NOVEL HYBRID DEEP-LEARNING APPROACH TO ACCELERATE DETECTION OF NETWORK INTRUSIONS

NISHARA SHAVINDI RAMASINGHE

A dissertation submitted in partial fulfilment of the requirement for Bachelor of Engineering (Honours) degree in Software Engineering

Department of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2021

Abstract

With society's increasing dependency on computer networks for collaboration, information, profit and recreation, there is also a greater need for maintaining the security and safety of our communication channels.

Reducing malicious network traffic starts with accurate identification of network intrusions which is usually achieved using attack signatures or detecting anomalies in traffic patterns. Research into finding better attack detection systems have extended to artificial intelligence techniques of creating suitable algorithmic models based on machine learning (ML) and deep learning (DL).

This research set out to develop a suitable AI model to detect novel network intrusions with improved accuracy and a reduced false alarm rate using a hybrid of ML & Dl algorithms, using a small number of network features.

Compared to existing systems reported in literature, the system developed performs equally or better in detecting network intrusions and reducing the false alarm rate significantly. The detection module was developed with DNN and RNN with optimal feature selection process.

A prototype system was developed with an easy user-interface to a) demonstrate the capabilities of the developed model and b) to enable testing of the prototype against new attack traffic. The prototype may be re-purposed into an open-source network intrusion detection system with the integration of an appropriate in-line network feature extractor.

The developed detection engine can be improved further by fine-tuning the model using newer network attack datasets. This would enable the detection of modern variants of legacy attacks and would increase the chances of novel attack detection in future.

Keywords:

Network Intrusion Detection, Machine Learning, Deep Learning, Hybrid Algorithm