Cluster based Statistical Anomaly Intrusion Detection for Varied Attack Intensities

M.Thangavel
Assistant Professor
Department of Computer Applications
Erode Sengunthar Engineering College
Thudupathi, Eorde – 638 057, India

Dr. P.Thangaraj
Professor& Head
Department of CSE
Bannari Amman Institute of Technology
Sathyamangalam, Erode-638 401, India

ABSTRACT
In today's Internet paradigm, the type of intrusion attacks becomes crucial in presenting effective improvement to anomaly intrusion attacks. Anomaly Traffic hacker attacks combined with traditional network intruders was a serious threat to network security. The existing work on intrusion detection and prevention of traffic attacks take much time, before which the intruder is spread across the network. The sensing mechanism in addition to rejection of an attack against intruders and keeps no record of the cause of the attack and its effects. In same time the actual happening of the attack detection method was left over unnoticing. This motivates to develop an effective attack mechanism of the cluster based anomaly intrusion detection.

Keywords
Network Traffic, Anomaly Intrusion Detection, Traffic Statistics, Cluster Data Streams.

1. INTRODUCTION
Our proposed cluster based statistical anomaly intrusion 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). Secondly, an intrusion alerts aggregation system introduced to generate meta-alerts from the statistical anomaly traffic intrusive data. 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 data stream approach (each observed alert is keep hold of for few seconds) to alert aggregation is highly time constraint. The cluster traffic streams contain all relevant information that is useful for the administrator, the process of intrusion detection to govern effectively.

The traffic data streams collected from the Net-Con server (Internet Service Provider popularly running at Erode Region) is statistically analyzed to detect anomaly intrusion attack by comparison with historical data sets of the standard Internet traffic steams. The statistically traffic anomaly intrusion detection rate is increased to 15% and the propagation delay is reduced to 7% compared to the existing ones. Then increase the data stream clustering of alerts in the second phase of our work produced, increase the throughput to 95%, while the number of missing clustering-alerts is extremely low. In addition, the cluster alerts are generated with a delay of few seconds after observing the first alert belonging to a new attack.

In intrusion detection systems on the Internet (IDS) is a measure for maximum protection for applications such as virtual private networks are converted to e-commerce applications, online banking transactions, etc., approaches examined to detect, prevent and reduce were malicious network traffic. For example, try to rule-based approaches such as IDS detect (Intrusion Detection System), issued the rules above apply to incoming traffic and possible attacks on the network intrusion in the vicinity of the victim. To the attacks of the novel, but need tools such as Snort IDS to be updated with the latest standards. Volume measurement studies on traffic numbers were used, are taken into account [2], and flows as potential signals analyzed to detect anomalies can in network traffic, while the system further treatment transport header, such as addresses and port numbers. Input data from multiple sources (ie all links in a network), while the work is focused on a single link at a time. Some approaches to proactively look for ways to remove the excess traffic at the source [3]. Controls on speed limits based have been taken to reduce the consumption of bandwidth monopoly to reduce the impact of the attacks, either at source or the target [3]. Previous work in [1] and work [2] examined the volume of traffic as a signal to the wavelet analysis and these previous studies have motivated much of our work. The proposal in this paper builds on earlier work and extends the statistical analysis of traffic data in the analysis over other packet header information such as addresses and port numbers in real time. It is significant predictability of the attacks, both in regard to its origin server and the input interface on a large ISP network. Small businesses seem to be the most common targets of these attacks. These results have important implications for attacking the defense.

IDS withstand various threats from the attackers, attack on the tools of network servers and hosts the exhibition through the misuse detection or anomaly detection techniques. IDS detects suspicious activity immediately created a warning that information about the origin, destination and the estimated rate of attack (eg SQL injection, buffer overflow or denial of service) contains. intrusive actions by an attack instance Unicast via network connections or causes many of the entries in the log file and the results in hundreds or even thousands of alerts. IDS is to detect attacks by nature, but does not focus on the distinction between cases of different attack. As a result of many IDS alerts generated at a low level of abstraction is extremely difficult for a human security expert to check the flood of calls and decisions -

