2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

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

National Science Foundation Award #1953740

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

Challenge:

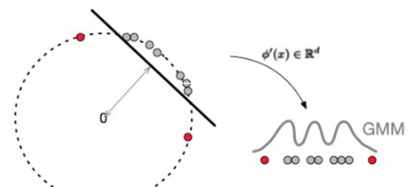
- IoT devices generate abnormal flows
- Each type of device generates new types of activities
  - Denial of service (DoS) attacks
  - New types of devices
  - New activities
  - Privacy and security threats
- **New procedures and tools to detect novel behavior**

Solution:

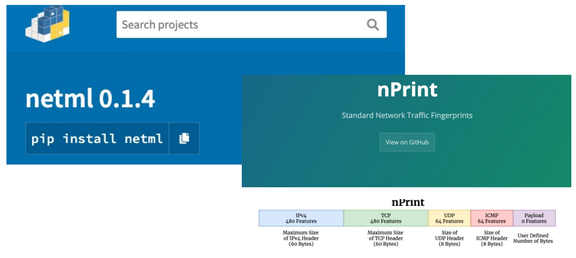
- Integration of new ML algorithms and software
- Algorithms:
  - Fast One-Class Support Vector Machine (OCSVM)
  - Data Aggregation/Representation for Network Traffic
- Software:
  - NetML (Python Library, public, open source)
  - IoT Inspector
  - nPrintML
  - Automated IoT firewall (AutoT)

NSF CPS #1953740
Nick Feamster (feamster@uchicago.edu)
Samory Kpotufe (skk2175@columbia.edu)
Arvind Narayanan (arvindn@princeton.edu)

Fundamental Algorithms



Open-Source Software



Applications

Scientific Impact:

- 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

Broader Impact:

- Application areas:
  - Network security
  - Critical infrastructure monitoring (case studies: campus networks)
  - Behavioral monitoring (Internet of Things lab with labeled human behaviors)
- Application partners:
  - University of Chicago Medicine
  - Northwestern Medicine
  - University of Chicago IT