ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING
Tome X (Year 2012) – FASCICULE 3 (ISSN 1584 – 2673)

[1.] Petar ČISAR, [2.] Sanja MARAVIĆ ČISAR

NETWORK STATISTICAL ANOMALY DETECTION BASED ON TRAFFIC MODEL

[1.] TELEKOM SRBIJA, SUBOTICA, SERBIA
[2.] SUBOTICA TECH, SUBOTICA, SERBIA

ABSTRACT: *Intrusion detection (ID) is the act of monitoring and capturing intrusions into computer and network systems which attempt to compromise their security. When an ID system identifies intrusions as unusual behavior that differs from the normal behavior of the monitored system, this analysis strategy is called anomaly detection. This paper explains the proposal of approximate curve of network traffic of major users based on historical data. Applying descriptive statistics on network samples in time intervals defined within traffic curve model for a longer measuring period, multiple control limits are calculated. These values are then treated as fixed network thresholds for another measurement. The analysis of false alarms confirmed the applicability of this anomaly detection method in network practice. In addition, the paper provides an overview of different approaches to anomaly detection as well as parameters for measuring the performance of statistical anomaly detection algorithms.*
KEYWORDS: *traffic curve, modeling, descriptive statistics, control limits, anomaly detection, false positives*

INTRODUCTION

With rapidly growing implementation of information and communication technologies, networked computer systems are playing an increasingly vital role in our society. Along with the important benefits that the Internet brings, it also has its negativities. Specifically, new threats are created everyday by individuals and organizations that attack and misuse computer systems. In addition, the severity and sophistication of the attacks is also growing. Earlier, the intruders needed profound understanding of computers and networks to launch attacks. However, today almost anyone can exploit the vulnerabilities in a computer system due to the wide availability of attack tools.

The standard approach for securing computer systems is to use well known security mechanisms, such as firewalls, authentication algorithms, Virtual Private Networks (VPN), that create a protective zone around them. Unfortunately, such security mechanisms frequently have inevitable vulnerabilities and they are usually not sufficient to ensure overall security of the infrastructure and to ward off attacks that are continually being adapted to exploit the system's weaknesses often caused by inadequate design and implementation flaws. This has created the need for security technology that can monitor systems and identify computer attacks. This component is called intrusion detection and is a complementary to conventional security mechanisms.

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.

Since the first concept of intrusion detection was developed, many IDSs have been proposed both in the scientific and commercial world. Although these systems are rather diverse in the applied techniques, most of them rely on a relatively general architectural framework (Figure 1), which consists of the following wholes [14]:

- *Data gathering device (sensor) is responsible for collecting data from the monitored system.*
- *Detector (ID engine) processes the data collected from sensors to identify intrusive activities.*
- *Knowledge base contains information collected by the sensors, but in preprocessed format (e.g. database of different attacks and their signatures, filtered data, data profiles, etc.).*
- *Configuration device provides information about the current state of the IDS.*
- *Response component initiates actions when an intrusion is detected. These responses can either be automated (active) or involve human interaction (inactive).*

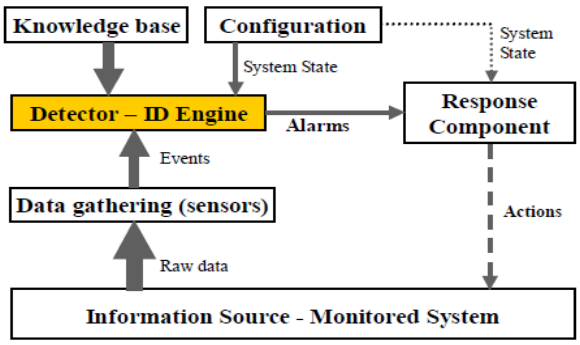

Figure 1. Basic Architecture of IDS

This paper deals with statistical analysis of network traffic curves of major users. Based on the identification of common characteristics, the general model will be formed and the function of traffic defined, which represents the necessary condition for creating an algorithm for statistical detection of network anomalies.