Follow-up notification only thing that could be wrong with a relatively high probability.
IDS to detect attacks rather the species, but not focus on the distinction between cases of different attack. Even if the low prices of false alarms could easily lead to a high number of false alarms, when thousands of network packets or log file entries are checked. As a result, many identifications create alerts on a low level of abstraction. It is extremely difficult for a human security expert to examine the flood of calls and decisions made Alerts only I could be wrong with a relatively high probability. Warnings from as low of IDS, firewall, etc Alert belonging to the instance of attack, is summarized and meta-alert should be generated for these groups. It is a generative model with probabilistic methods. Adopted assault cases are considered as random processes to produce attention, our goal, these processes using approximate maximum likelihood parameter estimation techniques model. The work proposed clustering algorithm for the aggregation of alerts, the parameter estimation technique with the probabilistic model.

2. RELATED WORK

Intrusion detection is an active research area for a long time been. Most research with the problem of how to improve is the performance of the IDS, for example, greater number of types of attacks to increase the detection rate and maintain low false alarm rate, etc. distributed in cooperative IDS, intrusion detection can be unreliable node a process of Global Intrusion Detection by an introduction scanning engine of the cooperative. The local detection engine based on the classification algorithm is based on rules. In a later work [8], Yi et al. extends previous work on the detection of local anomalies and conducted a comparative analysis of the function to explore the relationships between functions and other functions using a classification algorithm, decision tree. In [9], the authors took a different line of research by the application of theories of hypothesis testing and approximation of a statistical framework for intrusion detection in ad hoc networks to develop.

Cause, diagnosis and treatment of abnormalities such as disturbances and attacks are on time is an essential part of daily operation of systems. Operators need to identify these anomalies occur, and then classify, determine the appropriate response. The biggest challenge in the automatic detection and classification of anomalies is that the anomalies can provide a wide range of events from the network abuse (eg hacker attacks cover [4], exploration [5], [6 worms]) to equipment failure (as cuts) to an unusual customer behavior (eg sudden changes in demand, flash crowds, the high volume flows), and even new, previously unknown events. A comprehensive system for the diagnosis of anomalies, that is able to be seen a number of different structural abnormalities of distinguishing between different types of errors and anomalies similar group with the immune system [7].

Most existing IDS be optimized in order to detect attacks with high accuracy. A major drawback is the large number of warnings generated. Current research focuses on the correlation of the descriptions (possibly multiple) IDS [10]. One step on the road to the correlation that arises is the reconstruction attack thread that can be seen as a kind of attack recognition instance. Not with the clustering algorithm, but a strict selection of alerts within a time window of fixed length for the source, destination, and the classification of the attack (kind of attack). The definition of this type of situation is also used in [11] cluster notifications. Alert clustering is used to groups that belong to the same attack occurrence notification. Despite calling the group, there is a cluster algorithm in the classical sense.

Another approach to alarm correlation is presented in [12]. A weighted operator, the similarity of the Internet as is used to decide whether two alerts are merged or not. However, as already indicated in [13] and [14], suffers from this approach are set by the large number of parameters. The similarity operator is presented in [15] has the same disadvantage that there are a lot of parameters that are specified by the user and little or no guidance for finding good values. In [16], another clustering algorithm based on the similarity measures presented rationally Internet with user-defined parameters. However, a closer look shows the value of the parameter that deteriorates the degree of similarity, in fact, a strict selection process for the origin and destination IP addresses and ports of the descriptions.

The disadvantages that arise from this are mentioned the same as above. In [17] presented three different approaches to security alerts. The first, very simple notification groups according to their origin IP address only. The other two approaches rely on supervised learning techniques. In [18], an offline clustering solution on the CURE algorithm is presented. The solution is limited to numeric attributes. In addition, the number of groups can be set manually. This is problematic as it is hoped, in fact, believe that the security is expert knowledge about the actual number of cases of assault in progress. The solution to the group described carefully in [13] is for us. A clustering approach based on the alerts link to backup more than once widely used in other more. The intention is to discover the reasons for the existence of most warnings to remove them later. An example of attack on our senses can be seen as a kind of cause, but in [13] of the cases are generally not classified as held for attacks that can occur only within a persistent limited time window. The structure of the groups will be created as a filter to reduce the number of alerts. The same idea, but was presented on a cluster algorithm to other line in [19].

