Anomaly Detection Preprocessor for SNORT IDS System

Łukasz Saganowski, Marcin Goncerzewicz, and Tomasz Andrysiak

Institute of Telecommunications, University of Technology & Life Sciences in Bydgoszcz ul. Kaliskiego 7, 85-789 Bydgoszcz, Poland
{lukasz.saganowski,tomasz.andrysiak}@utp.edu.pl

Summary. In this paper we propose anomaly detection preprocessor for SNORT IDS Intrusion Detection System [1] base on probabilistic and signal processing algorithms working in parallel. Two different algorithms increasing probability of detecting anomalies in network traffic. 25 network traffic features were used by preprocessor for detecting anomalies. Preprocessor calculated Chi-square statistic test and energy from DWT Discrete Wavelet Transform subband coefficients. Usability of proposed SNORT extension was evaluated in local LAN network.

1 Anomaly Detection Algorithms

Intrusion Detection Systems (IDS) are based on mathematical models, algorithms and architectural solutions proposed for correctly detecting inappropriate, incorrect or anomalous activity within networked systems. Intrusion Detection Systems can be classified as belonging to two main groups depending on the detection technique employed: anomaly detection and signature-based detection.

Anomaly detection techniques, which we focus on in our work, 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.

1.1 Statistical Features

For anomaly detection in network traffic probabilistic techniques can be used [2, 3, 4, 5]. Random variables are created during observations of p variables at time t - $\mathrm{X} = (\mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_p)$. Random variables are created based on network traffic features shown in Table 1. The Chi-square multivariate test for Anomaly Detection Systems can be represented by equation 1:

R.S. Choraś (Ed.): Image Processing & Communications Challenges 4, AISC 184, pp. 225–232.
springerlink.com

$$X^2 = \sum_{i=1}^{p} \frac{(\mathrm{X}_i - \bar{\mathrm{X}}_i)^2}{\bar{\mathrm{X}}_i}, \tag{1}$$

where $\bar{\mathrm{X}} = (\bar{\mathrm{X}}_1, \bar{\mathrm{X}}_2, ..., \bar{\mathrm{X}}_p)$ is the sample mean vector.

Using only the mean vector in Equation 1 causes that Chi-square multivariate test detects only the mean shift on one or more of the variables. For detecting anomalies in network traffic first we have to create vectors of $\bar{\mathrm{X}}$. Vectors of $\bar{\mathrm{X}}$ are used for creation of "normal traffic" profiles (normal profiles have to be created from network traffic without anomalies). We used Chi-square test because it is not computationally complex. It is an important feature because we have to calculate statistics in real time from network traffic features.

1.2 Discrete Wavelet Transform Features

Second algorithm used for anomaly detection is based on Discrete Wavelet Transform[6, 7]. The main goal of wavelet transform is to decompose the input signal into family of some specific functions called wavelets. Wavelets are functions that are generated through a process of dilations and translations of one single function, which is usually named Şmother waveletŤ. The idea of wavelet transform was defined by J. Morlet [8]

$$W_d f(m,n) = \sum_{m,n} f(x) \cdot \Psi_{m,n}(x) \tag{2}$$

where $\Psi_{m,n}$ means a family of discrete wavelet functions. The discrete wavelet transform is computed by applying a separable $1-D$ filter bank to the input signal (see Figure 1). Given a signal s of length N, the DWT consists of $log_2 N$ stages at most. The first step produces, starting from s two sets of coefficients: approximation coefficients cA_1, and detail coefficients cD_1. These vectors are obtained by convolving s with the low-pass filter Lo_D for approximation, and with the high-pass filter Hi_D for detail, followed by dyadic decimation (downsampling). The next step splits the approximation coefficients cA_1 into two parts using the same scheme, replacing s with cA_1 and producing cA_2 and cD_2 and so on. Wavelet transformation with 3 decomposition levels is presented in Figure 2.

The wavelet decomposition of the signal s analyzed at level j has the following structure: $[cA_j, cD_j, ..., cD_1]$.

