Accepted Manuscript

Title: A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection

Author: Zouhair Chiba, Noureddine Abghour, Khalid Moussaid, Amina El omri, Mohamed Rida

PII: S0167-4048(18)30054-3
DOI: https://doi.org/10.1016/j.cose.2018.01.023
Reference: COSE 1285

To appear in: Computers & Security

Received date: 25-4-2017
Revised date: 18-1-2018
Accepted date: 30-1-2018


This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
A Novel Architecture Combined with Optimal Parameters for Back Propagation Neural Networks Applied to Anomaly Network Intrusion Detection

Zouhair Chiba *, Noureddine Abghour, Khalid Moussaid, Amina El omri, Mohamed Rida
LIMSAD Labs
Faculty of Sciences, Hassan II University of Casablanca
20100, Casablanca, Morocco
Corresponding author: chiba.zouhair@gmail.com

Mr Zouhair Chiba is a PhD Student at LIMSAD Labs within Faculty of Sciences, Hassan II University of Casablanca (Morocco). He had a Master in Computer and Internet Engineering in 2013, and a Bachelor of Mathematical Sciences. He research interests are in the area of Security, Big Data on Cloud Infrastructures, Computer Networks, Mobile Computing and Distributed Systems. E-mail: chiba.zouhair@gmail.com.

Dr. Noreddine Abghour is currently associate professor in the Faculty of Science of Hassan II University, Morocco. He received his Ph.D. degree from National Polytechnic Institute of Toulouse (France) in 2004. His research mainly deals with Security in Distributed Computing Systems. E-mail: n.abghour@fsac.ac.ma.

Dr. Khalid Moussaid is recently appointed director of Computer Science, Modeling Systems and Decision Support laboratory of the Hassan II University of Casablanca. He has a PhD in Oriented Object Database; a Master in Computer Science and a Bachelor of Science in Applied Mathematics. He is interested in Optimization, Algorithmic and especially in the field of Big Data and Cloud Computing. E-mail: khmoussaid@fsac.ac.ma.

Dr. Amina El omri is a professor of Higher Education in Computer Science at the Faculty of Sciences, University Hassan II Casablanca, Morocco. Her main scientific interests concern Algorithms, Optimization, Transport and the Logistic problems. She has participated with a lot of research papers in workshops and conferences, and published several journal articles. E-mail: a.elomri@fsac.ac.ma.

Dr. Mohamed Rida is a professor in Computer Science at the Faculty of Sciences, University Hassan II Casablanca (Morocco) and member of LIMSAD Labs within the same Faculty. He received his Ph.D. degree from University Hassan II Mohammadia in 2005, and his thesis subject was “Virtual Container Terminal: Design and Development of an object platform for the simulation of the operations of a container terminal”. His research area includes Transport, Geographic Information System and Big Data. E-mail: m.rida@fsac.ac.ma.

Abstract

Today, as attacks against computer networks are evolving rapidly, Network Intrusion Detection System (NIDS) has become a valuable tool for the defense-in-depth of computer networks. It is widely deployed in network architectures in order to monitor, detect and eventually respond to any anomalous behavior and misuse which can threat confidentiality, integrity and availability of network resources and services. In this paper, we have proposed an optimal approach to build an effective anomaly NIDS based on Back Propagation Neural Network (BPNN) using Back Propagation Learning Algorithm, and employed a novel architecture for that network. Our approach consists firstly of generation of all possible combinations of most relevant values of the parameters included in construction of such classifier, or influencing its performance in anomaly detection, like feature selection, data normalization, architecture of neural network and activation function. Secondly, we have built 48 IDSs corresponding to those combinations. Finally, after considering all performance measurements like detection rate, false positive rate, F-score, AUC (ability to avoid false classification) etc., we have selected the two best IDSs. Experimental results on KDD CUP’99 dataset indicate that our two best IDSs use the novel architecture, and that compared to several traditional and new techniques, our proposed approach achieves higher detection rate and lower false positive rate.

Keywords: Network IDS; Back propagation neural network; Anomaly detection; KDD Cup’99 dataset; Feature selection; Data preprocessing; Normalization; Back propagation learning algorithm.
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات