Usage of RBF Networks in prediction of network traffic

Maciej Szmit
Telekomunikacja Polska
Orange Labs
7 Obrzeżna Street
02-691 Warsaw Poland
Email: maciej.szmit@orange.com

Anna Szmit
Technical University of Lodz
Depatment of Management
266 Piotrkowska Street
90-924 Łódź Poland
Email: agorecka@p.lodz.pl

Marcin Kuzia
Telekomunikacja Polska
Orange Labs
7 Obrzeżna Street
02-691 Warsaw Poland
Email: marcin.kuzia@orange.com

***Abstract*—Prediction of future time series values is area of statistics and computer science research related to pattern recognition. Especially possibility of prediction of the future computer network traffic may be usable in detection of abnormal situations like DoS attacks or occurrence of problems with network infrastructure. The article is devoted to usage artificial neural networks, with radial basis activation function for prediction of network traffic in sample local area networks.**

I. Introduction

IN MANY areas the occurrence of atypical value (named anomaly or outlier) of the particular variable may indicate existence of undesirable phenomenon (especially threat), like symptom of the disease in medicine, change the characteristics of the process in engineering or security incident in telecommunication networks. Anomaly Detection (AD) also called Outlier Detection, is area of statistics and computer science research (see e.g. [1]) related to pattern recognition.

TABLE I.
INVESTIGATED NETWORKS DESCRIPTION. SOURCE: OWN RESEARCH.

Symbol	**Description**
W1	Amateur campus network consisting of circa 25 workstations. Snort has worked on the router which acts also as the gateway to the Internet and as FTP, www, SAMBA and TeamSpeak servers. Data were collected from 13th September to 5th December 2006 with a ten minute interval (a total of 11 969 measurements).
T2	Campus network provided by a mid-size Internet Access Provider – (about 400 clients). Data were collected from 3rd January to 16th March 2007 with ten-minute intervals (a total of 10 001 measurements) on the link between the network and the Internet in housing estates.
T3	A network in a block of flats; one of the subnetworks mentioned in the examples T2 containing about 20 clients. The data were collected from 20th November 2006 to 16th March 2007 with ten-minute intervals (a total of 16402 measurements) on the same link as above (T2) but with address filtering.
MM	Home network connected to the campus amateur network (with maximum speed of inbound traffic set on the bandwidth manager to 4 Mbps. Home network consists of five computers protected by corporate firewall and two intranet servers (ftp and PrintServer). The network has no servers providing outside services and there is no remote access to the home network from the outside. IDS was placed on the link to the campus network before the firewall. The data were collected from 12th February to 1st July 2011 (a total of 20113 measurements).
II	Local Area Network in small company (about 40 computers, two intranet servers). The data were collected from 3rd February 2011 to 4th July 2011 (a total of 21747 measurements).

Anomaly Detection approach needs firstly recognize a pattern of system behavior and next - find observations that differs from the expected ones. The first task may be done using various types of models form classic mathematical and statistical models up to Artificial Intelligence based ones.

Detection of anomalies in computer security domain is one of three approaches used in Intruder Detection Systems (among misuse detection systems and integrity verification – see e.g. [4], [25]). Especially the analysis may concern behavior of single hosts (HBAD – Host Behavior Anomaly Detection) or computer networks (NBAD – Network Behavior Anomaly Detection). NBAD research may focuses on single packets structure anomalies (monitoring phenomena like untypical flag sets in TCP packets, incorrect fragmentation of IP packets etc. – see e.g. [26]) or on network traffic flows (see [21]-[23]).

The previous works of us (see e.g.: [4]-[11], [18]) were according to time series modelling and forecasting using econometric and Artificial Intelligence methods on application of selected time series prediction models in computer networks security area and to methods of detection anomalies of network traffic at the packet level measurements (see e.g.: [12], [13], [19], [24]) using confidence band-based algorithms (see e.g.: [1]-[3]). We focus on classical statistical models like naïve method, autoregression-based (AR, SARIMA), exponential smoothing (Holt-Winters model and its modification) etc. Especially in the article [10] we tried to use multilayer perceptron (MLP) artificial neural networks for modelling and forecasting of network traffic in some local area and campus networks. The current article is devoted to usage of the other kind of neural networks, with radial basis activation function (called RBF Networks) in computer network traffic prediction.

II. The objectives and the method of the research

Like in previous researches we use time series with network traffic data collected from five computer networks described in Table i (detailed information about these networks and descriptive statistics of collected time series are described in [9]).

We collect several time series, containing data about network traffic (overall number of packets received by network probe in five minutes period) according to the three most popular network protocols: TCP, UDP and ICMP and next modeled these time series using RBF networks.

A radial basis functions (see e.g.: [14]-[16]) are a real-valued functions whose value depends only on the distance from the some other point c called a center

$$f(x, c) = f(\|x - c\|) \qquad (1)$$

The norm is often euclidean distance, however other distance functions are also possible.

