UNIWERSYTET TECHNOLOGICZNO-PRZYRODNICZY
IM. JANA I JĘDRZEJA ŚNIADECKICH W BYDGOSZCZY
ZESZYTY NAUKOWE NR 260
TELEKOMUNKACJA I ELEKTRONIKA 15 (2011), 37-48

NETWORK ANOMALY DETECTION BASED ON ADAPTIVE APPROXIMATION OF SIGNALS

Łukasz Saganowski, Tomasz Andrysiak

Institute of Telecommunications,
Faculty of Telecommunications and Electrical Engineering
University of Technology and Life Sciences (UTP)
ul. Kaliskiego 7, 85-789 Bydgoszcz, Poland
[luksag, andrys]@utp.edu.pl

Summary: In the article we present Anomaly Detection System for recognizing unknown threats in network traffic with the use of Matching Pursuit decomposition. We proposed further improvements of presented anomaly detection method. Efficiency of our method is reported with the use of extended set of benchmark test traces. At the end we compared achieved results with different methods based on signal processing, data mining and hybrid techniques.

Keywords: Anomaly Detection System, Matching Pursuit decomposition, Adaptive approximation of signals

1. INTRODUCTION

Anomaly detection approach is a new, emerging trend for network security especially for high-security networks (such as military or critical infrastructure monitoring networks). Such networks are currently exposed to many threats due to the fact that barriers between trusted and un-trusted network components do not successfully protect critical parts of the cyber domain. Most IDS/IPS (Intrusion Detection/Prevention Systems) cannot cope with new sophisticated malware (viruses, SQL injections, Trojans, spyware and backdoors) and 0-day attacks. Most current IDS/IPS systems have problems in recognizing new attacks (0-day exploits) since they are based on the signature-based approach. In such mode, when system does not have an attack signature in database, the attack is not detected. Another drawback of current IDS systems is that the used parameters and features do not contain all the necessary information about traffic and events in the network [1].

Intrusion Detection Systems (IDS) can be classified as belonging to two main groups depending on the detection technique employed:

- signature-based detection,
- anomaly detection.

Anomaly Detection techniques rely on the existence of a reliable characterization of what is normal and what is not, in a particular networking scenario. More precisely, Anomaly Detection techniques base their evaluations on a model of what is normal, and

classify as anomalous all the events that fall outside such a model. In this paper, a new solution for Anomaly Detection System (ADS) – system based on signal processing algorithm - is presented. ADS analyzes traffic from internet connection in certain point of a computer network. The proposed ADS system uses redundant signal decomposition method based on Matching Pursuit algorithm.

Our original methodology [29] for network security anomaly detection based on Matching Pursuit is presented and evaluated using network data traces from different sources [20, 21, 22]. We also compared Matching Pursuit approach to different methods based on signal processing (e.g. Discrete Wavelet Transform) and statistical analysis.

2. SIGNAL PROCESSING METHODS FOR NETWORK ANOMALY DETECTION

Signal processing techniques have found application in Network Intrusion Detection Systems because of their ability to detect novel intrusions and attacks, which cannot be achieved by signature-based approaches. It has been shown that network traffic presents several relevant statistical properties when analyzed at different levels (e.g. self-similarity, long range dependence, entropy variations, etc.) [4]. Approaches based on signal processing and on statistical analysis can be powerful in decomposing the signals related to network traffic, giving the ability to distinguish between trends, noise, and actual anomalous events. Wavelet-based approaches, maximum entropy estimation, principal component analysis techniques, and spectral analysis, are examples in this regard which have been investigated in the recent years by the research community [5-9]. A powerful analysis, synthesis, and detection tool in this field is represented by the wavelets. Indeed, time and scale-localization abilities of the wavelet transform, make it ideally suited to detect irregular traffic patterns in traffic traces. Recently many wavelet-based methods for detection of attacks have been tested and documented. Some are based on the continuous wavelet transform analysis, most of them however refer to the Discrete Wavelet transformation and the multiresolution analysis [4].

