Asian Journal of Information Technology 15 (1): 136-141, 2016
ISSN: 1682-3915

An Investigation on Neuro-Fuzzy Based Alert Clustering for Statistical Anomaly of Attack Detection

K. Saravanan and R. Asokan
Department of CSE, Erode Sengunthar Engineering College,
India Kongunadu College of Engineering and Technology,
Thudupathi, Erode, 638057 Trichy, Tamil Nadu, India

Abstract: At present the data transmission and communications commonly use both wired and wireless networks. Frequent detection systems are available more for wired networks than for wireless networks. The detection system developed for wired networks cannot be deployed in wireless networks due to the difference between the two types of networks. The wireless detection system is different from the conventional wired detection models. The data transmission of the wired network is a standard physical routing. However, the data stream routing of wireless network are based on radio signals with a variety of problems of evolution. So in both the wired and wireless networks of the internet scenario, it is necessary to deploy detection system efficiently from attackers. The proposed research offered in this thesis is based on anomaly detection of the statistical traffic which is carried out on the normal and abnormal anomaly traces in the packet header and traffic volume detection. The attacker's packet header data are acknowledged with a port number, option field parameters and IP address. The anomalies detection is carried out at a regular interval to monitor the traffic analyzed through statistical variance. The change detection detects the statistical variance of the traffic volume. The proposed anomaly traffic detection systems provide a better detection system compared with the existing anomaly detection system. The results obtained from the proposed system are compared with the existing attack detection systems with the propagation delay metric. It shows a reduction of nearly 10% and an improvement of 13% average throughput.

Key words: Attack, MAC frames, fuzzy system, DoS attack, clustering

INTRODUCTION

The attacks on the internet have increased rapidly parallel to the fast development of the internet. On the Internet, a denying service to the target system is called a Denial of Service attack (DoS). It is the single target system which denies service by way of a multitude of compromised systems attack. Distributed Denial of Service (DDoS) attack is part of the DoS attack. DDoS does not distinguished between different attacks but focuses on detecting attack types. More number of approaches are available to prevent the attack, to detect the attack and mitigate the effects of the malicious traffic. The proposed research work focuses on anomaly DDoS attack detection in the wireless and wired networks for the analysis and development of network technologies. The wired and wireless networks are used to detect the anomaly detection system, which identifies traffic data changes and these changes are measured by available statistical characteristics. The DDoS attack detection system has two major classes of exist and they are based on different approaches to the dilemma. First, misuse detection systems detect the signatures directly by recognizing and using the knowledge base of DDoS attack attempts.

The second detection methods comprise of anomaly based detection systems. Three most important schemes used are neural networks, clustering with outlier detection and fuzzy logic techniques. The neural networks have been adopted using models of simulation process of the human intelligence. Clustering techniques are measured based on a given similarity or distance measure and clusters are derived through the grouping of the observed data. Fuzzy set theory which analyses the conventional predicate logic accurately, results in fuzzy logic. The proposed research seeks to combine the features of both statistical and machine learning based techniques.

Corresponding Author: K. Saravanan, Department of CSE, Erode Sengunthar Engineering College,
India Kongunadu College of Engineering and Technology, Thudupathi, Erode, 638057 Trichy, Tamil Nadu, India

Literature review: DDOS attack detection remains as an active field of research for long time. The improvement in the performance of DDoS detection system is used by most researchers that addresses the detection problem. Hypothesis testing and approximation algorithms are used to develop a statistical framework. The network abuse (e.g., scans and worms) remains as a challenge in classifying and detecting anomalies.

