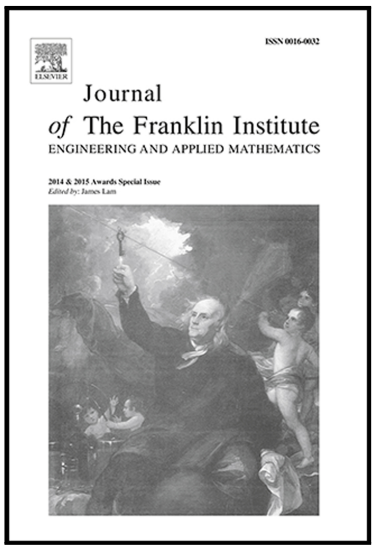

Adaptive and Online Network Intrusion Detection System using Clustering and Extreme Learning Machines

Setareh Roshan, Yoan Miche, Anton Akusok, Amaury Lendasse

PII: S0016-0032(17)30299-5
DOI: 10.1016/j.jfranklin.2017.06.006
Reference: FI 3024

To appear in: *Journal of the Franklin Institute*

Received date: 29 September 2016
Revised date: 31 March 2017
Accepted date: 16 June 2017

Please cite this article as: Setareh Roshan, Yoan Miche, Anton Akusok, Amaury Lendasse, Adaptive and Online Network Intrusion Detection System using Clustering and Extreme Learning Machines, *Journal of the Franklin Institute* (2017), doi: 10.1016/j.jfranklin.2017.06.006

Adaptive and Online Network Intrusion Detection System using Clustering and Extreme Learning Machines

Setareh Roshan[b,a], Yoan Miche[c], Anton Akusok[d], Amaury Lendasse[e]

[a] *F-Secure Corporation, Finland*
[b] *Aalto University, Finland*
[c] *Bell Labs, Nokia, Finland*
[d] *Arcada University, Finland*
[e] *The University of Iowa, USA*

Abstract

Despite the large volume of research conducted in the field of intrusion detection, finding a perfect solution of intrusion detection systems for critical applications is still a major challenge. This is mainly due to the continuous emergence of security threats which can bypass the outdated intrusion detection systems. The main objective of this paper is to propose an adaptive design of intrusion detection systems on the basis of Extreme Learning Machines. The proposed system offers the capability of detecting known and novel attacks and being updated according to new trends of data patterns provided by security experts in a cost-effective manner.

Keywords: Intrusion Detection System, Anomaly Detection, Clustering, ELM, Neural Networks

1. Introduction

In today's world, internet and computer networks are widely used in different businesses. Business requirements have made corporations deploy their own information systems on internet. These information systems may utilize different technologies such as distributed data storage systems, encryption and authentication techniques, remote access and web services [21]. While the usage of these technologies provides lots of opportunities for enterprises to achieve