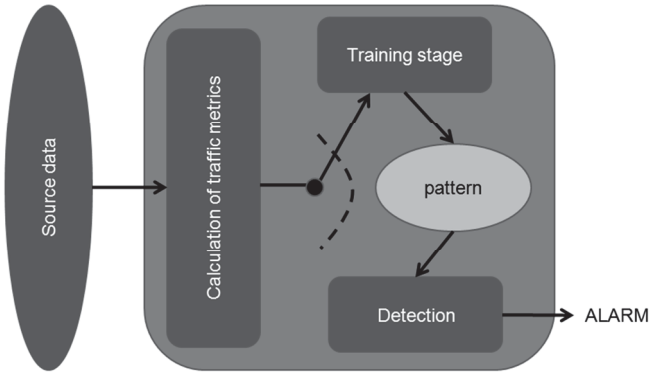

Fig. 1. Basic conception of Anomaly Detection System for network traffic [30].

However, Discrete Wavelet Transform provides a large amount of coefficients which not necessarily reflect required features of the network signals. Therefore, in this

paper we propose another signal processing and decomposition method for anomaly/intrusion detection in networked systems. We developed original Anomaly Detection ADS algorithm based on Matching Pursuit [29]. The general overview of our Anomaly Detection System is presented in Figure 1.

3. ADAPTIVE APPROXIMATION OF SIGNAL FOR ANOMALY DETECTION

Given an overcomplete set of functions called dictionary $D = \{g_{\gamma_0}, g_{\gamma_1}, \dots, g_{\gamma_{n-1}}\}$ such that norm $\|g_{\gamma_i}\| = 1$, we can define an optimal M – approximation as an expansion, minimizing the error δ of an approximation of signal $f(t)$ by M waveforms g_{γ_i} called atoms:

$$\delta = \left\| \mathrm{f(t)} - \sum_{\mathrm{i=0}}^{\mathrm{M-1}} \alpha_{\mathrm{i}} \mathrm{g}_{\gamma_{\mathrm{i}}} \right\|, \tag{1}$$

where functions $g_{\gamma_i} \in L^2(R)$ and $\{\gamma_i\}_{i=1,2..,M}$ represents the indices of the chosen functions g_{γ_i} [12]. Finding such an optimal approximation is an NP-hard problem [13]. A suboptimal expansion can be found by means of an iterative procedure, such as the matching pursuit algorithm.

3.1. Matching pursuit overview

Matching pursuit is a recursive, adaptive algorithm for signal decomposition [11]. The matching pursuit decomposes any signal into linear expansion of waveforms witch are taken from an overcomplete dictionary D. Signal f can be written as the weighted sum of dictionary elements:

$$f = \sum_{i=0}^{N-1} \alpha_i g_{\gamma_i} + R^n f, \tag{2}$$

where $R^n f$ is residual in an n – term sum.

In the first step of Matching Pursuit algorithm, the waveform g_{γ_0} which best matches the signal f is chosen. The first residual is equal to the entire signal $R^0 = f$. In each of the consecutive steps, the waveform g_{γ_n} is matched to the signal $R^n f$, which is the residual left after subtracting results of previous iterations:

$$R^n f = R^{n-1} f - \alpha_n g_{\gamma_n}, \tag{3}$$

where

$$\alpha_n = \langle R^{n-1} f, g_{\gamma_n} \rangle \tag{4}$$

and

$$g_{\gamma_n} = arg \max_{g_{\gamma_i} \epsilon D} \left| \langle R^{n-1} f, g_{\gamma_i} \rangle \right|. \tag{5}$$

When $R^n f$ is minimized for a given $g_{\gamma_{n-1}}$, the projection between the previous residue and actual atom $\langle R^{n-1} f, g_{\gamma_{n-1}} \rangle$ is maximized. Iteratively, we obtain for N atom:

$$R^N f = f - \sum_{n=0}^{N-1} \langle R^n f, g_{\gamma_n} \rangle g_{\gamma_n}, \tag{6}$$

where $R^n f \to 0$ when $N \to \infty$ [11][12]. This describes the decomposition process.