Garg and Reddy emphasized that in a distributed cooperative detection system, the low confidence of the node detecting attack is initiated through the cooperative detection engine of the global DDoS attack detection procedure. In that method, the Rule-Based Classification (RBC) algorithm is used to built the local detection engine. Huang *et al.* (2003) introduced a cross-feature analysis of the new data mining method. Normal traffic of correlation patterns are detected by new data mining methods. In general, anomalies/variation detections are found out by using correlation patterns. Subhadrabandhu have implemented attack detection in ad hoc networks with statistical framework. Fadlullah *et al.* (2010) monitored the network traffic at regular intervals to attain data which were analyzed by intelligent techniques or statistical techniques for an investigation of the anomalies. The design has been implemented to accumulate data from perceived eventual anomalies in normal traffic (historical data).

Roesch (1999) proffered a mechanism for network based data mining approach to DDoS attack detection. It provides an occasion to train network users by mining the data trails of their activities. Zhong *et al.* (2007) implemented the recent research on clustering. The data mining for DDoS poses significant challenges and attack detection could be unfamiliar. The attack detection model for the networks does not require the training data in the network environment. Buchtala has applied network audit data with no prior knowledge of the relationships between attributes and attack types. Zhong *et al.* (2007) have implemented the K-means clustering algorithm with multiple centroid-based unsupervised DDoS attack detection system. Ohsita *et al.* (2010) have implemented a scheme where the anomalies are malicious or accidental and it is significant to scrutinize them.

Smitha have detected an operational standpoint for stress resource and congestion in the network consumption. Autrel and Cuppens proffered a mechanism with a lot of parameters used to improve the scalability. There is no guidance available to locate good standards that must be set by the user. The same approaches are stated by Julisch (2003) and Pietraszek (2004), to set scalability and adoptability parameters. Perdisci *et al.* (2006) presented a user-defined parameter clustering algorithm based on similarity measures used attribute-wise. Francois *et al.* (2012) have implemented FireCol Method. It is used to capture flooding DDOS attacks earlier. FireCol is made of Prevention System (PS) which is placed at Internet Service Provider (ISP) level.

Multilayer perceptrons, a basic least-square, error approach, decision trees and the networks are used to arrive at a decision. The existing meta-alert is used to decide the detection of the attack with only a few new alerts. The above mentioned methods are used to detect the attack with minimum limitations. Dain and Cunningham (2001) have implemented fuse alerts with three different approaches. The first one is according to their source IP address only and simple to group's alerts. Bhuyan *et al.* (2014) did a comprehensive survey on current DDoS attack highlighting some open issues, research challenges and possible solutions, architectures and existing detection methods. Though, it didn't guarantee attack detection.

Hofmann have implemented the off-line setting algorithm. The algorithm can generate the historical alert logs. Pietraszek (2004) have implemented the method that focuses on decreasing the false positive rate. Using filters, the amount of created alerts is reduced and the cluster structure is created in the system. Mahajan *et al.* (2002) proffered a mechanism for detecting and controlling high bandwidth aggregate at a single router. Boppana and Su (2010) devised a method of false positives detection for the networks. Wei *et al.* (2013) have implemented the Rank Correlation Based (RCB) algorithm. The RCB is concentrated only on Distributed Reflection DoS (DRDoS) attacks. If suspicious flows are found, the RCB algorithm will calculate the rank correlation between the flow pairs and presents last alert as per fixed thresholds.

The Material Removal Rate (MRR) has created the new approach of the predict method and WithIn Wafer Non Uniformity (WIWNU) inCMP by Lih *et al.* (2008) created the sparse-data sets to generate the silicon wafers. AdaptiveNeuro-Fuzzy Inference System (ANFIS) is involved in the detection system. The current technique uses fuzzy logic and clusteringdata to establish a link between simulated atmospheric profiles and sounder observations. This relationship is further fortified using the ANFIS (Ajil *et al.*, 2010) which exists in the fuzzy-rule base by way of altering. Khezri and Jahed (2011) have implemented a mechanism to identify hand motion commands for attack detection.

