A Flow-based Algorithm for Statistical Anomaly Detection

Petar Čisar

Telekom Srbija, Subotica, petarc@telekom.yu

Sanja Maravić Čisar

Polytechnical Engineering College, Subotica, sanjam@vts.su.ac.yu

Abstract: This paper deals with statistical anomaly detection as one of the essential parts of intrusion detection systems. With help of data mining, combined with statistical quality control, the authors tried to work out a way of determining maximal tolerated traffic. This value can be used as input data for network monitoring and alerting software (NMS). Besides that, the paper presents a flow-based algorithm for statistical description of 'normal' network's behaviour.

Keywords: IDS, threshold, false alarms, statistics, algorithm, network monitoring, anomaly detection

1 Introduction

An Intrusion Detection System (IDS) generally detects unwanted manipulations to systems. The manipulations may take form of attacks by skilled malicious hackers or using automated tools. An IDS is required to detect all types of malicious network traffic and computer usage that can not be detected by a conventional firewall. Even the best packet - filtering can miss quite a lot of intrusions.

An IDS may be categorized by its detection mechanism on: anomaly - based, signature – based or hybrid (uses both of previous technologies).

The performance of a network IDS can be more effective if it includes not only signature matching but also traffic analysis. By using traffic analysis, anomalous traffic is identified as a potential intrusion. Traffic analysis does not deal with the payload of a message, but its other characteristics.

2 Network Statistical Anomaly Detection (NSAD)

NSAD attempts to dynamically understand the network and statistically identify traffic that deviates from normal traffic usage and patterns.

NSAD systems can be broken down further into threshold, baseline and adaptive systems, with each looking for different triggers to identify anomalous behaviour.

Threshold NSAD Systems – These systems allow the administrator to configure thresholds to certain network usage parameters and report the passing of a configured threshold as a potential attack. For instance, threshold NSAD may allow the administrator to configure a threshold of 3000 request/minute to a Web server. Then, any time that the system measures more then 3000 requests in a minute it will be reported as an anomaly and a potential attack.

Baseline NSAD Systems – This systems detect and report statistical anomalies by establishing a baseline of some network usage pattern and then reporting deviations from that baseline as a potential intrusions. For example, baseline NSAD can look at total network traffic volume by hour and establish a range of 'normal' values for that parameter. For example, 'on Mondays between 9am and 10am the total traffic volume is expected to be between 80 and 120 megabytes'. Then, if the system detects more or less traffic in that hour, it is reported as an anomaly and a potential attack.

Adaptive NSAD Systems – Since usage patterns change over time, NSAD systems attempt to adapt to these changes continually. Adaptive systems accomplish this by using 'statistical usage profiling'. Basically, the system maintains two sets of usage data – a long – term usage profile and a short – term observed usage. To detect attacks, a modern NSAD system compares the short – term usage to the long – term profile and reports deviations that are considered 'statistically significant' as a potential attacks. The system further blends the short – term observed usage into the long – term usage profile to realize adaptation.

The advantages of NSAD:

- it can detect attacks that would be missed by other detection mechanisms and is much more successful at detecting modified, novel and new attacks than signature-based IDS

The weaknesses of NSAD:

- attack reporting is hard to interpret or turn into an action
- traffic in large organizations is constantly changing, making it virtually impossible to establish a baseline
- attacks can be contained within the baseline and an organization would never know
- attackers can train the adaptive system to see attack traffic as normal

- false alarms generation
- robust and massive profiles

2.1 Malicious NSAD Training

As adaptive NSAD systems continually update their long – term usage profile to adapt to changing network usage patterns, the systems open themselves up to a serious and detrimental attack, usually referred to as the 'NSAD training attack'. An attacker that knows that there is an NSAD system monitoring the network can influence the monitored usage pattern slowly enough to not be detected and in such a way that the attacker will eventually get the adaptive baseline to a point where it recognizes an attack as normal traffic.