3.2. Dictionary of Gabor functions

In the described IDS solution we proposed a waveform from a time-frequency dictionary can be expressed as translation (u), dilation (s) and modulation (ω) of a window function $g(t) \in L^2(R)$

$$g_\gamma(t) = \frac{1}{\sqrt{s}} g\left(\frac{t-u}{s}\right) e^{i\omega t}, \tag{7}$$

where

$$g(t) = \frac{1}{\sqrt{s}} e^{-\pi t^2}. \tag{8}$$

Optimal time-frequency resolution is obtained for Gaussian window $g(t)$, which for the analysis of real valued discrete signals gives a dictionary of Gabor functions

$$g_\gamma(x) = C(\gamma, \varphi) g\left(\frac{x-u}{s}\right) \sin\left(2\pi \frac{\omega}{N}(x-u) + \varphi\right), \tag{9}$$

where N is the size of the signal for which the dictionary is constructed, $C(\gamma, \varphi)$ is normalizing constant used achieve atom unit energy $\|g_\gamma\| = 1$ and $\gamma = \{s, u, \omega, \varphi\}$ denotes parameters of the dictionary's functions [16][17].

We implemented the dictionary originally by Mallat and Zhang in [11], the parameters of the atoms are chosen from dyadic sequences of integers. Scale s, which corresponds to an atom's width in time, is derived from the dyadic sequence $s = 2^j, 0 < j < L$ (signal size $K = 2^L$ and j is octave). Parameters u and ω, which correspond to an atom's position in time and frequency, are sampled for each octave j with interval $s = 2^j$.

In order to create an overcomplete set of Gabor functions, dictionary D was built by varying subsequence atom parameters: scale (s), translation (u), modulation (ω) and phase (φ). Base functions dictionary D was created with using 10 different scales and 50 different modulations. In Figure 2 example atoms from dictionary D are presented.

3.3. Search in the dictionary of atoms

In basic Matching Pursuit algorithm atoms are selected in every step from entire dictionary which has flat structure. In this case algorithm causes significant processor burden. In our coder dictionary with internal structure was used Fig. 2.

Dictionary is built from:

- Atoms,
- Centered atoms.

Centered atoms groups such atoms from D that are as much correlated as possible to each other. To calculate measure of correlation between atoms, function $o(a, b)$ can be used [15] :

$$\boldsymbol{o(a,b)} = \sqrt{\mathbf{1} - \left(\frac{|\langle \boldsymbol{a},\boldsymbol{b}\rangle|}{\|\boldsymbol{a}\|_2 \|\boldsymbol{b}\|_2}\right)^2}. \tag{10}$$

The quality of centered atom can be estimated according to (9):

$$\boldsymbol{O_{k,l}} = \frac{\mathbf{1}}{|\boldsymbol{LP_{k,l}}|} \sum_{\boldsymbol{i} \in \boldsymbol{LP_{k,l}}} \boldsymbol{o}\left(\boldsymbol{A_{c(i)}}, \boldsymbol{W_{c(k,l)}}\right), \tag{11}$$

where $LP_{k,l}$ is a list of atoms grouped by centered atom. $O_{k,l}$ is a mean of local distances from centered atom $W_{c(k,l)}$ to the atoms $A_{c(i)}$ which are strongly correlated with $A_{c(i)}$. Centroid $W_{c(k,l)}$ represents atoms $A_{c(i)}$ which belongs to the set $i \in LP_{k,l}$. List of atoms $LP_{k,l}$ should be selected according to the equation (12):

$$\mathbf{max}_{i \epsilon LP_{k,l}} \, o\left(A_{c(i)}, W_{c(k,l)}\right) \leq \mathbf{min}_{j \in D \setminus LP_{k,l}} \, o\left(A_{c(j)}, W_{c(k,l)}\right). \tag{12}$$

