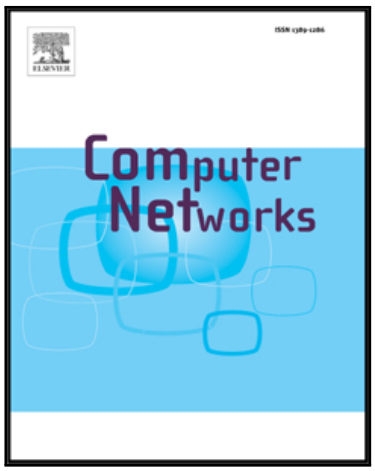

An Evaluation of the Performance of Restricted Boltzmann Machines as a Model for Anomaly Network Intrusion Detection

Tamer Aldwairi , Dilina Perera , Mark A. Novotny

PII: S1389-1286(18)30600-5
DOI: https://doi.org/10.1016/j.comnet.2018.07.025
Reference: COMPNW 6555

To appear in: *Computer Networks*

Received date: 28 December 2017
Revised date: 3 July 2018
Accepted date: 25 July 2018

Please cite this article as: Tamer Aldwairi , Dilina Perera , Mark A. Novotny , An Evaluation of the Performance of Restricted Boltzmann Machines as a Model for Anomaly Network Intrusion Detection, *Computer Networks* (2018), doi: https://doi.org/10.1016/j.comnet.2018.07.025

An Evaluation of the Performance of Restricted Boltzmann Machines as a Model for Anomaly Network Intrusion Detection

Tamer Aldwairi[a,*], Dilina Perera[a,b], Mark A. Novotny[a,b]

[a]Distributed Analytics and Security Institute, High Performance Computing Collaboratory, Mississippi State University, Starkville, Mississippi 39762

[b]Department of Physics and Astronomy, Mississippi State University, Mississippi State, Mississippi 39762

Abstract

The continuous increase in the number of attacks on computer networks has raised serious concerns regarding the importance of establishing a methodology that can learn and adapt to new and novel attacks, such a model should be able to act or react to such threats within a timely manner, so that measures are undertaken to counter any potential breaches within the network. Training a model to distinguish between normal and anomalous network behavior is a difficult task due to the high dimensionality of the network traffic data. One of the key requirements of a successful Anomaly Network Intrusion Detection Systems (A-NIDS) is the ability to recognize new patterns of attacks that it has never before seen. This objective can be achieved through incorporating machine leaning techniques in the learning model of the A-NIDS. In this study, we demonstrate the use of a powerful machine learning technique called the Restricted Boltzmann Machine (RBM) to distinguish between normal and anomalous NetFlow traffic. We evaluate our approach through testing it on the newly renowned Information Security Center of Excellence (ISCX) dataset. Our results indicate that RBMs can be trained successfully to classify normal and anomalous NetFlow traffic. Unlike previous studies, we employ measures of true positives and negatives along with the accuracy to test the effectiveness of RBM as a classifier for A-NIDS. We also utilize the usage of a balanced set to reduce any biases that appear during the RBM training.

*Corresponding author Tel.: +1 6623138462
E-mail address: taa70email@gmail.com