

CPS: Medium: Detecting and Controlling Unwanted Data Flows in the Internet of Things



<https://netml.io/>

Nick Feamster, University of Chicago; Samory Kpotufe, Columbia University; Arvind Narayanan, Princeton University

Challenge:

- IoT devices generate abnormal flows
- Each type of device generates new types of activities
 - Denial of service (DoS) attacks
 - New types of devices
 - New activities
 - Privacy and security threats

Algorithms:

- Fast One-Class Support Vector Machine (OCSVM)
- Data Aggregation/Representation for Network Traffic

Applications:

- Critical Infrastructure
- Health and Medicine
- Consumer Protection

Scientific Impact:

- Fast anomaly detection (up to 20x speedup over state of the art)
- General representations of network traffic, anomalous/normal behavior
- Largest dataset of (consumer) IoT devices (6,000+ homes)
- Public software libraries for novelty detection in IoT, with reference implementations

Software:

- NetML (Python library)
- IoT Inspector
- nPrintML
- Automated IoT firewall (AutoT)

External Partners and Outreach:

- University of Chicago Medicine
- Northwestern Medicine
- University of Chicago IT
- Federal Trade Commission
- Media

Fast Algorithms

Method \ Dataset	UNB	CTU	MAWI	MACCDC	SFRIG	AECHO	DWSHR
OC-KJL: AUC Retained	1.42 ± 0.03	1.15 ± 0.07	0.99 ± 0.02	1.08 ± 0.03	1.00 ± 0.01	1.06 ± 0.01	1.01 ± 0.02
Train Speedup	1.98 ± 0.04	2.24 ± 0.05	3.82 ± 0.15	2.02 ± 0.06	2.19 ± 0.11	2.35 ± 0.06	1.96 ± 0.05
OC-KJL-QS: AUC Retained	1.41 ± 0.04	1.06 ± 0.04	0.91 ± 0.05	1.01 ± 0.02	1.00 ± 0.01	1.04 ± 0.02	0.98 ± 0.01
Train Speedup	1.23 ± 0.03	1.03 ± 0.02	1.88 ± 0.07	1.03 ± 0.03	1.03 ± 0.05	1.27 ± 0.03	1.00 ± 0.02
OC-Nyström: AUC Retained	1.56 ± 0.01	1.35 ± 0.05	0.98 ± 0.02	1.08 ± 0.02	0.98 ± 0.02	1.06 ± 0.01	1.04 ± 0.01
Train Speedup	2.56 ± 0.06	2.20 ± 0.05	3.74 ± 0.15	2.05 ± 0.06	2.30 ± 0.11	2.50 ± 0.07	1.97 ± 0.05
OC-Nyström-QS: AUC Retained	1.55 ± 0.01	1.20 ± 0.06	0.96 ± 0.02	1.04 ± 0.04	1.00 ± 0.01	1.05 ± 0.01	0.99 ± 0.01
Train Speedup	1.04 ± 0.02	1.02 ± 0.02	1.88 ± 0.07	1.03 ± 0.03	1.06 ± 0.05	1.23 ± 0.03	0.95 ± 0.02

Open-Source Software

The screenshot shows the netml 0.1.4 software interface. It includes a search bar for projects, the nPrint logo (Standard Network Traffic Fingerprints), and a section for 'Device Activities for Office Chromecast'. The device activities section shows a bar chart of traffic over time, with a legend for various domains like google.com and apple.com. Below the chart is a table of nPrint features:

IPV4 L80 Features	TCP L80 Features	UDP 64 Features	ICMP 64 Features	Payload n Features
Maximum Size of IPv4 Header (64 Bytes)	Maximum Size of TCP Header (64 Bytes)	Size of UDP Header (8 Bytes)	Size of ICMP Header (8 Bytes)	User Defined Number of Bytes

Applications and Testbeds