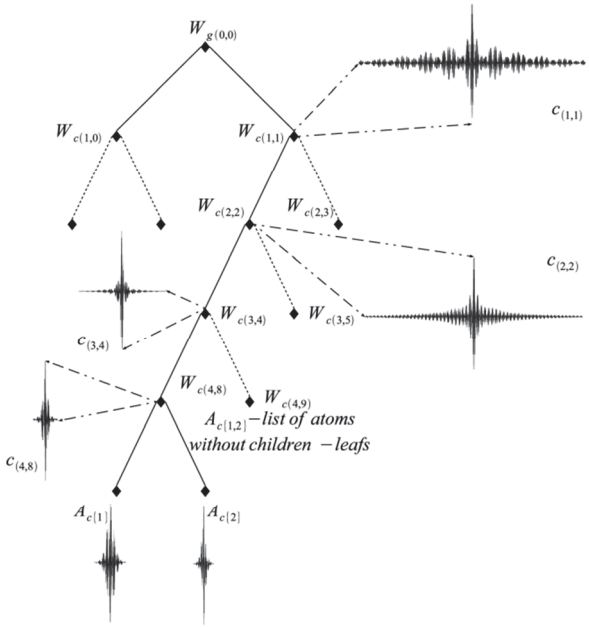

Fig. 2. Base functions dictionary structure.

4. EXPERIMENTAL RESULTS

We modified algorithm [15] in order to improve the input signal approximation. Instead of calculating projection during creation tree structure of Base Function Dictionary-BFD we used cross correlation as a measure of similarity between different atoms a and b in atoms set.

Cross-correlation can be calculated according to equation (13):

$$R_{a,b}(t) = \sum_{m=-\infty}^{\infty} a^*(m) b(t+m), \tag{13}$$

where $R_{a,b}(t)$ – cross-correlation, a and b atoms from dictionary, a^* – conjugation of atom a, t – subsequent value of cross-correlation, m – index of atom values. Proposed algorithm modification allows us to improve process of creation tree structure BFD. As a result we achieve better input signal approximation Fig. 3.

The matching pursuits algorithm produces three important elements of information: the set of projection coefficients $\alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, the set of residues $Rf = \{R^0 f, R^1 f, \ldots, R^{n-1} f\}$ and the list of dictionary elements chosen to approximate

of $f(x)$, represented as $g_\gamma = \{g_{\gamma_0}, g_{\gamma_1,\ldots,}g_{\gamma_{n-1}}\}$. This three factors α, Rf and g_γ completely define the discrete signal $f(x)$.

The main steps of algorithm are presented in subsequent points:

1) Base functions and the tree structure dictionary calculation (off-line):
   a) generation of all base functions,
   b) calculation of cross-correlation between atoms,
   c) tree structure dictionary calculation with the use of k-means clustering algorithm:
      i. centroid calculation,
      ii. distance calculation between atoms and centroid,
      iii. setting up connections between nodes in the tree structure,
      iv. scalar product between atoms updates;
2) Atom search process in the tree structure dictionary (on-line process):
   a) calculate scalar products (with the use of FFT) of present network 1-D signal with root node's children,
   b) set position in the tree structure for the best children (with highest scalar product) of the root node,
   c) calculate scalar products (by means of projection operation) until leaf node of the tree structure is reached,
   d) store parameters (projection, index of atom in dictionary and signal residue) of the best leaf atom.

For anomaly detection classification we used two parameters:

- Matching Pursuit Mean Projection (MP-MP)

$$MP - MP = \frac{1}{n}\sum_{i=0}^{n-1} \alpha_i, \tag{14}$$

- Energies of coefficients, residues and dictionary elements

$$E_{(k)} = \left\|\alpha^{(k)}\right\|^2 + \left\|Rf^{(k)}\right\|^2 + \left\|g_\gamma^{(k)}\right\|^2. \tag{15}$$