In case of proposed ADS system signal represents parameters of network traffic (see Table 1). For detecting anomalies in ADS we are using as a parameter energy of DWT coefficients:

$$Ensub_i = \sum_{n=1}^{K} cP_i^2(n) \tag{3}$$

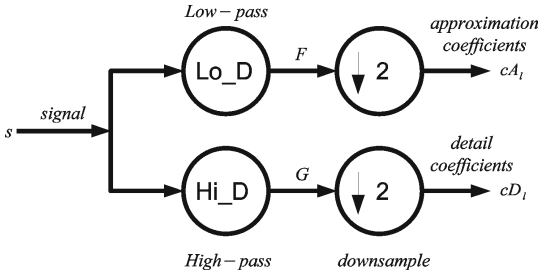


Fig. 1 Practical realisation of 1-D Discrete Wavelet Transform

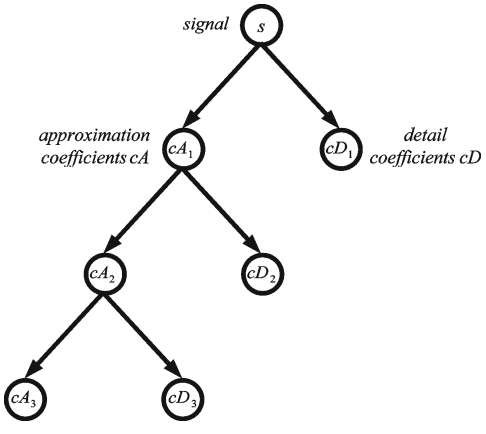


Fig. 2 Wavelet transformation with 3 decomposition levels

where P_i - DWT coefficients of approximation or detail subbands. Profiles are built from approximation cA and detail cD coefficients calculated during 3 level DWT decomposition.

Additionally, we added to preprocessor calculation of wavelet transform by using Lifting Scheme [9]. Lifting Scheme is an efficient implementation of Wavelet decomposition, where the number of operation can be reduced by a factor of two.

2 Proposed ADS Preprocessor for SNORT IDS

In Figure 3 block diagram of proposed ADS SNORT preprocessor is presented. ADS preprocessor (written in C language) is an extension to SNORT IDS system. We are using SNORT as a kind of sniffer which provides different traffic features (see Table 1). For detecting anomalies we are using Chi-square statistic test and coefficients calculated from Discrete Wavelet Decomposition.

For both algorithms first we have to built normal traffic profiles (see stepped lines in Figures 4-5). Traffic profiles were calculated from network traffic collected in 6 weeks. So far the preprocessor was tested with the use of small LAN network to prove usefulness of proposed ADS algorithms (in the next step we are planning to connect our preprocessor to large university network where we will be able to test traffic redirected to our preprocessor from many LAN networks). Network traffic was analyzed in 10 minutest windows [10] for each 25 features. Analysis window can be arbitrarily set during preprocessor start.

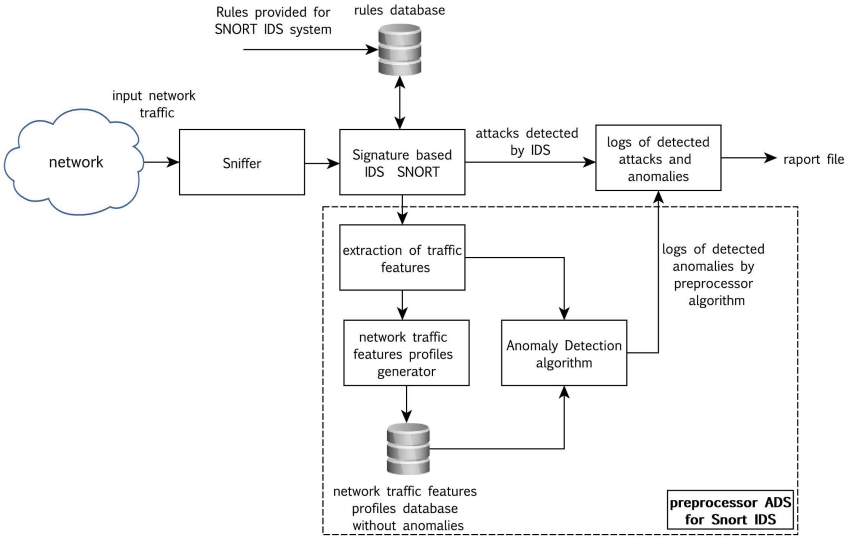


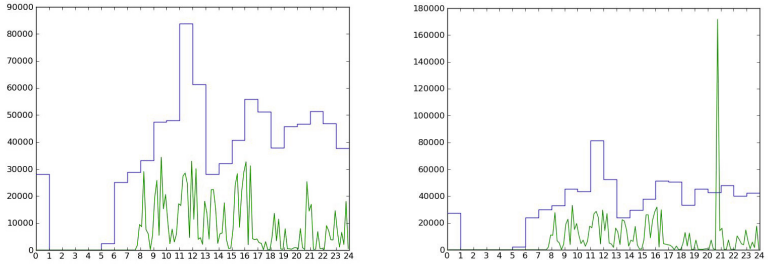
Fig. 3 Anomaly Detection preprocessor block diagram for SNORT IDS system

Traffic profiles are stored in local preprocessor database (preprocessor can update traffic profiles in any time by switching preprocessor to appropriate mode). During normal work preprocessor calculates Chi-square test and energies from DWT subbands coefficients and compare it to the network profiles collected in database. Preprocessor indicates anomalies when the parameters calculated by ADS algorithms during normal work exceed boundaries designated by interval $< \mu - 3\sigma, \mu + 3\sigma >$
where: μ - is a mean calculated for one analysis window for a given network profile; σ - standard deviation calculated for one analysis window for a given network profile.