Radial basis function networks are artificial neural networks uses radial basis functions as activation functions. Typically RBF networks typically contains from three layers: input layer which is designed only to sends input signals for all neurons in hidden layer, a hidden layer with radial activation function and a linear output layer so the output of the network are a linear combination of radial basis functions of the inputs and neuron parameters (see Fig. 1).

The value on j output neuron network may be described as a function of the input vector x given by the equation

$$y_j = \sum_{i=1}^{N} w_i f\left(\|x - c_i\|\right) \qquad (2)$$

where:

N is the number of neurons in the hidden layer,

x is the input vector,

c_i is the center vector for neuron i and

w_i is the weight of neuron i in the linear output neuron.

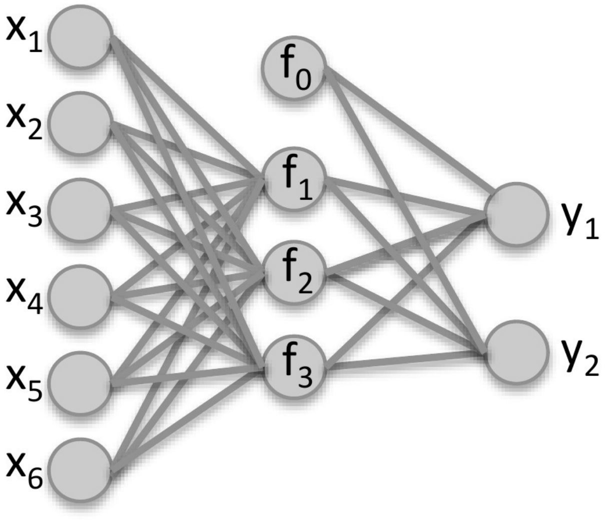

Fig. 1. Sample RBF Network. Source: own research.

We used RBF ANN simulator build in Statistica packet with default algorithm of network structure determination.

Like in previous research we decided to use MAE (Mean Absolute Error), rather than MSE (Mean Squared Error) based measure because there were a lot of so-called outliers are noted in the analysed samples and MSE-based measure can be oversensitive in those cases (see e.g.:[17]). As a meter of model fit we use a quotient:

$$\frac{Mean\_Absolute\_Error}{Mean}$$

expressed as a percentage.

III. Results and conclussions

For each time series we tried to predict single value (number of particular packets in the next 5 minutes), so all of the networks has one neuron in output layer. On the input ANNs can get information about previous value of time series. In all of cases the explanatory variable were value of the series delayed by 1, 2 and 3 periods, and in the most of cases additionally the explanatory variables were value of the series delayed by 144 and 145 periods (that mean delayed by one

TABLE II.
RBF AND MLP ANNS STRUCTURES AND FIT. SOURCE: [10], OWN RESEARCH.

Series	Protocol	MLP Topology	MLP MAE/M	RBF Topology	RBF MAE/M
W1	TCP	2-1-1 (-1,-3)	**46,18%**	4-7-1	47,33%
W1	UDP	1-2-1 (-1)	**31,73%**	3-7-1	33,28%
W1	ICMP	4-2-1 (-1, -2, -3, -144)	**34,54%**	6-7-1	36,63%
T2	TCP	1-1-1 (-1)	**4,23%**	3-10-1	4,28%
T2	UDP	5-1-1 (-1, -2, -3, -144, -1009)	**15,41%**	5-2-1	17,07%
T2	ICMP	2-2-1 (-1, -2)	**8,66%**	3-12-1	9,65%
T3	TCP	1-1-1 (-1)	**4,07%**	3-7-1	4,31%
T3	UDP	1-1-1 (-1)	**15,05%**	5-2-1	22,13%
T3	ICMP	3-1-1 (-1, -3, -1008)	**8,91%**	5-2-1	21,86%
MM	TCP	2-2-1 (-1, -2)	**75,72%**	6-10-1	82,64%
MM	UDP	4-1-1	30,12%	3-7-1 (-1,-2,-3)	**29,11%**
MM	ICMP	3-1-1	10,93%	3-13-1 (-1,-2,-3)	**10,77%**
II	TCP	2-1-1	41,14%	4-10-1 (-1, -2, -3, -1008)	**38,97%**
II	UDP	5-1-1 (-1, -2, -3, -144, 1008)	**48,42%**	5-8-1	49,24%
II	ICMP	1-1-1	116,44%	3-7-1 (-1,-2,-144)	**114,43%**

day and one and five minutes) and in several cases the algorithm select also values delayed by 1008 and 1009 that means week and week and five minutes).

The Table ii includes number of neurons in input, hidden and layer in each RBF ANN. presents fits of the model (MAE/M) compared with results gets by Multilayer Perceptron (MLP) ANN described in article [10]. For winner ANNs its topology and explanatory variables are described.

As one can see RBF ANNs structure determination algorithm tend to choose a larger number of explanatory variables comparing the analogous one for MLP ANNs, but it does not often lead to better model fit. Only in TCP in II network traffic time series the results of RBF were significantly better then MLP.