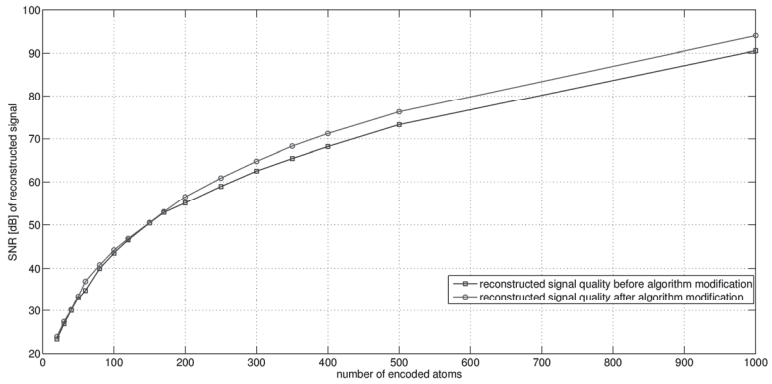

Fig. 3. Quality of reconstructed signal after algorithm modification.

In Tables 1-7 there are results for proposed ADS. Our system was tested with the use of public available benchmark test traces [20][21] and traces obtained from other sources [22].

Table 1. Detection Rate for W5D5 (FifthWeek, Day 5) [20] trace.

Network Traffic Feature	Total number of attack	Detected number of attack	Detection Rate [%]
ICMP flows/minute	68	50	73.52
ICMP in bytes/minute	68	57	83.82
ICMP out bytes/minute	68	55	80.88
ICMP in frames/minute	68	60	88.23
ICMP out frames/minute	68	57	83.82
TCP flows/minute	68	38	55.88
TCP in bytes/minute	68	42	61.76
TCP out bytes/minute	68	24	35.29
TCP in frames/minute	68	32	47.05
TCP out frames/minute	68	33	48.53
UDP flows/minute	68	67	98.53
UDP in bytes/minute	68	63	92.64
UDP out bytes/minute	68	61	89.70
UDP in frames/minute	68	63	92.53
UDP out frames/minute	68	61	89.70

Table 2. Cumulative DR – detection rate takes into consideration attacks recognized by all traffic features presented in Table 1. Results were compared to results achieved for fifth test week (Week5 Day1-5) of [20] traces.

Test Days	W5D1	W5D2	W5D3	W5D4	W5D5
DR [%] for all attack instances – DWT [19]	94.67	66.1	49.52	74.33	26.7
DR [%] for all attack instances MPMP (Matching Pursuit Mean Projection)	100	100	100	100	100
DR [%] attack types (DoS, U2R,R2L,PROBE) – DWT [19]	100	75	71.43	88.89	74.1
DR [%] attack types (DoS, U2R,R2L,PROBE) – MPMP (Matching Pursuit Mean Projection)	100	100	100	100	100

Table 3. Matching Pursuit Mean Projection - MP-MP for TCP trace with DDoS attacks (20 min. analysis window).

TCP trace (packet/second) CAIDA [22]	Window1 MPMP	Window2 MPMP	Window3 MPMP	MPMP for trace	MPMP for normal trace
Backscatter 2008.11.15	147.64	**414.86**	**368.25**	315.35	155.76
Backscatter 2008.08.20	**209.56**	162.38	154.75	157.38	155.76

Table 4. Matching Pursuit Energy parameter for TCP trace with DDoS attacks (20 min. analysis window).

TCP trace (packet/second) CAIDA [22]	Window1 $E_{(k)}$	Window2 $E_{(k)}$	Window3 $E_{(k)}$	$E_{(k)}$ for trace	$E_{(k)}$ for normal trace
Backscatter 2008.11.15	4.52e+7	**3.51e+8**	**2.16e+8**	2.01e+8	4.75e+7
Backscatter 2008.08.20	**9.54e+7**	4.27e+7	5.376e+7	6.76e+7	4.75e+7

Table 5. Matching Pursuit Mean Projection -MP-MP for TCP trace (20 min. analysis window).