The approach in this aspect of the role in the aggregation of alerts to improve the scalability and effectively with cases of anomalies in the flow of each proposed attack apparently not final. The statistical analysis for the effective detection of anomalies are a multidimensional indicator using the correlation of port numbers and the number of flows. In addition, our work produced in this working group of the tender by the statistical analysis on anomaly intrusion attacks seen. Warnings grouping shows all information with the anomaly detection of data traffic should flow in both normal and exceptional character. Items marked the follow-up evaluation of the simulation of our group on the aggregation of anomaly intrusion detection alarm on traffic statistics, based drove an effective means of detecting anomalies close to the source of any kind

3. STATISTICAL TRAFFIC ANOMALY INTRUSION DETECTION MODEL

The sources of traffic from servers between the client and spreads through the network generated. The traffic monitoring in the home network enables a detector to intruders, who escapes

the rules of access can be seen on the network. In addition to the intrusion of traffic generated by traffic sources with the normal circulation compared to the intrusion detection of traffic disruptions anomalies occur in the network. Abnormal intrusion traffic generated spread is measured by the statistical analysis by comparing the ratio of demand traffic load standard for data traffic for online time.

3.1 Traffic regulations Anomaly-based Intrusion Detection

The penetration of the transport anomaly is on sharing the functions of the network traffic and processing of statistical data. The scheme for the analysis of attack traffic anomaly shown in Figure 3.1. The traffic light splitter generates network traffic packet header traces or records data flow. The analysis of statistical data processing with the nature of the traffic sources by assessing its load demand through out the Internet (ie IP address, port number, the data transmission rate, delay, data loss and the bandwidth) correlated different time scales. Then, to detect attacks and anomalies are controlled by the speed bumps normal and abnormal traffic. The information discusses the historical thresholds are compared to see if traffic patterns outside the normal rules. created with the function to detect the source traffic to the network administrator of anomalies in network traffic alert.

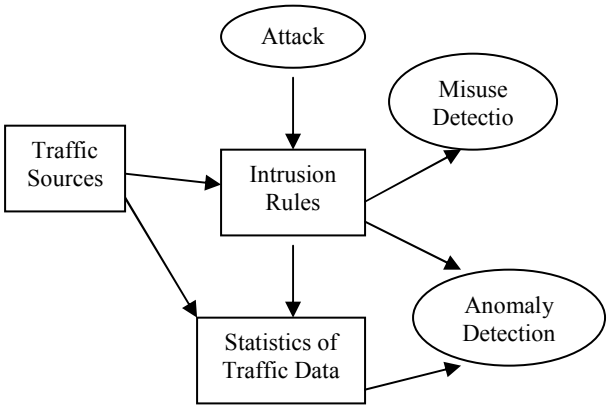

Figure 1: Anomaly Traffic Attack Analysis

3.2 About statistical processing of data traffic characteristics

The analysis of the demand for freight transport is carried out with the flow behavior of data over the network. 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 intrusion. 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 intrusion 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 intrusion 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 Intrusion 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, ie 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.

4. CLUSTER AGGREGATION ABNORMALITIES

Alarm Intrusion Detection the cluster-based alert aggregation, intrusion detection anomaly consists of three stages, ie the collection of the detected anomaly intrusion from the statistical analysis of data traffic and alerting, data stream aggregation and grouping the aggregated alarm.

4.1 Collection of intrusion detection and alarm anomalies

In this phase, discovered the abnormal intrusion traffic source, obtained from the statistical analysis of traffic the first to collect and save their homes are data path traffic. Stock Alerts recognized acquired features of incoming data from the network and client users. To extract the collection of detailed data, interesting and potentially valuable information (eg statistics) needed to build an appropriate event. The intrusion detection anomaly to evaluate the events of the attack and the search for known attack signatures (misuse detection) and the suspicious behavior (anomaly detection). The attack suspicious behavior collection creates anomaly intrusion detection alerts and to generate alerts. In the alert phase, alerted the accumulation of alert, and it connects to a specific instance or type of attack.

