Systematic Review of Unsupervised Learning Techniques in Anomaly-Based Network Intrusion Detection Systems

Shadnan Azwad Khan[†], Tarem Ahmed[§], Salva Daneshgadeh Çakmakçi[*]

[†] *Sorbonne Université*, France
[§] *Independent University, Bangladesh (IUB)*, Bangladesh
[*] *DECOIT GmbH & Co. KG, Bremen*, Germany

Abstract

In an increasingly digital world, the prevalence of network anomalies and cyber-attacks poses significant threats across various sectors, including social security, military intelligence, market economies, and healthcare. Traditional intrusion detection systems (IDSs) based on signatures and supervised learning often fall short in identifying novel attacks, leading to a growing interest in unsupervised anomaly detection techniques. This paper presents a systematic literature review (SLR) focused on unsupervised anomaly-based network intrusion detection systems (NIDS). We provide an extensive taxonomy of the field, list public datasets commonly used for benchmarking, and conduct a meta-analysis of the reviewed papers. Furthermore, we propose a generalized framework for unsupervised anomaly-based NIDS. Our review thoroughly examines various anomaly detection approaches, including neighborhood-based, density-based, clustering, classification, statistical, subspace-based, and angle-based algorithms. Current performance benchmarks are discussed, along with an exploration of open issues, unresolved problems, and future research directions in the domain. This comprehensive analysis aims to guide researchers and practitioners in developing more effective and robust network security solutions.

Keywords

Anomaly detection, intrusion detection, machine learning, network security, unsupervised algorithms.