Attack Circuits for IoT Network Security

Josh Payne

joshp007@stanford.edu

Who Are We?

Josh Payne
Stanford University
IBM Research

Karan Budhraja
University of Maryland, Baltimore County
Infinite Analytics

UMBC

Ashish Kundu
IBM Research
Nuro.ai

How Secure is Your IoT Network? IEEE ICIOT '19

The Internet of Things permeates many spaces.

- Smart Homes
- Workplaces
- Hospitals
- Schools
- ...etc.

How can we assess the **security** of an IoT network?

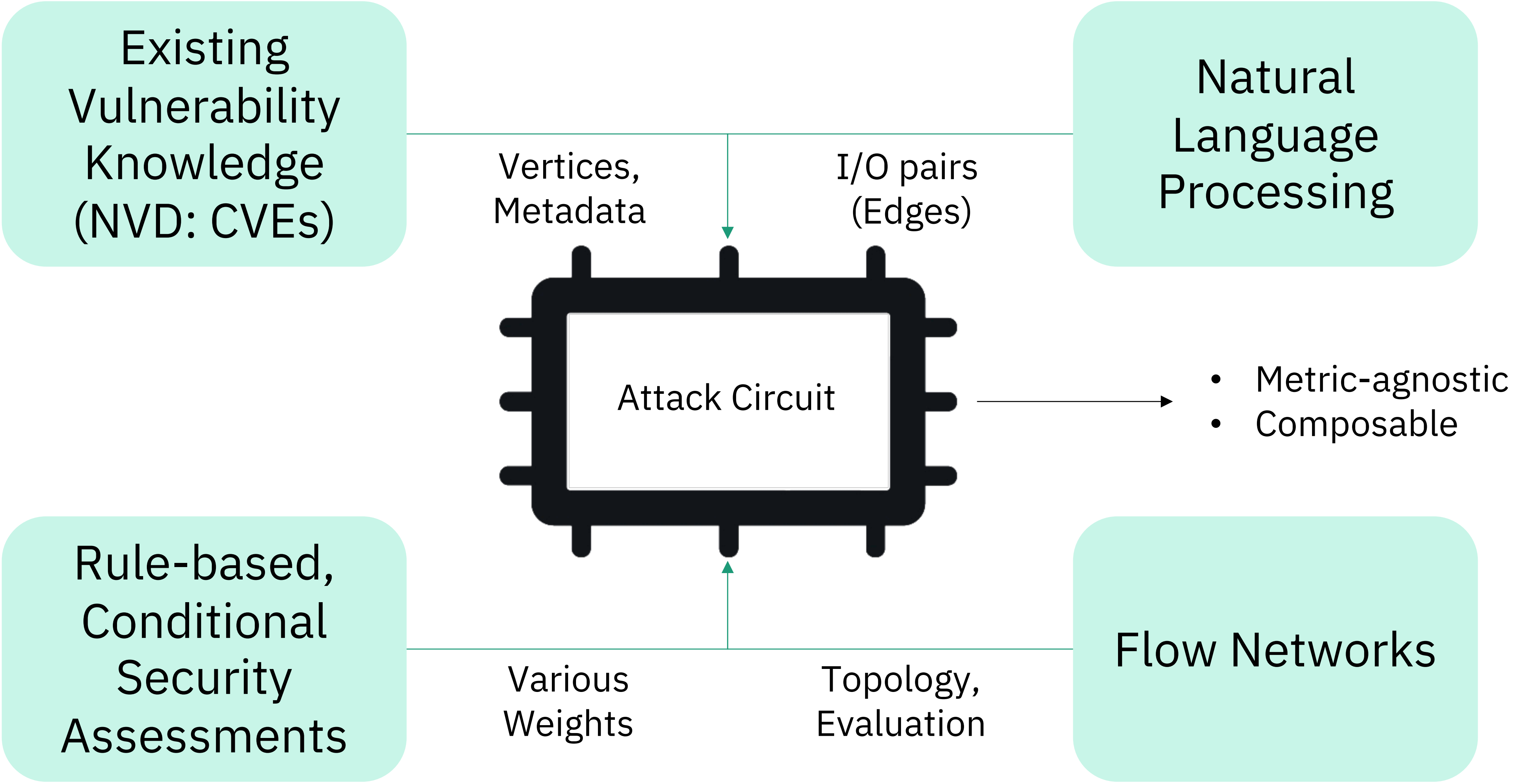
Proposed: $\langle R, E, I \rangle$

R := Risk, defined as: $\langle R_{Conf}, R_{Integ}, R_{Avail} \rangle$

E := Exploitability

I := Impact

The Attack Circuit



Existing Vulnerability Knowledge (NVD: CVEs)

Natural Language Processing

Vertices, Metadata

I/O pairs (Edges)

Attack Circuit

- Metric-agnostic
- Composable

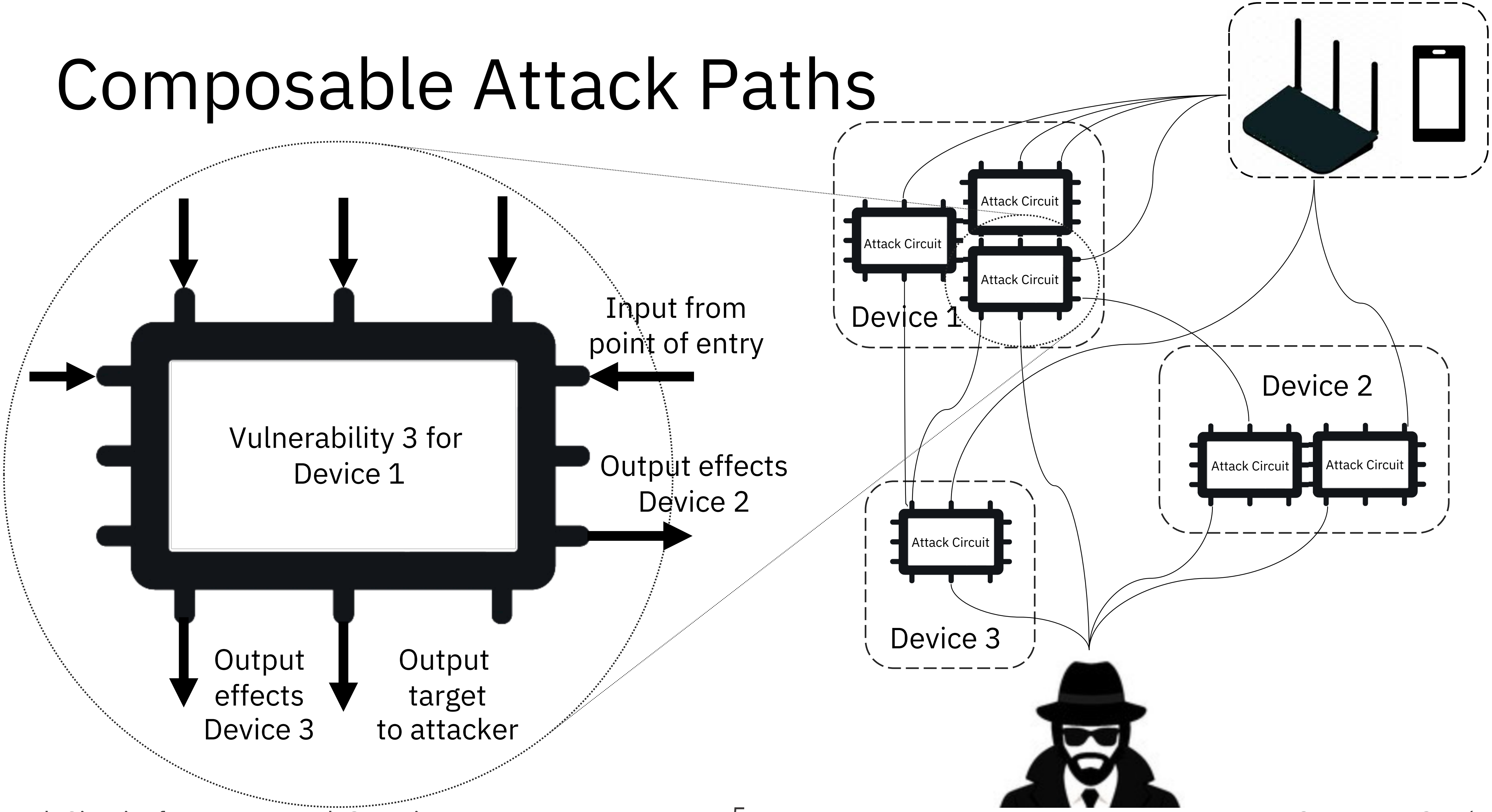
Rule-based, Conditional Security Assessments

