Comparative Analysis of Machine Learning Models for Network Intrusion Detection

Anthony Landrain[1], Konstantinos Karampidis[2], Giorgos Papadourakis[2]

[1]Télécom SudParis,
France
anthonylandrain@proton.me

[2]Hellenic Mediterranean University
Department of Electrical and Computer Engineering
Heraklion, Crete 71410, Greece
{karampidis@hmu.gr}
{papadour@hmu.gr}

Abstract: With the prevalence of sophisticated cyberattacks, it is imperative to utilize advanced techniques to protect computer systems from potential threats. Intrusion detection tend to plays a crucial role in the security of computer systems by detecting potential attacks and enabling proactive responses to them. Various methods have been proposed to detect attacks, including signature-based, anomaly-based, and behavior-based methods. However, traditional intrusion detection methods based on signatures and predefined rules reach their limits when faced with complex and evolving attacks. In this work we analyze, experiment and compare the effectiveness of different models e.g., Artificial Neural Networks, Support Vector Machines and Random forests for network intrusion detection. The obtained results from the conducted experiments on a benchmark dataset, revealed that although the Random Forest classifier outperformed the rest of the aforementioned methods, machine learning algorithms offer a promising approach to improve the accuracy and efficiency of intrusion detection systems.