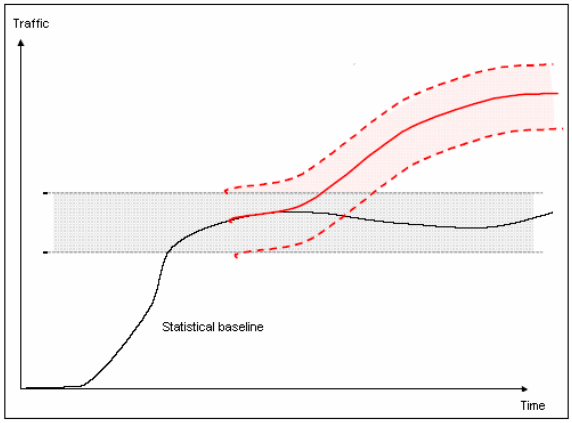

Figure 1
NSAD training

For example, imagine an NSAD system that monitors network volume. Assume that the current baseline is 80 to 120 megabytes per – hour and that the attack wants to flood the network with 500 megabytes per – hour. The attack can start by maintaining a constant network volume of 110 megabytes per – hour. This may bring the beseline to the range of 100 to 140 megabytes, at which time the attacker will increase the volume to 130 megabytes per – hour, and so on. The attacker can repeat this process until the system's baseline is in the vicinity of 500 megabytes per – hour. At this point the attacker can launch his attack and the system will never spot it.

3 Approaches to Anomaly Detection [7]

Alarm – an event when behaviour deviates from normal.

Normal behaviour can be:

- specified, i.e. with threshold establishing (e.g. load < 0.7)
- learned
    - ✓ mean and standard deviation statistics
    - ✓ time series analysis – the advatage is that they take into account time correlation
    - ✓ other approaches: bayesian statistics, neural networks, expert systems, statistical decision theory etc.

Approaches to anomaly detection:

I

- non – adaptive (fixed threshold) - This approach is not robust enough. Fixed threshold will probably fail due to normal / regular traffic variations.
- adaptive
    - ✓ adaptive threshold (AT) – adaptively measuring of the mean rate. Alarm event – when the mean rate in interval T becomes greater than some percentage (e.g. > 150% of the mean).
    - ✓ adaptive threshold (AT - k) – Alarm event – when the threshold is exceeded in #k consecutive intervals.
    - ✓ CUSUM (Cumulative Sum) – sum the volume sent above the average factor. Alarm event – when the volume becomes greater than some threshold.
    - ✓ other algorithms

II

- flow-based anomaly detection
- packet-based anomaly detection

Variables that can be measured:

- aggregate traffic volume
- traffic volume per flow
- source/destination IP address
- source/destination port

- network protocol (IP, ICMP, ...)
- application protocol (distinguished by port number)
- protocol options
- content (size, type, characteristic strings, ...)
- other features (sequence number, TCP flags, TTL, ...)

4 Performance Measurement

There are several parameters for measuring the performance of NSAD algorithm. Some of them are:

- attack detection ratio
- false alarm ratio
- detection delay – computational efficiency
- robustness
- how tunable the algorithm is – tradeoff between detection ratio, false alarm ratio and detection delay
- evaluate above for different attack types: intensity of attack (amplitude), how fast it reaches the peak etc.

Definition of detection rate:

✓ An instance of anomaly identified as normal is a case of missed detection.

✓ N_{attack}: the total number of attacks in the test set

✓ N_{missed}: the number of missed instances

✓ %detected = $(N_{attack} - N_{missed}) / N_{attack} * 100$

Definition of false positives:

✓ An instance of normal record falsely identified as anomaly is a false positive.

✓ N_{normal}: the number of normal records in the test set

✓ N_{false}: total number of false positives

✓ %falsepositives = $N_{false} / N_{normal} * 100$

On the basis of experimental results of several researchers [7], performance of NSAD depends on attack characteristics: intensity of attack (peak - value), time to reach the peak.

5 A Suggestion of a Method for Determining Maximal Tolerated Traffic

In order to eliminate the malicious NSAD training by a hacker and according to considerations from the chapter 2.1, the authors of this paper are of the opinion that it is needed to define the maximal tolerated value of traffic. This value would incorporate normal / regular traffic variations and would represent the highest threshold.

Maximal value of traffic is possible to determine, with accepted probability, by usage of descriptive statistics, method of confidence interval and 6σ concept. In order to achieve the highest possible accuracy in determining the maximal value of traffic, descriptive statistics will be applied on local maximums of the traffic curve at a definite time interval. Traffic samples are taken in moments when the traffic curve reaches the local maximums. Namely, if analysis is done with random samplings, the result would not include a sufficient number of representative maximum points, so then the final result would not be precise enough. In that way, a set of local maximums is created on which further adequate methods will be apllied.