When the preprocessor indicates anomaly a report is generated to a log file. A log file consist of the information when anomaly starts and ends, the traffic feature which indicates alarm and about confidence level of a given alarm.

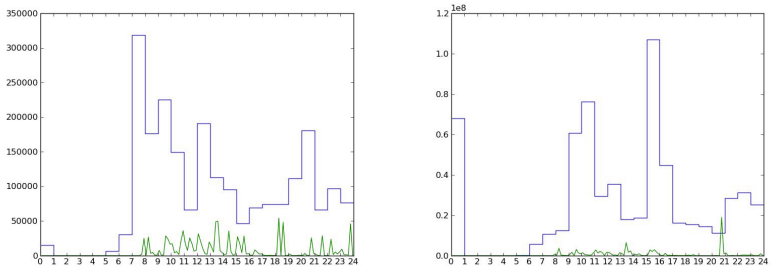
Table 1 Network traffic features captured by SNORT ADS preprocessor

f_1	number of TCP pockets	f_{14}	out TCP pockets (port 80)
f_2	in TCP pockets	f_{15}	in TCP pockets (port 80)
f_3	out TCP pockets	f_{16}	out UDP datagrams (port 53)
f_4	number of TCP pockets in LAN	f_{17}	in UDP datagrams (port 53)
f_5	number of UDP datagrams	f_{18}	out IP traffic [kB/s]
f_6	in UDP datagrams	f_{19}	in IP traffic [kB/s]
f_7	out UDP datagrams	f_{20}	out TCP traffic (port 80) [kB/s]
f_8	number of UDP datagrams in LAN	f_{21}	in TCP traffic (port 80) [kB/s]
f_9	number of ICMP pockets	f_{22}	out UDP traffic [kB/s]
f_{10}	out ICMP pockets	f_{23}	in UDP traffic [kB/s]
f_{11}	in ICMP pockets	f_{24}	out UDP traffic (port 53) [kB/s]
f_{12}	number of ICMP pockets in LAN	f_{25}	in UDP traffic (port 53) [kB/s]
f_{13}	number of TCP pockets with SYN and ACK flags		



(a) (b)

Fig. 4 Chi-square profile (stepped line) and value of Chi-square 24 hour test (axis x - time in hours) for current network traffic (a) without anomaly (b) with anomaly



(a) (b)

Fig. 5 DWT coefficient energy profile (stepped line) and value of DWT energy coefficients during 24 hour test (axis x - time in hours) for current network traffic (a) without anomaly (b) with anomaly

Exemplary profiles (stepped line) together with real time calculated values (values of Chi-square test and energy from DWT coefficients) during normal preprocessor work are shown in Figures 4-5.

3 Experimental Results

Proposed ADS preprocessor was evaluated with the use of local LAN network. The preprocessor examined summary traffic from entire subnet. Usability of proposed solution was evaluated by simulating different attack on tested LAN network. We used Back Track [11] Linux distribution for simulating different attack such as eg. various port scanning, DoS, DDoS, Syn Flooding, pocket

Table 2 Detection Rate DR [%] achieved by subsequent network traffic features

Feature	Chi-sqaure	Mallat	Lifting scheme	Feature	Chi-sqaure	Mallat	Lifting scheme
f_1	5.26	5.26	5.26	f_{14}	0.00	5.26	10.52
f_2	5.26	10.52	10.52	f_{15}	0.00	10.52	10.52
f_3	0.00	10.52	10.52	f_{16}	0.00	0.00	0.00
f_4	15.78	10.52	10.52	f_{17}	5.26	5.26	5.26
f_5	10.52	10.52	10.52	f_{18}	10.52	10.52	10.52
f_6	0.00	0.00	0.00	f_{19}	5.26	5.26	10.52
f_7	0.00	0.00	0.00	f_{20}	10.52	5.26	5.26
f_8	15.78	31.58	31.57	f_{21}	5.26	10.52	10.52
f_9	94.73	94.73	84.21	f_{22}	0.00	0.00	0.00
f_{10}	73.68	94.73	78.95	f_{23}	0.00	0.00	0.00
f_{11}	0.00	5.26	0.00	f_{24}	0.00	0.00	0.00
f_{12}	68.42	78.95	15.78	f_{25}	5.26	0.00	0.00
f_{13}	10.52	10.52	10.52				