NETWORK TRAFFIC CURVES

This research is focused on the study of forms of network traffic curves, in order to determine the specific periodic regularities. Confirmed conclusions would be the basis for the formulation of statistical algorithm for detecting network anomalies based on fixed thresholds. The correctness of this approach is tested by numerical values of network flow in the measuring period of a month. For the calculation of the upper threshold, the flow rates for the first 15 days were used, while the testing of obtained results was realized on network values for another 15 days.

For the analysis of network traffic curves, the research uses daily, weekly and monthly graphic illustration of several larger Internet users that derives from the popular network software MRTG (Multi Router Traffic Grapher), which is related to the period of one day, week and month. Without the loss of generality, the graphical presentation of curves from three users is given below, noting that the observed traffic curves of other users do not deviate significantly from the forms shown here [3].

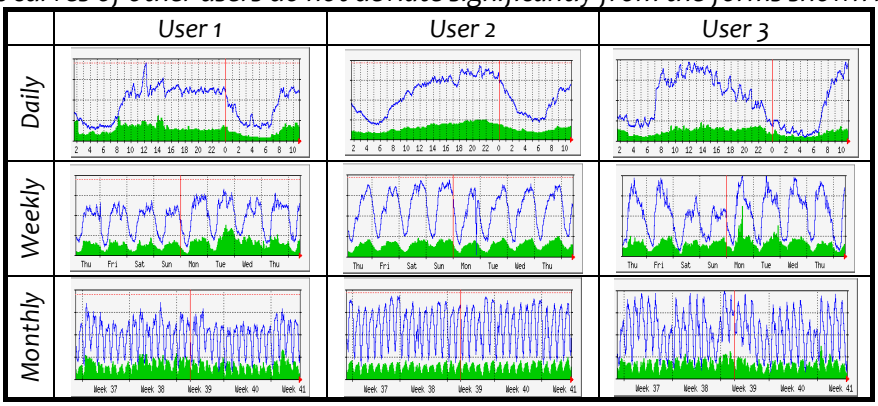

Figure 2. Traffic Curves of Different Users

Having in mind the shapes of previous curves, an aproximate periodic traffic trend can be recognized (the curve formed of long-term averages of traffic in specific time intervals) with period T=24 h, which results in the following figure [4]:

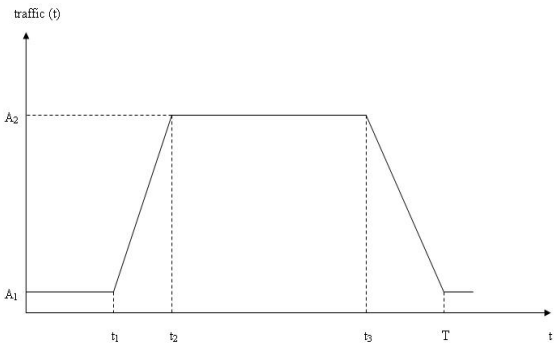

Figure 3. Model of Traffic Curve

In accordance with the previous figure, the periodic traffic trend curve is defined as:

- *for the interval 0 – t_1 (night traffic): $y(t) = A_1$*
- *for the interval t_1 – t_2 (increase of morning traffic): $y(t) = A_1 + (A_2 - A_1) \cdot \frac{t - t_1}{t_2 - t_1}$*
- *for the interval t_2 – t_3 (daily traffic): $y(t) = A_2$*
- *for the interval t_3 – T (fall of night traffic): $y(t) = A_2 - (A_2 - A_1) \cdot \frac{t - t_3}{T - t_3}$*

where A_1, A_2, t_1, t_2, t_3 and T represent the values whose meaning is shown in the Figure 2 and they vary from user to user.

In the case of some users (for example, User 3 in Figure 2) in the weekend days the fall of average daily traffic is about 25%. In this sense, the value of A_2 for the same user cannot be considered as constant in all periods T.

STATISTICAL ANOMALY DETECTION ALGORITHM

Statistical methods monitor the user or system behavior by measuring certain variables over time (e.g. login and logout time of each session). The basic models keep averages of these variables and detect whether thresholds are exceeded based on the standard deviation of the variable. More advanced statistical models also compare profiles of long-term and short-term user activities. These

statistical models are used in host-based IDSs, network-based IDSs, as well as in application-based IDSs for detecting malicious viruses [14].

