

Advancing Network Intrusion Analysis: A Hybrid Approach from Detection to Classification

B. Vithusha, V. Sankeetha, T. Abiramithan, and N. Lojenaa

Department of ICT, Faculty of Technological Studies, University of Vavuniya, Sri Lanka

Abstract

Effective network security requires both accurate detection of anomalies and meaningful classification of detected threats. While supervised machine learning models are proficient in identifying anomalous traffic, categorizing those anomalies into specific attack types, particularly under limited labelling conditions, remains a challenge. In this study, we propose a two-stage hybrid framework that first employs LightGBM for high-accuracy anomaly detection, followed by a semi-supervised, graph-based technique referred to as Label Propagation to classify the detected anomalies. Our approach addresses the gap between detection and interpretation in intrusion detection systems by uncovering hidden attack structures in a data-efficient manner. The proposed method is validated using a labelled network dataset, achieving high detection accuracy and strong clustering performance, highlighting its potential for scalable and adaptive threat analysis.

Keywords: LightGBM, Label propagation, Network intrusion, Attack pattern, Anomaly detection