Automated and Improved Detection of Cyber Attacks via an Industrial IDS Probe

Almamy Touré*[1]

[1]LAMIH – Antoine Gallais – France

Résumé

A proper classification of network flows is crucial for detecting anomalous behaviors. Therefore, we present in this paper an approach for classifying network flows based on 1D Convolutional Neural Networks (1D-CNN). Our solution enables dual feature extraction: the first is based on the diverse exchange processes within a network flow, while the second leverages a
characteristic of CNN, particularly the feature detector. This methodology facilitates the extraction of attributes common to
all types of network flows, regardless of context, and performs a secondary extraction to effectively classify collected flows and
detect security incidents. We evaluate our approach using the widely applied UNSW-NB15 public dataset. Results, ranging from
85% to 90% accuracy, demonstrate superior detection of attack classes while reducing the number of features and consequently, the model's execution time.

*Intervenant