The different traffic models each have its own advantages and disadvantages. The type of network under study and the traffic characteristics strictly influence the choice of the traffic model used for analysis. Traffic models that cannot capture or describe the statistical characteristics of the actual traffic on the network are to be avoided, since the choice of such models will result in under-estimation or over-estimation of network performance.

There is no one single model that can be used effectively for modeling traffic in all kinds of networks. For heavy-tailed traffic, it can be shown that Poisson model under-estimates the traffic [12]. In case of high speed networks with unexpected demand on packet transfers, Pareto based traffic models are excellent candidates since the model takes into the consideration the long-term correlation in packet arrival times [13]. Similarly, with Markov models, though they are mathematically tractable, they fail to fit actual actual traffic of high-speed networks.

The available literature is not completely certain what type(s) of probability distribution best models network traffic. Thus, for example, the uniform, Poisson, lognormal, Pareto and Rayleigh distributions were used in different applications. Statistical analysis presented in [10] showed how skewness and kurtosis of network traffic samples in a certain time interval may be criterions for selection of appropriate distribution type. Among analyzed types of distribution, based on kurtosis and skewness as criteria for describing network traffic, the appropriate are uniform, normal, Poisson, lognormal and Rayleigh distribution.

Approach by statistical quality control – Statistical quality control is the term used to describe the set of statistical tools for evaluation of organizational quality. Statistical quality control can be divided into three broad categories:

1. *Descriptive statistics are used to describe quality characteristics and relationships. Included are statistics such as the mean, standard deviation, the range, and a measure of the distribution of data.*
2. *Statistical process control (SPC) involves inspecting a random sample of the output from a process and deciding whether the process is producing products with characteristics that fall within a predetermined range. SPC answers the question of whether the process is functioning properly or not. Key tools in SPC are control charts (also known as Shewhart charts or process-behaviour charts).*
3. *Acceptance sampling is the process of randomly inspecting a sample of goods and deciding whether to accept the entire lot based on the results.*

The tools in each of these categories provide different types of information for use in analyzing quality. Descriptive statistics are used to describe certain quality characteristics, such as the central tendency and variability of observed data. Although descriptions of certain characteristics are helpful, they are not enough to help us evaluate whether there is a problem with quality. Acceptance sampling can help us do this. Acceptance sampling helps us decide whether desirable quality has been achieved. Although this information is helpful in making the quality acceptance decision, it does not help us identify and catch a quality problem during the process. For this we need tools in the statistical process control category.

In order to determine the range of expected traffic in a certain moment during the day, traffic values were collected and analyzed for each characteristic time segment. Following that, taking into consideration the clearly identified central lines and the traffic values distributed around them, descriptive statistics is applied, with the aim of calculating the lower and upper control limit.

The center line for the control chart is the target value or the mean of network traffic (y_0). The upper (UCL) and lower control limits (LCL) are:

$$UCL = y_0 + k\sigma \quad (1)$$

$$LCL = y_0 - k\sigma \quad (2)$$

where the factor k is either set equal 3 (the 3-sigma control limits) or chosen using the Lucas and Saccucci tables [9], while σ is standard deviation of used values.

In this sense, the arithmetic mean and standard deviation of samples are calculated, and on the basis of them, the upper and lower control limits (maximum and minimum of expected traffic) are determined [5,7] with a confidence interval 99.7% (i.e. 3σ). Any network value that falls outside this interval, in statistical terms represents an anomaly suspicious on attack. The daily outgoing traffic (in this case, for September 21, 2010, Tuesday) of a typical user is taken as an example, in which the following four characteristic intervals can be identified (Figure 4): 02–06 h (night traffic), 06-10 h (morning traffic), 10-22 h (daily traffic) and 22-02 h (night traffic).

Using the ability of monitoring software PRTG [8] to provide numeric values also (Figure 5), 349 consecutive hourly averages were taken for the first 15 days of monthly period (Aug 24 – Sep 06).

