Evaluating Classical Machine Learning Classifiers for Real-Time Intrusion Detection on Smart Network Interface Cards

Md.Tanjeed Islam[1], Atiqur Rahman[2*]
[1]*Dept. of Computer Science and Engineering, Jahangirnagar University, Savar, BGD*
[2*] *Dept. of Mechanical and Aerospace Engineering, Missouri University of Science and Technology, Rolla, USA*
tanjeedislamr@gmail.com , a.rahman@mst.edu

***Abstract*—The rapid growth of network traffic and the number of attack vectors, and the ever more advanced nature of cyberattacks have imposed serious difficulties on traditional Intrusion Detection Systems (IDS). These systems can often be burdened with high traffic and newer network requirements of real-time processing. Smart Network Interface Cards (SmartNICs), which free CPUs from data-plane tasks, are the best candidate to help strengthen network security by accelerating packet processing with higher throughput and lower latency. However, offloading ML algorithms on SmartNICs suffers from limitations such as computational efficiency and resource constraints. In this work, we present a comparative study on three typical ML classifiers decision tree (DT), random forest (RF), K-Nearest Neighbor (KNN) for SmartNIC-based real-time intrusion detection and compare them systematically. On the NSL-KDD dataset, a standard benchmark dataset for network traffic analysis demonstrates the performance, efficiency, and hardware viability of all models. The experimental results demonstrate that RF provides the best trade-off between accuracy and inference time, compared with DT and KNN. Secondly, this study also highlights the significance of the data pre-processing, including feature selection and encoding, that contributes to tuning the model performance under resource-constrained SmartNIC platforms. This study aims to help researchers and practitioners in designing scalable, low-latency IDSs that are more insightful toward the deployment of Machine Learning (ML)-powered security on SmartNICs and moving cyber-security towards more robust and efficient infrastructures.**

***Keyword*—SmartNIC, Intrusion Detection Systems, Machine Learning (ML), Decision Tree, Random Forest, Nearest Neighbors, Network Security, Real-Time Processing, NSL-KDD Dataset**

Md.Tanjeed Islam is currently pursuing a Master of Science (MSc) in Computer Science and Engineering at Jahangirnagar University, Bangladesh, after completing his Bachelor of Science (BSc) at the American International University-Bangladesh (AIUB) in 2023. His research focuses on Machine Learning and Natural Language Processing (NLP), aiming to develop adaptive, intelligent systems that bridge theory with practical applications. He aspires to drive innovation in AI, enhancing human productivity and decision-making.

Atiqur Rahman is currently a doctoral studentmajoring in mechanical engineering at Missouri University of Science and Technology, USA. He received his Bachelor of Engineering degree in mechanical engineering from the University of Science and Technology Beijing (USTB), China, under Chinese Government Scholarship. His main research includes, but is not limited to, material characterization, computer coupling of phase diagrams and thermochemistry (CALPHAD), additive manufacturing, multi-physics simulation, and Machine Learning.