MATERIALS AND METHODS

Statistical anomaly DDOS attack traffic detection model: The anomaly based attack detection system attempts to

estimate the system protected and generates an anomaly alarm. The threshold value carried out shows the deviation between exceeding the normal behavior value and a given observation at an instant. The detectors system is used to detect the abnormal behavior of the method and the difference between given limit of the expected one and the observed behavior creates an alarm when the difference between probable one falls below the experimental behavior. The anomaly-based statistical detection system determines normal network activity like the type of bandwidth to be used, protocols to be considered and ports and devices to be connected. The system captures the profile representing its stochastic behavior and traffic activity of the network.

Statistical anomaly traffic DDOS detection: The enhanced anomaly detection work consists of three stages. First, packet header is established for the network traffic signal. In the second stage, statistical data transformation analysis is carried out with wavelet transforms of option field's (time to live, type of services, version, stream identifier, strict source routing loose source routing, protocol and internet time stamp), port number and IP address. In the detection systems, using threshold value based anomalies and attacks are checked. The information analyzed is compared with the characteristics of the traffic and historical thresholds to check out expected norms. The statistical discrete wavelet transforms work on the concurrencies of the required fields of options such as strict source routing, time stamp, loose source routing, stream identifier and the type of versions. This is necessary to evaluate the normal and abnormal traffic streams with anomalies in various time zones of the recorded data input header files. The discrete wavelet transform for wired mode is given in Eq. 1 where, n = 0,1,2,...j-1, 'P_n' refers to wavelet filters applied in the wired mode and 'j' refers to the length of the filter:

$$DWT_i = \sum Y_{21-n} P_n(x)1 \quad (1)$$

Statistical variance is identified to detect the anomaly by analyzing the correlation of port numbers and IP address in addition to the four parameters such as maintenance of record route, abnormality in internet time stamp, switching between loose source routing and strict source routing and changes in stream identifier. The information analyzed is compared with the historical threshold to identify whether the traffic's characteristics are regular norms or not.

Traffic data streams: The network domains of the routers are used to generate the data values from traffic source and it is measured for evaluation. The enhanced anomaly detection traffic monitoring detector detects the attacks by source network. Outbound filtering leads to address spoofing, advocated for limiting the possible. With such filtering in place, destination addresses, port numbers and option field (version and type of services, internet time stamp, stream identifier, time to live, strict and loose source routing and protocol) of the outgoing traffic are taken for the purpose of analysis.

Data filtering and signal generation: The amount of packets sent to every IP address/MAC address at a particular sampling instance is counted. To observe the anomalies packet header fields are investigated in the traffic data. The packet header data for the individual fields in the discrete values are measured in the sample space of the discontinuities. If an address periods of the 2 sampling points are 'n-1' and 'n', then the sampling point n address correlation signal obtains a +ve contribution, to investigate a simplified correlation of time series sequence. The random process is employed for computational effectiveness. The correlations of the address in two success samples are computed by the detection model filters. To produce the correlation address signal at each segment correlation, sampling point end is multiplied with scaling factors. The packet count through the scaling IP address for the j in ith field is recorded by using a location count, count[i,j]. It provides the address instead of 232 locations as described to store the address.

Discrete wavelet transform: In universal terms, the signals generated are analyzed by the techniques that are employed such as Wavelet Transform and Fast Fourier Transform (FFT). The main difference between the changes is that the local wavelets in terms of both frequency and time. The Fourier transform is localized in terms of frequency only. The better signal representations of the wavelets use the multi resolution analysis. Discrete Wavelet Transform (DWT) consists of synthesis/reconstruction and analysis/decomposition process. Decompositions: the objective of the analysis process is to find a hierarchy of derived signals, which it can extract from the original signal. The iterative process is applied in the above mentioned techniques. The signal x of length N is the input for each iteration. Two or more derived signals are collected each of length N/2 is the output. By way of convolving x with a filter F, each output signal is acquired and then the convolution product is seen decimating every other coefficient. Output signal so

far obtained is represented by F(x). One of the special filters 'L' has a smoothing effect and its equivalent low-frequency output is called output L(x). The filters, $H_1,\ldots, H_r$ (r = 1) are called as signal x of high-frequency content. Further decomposition of L(x) continues with iterations, thereby shorter signals $L^2(x)$, $H_1L(x)$, …., $H_rL(x)$ are generated. The performance of statistical anomaly attack detection is measured with attack traces on the wireless and wired networks traffic on time bands that are multiple sampled. The standard deviation, mean and arithmetic of samples are calculated. The statistical analysis deals with variation of characteristic values establishing the size of the traffic in dissimilar time eras.

Cluster aggregation of statistical anomaly DDOS detection system: The cluster based alert aggregation of anomaly DDoS detection comprises of the following phases i.e., collecting the detected DDoS from statistical traffic analysis, alert generation and data stream of alert aggregation and clustering of aggregated alert.

Collection of detected anomaly DDoS attacks and alert generation: In this phase, the detected anomaly DDoS traffic source is obtained from the statistical traffic analysis. It is first collected and stored with its actual characteristic of traffic data traversed. The incoming data from the client users and both the networks are collected with the detected alerts. An appropriate event through the incoming data collection extracts the valuable (e.g., statistical) information. The anomaly detection system is based on the suspicious behavior attack signatures. The attack detection system works on the attack, creates alerts and forwarded to the alert generation. At the alert generation phase, accumulation of alert combines the alerts and makes it specific to an attack instance or type.

Generation of meta-alerts: The dire need of the new component created by an appropriate meta-alert is to produce and represent the abstract way component information. At any time, a component fresh alert is mixed and the equivalent meta-alert is also found. The following task is used to create a meta-alert:

- The scenario of the attack detection is more complicated and the meta-alerts sequences may be explored
- The detection of the distributed attacks (one-to-many attacks), interchanged between the meta-alerts and other attack agents
- The detection of the ongoing attack situation, is to inform a human security expert as to how they are generated by reports based on the meta-alerts stored information

Various attack instances are used to create a meta-alert from the most important formation until the removal of the equivalent component. For example, reports can be formed instantaneously subsequent to the formation of the component or updating reports of the sequence can be created at time intervals frequently.

Various tasks of the meta-alerts are used through they may add dissimilar characteristics. Those characteristics may include:

- Alert characteristics that an aggregated (e.g., Interval time that marks the commencement or intervals of source addresses and the end or lists, if accessible, of the attack incidence or targeted service ports)
- Using probabilistic model, attributes are extracted (e.g., the number of alerts allocated to the module or the distribution parameters)
- The detection layer is used to evaluate the aggregated alert (e.g., the categorization assurance or the attack type categorization)
- The current attack situation contains the information (e.g., the links to faults that originate from the similar or an analogous source or the number of current attacks of the identical or an analogous type)

Clustering of aggregated alerts: The attribute values are measured by way of number of alerts. The attack situation is important information and the lossless information is the quantity of data reduces attacker. The alerts originate from the attack instance to the clustered alerts. The alerts are generated based on abstract description of the alerts. The unlabeled observations carried out by the cluster structure for the attribute space analyzing the estimation task of the assignment to instances attack through the alert aggregation. The approach adopted is Maximum Likelihood (ML) estimation to improve the quality of clustering alerts. The several attributes are composed with alert space.

RESULTS AND DISCUSSION

Anamoly ddos attack detection for wired and wireless network algorithm

Step 1 (Initialization): The wired and wireless networks initialize specified time intervals that carries the input data stream.

Step 2 (Characteristic extraction): The initialized specific time data streams extract the data characteristics.

Step 3 (Evaluation of DDoS attack rule): The time specified data streams filtering evaluate attacker rules by the administrator. Step 2 provides the attacker rules.

Step 4 (Derive black listed rules): From standard black lists available in www lists are driven from the admin specified rules.

Step 5 (DDoS attack detection system using statistical attribute): The wireless and wired characteristics are extracted from the data stream (step 2), attack rules are carried out from the statistical features (step 3) and (step 4) measures the black list rules of attack alerts that are identified.