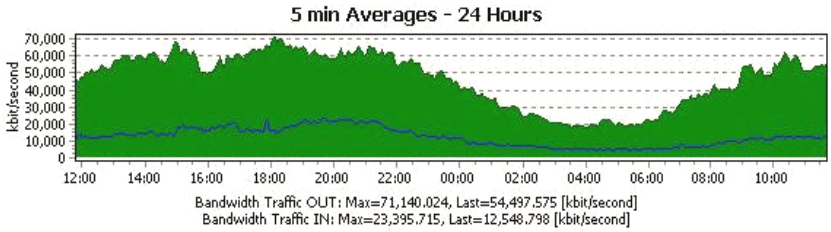

Figure 4. Daily Traffic Curve

30 Days, Hourly Averages

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
9/21/2010 11:00 AM - 12:00 PM	5,383,105,457	12,250,542	23,238,854,739	52,871,764	28,715,960,196	65,122,306	100
9/21/2010 10:00 AM - 11:00 AM	5,392,861,792	12,272,472	25,129,345,860	57,197,688	30,522,147,652	69,460,461	100
9/21/2010 9:00 AM - 10:00 AM	4,833,874,705	11,000,090	22,449,961,922	51,069,825	27,283,936,627	62,069,915	100
9/21/2010 8:00 AM - 9:00 AM	3,937,264,794	8,960,037	18,205,790,977	41,431,366	22,143,055,791	50,391,433	100
9/21/2010 7:00 AM - 8:00 AM	2,641,230,638	6,009,386	15,873,110,531	36,102,020	18,514,340,509	42,155,306	100
9/21/2010 6:00 AM - 7:00 AM	2,320,986,536	5,281,755	11,298,962,754	25,712,547	13,619,243,290	30,994,302	100
9/21/2010 5:00 AM - 6:00 AM	2,193,785,499	4,991,944	8,767,921,377	19,953,112	10,961,536,866	24,945,055	100
9/21/2010 4:00 AM - 5:00 AM	2,156,184,126	4,906,748	8,944,382,956	20,354,402	11,100,567,082	25,261,150	100
9/21/2010 3:00 AM - 4:00 AM	2,223,322,736	5,060,055	8,490,843,354	19,322,597	10,714,066,091	24,383,252	100
9/21/2010 2:00 AM - 3:00 AM	2,337,776,973	5,457,788	10,392,719,130	23,650,261	13,230,496,103	30,108,049	100
9/21/2010 1:00 AM - 2:00 AM	3,304,298,420	7,519,553	13,292,764,973	30,250,234	16,597,063,392	37,769,788	100
9/21/2010 12:00 AM - 1:00 AM	3,905,435,773	8,886,773	16,903,052,903	38,465,759	20,808,488,677	47,352,532	100
9/20/2010 11:00 PM - 12:00 AM	5,299,238,572	12,059,348	20,872,982,080	47,499,823	26,171,220,752	59,559,171	100
9/20/2010 10:00 PM - 11:00 PM	6,260,180,995	14,246,102	24,062,516,303	54,759,331	30,322,697,298	69,004,433	100
9/20/2010 9:00 PM - 10:00 PM	8,400,028,455	19,115,097	27,200,047,928	62,035,545	35,600,076,383	81,151,232	100
9/20/2010 8:00 PM - 9:00 PM	9,457,290,339	21,521,560	27,132,623,986	61,745,224	36,589,920,325	83,266,783	100
9/20/2010 7:00 PM - 8:00 PM	9,443,938,224	21,491,281	26,971,252,961	61,360,426	36,415,191,185	82,841,707	100
9/20/2010 6:00 PM - 7:00 PM	7,819,751,700	17,795,333	29,604,036,688	67,281,533	37,383,788,388	85,073,867	100
9/20/2010 5:00 PM - 6:00 PM	7,253,592,590	16,506,284	27,938,985,083	62,783,750	34,842,577,673	79,290,036	100
9/20/2010 4:00 PM - 5:00 PM	8,129,126,626	18,499,307	24,653,659,247	56,104,395	32,782,785,873	74,603,703	100
9/20/2010 3:00 PM - 4:00 PM	7,711,698,312	17,565,797	25,803,350,110	58,720,219	33,523,308,422	76,286,016	100
9/20/2010 2:00 PM - 3:00 PM	6,136,885,813	13,965,223	26,541,116,454	60,399,476	32,677,802,267	74,364,699	100
9/20/2010 1:00 PM - 2:00 PM	6,265,081,151	13,802,311	25,880,543,959	58,096,378	31,945,625,110	72,898,689	100
9/20/2010 12:00 PM - 1:00 PM	5,368,340,255	12,216,069	22,617,991,234	51,471,498	27,986,331,539	63,687,567	100
9/20/2010 11:00 AM - 12:00 PM	5,441,315,249	12,382,000	20,419,470,777	46,498,093	25,860,786,226	58,880,093	100
9/20/2010 10:00 AM - 11:00 AM	4,979,912,022	11,332,065	20,982,817,233	47,750,086	25,962,729,256	59,082,751	100

