Supplementary Materials

Secure Cyber Defense: An Analysis of Network Intrusion-based Dataset CCD-IDSv1 with Machine Learning and Deep Learning Models

Table S1. Attacks Description

Attacks	Description
ARP Poisoning	ARP Poisoning generates minimum web traffic. It is extremely challenging for IDS to pick up the signature of this type of attack. We wanted to see how well our IDS can handle this attack signature with limited trace.
ARP DoS	This attack leaves plenty of 'breadcrumbs' for IDS to pick up. We sent 600,000 messages at our only available socket at a one-second interval continuously for 16 hours in each machine.
UDP Flood	Similar to the previous attack, however this attack uses a different protocol. We wanted to test how our IDS handle network traffic with different protocols.
Hydra Bruteforce with Asterisk protocol	This type of attack attempts to gain authentication using commonly used password combinations. Hydra is a well-known attack toolkit. The Asterisk protocol is an interesting choice for our attack selection because it is a protocol that is standard for voice-over-IP, which relates to many users that rely on communication tools such as Zoom, Skype, WeChat, Whatsapp during the COVID-19 pandemic.
SlowLoris	SlowLoris is a new representation for low-bandwidth Distributed Denial-of-Service attacks. First developed by a hacker named Robert "RSnake" Hansen, this attack can bring down high-bandwidth servers with a single botnet computer, as evidenced in the 2009 Iranian presidential election.

Table S2. 10-fold Cross validation for different CNN configurations

CNN configuration	Mean Accuracy	Execution Time (seconds)
1 Convolutional layer and 1 Maxpooling layer	95.86 ± 0.42	71.03
2 Convolutional layer and 1 Maxpooling layer	96.21 ± 0.39	82.67
3 Convolutional layer and 1 Maxpooling layer	96.86 ± 0.34	90.16
4 Convolutional layer and 2 Maxpooling layer	96.89 ± 0.31	117.80