Table 3 False Positive FP [%] achieved by subsequent network traffic features

Feature	Chi-sqaure	Mallat	Lifting scheme	Feature	Chi-sqaure	Mallat	Lifting scheme
f_1	4.46	7.43	8.96	f_{14}	3.73	7.48	9.64
f_2	4.07	7.99	9.42	f_{15}	3.91	7.17	9.32
f_3	4.49	7.96	9.69	f_{16}	0.02	0.02	0.02
f_4	4.24	6.06	6.90	f_{17}	0.34	0.39	0.39
f_5	4.57	5.62	3.94	f_{18}	3.90	8.74	9.95
f_6	2.86	4.14	2.23	f_{19}	4.37	8.36	10.26
f_7	5.18	5.33	5.98	f_{20}	3.71	8.50	9.95
f_8	4.20	8.28	8.62	f_{21}	3.81	7.09	9.11
f_9	6.69	9.13	0.05	f_{22}	2.36	3.08	1.60
f_{10}	0.47	0.48	0.48	f_{23}	3.76	3.07	3.42
f_{11}	4.07	12.06	12.64	f_{24}	0.02	0.00	0.00
f_{12}	5.42	4.34	0.05	f_{25}	0.37	0.02	0.02
f_{13}	4.15	7.07	8.14				

fragmentation and others. When the preprocessor indicates a possible anomaly a log is generated to a text file. Granularity of analysis depends on window analysis time. Time of analysis window can be arbitrarily set during start of preprocessor.

Detection rate DR and false positive FP for 25 traffic features were presented in Table 2 and Table 3. The best results were achieved for features f_9 and f_{10}. Detection rate and false positive depends on ADS algorithm and calculated traffic feature. $DR[\%]$ for f_9 and f_{10} changes in boundaries $73.68 - 94.73$ in turn $FP[\%]$ has values between $0.05 - 9.13$.

4 Conclusion

This paper presents proposition of anomaly detection preprocessor for SNORT IDS system. The major contributions are: proposition of new SNORT preprocessor where at the same time two different algorithms (Chi-square and DWT) were used to detect anomalies. The preprocessor was examined in real network. The presented results prove that the presented algorithms can be used for improving cybersecurity and resilience of the network infrastructures.

References

1. SNORT IDS, `http://www.snort.org/`
2. Ye, N., Chen, Q., Emran, S.M.: Chi-squared statistical profiling for anomaly detection. In: Proc. IEEE SMC Inform. Assurance Security Workshop, West Point, pp. 182–188 (2000)
3. Scherrer, A., Larrieu, N., Owezarski, P., Borgant, P., Abry, P.: Non-Gaussian and Long Memory Statistical Characterizations for Internet Traffic with Anomalies. IEEE Trans. on Dependable and Secure Computing 4(1) (2007)
4. Choraś, M., Saganowski, Ł., Renk, R., Hołubowicz, W.: Statistical and signal-based network traffic recognition for anomaly detection. Expert Systems: The Journal of Knowledge Engineering (2011), doi:10.1111/j.1468-0394.2010.00576.x
5. Ye, N., Li, X., Chen, Q., Masum Emran, S., Xu, M.: Probabilistic techniques for intrusion detection based on computer audit data. IEEE Trans. on Systems, Man and Cybernetics-Part A: Systems and Humans 31(4) (2001)
6. Dainotti, A., Pescape, A., Ventre, G.: Wavelet-based Detection of DoS Attacks. In: IEEE GLOBECOM, San Francisco, CA, USA (November 2006)
7. Wei, L., Ghorbani, A.: Network Anomaly Detection Based on Wavelet Analysis. EURASIP Journal on Advances in Signal Processing, Article ID 837601, 16 pages (2009), doi:10.1155/2009/837601
8. Grossman, A., Morlet, J.: Decompositions of Functions into Wavelets of Constant Shape, and Related Transforms. Mathematics and Physics: Lectures an Recent Results, L. Streit (1985)

9. Sweldens, W.: The Lifting Scheme: A Custom-Design Construction of Biorthogonal Wavelets. Applied and Computational Harmonic Analysis 3(15), 186–200 (1996)
10. Lakhina, A., Crovella, M., Diot, C.H.: Characterization of network-wide anomalies in traffic flows. In: Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement, pp. 201–206 (2004)
11. BackTrack Linux, http://www.backtrack-linux.org/