Figure 5.PRTG - Traffic Samples (example)

During the period of observation no attack situation is detected, so the measuring results can be considered as attack-free. Descriptive statistics applied on the used data (with the aim of defining fixed control limits) leads to the following results (in kbit/s):

Upper and lower control limits in the previous table define the minimum and maximum expected values of traffic at certain time intervals.

Table 1. Descriptive Network Statistics and Control Limits (the first period)

	02-06	06-10	10-22	22-02
Mean	24237,53236	35240,97532	58378,65	44.406,06
Standard Error	496,7067799	1223,139254	386,6292	1.125,28
Median	23706,8165	35715,9745	58789,77	43.547,01
Mode	#N/A	#N/A	#N/A	#N/A
Standard Deviation	3717,013184	9153,136048	5172,747	8.569,85
Sample Variance	13816187,01	83779899,52	26757307	73.442.393,17
Kurtosis	-0,343842343	-1,153976393	0,391492	-1,04
Skewness	0,396455629	0,04747584	-0,63688	0,08
Range	15927,125	34161,572	28378,16	30.795,38
Minimum	17866,862	18815,316	40195,81	29.534,68
Maximum	33793,987	52976,888	68573,97	60.330,06
Sum	1357301,812	1973494,618	10449778	2.575.551,21
Count	56	56	179	58
Confidence Level	995,4226241	2451,225824	762,9667	2253,328157
Upper Control Limit	35388,57191	62700,38347	73896,89	70115,61659
Lower Control Limit	13086,49281	7781,567176	42860,41	18696,49413

Table 2. Differences in Characteristic Values of Traffic

	Daily 1 [Mb/s]	Daily 2 [Mb/s]	Diff. [%]	Weekly 1 [Mb/s]	Weekly 2 [Mb/s]	Diff. [%]	Monthl y 1 [Mb/s]	Monthl y 2 [Mb/s]	Diff. [%]
User 1									
Max.	33,9	33,1	-2,4	29,7	33,4	12,4	9,7	9,8	1
Average	16,5	19,1	15,8	17,0	21,1	24,1	6,01	6,6	9,8
User 2									
Max.	3,94	3,63	-7,8	3,98	3,68	-7,5	48,2	49,2	2
Average	2,35	2,09	-11	2,28	2,09	-8,3	30,9	30	-3
User 3									
Max.	9,31	10,0	7,4	9,71	9,99	2,9	9,9	9,7	-2
Average	5,71	6,01	5,2	5,63	6,64	17,9	5,4	4,9	-9,2
User 4									
Max.	9,69	9,99	3,1	10,0	9,91	-0,9	10	10	0
Average	4,96	5,14	3,6	5,2	4,94	-5	7,4	7,6	2,7
User 5									
Max.	48,2	46,3	-3,9	48,5	45,2	-6,8	1,8	1,8	0
Average	29	24,4	-15,9	30,4	26,4	-13,1	0,14	0,14	0
User 6									
Max.	10,1	10,1	0	10,0	10,0	0	3,94	3,66	-7,1
Average	7,78	7,95	2,2	7,43	8,14	9,6	1,9	2,03	6,8
User 7									
Max.	3,98	3,97	-0,02	3,94	3,99	1,2	3,9	3,9	0
Average	1,74	1,79	2,9	1,88	1,99	5,9	1,9	2	5,2

Since the working principle is based on exceeding the upper threshold, this approach is particularly suitable for detection of high intensity attacks – whose mean amplitude is 250% higher than the mean traffic rate [11].