TCP trace (packet/second) MAWI [21]	Window1 MPMP	Window2 MPMP	Window3 MPMP	MPMP for trace	MPMP for normal trace
Mawi 2004.03.06 tcp	214.32	177.81	300.11	248.01	242.00
Mawi 2004.03.13 tcp	279.11	216.23	217.65	238.33	242.00
Mawi 2004.03.20 tcp (attacked: Witty)	**321.54**	**367.45**	348.65	350.48	242.00
Mawi 2004.03.20 tcp (attacked: Slammer)	323.23	482.43	388.43	401.00	242.00

Table 6. Matching Pursuit Energy parameter - for TCP trace (20 min. analysis window).

TCP trace (packet/second) MAWI [21]	Window1 $E_{(k)}$	Window2 $E_{(k)}$	Window3 $E_{(k)}$	$E_{(k)}$ for trace	$E_{(k)}$ for normal trace
Mawi 2004.03.06 tcp	7.1e+7	7.52e+7	6.45e+7	7.23e+7	7.73e+7
Mawi 2004.03.13 tcp	8.56e+7	7.77e+7	8.54e+7	8.67e+7	7.73e+7
Mawi 2004.03.20 tcp (attacked: Witty)	**2.03e+8**	**1.46e+8**	**1.83e+8**	1.77e+8	7.73e+7
Mawi 2004.03.20 tcp (attacked: Slammer)	**3.34e+8**	**2.42e+8**	**3.4e+8**	3.34e+8	7.73e+7

Table 7. Proposed MP based ADS in comparison to DWT based ADS [19]. Both solutions were tested with the use of DARPA [20] tested (results in table are forWeek5 Day1 test day; DR-Detection Rate [%], FP-False Positive [%]) for MP-MP and $E(k)$ energy parameter.

Traffic Feature	MP-MP DR[%]	MP-MP FP[%]	$E_{(k)}$ DR[%]	$E_{(k)}$ FP[%]	DWT DR[%]	DWT FP[%]
ICMP flows/minute	69.49	20.23	91.54	38.35	14.00	79.33
ICMP in bytes/minute	80.45	21.69	95.34	37.35	83.33	416.00
ICMP out bytes/minute	74.97	30.72	95.67	36.72	83.33	416.00
ICMP in frames/minute	79.08	28.76	85.98	35.24	32.00	112.00
ICMP out frames/minute	73.60	30.33	95.34	35.61	32.00	112.00
TCP flows/minute	89.54	35.56	98.95	38.72	26.67	74.67
TCP in bytes/minute	48.98	34.67	94.23	41.00	8.67	23.33
TCP out bytes/minute	81.22	28.34	96.67	34.24	6.67	36.00
TCP in frames/minute	37.98	26.11	96.98	36.09	2.00	36.00
TCP out frames/minute	39.55	28.34	96.78	34.24	2.00	74.67
UDP flows/minute	90.04	41.22	91.56	38.87	10.00	66.67
UDP in bytes/minute	99.63	42.19	99.73	46.34	11.33	66.67
UDP out bytes/minute	100.00	46.56	100	44.57	11.33	66.67
UDP in frames/minute	99.63	40.23	98.43	46.23	12.67	66.67
UDP out frames/minute	100.00	46.47	100	46.34	12.67	66.67

5. OVERALL DETECTION RATE

Overall detection rate is a measure of presented Anomaly Detection System performance. Overall Detection Rate – ODR is calculated for DR and FPR parameter. ODR takes into consideration set of traffic metrics where at the same time FPR is lowest and DR has highest value. ODR is also calculated for different ADS systems presented in [19, 10, 23, 25]. For presented system we obtain 97%-100% DR and 13-15% FPR for DARPA trace and DR = 94,20% FPR = 11,3% for all tested traces [20, 21, 22].

Table 8. Comparison of different methods of proposed ADS algorithm.