REFERENCES

[1] Markou M., Singh S.: Novelty detection: a review part 1: statistical approaches, Signal Processing, vol. 83, pp. 2481 – 2497, Decemeber 2003;

[2] Brutlag J. D.: Aberrant behavior detection in time series for network monitoring, Proceedings of the 14th System Administration Conference, pp. 139–146, New Orleans, Fla, USA, 2000.

[3] Liu, W; Lin S., Piegorsch W. W.: Construction of Exact Simultaneous Confidence Bands for a Simple Linear Regression Model, International Statistical Review 76 (1): 39–57. doi:10.1111/j.1751-5823.2007.00027.x.

[4] Szmit M., Adamus S., Bugała S., Szmit A.: Implementation of Brutlag's algorithm in Anomaly Detection 3.0, Federated Conference on Computer Science and Information Systems, Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 685–691, PTI, IEEE, Wrocław 2011

[5] Szmit M., Szmit A.: Use of Holt-Winters method in the analysis of network traffic. Case study, Springer Communications in Computer and Information Science vol. 160, 18th Conference Computer Networks, 2011, s. 224-231, ISSN: 1865-0929; ISBN: 978-3-642-21770-8, DOI: 10.1007/978-3-642-21771-5_24

[6] Szmit M., Szmit A.: Usage of Modified Holt-Winters Method in the Anomaly Detection of Network Traffic: Case Studies, Journal of Computer Networks and Communications, vol. 2012, DOI:10.1155/2012

[7] Szmit M., Szmit A.: Usage of Pseudo-estimator LAD and SARIMA Models for Network Traffic Prediction. Case Studies, Communications in Computer and Information Science, 2012, Volume 291, 229-236, DOI: 10.1007/978-3-642-31217-5_25

[8] Szmit A., Szmit M.: O wykorzystaniu modeli ekonometrycznych do prognozowania ruchu sieciowego, Zarządzanie rozwojem organizacji, Spała 2013 (accepted for publication)

[9] Szmit M.: Využití nula-jedničkových modelů pro behaviorální analýzu síťového provozu, Internet, competitiveness and organizational security, TBU, Zlín 2011

[10] Szmit M., Szmit A., Adamus S., Bugała S.: Usage of Holt-Winters Model and Multilayer Perceptron in Network Traffic Modelling and Anomaly Detection, Informatica Vol. 36, Nr 4, pp. 359-368

[11] Jašek R., Szmit A., Szmit M.: Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling, Advances in Intelligent Systems and Computing Volume 210, 2013, pp. 435-444 (Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems), DOI:978-3-319-00542-3_43

[12] Münz G.: Traffic Anomaly Detection and Cause Identification Using Flow-Level Meas- urements, TUM, Müchen 2010, http://www.net.in.tum.de/fileadmin/TUM/NET/NET- 2010-06-1.pdf

[13] Wang Y.: Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection, IGI Global 2009

[14] Broomhead D. S. LoweD.: Radial basis functions, multi-variable functional interpolation and adaptive networks, Technical report 4148, RSRE 1988, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA196234

[15] Yanwei F., Yingying Z., Haiyang Y.: Study of neural network technologies in intrusion detection systems, Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing (WiCOM'09). IEEE Press, NJ 2009 pp. 4454-4457

[16] Yang Z.: An intrusion detection system based on RBF neural network, Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, 2005, pp. 873 - 875 Vol. 2

[17] Rousseeuw P. J., Leroy A. M.: Robust Regression and Outlier Detection, Wiley, 1987

[18] Szmit A., Szmit M.: O wykorzystaniu modeli ekonometrycznych do prognozowania modeli ruchu sieciowego, Zeszyty Naukowe Organizacja i Zarządzanie Nr 1154 (55), Politechnika Łódzka, Łódź 2013, pp. 193-201, ISSN: 0137-2599

[19] ITU-T E.507 Models for Forecasting International Traffic, ITU 1998, http://www.itu.int/rec/T-REC-E.507-198811-I/en

[20] Villén-Altamirano M.: Overview of ITU Recommendations on Traffic Engineering, Paper presented in the ITU/ITC workshop within 17th ITC.

[21] Rajahalme J., Conta A., Carpenter B., Deering S.: IPv6 Flow Label Specification, RFC 3697, Network Working Group 2004

[22] Quittek J., Zseby T., Claise B., Zander S.: Requirements for IP Flow Information Export (IPFIX), RFC 3917, Network Working Group 2004

[23] Brownlee N., Mills C., Ruth G.: Traffic Flow Measurement: Architecture, RFC 2722, Network Working Group 1999

[24] ITU-T Recommendation E.490.1: Overview of Recommendations on traffic engineering, ITU 2003, http://www.itu.int/rec/T-REC-E.490.1-200301-I/en

[25] Vala R., Malanik D., Jašek, R. "Usability of Software Intrusion-Detection System in Web Applications", Advances in Intelligent Systems and Computing, Vol. 189, pp. 159-166, Springer-Verlag, Berlin 2013

[26] V. A. Siris and F. Papaglou, "Application of anomaly detection algorithms for detecting syn floodinfg attacks," in Proceedings of the IEEE Global Telecommunications Conference, vol. 4, pp. 2050–2054, 2004