The research also dealt with establishing the size and variation of characteristic values of the traffic in different time periods. In this regard, the observed values were the average and maximum traffic of several users, in daily, weekly and monthly periods. In order to check the calculated values, two measurements were made in the range of a month and obtained were the following results, presented in Table 2.

By comparison of data from table it can be concluded that the changes in maxima and average values of traffic are relatively small - the average value of difference in maximum traffic is 3,26% while in average value is 8,44%.

EVALUATION

The evaluation of the previously determined statistical algorithm (Table 1) is performed on another 15 days of monthly data (Figure 6, Sep 07 – Sep 21), divided into corresponding four daily intervals. The key idea of evaluation is to determine whether occurred at appropriate intervals exceeding the control limits specified in the first measurement (Figure 6, Aug 24 – Sep 06). The result of descriptive statistics applied on these data is presented in Table 3. The aim of this calculation is to determine the maximum and minimum traffic value at appropriate intervals.

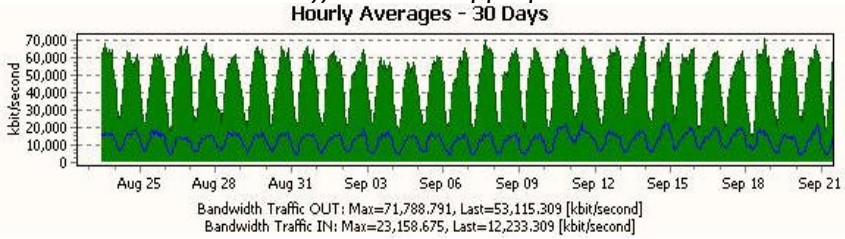

Figure 6. Monthly Traffic Curve

Table 3. Descriptive Network Statistics (the second period)

	02-06	06-10	10-22	22-02
Mean	24257,5589	35006,70425	59658,86008	46853,98003
Standard Error	556,3660307	1242,071044	405,7866418	1385,21244
Median	23998,081	36360,432	60359,4485	47481,368
Mode	#N/A	#N/A	#N/A	#N/A
Standard Deviation	4309,592743	9621,040938	5290,810502	10549,46365
Sample Variance	18572589,61	92564428,74	27992675,77	111291183,3
Kurtosis	-0,224175194	-0,740910158	-0,079311647	-0,796621206
Skewness	0,461121744	-0,229295021	-0,517610499	0,172489813
Range	19167,925	37420,539	26638,567	43954,974
Minimum	15517,191	14129,554	45113,513	27833,817
Maximum	34685,116	51550,093	71752,08	71788,791
Sum	1455453,534	2100402,255	10142006,21	2717530,842
Count	60	60	170	58
Confidence Level	1113,285847	2485,378398	801,0635755	2773,840045

Comparing obtained extremes (the minimum and maximum, Table 3) with the corresponding control limits from the first measurement (Table 1), it can be concluded that only for the interval 22-02, the detected maximum (71 788.79 kb/s) exceeded the upper control limit (70 115.62 kb/s), causing the situation of statistical anomaly (or statistical false alarm). The calculated false alarm rate was 0.3% (one false event on the total of 349 analyzed samples).

ADAPTIVE THRESHOLD ALGORITHM

In addition to algorithm with fixed thresholds, algorithm with adaptive threshold is also used for intrusion detection. This relatively simple algorithm relies on testing whether the traffic, i.e. number of packets, over a given interval exceeds a particular threshold. In order to account for seasonal (daily and weekly) traffic variations, the value of the threshold is set adaptively, based on an estimate of the mean number of packets, which is computed from recent traffic measurement.

If x_n is the number of packets in the n-th time interval and μ_{n-1} is the mean rate calculated from measurements prior to n, then the alarm is active if [11]:

$$x_n \geq (\alpha + 1) \cdot \overline{\mu}_{n-1} \tag{3}$$

Then alarm is signalized at the moment n. Here α > 0 is the parameter that indicates the percentage above the mean value that we consider to be an indication of anomalous behavior. The mean μ_n can be computed over some past time interval or using the EWMA of previous measurements [11]:

$$\overline{\mu}_n = \lambda \cdot \overline{\mu}_{n-1} + (1 - \lambda) \cdot x_n \tag{4}$$

where λ is the EWMA factor.