Publication	System algorithm	Network traces	DR [%]	FPR [%]	Comments
Presented ADS	MP	DARPA	97-100	13%-15	overall performance
Presented ADS	MP	all traces [20, 21, 22]	94,20	11,13	overall performance
Network Anomaly Detection Based on Wavelet Analysis [19]	DWT	DARPA	mean 23.37 overall 74.1-100	111,30	
Wavelet-based Detection of DoS Attacks [10]	CWT	DARPA + local campus network	94	24	overall performance
Non-Gaussian and Long Memory Statistical Characterizations for Internet Traffic with Anomalies [23]	statistic – LRD	campus network, artificial attacks	DDOS 40-96 FC 14-25	DDOS 20 FC 20	only DDOS or FC-Flash Crowd
Learning nonstationary models of normal network traffic for detecting novel attacks [24]	statistic – nonstationary models	DARPA	39	41	
Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic [25]	fuzzy logic and data mining	DARPA + local network	69.6-98.4	24.70	
Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes [26]	SNORT 2.1 + ADS (data mining)	DARPA + campus network	60	30	
The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset [27]	SNORT 2.6 + preprocessors	DARPA	31.00	69.00	for SNORT IDS + preprocessors

- Network traffic feature: TCP byte in , ICMP flows: FPR = 13%, DR = 100%,
- Network traffic feature: TCP byte in, TCP flows: FPR = 15%, DR = 100%,
- Network traffic feature: TCP flows, UDP flows: FPR = 20%, DR = 100%.

It can be noticed that overall detection rate depends on set of network traffic features. Different sets of traffic features did not allow to achieve better DR and FPR.

6. CONCLUSIONS

In the article our developments in feature extraction for Intrusion Detection systems are presented. We showed that Matching Pursuit may be considered as very promising methodology which can be used in networks security framework. Upon experiments we may conclude that mean projection and energy parameter differs significantly for normal and attacked traces. Therefore, our system easily detects attacked traffic and triggers an alarm. The major contribution of this paper is a novel algorithm for detecting anomalies based on signal decomposition. In the classification/decision module we proposed to use developed matching pursuit features such as mean projection and energy parameter. We tested and evaluated the presented features and showed that experimental results proved the effectiveness of our method. We compared our solution to different ADS systems based on signal processing, data mining and hybrid algorithms.

BIBLIOGRAPHY

[1] Esposito M., Mazzariello C., Oliviero F., Romano S.P., Sansone C., 2005. Real Time Detection of Novel Attacks by Means of Data Mining Techniques. ICEIS (3) pp. 120-127.

[2] Davis G., Mallat S., Avellaneda M., 1997. Adaptive greedy approxima-tions, Journal of Constructive Approximation, vol. 13, pp.57-98.

[3] Esposito M., Mazzariello C., Oliviero F., Romano S.P., Sansone C., 2005. Evaluating Pattern Recognition Techniques in Intrusion Detection Systems. PRIS, pp. 144-153.

[4] FP7 INTERSECTION Project, Deliverable D.2.1: SOLUTIONS FOR SECURING HETEROGENEOUS NETWORKS: A STATE OF THE ART ANALYSIS.

[5] FP7 INTERSECTION (INfrastructure for heTErogeneous, Reislient, Secure, Complex, Tightly Inter-Operating Networks) Project Description of Work.

[6] Cheng C.-M., Kung H.T., Tan K.-S., 2002. Use of spectral analysis in defense against DoS attacks, IEEE GLOBECOM, pp. 2143-2148.

[7] Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies, ACM SIGCOMM Internet Measurement Workshop 2002.

[8] Huang P., Feldmann A., Willinger W., 2001. A non-intrusive, wavelet-based approach to detecting network performance problems, ACM SIGCOMM Internet Measurement Workshop.

[9] Li L., Lee G., 2003. DDos attack detection and wavelets, IEEE ICCCN03, pp. 421--427.

[10] Dainotti A., Pescape A., Ventre G., 2006. Wavelet-based Detection of DoS Attacks, 2006 IEEE GLOBECOM, San Francisco (CA, USA).