Step 6 (To create cluster alerts): Attack alerts of the clusters (from step 5) carries out the abnormal, normal and anomaly characteristics.

Step 7 (Create iteration): The anomaly DDoS detection rates are iterated from step 3-6.

Cluster validation of anomaly traffic attack alert instances: The performance of clustering the alert aggregation is evaluated with parameters such as detected instance, number of clusters, alert reduction rate, average run time and alert aggregation delay. Detected instance is measured as the clustering of alerts generated for particular instances. The number of clusters is estimated by aggregating the alerts and association of similar property alerts to a cluster. The alert reduction rate is the aggregation of the alert to one instance.

The size of the cluster increases with increased traffic volume, measured across various sessions. In addition, the size of the session is proportional to the size of the cluster. This shows that the missing data characteristics of traffic volume on alert aggregation for any instance are minimized. The association of traffic characteristic assigned in any one of the cluster for any given instances shows the performance of cluster based anomaly traffic attack. The traffic attacks are detected to the maximum level at minimum time of alert aggregation.

Neuro-fuzzy based clustering of ddos attack detection in network: The anomaly cluster and normal clusters are measured by the distance based values from the anomaly traffic data aggregates values. On the other hand, regular deviations on the data propagation modify the traffic data packets influenced by scrupulous nodes polluting the normal data packets. To establish the cluster of improper data aggregation traffic to the alternate changes in the propagation data.

To overcome the deficiency of improper traffic data clustering, the more interpretable and accuracy possession model of neuro-fuzzy is introduced to generate anomaly interrupt data packet clusters and normal data clusters from the traffic data streams. The fuzzy logic rules enable the cluster objects to appropriate clusters with testified data of the traffic streams detected with the statistical anomaly traffic attack detection model. Neural network is used to recognize the normal and anomaly data field patterns with advanced accuracy rate.

The proposed research has implemented the neuro-Fuzzy based clustering technique for a detection system. The fundamental insufficiency of clustering is used to initiate the value of K, a number which computes the count of clusters to be formed. This classification is done by applying the neuro-fuzzy clustering technique to deal with two segregations as normal and abnormal in which K is assigned to two values.

Performance measure of network anomaly detection: The simulations of the detection system are carried out at the ISP servers of the real time data traffic. The simulation performances are evaluated by the communication overhead and accurate detection of the proposed system. The default limit value is 5 for the retransmission. Harsh radio condition produces 10% error rate in channel.

The proposed method metrics evaluated the communication overhead and rate of detection in the proposed and existing schemes. The results show that attack time response of the detection rate is higher than the classical attack detection scheme. The response time of the detection rate is nearly 17% more for the network data traffic anomaly detection.

Identification of anomaly DDoS attack enhances response time on wired and wireless networks. The proposed system result shows that, rate of false negatives acquired are the fraction of frames created from wired and wireless attacks which is precisely evaluated in our scheme. The result shows that reduced set of features improves detection rate and the identification of false alarm positives rate which is minimal than proposed.

CONCLUSION

Internet traffic monitoring needs effective clustering algorithms for the real time data traffic analysis. Initially statistical techniques are deployed to independent data traffic streams. The statistical anomaly attack measurement performs of better analysis of several traffic anomaly properties that are usually hard to evaluate with conventional attack measures. The performance result concludes that the difference of the average in maximum traffic is 2.86 and the values are low for the average traffic. The anomaly detection efficiency is improved due to the clustered alert traffic data streams. The simulation shows that the cluster based alert aggregation anomaly detection increases its efficiency by the number of alerts that are reduced with respect to the detection attack simulation

result of 95%. The attack instances of the number of missing is near or equal to even zero and the attack instances of the delay for the detection differs only by 5 sec.