Direct application of the above algorithm would yield a relatively high number of false alarms (false positives). A simple modification that can improve its performance is to signal an alarm after a certain number of consecutive violations of the threshold # (Fig. 7). In this case, the alarm is active if [11]:

$$\sum_{i=n-k+1}^{n} 1_{\{x_i \geq (\alpha+1)\overline{\mu}_{i-1}\}} \geq k \tag{5}$$

where k > 1 is the parameter that indicates the number of consecutive intervals the threshold must be exceeded for generating an alarm.

The configurable parameters of this algorithm are the threshold factor α, the number of successive threshold violations k before signaling an alarm, the EWMA factor λ and the time interval T over which the number of packets are taken.

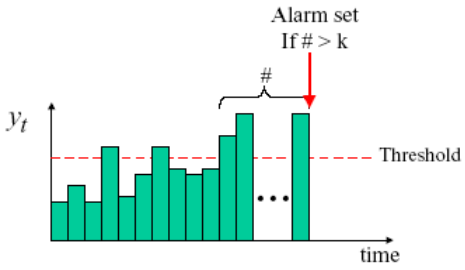

Figure 7. Adaptive Threshold – k

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 4000 request/minute to a Web server. Then, any time that the system measures more then 4000 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 Fridays between 10am and 11am the total traffic volume is expected to be between 90 and 130 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.*

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.

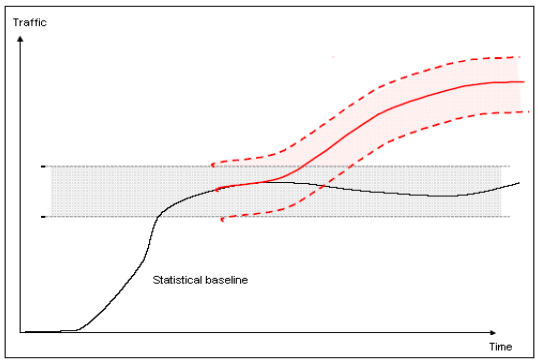

Figure 8 [1]. NSAD Training

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.

FALSE POSITIVES

False positives happen when an IDS falsely reports an attack. NSAD systems have the worst false positive rates among all intrusion detection mechanisms due to the way networks operate. Deviations from baseline usage patterns can happen both during an attack and as part of normal network operation.

For example, an NSAD system that monitors e-mail usage will establish a baseline in terms of the number of e-mail messages that a company receives in a given period, such as one day. The problem is that deviations from this baseline can happen at any time. Deviations are not just the result of a mail server being under a DoS (Denial of Service) attack. More likely, deviations could be the result of an e-mail – based marketing campaign, a holiday that prompts the exchange of greetings, a major news announcement that prompts a lot of requests to the sales department and many other scenarios.

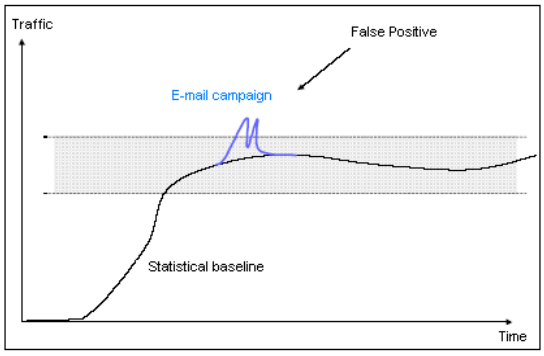

Figure 9 [1]. False Positive (example)

The false positive rates of NSAD systems are so bad that industry experts consider systems that generate less than a 95% false positive rate (i.e. 19 false alarms for each real one) as outstanding [1].

APPROACHES TO ANOMALY DETECTION

This chapter provides an overview of different approaches to anomaly detection. At first, it is necessary to explain the meaning of the term alarm. Alarm can be understood as an event when (network) behaviour deviates from normal. Normal behaviour can be:

- *specified - i.e. with threshold establishing,*
- *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 # consecutive intervals (Chapter 5).*
  - *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, ...)*

PERFORMANCE MEASUREMENT

There are several parameters for measuring the performance of NSAD algorithms. 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.