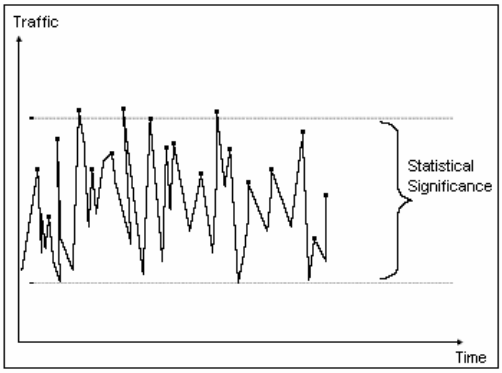

Figure 2
Local maximums

This approach to the problem is the more accurate the longer the time interval of observation is and the more local maximum points are included. In spite of that, it is necessary to pay attention to taking the largest values of all observed local maximums, because their influence on final result is the most significant. We can treat this sampling as a random sample. If the number of samples n is large enough (n>30), i.e. it is the case of a large sample, it can be considered that this sampling has normal distribution.

5.1 The Analysis of Suggested Method

The method above will be applied to authentical data got by traffic analizer in Polytechnical Engineering College in Subotica and its grafical review of traffic intensity for different period of observation.

The results obtained by these suggested methods considerably differ from each other. In order to decide which fit results best to the real situation shown on diagrams, it is necessary to compare the obtained results with the values from diagrams. It has to be stated that the diagrams represent the network status without attacks on it. The threshold set to 6σ-value gives less false alarms, but tolerates greater possible malicious traffic. But, lower threshold in the same time means that IDS will react to a real alarm earlier and, unfortunately, will generate more false alarms.

On the basis of statements made above, the authors of this paper are of the opinion that as optimal value, from the aspect of sensitivity to real alarm and the number of false alarms, the mean of maximal values obtained from described two methods could be accepted. In the actual case, that value would be (136,956 kBytes + 371,644 kBytes/s) / 2 = 254,3 kBytes/s, which excellently fits in real situation.

6 An Algorithm for Statistical Anomaly Detection

One of the possible ways for defining 'normal' behaviour of a network traffic is, in case of none attack, to establish several appropriate volume levels. For example: $T_3 = 3/7\ T_{max}$, $T_4 = 4/7\ T_{max}$, $T_5 = 5/7\ T_{max}$ and $T_6 = 6/7\ T_{max}$, where T_{max} is the maximal tolerated traffic. After that, the traffic curve should be followed and count the number of cutting points with these thresholds. Thus, we get the referent number of cuttings N_i related to a concrete level and long enough time interval T: N_3, N_4, N_5 and N_6. If some of the measured number during the traffic investigation Δt becomes greater than appropriate referential $n_i = N_i \times (\Delta t/T)$, that moment indicates the appearance of anomaly.

Due to easy setting the triggers, this algorithm is suitable for usage in network monitoring and alerting softwares.

With aim of detecting different types of traffic, two thresholds are important to be recognized, as triggering values:

$T_1 = 1/7\ T_{max}$ – threshold of minimal traffic (e.g. night traffic).

$T_2 = 2/7\ T_{max}$ – threshold of minimal normal traffic. If the average traffic exceeds T_2, then we can say that in network exists normal traffic (during working time with a greater part of active computers).

If T_1 is set too low, some of employees working during the night could generate false alarms.

Because of the results given in [8], the observation interval for average Δt shoud not be longer than 15 minutes. It means if the average traffic is less than T_1 for a period of 15 minutes, then we speak about none traffic. Between T_1 and T_2 is low traffic, while for average greater than T_2, the traffic is intensive.

According to all of said above, it is possible to define the following table of actions, depending on some characteristic situations.

Previous value	Last value	Action
$< T_1$	$> T_1$	attack - alarm
$> T_2$	$> T_2$	conditions check n_i – attack ?
x	$< T_1$	no attack - no alarm
$x > T_1$	$T_1 <$ value $< T_2$	no attack - no alarm
x	$> T_{max}$	attack - alarm

Table 1
Definition of actions

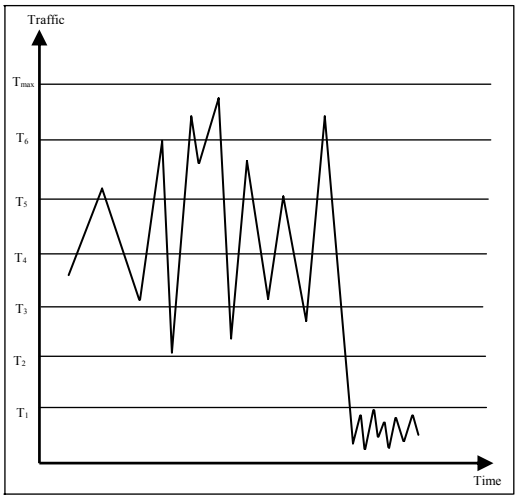

Figure 3
Illustration of the algorithm

7 Using of Network Monitoring Software (NMS)

In practice, there are softwares for network monitoring and alerting. They are capable for adjusting triggers and actions. In that sense, administrator can set the threshold value and duration of changes at the same time. It means that the software can count and alert on all changes in traffic when the defined thresholds and durations are exceeded.

