Contents lists available at ScienceDirect

Journal of Computational Science

journal homepage: www.elsevier.com/locate/jocs

Hybridization of computational intelligence methods for attack detection in computer networks

A. Branitskiy, I. Kotenko*

Saint-Petersburg Institute for Informatics and Automation of RAS, Saint-Petersburg, Russian Federation

ARTICLE INFO

Article history:
Received 9 December 2015
Received in revised form 30 May 2016
Accepted 22 July 2016
Available online xxx

Keywords:
Computational intelligence
Network security
Network attacks
Attack detection
Neural networks
Immune detectors
Neuro-fuzzy classifiers
Support vector machines
Principal component analysis
Hybrid classification

ABSTRACT

The paper is devoted to identification and classification of network traffic connections by various hybridization schemes with the goal of efficient network attack detection. For this purpose the combination of different methods of computational intelligence is used, namely neural networks, immune systems, neuro-fuzzy classifiers and support vector machines. To increase the speed of processing of input vectors it is proposed to apply the method of principal components. A distinctive feature and advantage of the approach suggested is a multi-level analysis of network traffic, providing the possibility to detect attacks by a signature based technique and combining a set of adaptive detectors based on computational intelligence methods. The paper describes a software tool that is built on the basis of the proposed hybridization mechanisms. Computational experiments were carried out that serve as evidence of their effectiveness in detection of both known and unknown attacks.

1. Introduction

The emergence of a network data transmission technology has become the source of a number of issues related to security of information resources connected through the Internet. According to the statistics given in the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) the level of computer threats each year remains high [55]. Fig. 1 shows the indicators that reflect the number of security incidents registered in the United States and which reports were provided by organizations of critical infrastructures. The majority of security incidents covers different classes of network attacks, namely DoS attacks, network scanning, SQL injections, etc. Among them organizations are presented in the field of banking, energy, telecommunication, dams, transportation, critical manufacturing, healthcare, etc. Computer network attacks affect both large business enterprises and public sector organizations and end users. Today every device connected to the computer network has a number of vulnerabilities and weaknesses in the implementation of the algorithms and software which are laid in their operation. In addition publicly available information allows even inexperienced users, that have access to a network space, to make the network attacks of various types.

It is yet worth noting a number of other reasons which affect the network security. During a continuous development of information and network technologies attacker skills and instruments are improved, which are fundamental factors leading to security breaches. Moreover the association of individual computers in local area networks creates an additional number of problems associated with ensuring their security. Therefore the task of detection and prevention of network attacks based on new tools and techniques is an actual area of scientific research.

To solve the problems of network attack detection different approaches realizing signature based techniques, computational intelligence methods, for example, neural networks, immune systems, neuro-fuzzy classifiers, support vector machines (SVM), etc. and their combination can be used.

In the paper the problem of network attack detection is solved by a hybrid approach, the novelty of which is in combining the traditional signature based detection model and several additional models – a statically trained feed-forward neural networks, neuro-fuzzy classifiers, SVM and dynamically trained immune detectors which are indicators of the multi-level and adaptive network attack detection.

The use of neural networks, neuro-fuzzy classifiers and support vector machines assumes that the nature of the intrusive

* Corresponding author.
E-mail addresses: branitskiy@comsec.spb.ru (A. Branitskiy), ivkote@comsec.spb.ru (I. Kotenko).

http://dx.doi.org/10.1016/j.jocs.2016.07.010
1877-7503/© 2016 Elsevier B.V. All rights reserved.

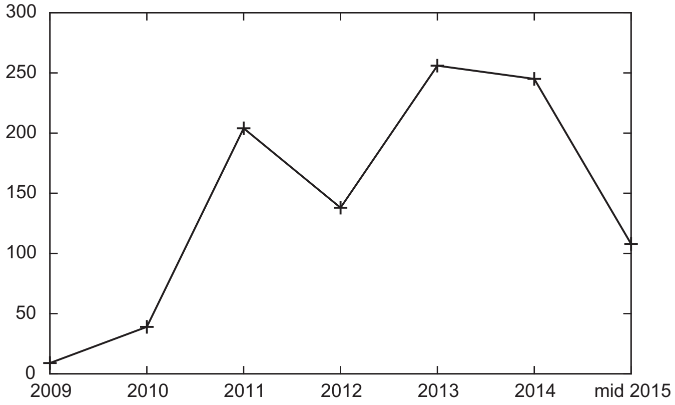

Fig. 1. ICS incidents reported (in thousands).

