic anomaly DDoS attack measurements additionally provide information inaccessible to traditional network DDoS attack detection measurements, enabling us to better understand how to defend against attacks. A lot of techniques have been developed in order to detect, identify and prevent propagation of malicious traffic over networks. The system differentiate between two classes of DDoS attack detection techniques (Saravanan *et al*., 2014): misuse detection and anomaly detection (Wang and Reiter, 2008). The Misuse Detection Systems try to detect DDoS attack by comparing the current activity of the audited resource to a database of known attack scenarios. Those techniques cannot detect unknown attacks. However, the Anomaly DDoS Detection Systems try to detect the DDoS attack by comparing the current activity of the audited resource to an established normal activity represented in form of a profile.

The role of DDoS attack detection is to warn administrators of suspicious and potentially malicious computer activity. The systems are passive warning devices that must be monitored by trained professionals. Some DDoS attack detections, however, feature active response mechanisms to automate the DDoS attack recovery process. Of the active response DDoS attack detections, some target the attacker and launch countermeasures to inhibit the attacker system. The difficulty with launching countermeasures is ensuring the authenticity of the attacker. Hackers often spoof IP addresses or use intermediary hosts during a break-in. Disabling an alleged attacking system in such a scenario disrupts an innocent machine and leaves the real attacker system unaffected.

Another approach to active response is to target the victim system. Typical victim responses attempt to repair the system, stop the current attack or prevent the machine from being exploited in the future. Unfortunately, measures taken against the victim system are not always effective because it is difficult to determine the success of an attack and the resulting damage. Incorrect responses may have ill effects on the victim system. Regardless, repair takes a machine offline which is costly for production systems. The biggest problem with active response mechanisms, however, is the current state of DDoS attack detection technology (Savage *et al*., 2000). Network DDoS attack detection is to analyze the audit data on each host of the network and correlate the evidence from the hosts. Using a packet capturing program network DDoS attack detection is to monitor the network traffic directly.

CLUSTERING OF TRAFFIC ANOMALY DDOS ATTACK

A network is connected with many number of sensor devices. The job of sensor event is to monitor the traffic in network. They are fed as input to the statistical traffic anomaly detection and k-means Clustering algorithm is applied to the traffic anomaly detection so that the objects are grouped. In this way, any anomaly DDoS detection whether identified as good node or bad node remains in the cluster.

Algorithm: The traffic anomaly detection approach deploys the k-mean Clustering algorithm in order to separate the routing network with normal and anomalous traffic in the training dataset. The resultant obtained cluster centroids are then used for fast anomaly detection (Peng *et al*., 2007):

- Step 1: apply k-means clustering to the traffic data set-packet data such as header information, start and end time stamps, number of packets (total number of packets sent) and bytes (total number of bytes sent)
- Step 2: determining the initial partition. Initialize K clusters by selecting packet, time stamps and bytes as elements
- Step 3: determine the optimal number of clusters based on Optimization algorithm
- Step 4: update the clusters. Apply Iteration algorithm to the training traffic data set. Calculate the distance using the Euclidean distance formula. Assign each and every object to the cluster with the nearest obtained centroid value
- Step 5: recalculate the centroid value of the modified clusters
- Step 6: repeat step 4 until the centroid values do not change

The system apply the k-means Clustering algorithm to training datasets which may contain both normal and anomalous traffic The clustering technique used behind this approach is that normal and anomalous traffic form different clusters. The clustering algorithm divides the training data into K clusters but does not determine if a cluster contains normal or anomalous traffic. Even the good nodes may be considered as anomalous and bad nodes may be treated as normal node.

AGGREGATION OF CLUSTERED ANOMALY DDOS DETECTION (SIMILARITY OF ATTACK INTENSITIES)

Network DDoS Attack Detection Systems can be divided into two types as either signature based or anomaly based. A signature detector examines traffic for attacks that are known to the system using the rules which have been written by experts or administrator. When some other attack is occurred, new rules must be written and distributed into the system. An anomaly detection system models the normal traffic which distributes the IP addresses and ports. Hostile traffic module falls outside this distribution model. In case of anomaly detection, it can detect novel attacks without having the rules to be written. But, it suffers from the disadvantage that it cannot consider about the nature and type of attack as it is a novel type and as such normal traffic can also deviate from the model which generates false alarms. The job of anomaly detector is to bring the suspicious traffic to the attention of administrator who must then note it out, if anything needs to be done to alter it.