- *Nnormal: the number of normal records in the test set,*
- *Nfalse: total number of false positives,*
- *% false positives = Nfalse / Nnormal * 100.*

CONCLUSIONS

In this research the proposed multiple fixed control limits of network traffic are checked in different time periods and in the case of time-distant measurement. While analyzing the shapes of network traffic curves a clear and stable periodicity can be recognized. In this sense, once determined parameters can stay actual for a longer period of time without the need of frequent updates, which is very favorable in terms of efficiency and simplicity of the proposed statistical algorithm. With the goal of providing adaptive character of this algorithm, periodic routines can be made to generate possible corrections of coefficients A_1 *and* A_2.

By dividing the daily measurement interval into several shorter intervals and determinating of partial control limits for them, higher level of detection of network anomalies is achieved in relation to the situation with a constant control limits.

REFERENCES

[1.] *Sorensen, S.: Competitive Overview of Statistical Anomaly Detection, White Paper, Juniper Networks, (2004)*

[2.] *Gong, F.: Deciphering Detection Techniques: Part II Anomaly – Based Intrusion Detection, White Paper, McAfee Security, (2003)*

[3.] *Čisar, P., Maravić Čisar, S.: Model-based algorithm for statistical intrusion detection, Proceedins of the 10th International Symposium of Hungarian Researches on Computational Intelligence and Informatics, CINTI 2009, Budapest, pp. 625-631 (2009)*

[4.] *Čisar, P.: Methods of detecting Internet traffic malfunctions in e-business, PhD thesis, The Faculty of Economics, Subotica, (2010.*

[5.] *Montgomery, D.: Introduction to Statistical Quality Control, 5th Edition, John Wiley & Sons, 2005., Available: www2.isye.gatech.edu/~rbilling/courses/isye3039/.../ch05.ppt*

[6.] *Reid, R.D., Nada R. Sanders, N.R.: Operations Management, April 2008, ISBN: 978-0-470-28351-6, Chapter 6: Statistical Quality Control, Available: http://www.wiley.com/college/sc/reid/chap6.pdf*

[7.] *NIST/SEMATECH e-Handbook of Statistical Methods, Chapter 6: Prins, Jack.: Process or Product Monitoring and Control, Available: http://www.itl.nist.gov/div898/handbook/pmc/section3/pmc31.htm*

[8.] *Paessler AG the Network Monitoring Copmany, PRTG Network Monitor, Available: http://www.paessler.com/prtg*

[9.] *Lucas, J.M., Saccucci, M.S.: Exponentially weighted moving average control schemes: Properties and enhancements, Technometrics, Vol. 32, No. 1, pp. 1-29., (1990)*

[10.] *Čisar, P., Maravić Čisar, S.: Skewness and Kurtosis in Function of Selection of Network Traffic Distribution, Acta Polytechnica Hungarica, Vol.7, No.2, pp. 95-106, (2010)*

[11.] *Siris, A.V., Papagalou, F.: Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, Proceedings of IEEE Global Telecommunications Conference, GLOBECOM '04. Dec. 2004, Volume 4, pp. 2050-2054. Available: http://www.ist-scampi.org/publications/papers/siris-globecom2004.pdf*

[12.] *Paxson, V., Floyd, S.: Wide-area Traffic: The Failure of Poisson Modeling, IEEE/ACM Transactions on Networking, 3(3), pp. 226-244, June (1995), Available: http://www.cs.ucsb.edu/~ravenben/classes/276/papers/pf95.pdf*

[13.] *Adas, A.: Traffic Models in Broadband Networks, IEEE Communications Magazine, Vol.35, Issue 7, pp.82-89, July 1997. doi: 10.1109/35.601746*

[14.] *Lazarevic, A., Kumar, V., Srivastava, .: Managing Cyber Threats: Issues, Approaches and Challenges, Chapter: A survey of Intrusion Detection techniques. Boston: Kluwer Academic Publishers, (2005)*

ANNALS OF FACULTY ENGINEERING HUNEDOARA

– INTERNATIONAL JOURNAL OF ENGINEERING