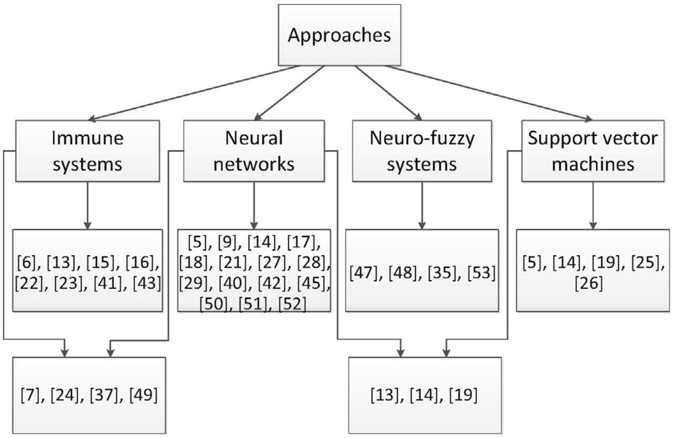

Fig. 2. Computational intelligence methods for information security.

actions over time remains constant and predictable. While applying immune detectors, we take into account the dynamic component of attacker's behavior: in the detection mode the classifiers continue to be trained on new features of detected attacks. In order to accelerate the training, testing and launching of the detectors it is proposed to use a technique that implements the principal component analysis.

Thus, the goal of the paper is to develop and evaluate a hybrid approach to detect network attacks based on a multi-level integration of traditional (signature based) mechanisms and computational intelligence detection models, including the development of an intrusion detection tool based on this approach and performing a set of experiments.

The paper is based on the article [8] which has been significantly expanded by the realization and evaluation of different hybridization mechanisms. This paper discusses several hybridization schemes combining intelligent classifiers, namely (1) a simple voting technique, (2) an improved stacking algorithm, (3) a technique using the referee (arbiter) based on the dynamic areas of competence and (4) a classification tree with neural networks as nodes. The main contribution of the paper is in the theoretical and practical aspects of the applicability of the proposed combination schemes.

The paper is organized as follows. Section 2 presents an overview of related works which consider network attack detection approaches using artificial neural networks, immune systems, neuro-fuzzy systems, SVM and their combination. Section 3 outlines the proposed neural network model. The immune approach is discussed in section 4. Sections 5 and 6 describe general concepts related to the neuro-fuzzy classifiers and support vector machines. The realization of the principal component analysis is presented in section 7. Section 8 provides a general hybridization scheme and used methods of classifier combination. Section 9 contains the description of the computational experiments. In conclusion the performed results are summarized, and the further research tasks are suggested.

2. Related work

Artificial neural networks, immune systems, neuro-fuzzy classifiers, SVM and their combination provide adaptive mechanisms for information processing which enable to solve many problems related to information security. These approaches are of particular interest for researchers in network attack detection. At the present time there are many papers investigating the applicability of different methods in network security, but we are focusing on these four approaches and their combination.

Figs. 2 and 3 summarize characteristics of some related works using these methods to solve the problems related to information security, including detection of anomalous processes [13,52], user identification [40], detection and classification of network attacks [18,21,29,43], detection of malicious software [7], detection of anomalous user behavior [17,45].

Let us describe some of papers in details.

In [42,50] for detecting the network attacks it is suggested to use a multilayer neural network which is trained on data from the set of Snort signatures. In many papers, e.g. [27,51], the KDD Cup 99 dataset is used as a training data set. Another source of data includes simulated network connections.

The paper [9] is devoted to describing and applying a three-layer back propagation neural network as a binary classifier of network connections. The classifier is constructed so that it can only detect whether the connection is anomalous or not.

Combining several radial basis function (RBF) neural networks is presented in [4]. Ensemble of neural networks receives the input parameters obtained from the fuzzy clustering module, and is combined in such a way that their output values are input for a multilayer perceptron, which task is to reduce the number of mistakes made by previous classifiers. The developed approach was compared with the construction of classificators according to schemes

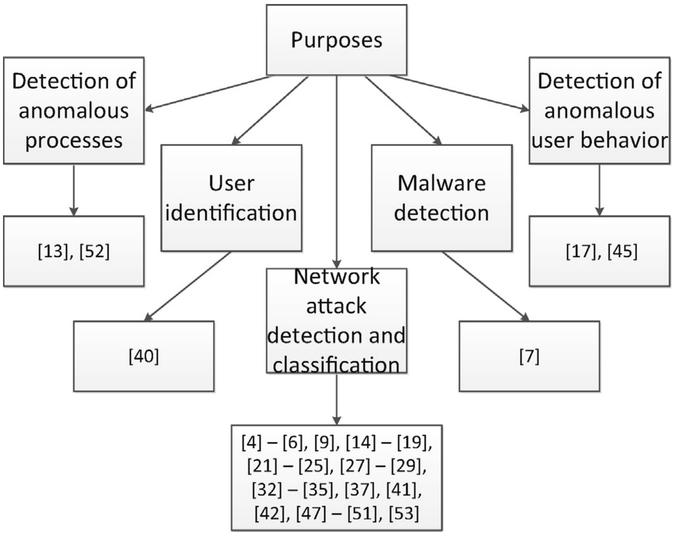

Fig. 3. Domains of application of computational intelligence methods in information security.

Please cite this article in press as: A. Branitskiy, I. Kotenko, Hybridization of computational intelligence methods for attack detection in computer networks, J. Comput. Sci. (2016), http://dx.doi.org/10.1016/j.jocs.2016.07.010