There are two main methods of DDoS attack. They are Network DDoS Attack Detection System (NDDoS) which is an independent platform which main work is to identify the DDoS attack occurred by way of examining the network traffic and at the same time monitors multiple hosts. The sensors capture all different types of network traffic and determine the content of individual packets for detecting malicious traffic. An example of a NDDoS is Snort. The other type of DdoS attack is host-based DDoS Attack Detection System. This type consists of an intermediator which identifies the DDoS attack detections by way of analyzing the system calls, file modifications and other states.

The analysis of the demand for freight transport is carried out with the flow behavior of data over the network. It uses the statistical properties of several variants correlation time scales and the different characteristics of traffic distribution. The analysis of traffic sources reveal the extent and frequency characteristics of the temporal dynamics at the same time, in contrast to other electronic data processing as a fourier transform. The transformation of the statistical data generated correlation direction of sources in several measuring points. Normal traffic and detects abnormal traffic conditions within certain time limits including the frequency of variation of speed of data transmission and few other positions of the time: is the timing information removed for the detection of traffic anomalies recorded DDoS attack detection. The model of statistical data processing is a multi-dimensional traffic data analysis is repeated up to 6 levels.

The time stamp recorded traffic data sources show that the lowest levels of the characteristics of the traffic is identified until the traffic anomaly DDoS attack detection with the ultimate transfer of ownership. The signal from each level has an effect of prolonging the sampling interval in the range of 2 times. Is the use of t minutes sampling interval, the time range spanned j to a detection limit of the source of traffic for anomaly DDoS attack detection in minutes * t 2j. This period can independently restore the sample and frequency of statistical traffic data individual fields in the packet header is analyzed to observe traffic anomalies. Individual fields in the header traffic data take discrete values and shows discontinuities in the sample space. The analysis was performed with the sequence of a random process, the traffic statistical data processing of the correlation of the series in computational efficiency in anomaly DDoS attack detection. For each direction on the number of packets sent instant traffic data sampling.

To calculate the direction of traffic data correlation consider two adjacent sampling instants. The

Demonstration Model defines the direction of traffic data correlation of the donor site. If one extends from the two measuring points, i.e., n-1, you get a positive contribution. In order to minimize storage and processing complexity, use a linked data structure. A report on location is used to record the number of packages to address the IJ in IP address with the extension. The use of the approximate representation of addresses allows us to reduce requirements for calculating and storing a key factor. To create the correlation of signaling messages at the end of the sampling point, multiply each segment of the correlation of the scales. From a statistical point of view on average about the same and the standard deviation of the dispersion and cross-correlation coefficient.

Cluster based statistical anomaly DDoS attack detection scheme measures the statistics of the traffic traces of non intrusive packet header data. Traffic is monitored at regular intervals and analyzed using the statistical method by comparing it to historical norms to find anomalies (change detection). Assault cases are regarded as random processes update for the approximate maximum likelihood parameter produce. With these random processes, from top to bottom of attack instances are detected. The cluster traffic streams contain all relevant information that is useful for the administrator, the process of DDoS attack detection to govern effectively.

Aggregation is an important subtask of DDoS attack detection. The goal is to identify and to cluster different aggregates-produced by low-level DDoS attack detection systems, firewalls, etc., belonging to a specific attack instance which has been initiated by an attacker at a certain point in time. Thus, aggregation can be generated for the clusters that contain all the relevant information whereas the amount of data (i.e., alerts) can be reduced substantially. Basically, it can be regarded as a data stream version of a maximum likelihood approach for the estimation of the model parameters. With three benchmark data sets, they demonstrate that it is possible to achieve reduction rates of up to 99.96% while the number of missing meta-alerts is extremely low. The goal of aggregation is to reduce the complexity of hyper alert correlation graphs without sacrificing the structures of the attack scenarios; it allows analysts to get concise views of correlated alerts. For this reason, the system also refer to aggregation as graph reduction. Aggregation allows analysts to selectively disaggregate certain aggregate thus providing the ability to examine the details of select aggregation.

SIMULATION OF CLUSTERING OF STATISTICAL ANOMALY DDoS ATTACK

The simulation is conducted to perform the evaluation of new aggregation approach. The simulation deployed different data sets to demonstrate the feasibility of the proposed method. The first is the well-known DDoS attack detection evaluation data set for the second used real-life network traffic data collected at Global ISP gateway server and the third contains firewall log messages from a commercial internet service provider. All experimental simulation was conducted on a PC with 2.20 GHz and 2GB of RAM in NS2 simulator.

Several weeks of training and test data have been generated on a test bed that emulates a small confidential data site. The network architecture as well as the generated network traffic has been designed. The simulation used the TCP/IP network dump as input data and analyzed all 104 TCP-based attack instances (corresponding to >20 attack types) that have been launched against the various target hosts. Sensors extract statistical information from the network traffic data. By applying a varying threshold to the output of the classifier, a so-called Receiver Operating Characteristics (ROC) curve can be created. The ROC curve plots the True Positive Rate (TPR, number of true positives divided by the sum of true positives and false negatives) against the False Positive Rate (FPR, number of false positives divided by the sum of false positives and true negatives) for the trained SVM. Each point of the curve corresponds to a specific threshold. Four Operating Points (OP) are marked. OP 1 is the one with the smallest overall error but as, we want to realize a high recall, we also investigate three more operating points which exhibit higher TPR at the cost of an increased FPR. As attributes for the aggregation, we use the source and destination IP address, the source and destination port, the attack type and the creation time differences (based on the creation time stamps).

The number of aggregates produced for the different OP and also for the idealized condition. We have 104 attack instances in the data set altogether. For OP 1, there are three attack instances for which not even a single alert is created, i.e., these instances are already missed at the detection layer. The three instances are missed because there are only a few training samples of the corresponding attack types in the data set which results in a bad generalization performance of the SVM. Switching from OP 1-2 alerts are created for one more instance. OP 3 and 4 do not yield any further improvement.

In order to demonstrate that the proposed technique can also be used with a conventional signature-based detector, the captured traffic was analyzed by the open source IDS which detected all attack instances that have been launched and produced. The aggregate format equals the one used for the SVM detector, i.e., the

aggregate exhibit the source and destination IP address, the source and destination port, the attack type and creation time differences. Snort was configured to match the network topology and we turned off rudimental aggregation features. In order to achieve a high recall, we activated all available rule sets the official rule sets as well as available community rules which both are available at the Snort web page. Activating all rules leads to a false aggregate rate of 0.33%. The FPR is based on the assumption that all aggregates that are not classified with the attack type that we launched are false aggregates. It cannot be guaranteed that there are unknown attacks in the data set that were started by real attackers and do not know exactly how many alerts should be created by the attacks are launched.

PERFORMANCE EVALUATION OF AGGREGATED CLUSTER ANOMALY DDoS DETECTION

In order to assess the performance of the aggregation, evaluate the following measures.

Percentage of detected instances (p): An attack instance is being detected if there is at least one meta-alert that predominantly contains aggregation of that particular instance. The percentage of detected attack instances p can thus be determined by dividing the number of instances that are detected by the total number of instances in the data set. The measure is computed with respect to the instances covered by the output of the detection layer, i.e., instances missed by the detectors are not considered.

Number of aggregates (A) and reduction rate (r): The number of aggregates (A) is further divided into the number of attack. MA attack which predominantly contain true aggregates and the number of non-attack aggregates MA non-attack which predominantly contain false alerts. The reduction rate r is 1 min the number of created aggregates A divided by the total number of attacks A.

Average run-time (tavg) and worst case run-time (tworst): The average run-time is measured in milliseconds per aggregate. Assuming up to several hundred thousand aggregates a day, tavg should stay clearly below 100 msec per aggregate. The worst case run-time tworse which is measured in seconds, states how long it takes at most to execute the while loop.

Meta-aggregate creation delay (d): It is obvious that there is a certain delay until a meta-aggregate is created for a new attack instance. The meta-aggregate creation delay (d) measures the delay between the actual beginning of the instance (i.e., the creation time of the first aggregate) and the creation of the first meta-aggregate for that instance.

In the following, the results for the aggregation are presented in the Table 1. For all experiments, the same parameter settings are used. The system set the threshold θ that decides whether to add a new aggregate to an existing component or not to 5% and the value for the threshold γ that specifies the allowed temporal spread of the alert buffer to 180 sec. θ was set that low value in order to ensure that even a quite small degrade of the cluster quality which could indicate a new attack instance, results in a new component. A small value of θ of course, results in more components and thus in a lower reduction rate but it also reduces the risk of missing attack instances. The parameter γ which is used in the novelty assessment function, controls the maximum time that new aggregates are allowed to reside in the buffer B. In order to keep the response time short, we set it to 180 sec which we think is a reasonable value. For both parameters, there were large intervals in which parameter values could be chosen without deteriorating the results.

During the attack, the client of interest has zero link utilization, meaning the client completely stops getting HTTP data packets since almost all the bandwidth of the link 2-0 is used by the attack traffic. On the other hand, there is no visible difference in the link utilization of upstream server link nor in the link utilization of the bottleneck link after the attack. To detect this attack, the proposed aggregation use the nonlinear mutual information computed for the link utilization observed on the bottleneck link.

Figure 1 and 2 shows the mutual information plots for this experiment for different trials. It can be seen that there

Table 1: HTTP traffic parameters for random 50 and 100 node transit-stub topologies

	HTTP traffic							
Trials	No. of sessions	Intersession time	Session size	Interpage time	Page size (sec)	Interobject time (sec)	Average object size	Object size shape parameter
1	400	1	200	15	1	0.01	12	1.1
2	800	2	400	30	2	0.02	24	1.2
3	1200	3	600	45	3	0.03	36	1.3
4	1600	4	800	60	4	0.04	48	1.4
5	2000	5	1000	75	5	0.05	60	1.5

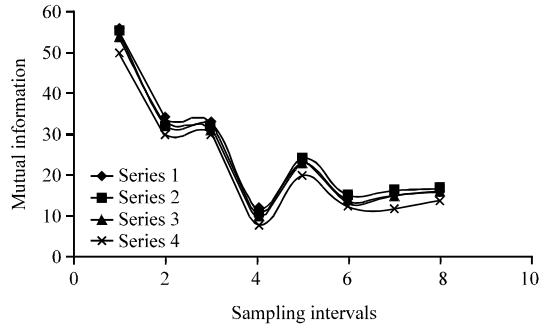

Fig. 1: Non-linear mutual information normal data

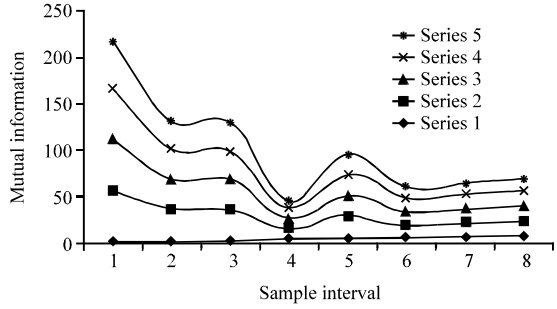

Fig. 2: Non-linear mutual information attack data

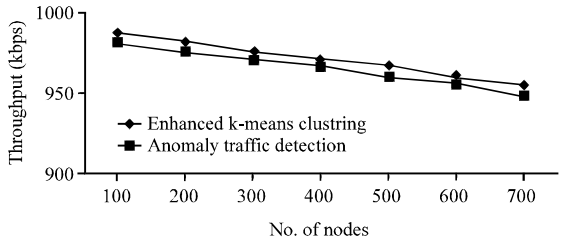

Fig. 3: No. of nodes vs. throughput

is a significant change in the mutual information, even though the attack cannot be seen by visual inspection of the link utilization plots. It is important to note that since the link utilization remains constant during the attack, count based methods that simply consider the amplitude of the link utilization during a sample period are unable to detect the attack.

