

## Accepted Manuscript

Title: Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model

Authors: Shadi Aljawarneh, Monther Aldwairi, Muneer Bani Yasin



PII: S1877-7503(16)30509-9  
DOI: <http://dx.doi.org/doi:10.1016/j.jocs.2017.03.006>  
Reference: JOCS 628

To appear in:

Received date: 24-12-2016  
Revised date: 5-2-2017  
Accepted date: 5-3-2017

Please cite this article as: Shadi Aljawarneh, Monther Aldwairi, Muneer Bani Yasin, Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model, Journal of Computational Science <http://dx.doi.org/10.1016/j.jocs.2017.03.006>

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.

# Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model

Shadi Aljawarneh<sup>1</sup>, Monther Aldwairi<sup>1,2</sup>, Muneer Bani Yasin<sup>1</sup>

[saaljawarneh@just.edu.jo](mailto:saaljawarneh@just.edu.jo), [monther.aldwairi@zu.ac.ae](mailto:monther.aldwairi@zu.ac.ae), [masadeh@just.edu.jo](mailto:masadeh@just.edu.jo)

<sup>1</sup>Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, Jordan

<sup>2</sup>College of Technological Innovation, Zayed University

\*Corresponding author information:

**Shadi Aljawarneh**

Email: [saaljawarneh@just.edu.jo](mailto:saaljawarneh@just.edu.jo)

Phone: +962 2 7201000

## Paper Highlights

- Utilise the NSL-KDD data set and the binary and multiclass problem with a 20% training dataset.
- This paper studied a new model that can be used to estimate the intrusion scope threshold degree based on the network transaction data's optimal features that were made available for training.
- The experimental result revealed that the hybrid approach had a significant effect on the minimisation of the computational and time complexity involved when determining the feature association impact scale. The accuracy of the proposed model was satisfactory at 99.77% and 99.63% for the binary class and multiclass NSL-KDD data sets, respectively.

## Abstract

Efficiently detecting network intrusions requires the gathering of sensitive information. This means that one has to collect large amounts of network transactions including high details of recent network transactions. Assessments based on meta-heuristic anomaly are important in the intrusion related network transaction data's exploratory analysis. These assessments are needed to make and deliver predictions related to the intrusion possibility based on the available attribute details that are involved in the network transaction. We were able to utilize the NSL-KDD data set, the binary and multiclass problem with a 20% testing dataset. This paper develops a new hybrid model that can be used to estimate the intrusion scope threshold degree based on the network transaction data's optimal features that were made available for training. The experimental results revealed that the hybrid approach had a significant effect on the minimisation of the computational and time complexity involved when determining the feature association impact scale. The accuracy of the proposed model was measured as 99.81% and 98.56% for the binary class and multiclass NSL-KDD data sets, respectively.

However, there are issues with obtaining high false and low false negative rates. A hybrid approach with two main parts is proposed to address these issues. First, data needs to be filtered using the Vote algorithm with Information Gain that combines the probability distributions of these base learners in order to select the important features that positively affect the accuracy of the proposed model. Next, the hybrid algorithm consists of following classifiers: J48, Meta Pagging, RandomTree, REPTree, AdaBoostM1, DecisionStump and NaiveBayes. Based on the results obtained using the proposed model, we observe improved accuracy, high false negative rate, and low false positive rule.

**Keywords:** feature reduction; intrusion detection; correlation analysis; association impact scale

Download English Version:

<https://daneshyari.com/en/article/6874394>

Download Persian Version:

<https://daneshyari.com/article/6874394>

[Daneshyari.com](https://daneshyari.com)