4.2 Data Flow Alarm Aggregation

The information in alerts, and alarm objects are grouped according to their size. Alert aggregation determines the values of attributes that are used as input for clustering alarm. Traffic

data used in the Internet in an event that is independent of a particular case of the attack for the aggregation. Traffic data used from the web on the instance of the attack are different in a process of aggregation of warnings to the various instances of attack. Dependent, as the source IP address of the attacker and independent as the destination port to identify the usually 80 in the case of Web-based attacks.

4.3 The group has warnings

Attack of the cases, the cause number of calls with different attribute values. The object of the aggregation alarm is the allocation of cases by the use value of unlabeled observations, and only by analyzing the structure of groups in the feature space. Reconstruct the attack scenario. Cluster generates alerts on the abstract description of the warning is coming from an instance of an attack based. The data set is strongly reduced without important information. Consider the example of the attack and the alarm will be generated randomly according to a certain multivariate probability distribution. The approach is Maximum Likelihood (ML) estimate the quality of the grouping to improve notification. The warning area is composed of several attributes. Categorical attributes of a multinomial distributed data cluster descriptions. Rebuilding an observed sample attack scenario, an estimate of all parameters of the mixture distribution.

5. SIMULATION OF CLUSTER-BASED STATISTICAL ANOMALY INTRUSION DETECTION

The simulation is performed for the evaluation of group-based intrusion anomalies aggregation approach warning. Use of simulation data sets from real data in the global network traffic gateway servers collected over ISP. The simulation was carried out on IBM PC-compatible computer with Intel Core 2 Duo 2.5 GHz carried out, 2GB RAM and 250 GB hddd in the NS2 simulator. The simulation uses the TCP / IP network stream as input and analyzed 104 cases of attacks against TCP (equivalent to more than 20 types of attacks) in response were launched against various target host. Extract statistical information from network traffic data. By applying a variable threshold to the output of the cluster aggregate attribute descriptions are listed with cases of attacks associated.

The onset of resistance properties in the amount of true positives (TPR, the number of true positives by the sum of true positives and false shared negatives) against false positive rate (FPR, the number of false positives, divided by the number of false positives and true negatives) for incoming traffic from the processing of statistical data to detect the anomaly intrusion alerts trained extracted. The attributes of the terms used are the source and destination IP address, port of origin and destination, the type of attack and the time differences created (based on the creation of time stamps).

The number of alerts that are generated from the traffic data from multiple sources stored in the storage of aggregates alarm. The number of cases of assault, which produces at least one alarm detector layer with 104 cases of attacks in the record. There are few cases of attacks only a single alarm is not created, ie, these cases have already been lost in the detection limit. These cases are lost because only a few samples of appropriate training attack types in the amount of data that results in poor generalization performance alert aggregation.

The traffic was recorded by the open-source IDS that all instances of the attack were released and produced recognizes analyzed. The alert is the same as the format used for anomaly intrusion detection. To set a high level of recovery that is activated all available rules the official standard, and the common law standard for intrusion detection. The activation of rules leads to a false alarm rate of 0.33%. The IPA is based on the assumption that all calls that are not classified to the type of attacks that are launched from false alarms.

6. RESULTS AND DISCUSSION OF GROUP-BASED INTRUSION ALARM STATISTICAL ANOMALIES

The intrusion detection performance is measured with statistical anomaly-based attack traces network traffic consists of several bands at the time of sampling. The weighted correlation traces of the traffic is used to transform statistical data anomalyl intrusions. smooth development of transport (with period T = 24 hours) can be defined as follows:

Interval 0 – t1 (night traffic) y(t) = A1
Interval t1 – t2 (increase of morning traffic)

$$y(t) = A_1 + (A_2 - A_1).\frac{t - t_1}{t_2 - t_1}$$

Interval t2 – t3 (daily traffic) y(t) = A2
Interval t3 – T (fall of night traffic)

$$y(t) = A_2 - (A_2 - A_1).\frac{t - t_3}{T - t_3}$$

where A1, A2, the amplitude of the traffic pattern t1, t2, t3 and T represent the values of time intervals and their values vary from user to user. For some users, in the days of the weekend in the fall of the average daily traffic of about 25%. In this sense, the value of A2 for the same user can not be regarded as constant in all periods of T. were to determine the range of expected values of the traffic in a given time during the day 24 samples from the curve of the traffic from all segments the time taken: 0 - t1, T1 - T2, T2 - Descriptive statistics were applied T. on them to calculate the limit of the upper and lower control - T3 T3. The arithmetic mean and standard deviation of the samples was about 95% confidence intervals, maximum and minimum traffic volume is determined calculated. The volume of traffic is outside the specified range is specified as a network anomaly (in terms of statistical estimates of attributes).