Properly chosen duration of changes can significantly decrease the false alarm ratio. According to [8], 50% of DoS attacks are less than ten minutes in duration, 80% are less than thirty minutes, while 90% last less than an hour. In that sense, the authors of this paper are in opinion that time interval of 10 – 30 minutes gives the best definition of the great part of attacks.

The table 1. could have practical importance if used with an adequate network monitoring software. The basic condition for usage of such a software is its ability of comparing an actual value with the value from the previous interval. In that sense, the great help is having functions such as, for instance:

change - returns the difference between last and previous value

count – number of succesfully retrieved values for period of time. Parameter defines the lenght of the period in seconds.

avg – average value for period of time. Parameter defines the lenght of the period in seconds.

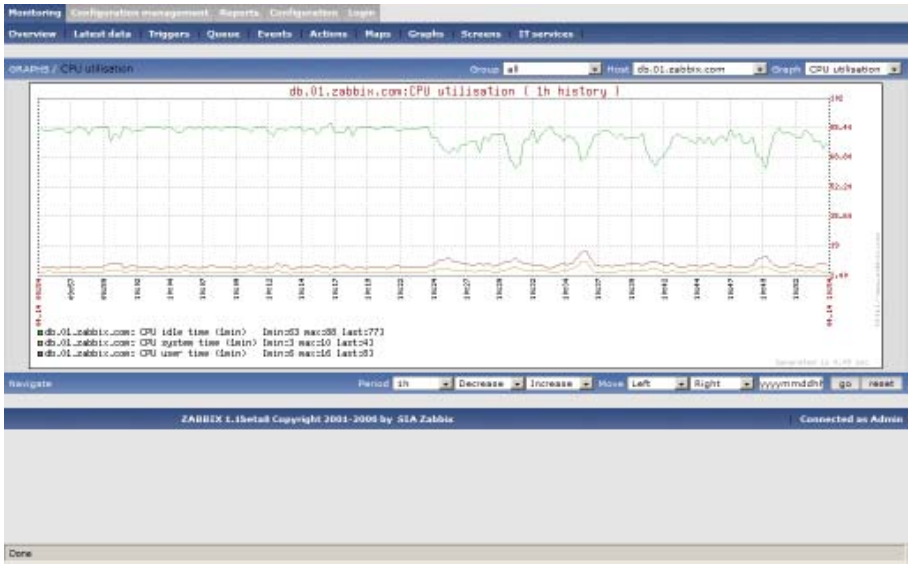

Figure 4
NMS diagram

Conclusion

The statistical flow-based algorithm presented in this paper differs from the majority of published flow-based approaches. It offers a simply usable statistical way for definition of anomalies, without need of creating massive profiles. Well defined multiple alarm events, in cooperation with appropriate network monitoring software, could provide satisfied tool for real – time network protection from unwanted attacks.

References

[1] Sorensen Sarah: Competitive Overview of Statistical Anomaly Detection, White Paper, Juniper Networks, 2004

[2] Gong Fengmin: Deciphering Detection Techniques: Part II Anomaly – Based Intrusion Detection, White Paper, McAfee Security, 2003

[3] SANS Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?, http://www.sans.org/resources/idfaq/anomaly_detection.php

[4] Intrusion - detection system – Wikipedia, http://en.wikipedia.org/wiki/Intrusion-detection_system

[5] Montgomery Douglas: Introduction to Statistical Quality Control, 5th Edition, John Wiley & Sons, 2005

[6] Statistical Quality Control, www.wiley.com/college/reid/0471347248/samplechapter/ch06.pdf

[7] Siris A. Vasilios: Denial of Service and Anomaly Detection, SCAMPI BoF, Zagreb, 2002

[8] CAIDA, the Cooperative Association for Internet Data Analysis: Inferring Internet Denial-of-Service Activity, University of California, San Diego, 2001

[9] Strong Richard: Intrusion Detection Systems: Fixed vs Learning Thresholds, http://www.ece.rutgers.edu/~parashar/Classes/03-04/ece572/project-reps/