[11] Mallat S., Zhang, 1993. Matching Pursuit with timefrequency dictonaries. IEEE Transactions on Signal Processing., vol. 41, no 12, pp. 3397-3415.
[12] Troop J.A., 2004. Greed is Good: Algorithmic Results for Sparse Appro-ximation. IEEE Transactions on Information Theory, vol. 50, no. 10.
[13] Tropp J.A., 2003. Greed is good: Algorithmic results for sparse approximation, ICES Report 03-04, The University of Texas at Austin.
[14] Gribonval R., 2001. Fast Matching Pursuit with a Multiscale Dictionary of Gaussian Chirps. IEEE Transactions on Signal Processing., vol. 49, no. 5.
[15] Jost P., Vandergheynst P., Frossard P., 2005. Tree-Based Pursuit: Algorithm and Properties. Swiss Federal Institute of Technology Lausanne (EPFL),Signal Processing Institute Technical Report.,TR-ITS-2005.013.
[16] Elad M., 2010. Sparse and Redundant Representations: From Theory to Applications in Signal and Image Processing, Springer.
[17] Gabor D., 1946. Theory of communication. Journal of Institution Electrical Engineering, vol. 93, no. 26, pp. 429-457.
[18] Janssen A., 1981. Gabor representation of generalized functions. Journal of the Mathematical. Analysis. and Applications, vol. 83, no. 2, pp. 377–394.
[19] Lu W., Ghorbani Ali A., 2009. Network Anomaly Detection Based on Wavelet Analysis, EURASIP Journal on Advances in Signal Processing, vol. 2009, Article ID 837601. doi:10.1155/2009/837601
[20] Defense Advanced Research Projects Agency DARPA Intrusion Detection Evaluation Data Set: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html
[21] WIDE Project: MAWI Working Group Traffic Archive at tracer.csl.sony.co.jp/mawi/
[22] The CAIDA Dataset on the Witty Worm - March 19-24, 2004. Colleen Shanon and David Moore, www.caida.org/passive/witty.
[23] Scherrer A., Larrieu N., Owezarski P., Borgant P., Abry P., 2007. Non-Gaussian and Long Memory Statistical Characterizations for Internet Traffic with Anomalies. IEEE Transactions On Dependable and Secure Computing, vol. 4, no. 1, pp. 56-70.
[24] Mahoney M.V., Chan P.K., 2002. Learning nonstationary models of normal network traffic for detecting novel attacks, Proceedings of the Eighth ACM SIGKDD, pp. 376-385.
[25] Shanmugam B., Idris N.B., 2011. Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic, Intrusion Detection Systems, InTech, pp. 135-154, http://www.intechopen.com/books/show/title/intrusion-detection-systems.
[26] Hwang K., Cai M., Chen Y., Qin M., 2007. Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes, IEEE Transactions on dependable and secure computing, vol. 4, no. 1, pp. 1-15.
[27] Tjhai G.C., Papadaki M., Furnell S.M., Clarke N.L., 2008. The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset, [in:] TrustBus 2008, LNCS 5185, Springer-Verlag, pp. 139-150.
[28] Choraś M., Saganowski Ł., Renk R., Hołubowicz W., 2011. Statistical and signal-based net-work traffic recognition for anomaly detection. Expert Systems. The Journal of Knowledge Engineering.
[29] Garcia-Teodoro P., Diaz-Verdejo J., Macia-Fernandez G., Vazquez E., 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers and security, Elsevier, vol. 28, pp. 18-28.

WYKRYWANIE ANOMALII SIECIOWYCH NA PODSTAWIE ADAPTACYJNEJ APROKSYMACJI SYGNAŁU

Streszczenie

W artykule zaproponowany został System Detekcji Anomalii w ruchu sieciowym z wykorzystaniem algorytmu dopasowania kroczącego. Zaproponowane zostały kolejne modyfikacje omawianej metody. Wydajność zastosowanego algorytmu została przedstawiona z użyciem testowych ścieżek ruchu sieciowego. Przedstawiono również porównanie zaproponowanej metody do innych rozwiązań systemów detekcji anomalii opartych o algorytmy: przetwarzania sygnałów, statystyczne oraz hybrydowe.

Słowa kluczowe: detekcja anomalii, dopasowanie kroczące, adaptacyjna aproksymacja sygnału