6.1 statistical anomaly intrusion detection traffic

Traffic monitoring samples are from the ISP with the mean, standard deviation, maximum and minimum values for the statistics against bands from various time points taken shown in Table1.

Table 1: Statistical Evaluation on the traffic samples

Statistical Datum	09-24 h (Mb/s)	24-03 h (Mb/s)	03-07 h (Mb/s)	07-09 (Mb/s)
Average	23.15	11.87	8.07	15.87
Standard deviation	3.65	3.36	1.83	4.93
Max (99%)	34.11	21.96	13.57	30.66
Min (99%)	12.18	1.77	2.57	1.07

In order to determine the extent of the expected values for traffic signs all instances. To determine whether the calculated values, two measurements are performed at intervals of one month and receive the maximum is shown in Table2:

Table 2: Maxima on two measures

	Daily (Mb/s)	Weekly (Mb/s)	Monthly (Mb/s)
1st measurement	33.9	29.7	30.9
2nd measurement	33.1	33.4	32.4

The analysis of the results of the above table to the conclusion that there is no case exceed the calculated maximum traffic (34.11 Mb / s, as in Table 6a). The statistical analysis includes the establishment of the size and variation in levels is characteristic of the different periods of time. In this sense, the observed values of average and maximum traffic from different users, in daily newspapers, weekly and monthly tickets. Figure 6b, it is concluded that changes are relatively small in the maximum and average daily traffic. The average value of the difference in traffic is up 3.26%, while the average value of 8.44%. If the statistical parameters of network traffic, such as mean and standard deviation are on the traffic distribution given the parameters given day is fixed for the other days also. The experiment was carried out a specific timeline of two months to monitor and analyze their statistical summary measures. Table throughput of data transmission through the detection of traffic anomalies penetration shown in Table 3.

Table 3: Performance of Traffic Anomaly Intrusion Detection

Number of Nodes	25	27	29	31
Throughput (kbps) (Statistical Anomaly Traffic Intrusion Detection)	990	985	980	975
Throughput (Kbps) (Existing Rule based Anomaly Detection)	982	975	970	960

Our experimental results shows the output of the simulation by varying the number of nodes in the network traffic for anomaly intrusion detection. There is a marked change in the perception of data communications for the proposed statistical anomaly intrusion detection based Intrusion Detection versus the rule. As the number of nodes increases, the power drop. For non-threshold model of the bandwidth of high performance anonymous traffic detection with the model of the bandwidth threshold.

Given the large number of attacks, it is quite difficult to accurately define the first line of attack time. Some attacks are immediately recognizable by the form of one or more packages of work for a short period of time. Each attack has a defined beginning, is the starting point is not always detectable at the time of occurrence. The proposed work recognizes these types of attacks seen in real time (real time detection) in real time, expressed as the time interval of 5 years - 5 min. The response time of security systems in the occurrence of attacks changed with time.

6.2 The cluster validation instances anomaly intrusion Traffic Alert

The performance of the alarm aggregation group is recognized as such analyzed parameters, the number of groups, the rate of reduction of the tender, the average delay career and alarm aggregation. The detected generated measured as a grouping of alerts for certain cases. The number of groups estimated by the aggregation of alerts and warnings association properties similar to a cluster. The reduction is the addition of warning to an instance. The average duration is measured in milliseconds, for each alarm. Alert aggregation delay is to make as the waiting time notification of the respective cases measured.

The results for the group based on anomaly intrusion alerts are shown in table 4. For all experiments used the parameter settings to them. The number of cases was about the availability of slot machines such as the traffic flow data provided. The traffic volume is such intrusion alarm generated for the detection of anomalies. The cluster size is measured by the number of warnings similar to the instance.