The performance of the detection scheme is related to the value of threshold. Figure 3 shows the relationship between the false alarm rate and threshold. A false alarm is said to occur if Sk exceeds threshold without attack. After a false alarm, S is reset to 0 and the time series is continued to be processed. As expected, as threshold grows, the false alarm rate decreases. No false alarms occurred for threshold above 160, hence, no points are included for threshold >160. However, as long as threshold is below 1600, the attack is detected.

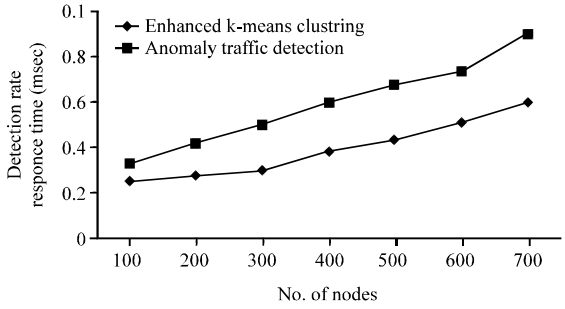

Fig. 4: No. of nodes vs. detection rate

There is a significant change in the throughput of the information communication. It is analyzed that when the number of nodes increases, the throughput decreases. When compared to the Statically Anomaly Detection Model, the throughput is found to be high in the cluster detection with bandwidth threshold model (Fig. 4).

CONCULSION

Cluster aggregates varies subtask of DDoS detection. A different aggregate produced by low-level DDoS detection systems, firewalls, etc. is evaluated to make the system more foolproof. It identifies and cluster DDoS attack detection to make the segregation of various attacks being generated. To improve the efficacy of DDoS attack detection system, aggregation are generated which contain all the relevant information The experiments demonstrated the broad applicability of the proposed aggregation approach. The simulation conducted for two different data sets and showed that machine learning based detectors, conventional signature based detectors and even firewalls can be used as aggregation generators. In all cases, the amount of data could be reduced substantially. Although, there are situations as described in clusters that are wrongly split the instance detection rate, none or only very few attack instances were missed. Run-time and component creation delay are well-suited for an on line application.

Here, we presented the technique for data stream aggregation and generation of resultant aggregate values. It has shown that the sheer amount of data that must be reported to a human security expert or communicated within a distributed DDoS Detection System for instance can be reduced significantly. The reduction rate with respect to the number of aggregates was up to 97 in the simulation. The number of missing attack instances is extremely low or even zero in some of the simulation and the delay for the detection of attack instances is within the range of some seconds only.

REFERENCES

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router-based defense against DDoS attacks. Proceedings of the 9th Symposium Network and Distributed System Security, February 6-8, 2002, San Diego, California, USA., pp: 1-12.

Kumarasamy, S. and R. Asokan, 2011. Distributed denial of service (Ddos) attacks detection mechanism. Int. J. Comput. Sci. Eng. Inform. Technol., 1: 39-49.

Kumarasamy, S., 2011. An effective defence mechanism for distributed denial-of-service (Ddos) attacks using router-based techniques. Int. J. Crit. Infrastructures, 6: 73-80.

Peng, T., C. Leckie and K. Ramamohanarao, 2007. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput. Surv., Vol. 39. 10.1145/1216370.1216373.

Saravanan, K., R. Asokan and K. Venkatachalam, 2014. Detection mechanism for Distributed Denial of Service (DDoS) attacks for anomaly detection system. J. Theor. Applied Inform. Technol., 60: 174-177.

Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2000. Practical network support for IP traceback. Comput. Commun. Rev., 30: 295-306.

Wang, X.F. and M.K. Reiter, 2008. A multi-layer framework for puzzle-based denial-of-service defense. Int. J. Inform. Security, 7: 243-263.

Yau, D.K.Y., J.C.S. Lui and Y. Yam, 2005. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Trans. Network., 13: 29-42.