In the anomaly traffic detection, the attack instances and conventional attack provides statistical traffic detection, characteristic and alert aggregation of the clustering. For the network traffic, data is generated from huge volume, heterogeneity and dimensionality. The real time performance of our algorithms for analysis is more acceptable. The simulation performs several traffic analysis of the cluster alert aggregation which is extremely complex with conventional detection systems in wireless and wired networks. The simulation results prove that neuro-fuzzy system clustering technique performs better on attack detection rate, throughput and propagation delay.

REFERENCES

Ajil, K.S., P.K. Thapliyal, M.V. Shukla, P.K. Pal and P.C. Joshi *et al*., 2010. A new technique for temperature and humidity profile retrieval from infrared-sounder observations using the adaptive neuro-fuzzy inference system. Geosci. Remote Sens. IEEE. Trans., 48: 1650-1659.

Bhuyan, M.H., H.J. Kashyap, D.K. Bhattacharyya and J.K. Kalita, 2014. Detecting distributed denial of service attacks: Methods, tools and future directions. Comput. J., 57: 537-556.

Boppana, R.V. and X. Su, 2010. On the effectiveness of monitoring for intrusion detection in mobile Ad hoc networks. IEEE Trans. Mobile Comput., 10.1109/TMC.2010.210.

Dain, O.M. and R.K. Cunningham, 2001. Building scenarios from a heterogeneous alert stream. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 5, 2001, West Point, NY, USA., pp: 1-6.

Fadlullah, Z.M., T. Taleb, A.V. Vasilakos, M. Guizani and N. Kato, 2010. DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACM. Trans. Netw., 18: 1234-1247.

Francois, J., I. Aib and R. Boutaba, 2012. FireCol: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Networking, 20: 1828-1841.

Huang, Y.A., W. Fan, W. Lee and P.S. Yu, 2003. Cross-feature analysis for detecting ad-hoc routing anomalies. Proceedings of the 23rd International Conference on Distributed Computing Systems, 2003, May 19-22, 2003, IEEE, New Jersey, USA., pp: 478-487.

Julisch, K., 2003. Using Root Cause Analysis to Handle Intrusion Detection Alarms. Universitat Dortmund, Dortmund, North Rhine-Westphalia, Germany, Pages: 148.

Khezri, M. and M. Jahed, 2011. A neuro-fuzzy inference system for sEMG-based identification of hand motion commands. Ind. Electron. IEEE. Transac., 58: 1952-1960.

Lih, W.C., S.T. Bukkapatnam, P. Rao, N. Chandrasekharan and R. Komanduri, 2008. Adaptive neuro-fuzzy inference system modeling of MRR and WIWNU in CMP process with sparse experimental data. Autom. Sci. Eng. IEEE. Trans., 5: 71-83.

Mahajan, R., S.M. Bellovin, S. Floyd, J. Joannidis, V. Paxson and S. Shenker, 2002. Controlling high bandwidth aggregates in the network. J. Comput. Commun. Rev., 32: 62-73.

Ohsita, Y., T. Miyamura, S.I. Arakawa, S. Ata and E. Oki *et al*., 2010. Gradually reconfiguring virtual network topologies based on estimated traffic matrices. IEEE/ACM. Trans. Netw., 18: 177-189.

Perdisci, R., G. Giacinto and F. Roli, 2006. Alarm clustering for intrusion detection systems in computer networks. Eng. Appl. Artif. Intelli., 19: 429-438.

Pietraszek, T., 2004. Using adaptive alert classification to reduce false positives in intrusion detection. Recent Adv. Intrusion Detection Proc., 3224: 102-124.

Roesch, M., 1999. Snort: Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX conference on System Administration, November 7-12, 1999, Seattle, Washington, USA., pp: 229-238.

Wei, W., F. Chen, Y. Xia and G. Jin, 2013. A rank correlation based detection against distributed reflection DoS attacks. Commun. Lett. IEEE., 17: 173-175.

Zhong, S., T.M. Khoshgoftaar and N. Seliya, 2007. Clustering-based network intrusion detection. Int. J. Reliability Qual. Safety Eng., 14: 169-187.