Table 4: Clustering of anomaly traffic intrusion alerts

Instances	Number of sessions	Traffic Volume (Kb)	Cluster size (No. of clusters)
1	26	120	13
2	23	114	9
3	28	142	15
4	20	98	7

The group based the proposals receive traffic anomaly intrusion showed in figure 3 and Figure 4. Figure 3 shows that are generated throughout the volume of traffic, session-based alerts for any event at the specified time interval. The presentation of the results shown in (Fig. 2) shows that the largest volume of traffic at the meeting for more. The variation of the session to reduce the volume of traffic that the detection of the associated alarm aggregation shows in groups

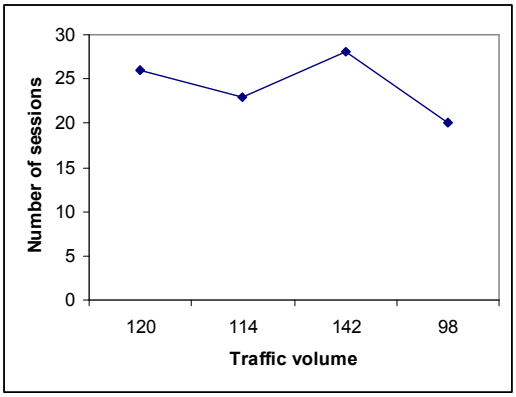

Figure 2: Instance Performance Session for the traffic volume on the base category Anomaly Intrusion Detection

Figure 3 shows a graph between the volume of traffic on the cluster size. Group increased with more traffic than one session. In addition, the session size is proportional to the size of the cluster, indicating that the properties of all traffic accidents occurred during the session somehow placed in one of the cluster. This shows that the absence of features of the traffic on the aggregation of the warning is minimized before a court. The Federation of Transport characteristics associated in any of the union of all instances because the cluster shows the performance-based intrusion traffic anomaly is detected at the highest level in the shortest time alarm aggregation.

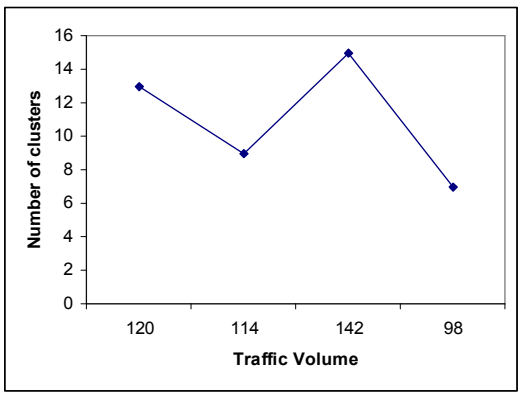

Figure 3: Performance cluster size for the volume of traffic on the basic category Anomaly Intrusion Detection

7. CONCLUSION

To prevent Internet traffic monitoring of multi-dimensional and heterogeneous data streams needs invaders anomalous effective clustering algorithms for the analysis of traffic data in real time. First, statistical methods in the marketing of independent data streams implemented the combined attack traditional intrusion and anomaly intrusion study. The characterization of this as the attack duration, number of packets, packet type, and the dominant protocol type correspond fairly well to the range of statistical data with historical data. The statistical measurement anomaly intrusion attack, better analysis of the different characteristics of traffic anomaly is usually difficult to measure with traditional measures of the intrusion.

The expected maximum (allowed) the value of the network traffic is checked for different users in different time periods and cases of distance measures in time. With performance results, we conclude that changes in the maximum and average daily traffic is relatively small, the average value of the difference in traffic to 2.86%. Intrusion group generated attention, the units will vary the properties involved in the attack anomaly intrusion detection. The efficiency of anomaly intrusion detection is improved because traffic streams contain clusters alert all relevant information to move carefully on the attack scenarios.

The simulation carried out by two different data sets and showed that cluster-based anomaly detection for intrusion alarm aggregation efficiency increases by the change detection and traffic reports grouped multiple streams of possible future attacks shows. The percentage reduction on the number of calls rose to 95% in our simulation. The number of missing cases of attack is very low or even zero in some of our simulation and the delay for the detection of cases of attack is in the range of a few seconds only.

8. REFERENCE

[1] A. Ramanathan, “WADeS: A tool for distributed denial of service attack detection” M.S. thesis, TAMU-ECE-2002-02, Aug. 2002.

[2] P. Barford et al., “A signal analysis of network traffic anomalies,” in ACM SIGCOMM Internet Measurement Workshop, Nov. 2002.

[3] J. Mirkovic, G. Prier, and P. Reiher, “Attacking DIntrusion at the source,” in IEEE Int. Conf. Network Protocols, Nov. 2002.[6] E. Kohler, J. Li, V. Paxson, and S. Shenker, “Observed structure of addresses in IP traffic,” in Proc. ACM IMW, Nov. 2002.

[4] Lin Chen, and Jean Leneutre, “A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks” IEEE Transaction on Information and Forensic and Security Vol.4 No.2, June 2009 165

[5] F. Naït-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks," in IEEE Communications Magazine. vol. 46, April 2008, pp. 127-133.

[6] S. Khurana and N. Gupta, "FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks," in Second International Conference on Emerging Security Information, Systems and Technologies, secureware

[7] Aickelin, U., J. Greensmith, and J. Twycross. "Immune System Approaches to Intrusion Detection - A Review ",Natural Computing, Springer, in print, 2007

[8] Y Huang, W Fan, W Lee, and P. S.Yu, “Cross-feature analysis for detecting ad-hoc routing anomalies,” in Proc 23th Int. Conf. Distributed Computing Systems (ICDCS) Providence , RI , May 2003

[9] D. Subhadrabandhu, S. Sarkar, and F. Anjum, “A statistical framework for intrusion detection in ad hoc networks,” in INFOCOM 2006, Barcelona , Spain

[10] F. Valeur, G. Vigna, C. Kr¨ ugel, and R. A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, 2004, pp. 146–169.

[11] D. Li, Z. Li, and J. Ma, "Processing intrusion detection alerts in large-scale network," in International Symposium on Electronic Commerce and Security, Guangzhou , China , 2008, pp. 545–548.

[12] A. Valdes and K. Skinner, "Probabilistic alert correlation," in Recent Advances in Intrusion Detection, ser. LNCS, W. Lee, L. Me, and A. Wespi, Eds., vol. 2212. Berlin , Germany : Springer, 2001, pp. 54–68.

[13] K. Julisch, "Using root cause analysis to handle intrusion detection alarms," Ph.D. dissertation, Universit¨at Dortmund, Germany, 2003.

[14] T. Pietraszek, "Alert classi.cation to reduce false positives in intrusion detection," Ph.D. dissertation, Universit¨at Freiburg, Germany, 2006

[15] F. Autrel and F. Cuppens, "Using an intrusion detection alert similarity operator to aggregate and fuse alerts," in 4th Conference on Security and Network Architectures, Batz sur Mer , France , 2005, pp. 312–322.

[16] G. Giacinto, R. Perdisci, and F. Roli, "Alarm clustering for intrusion detection systems in computer networks," in Machine Learning and Data Mining in Pattern Recognition, ser. LNCS, P. Perner and A. Imiya, Eds., vol. 3587. Berlin , Germany : Springer, 2005, pp. 184–193.

[17] O. Dain and R. Cunningham, "Fusing a heterogeneous alert stream into scenarios," in Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications, Philadelphia, PA, 2001, pp. 1–13.

[18] M. S. Shin, H. Moon, K. H. Ryu, K. Kim, and J. Kim, "Applying data mining techniques to analyze alert data," in Web Technologies and Applications, ser. LNCS, X. Zhou, Y. Zhang, and M. E. Orlowska, Eds., vol. 2642. Berlin , Germany : Springer, 2003, pp. 193–200.

[19] J. Song, H. Ohba, H. Takakura, Y. Okabe, K. Ohira, and Y. Kwon, "A comprehensive approach to detect unknown attacks via intrusion detection alerts," in Advances in Computer Science – ASIAN 2007. Computer and Network Security, services. LNCS, I. Cervesato, Ed., vol. 4846. Berlin, Germany: Springer, 2008, pp. 247–253