Flow Networks

Various Weights

Topology, Evaluation

Composable Attack Paths



Dynamic Activity Metrics using SIEM Logs

How does network behavior factor into the security state?

Large body of work in anomaly detection and scoring in network traffic patterns

We studied network uptime, encryption scheme, and blacklisted IP events*

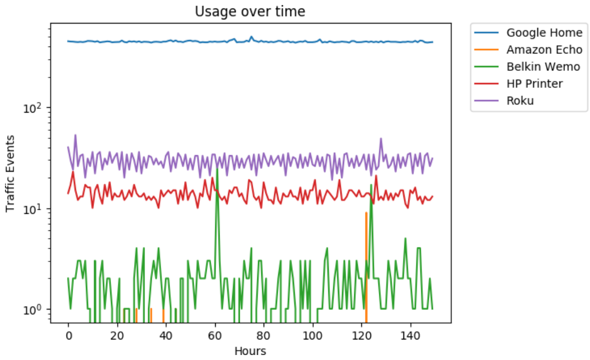
Our metrics were gathered from packet-sniffing on Wireshark

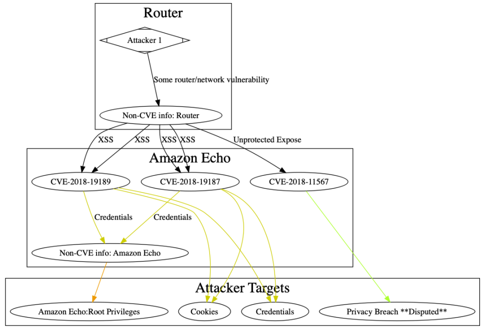
* https://myip.ms/browse/blacklist

Our Implementation

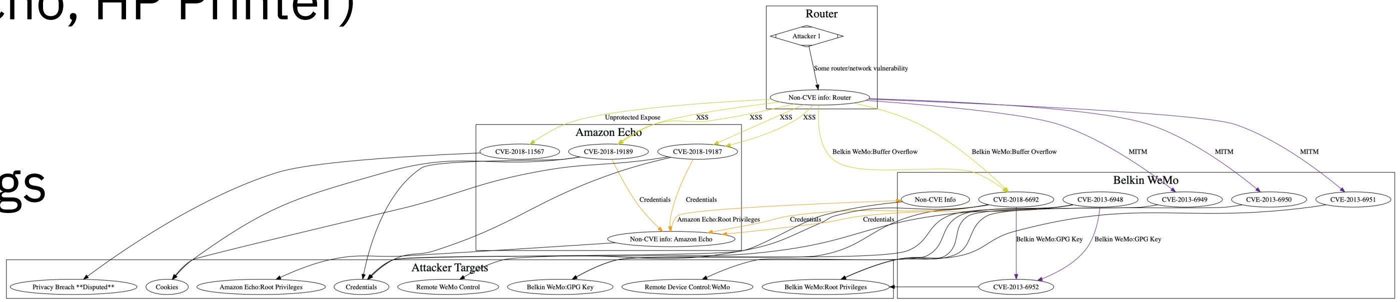
Construction and Evaluation

- 34 Total smart home devices
- 146 CVEs
- 5 Live smart home devices (Google Home, Belkin WeMo, Roku, Amazon Echo, HP Printer)
- 4 Days of packet-sniffing SIEM logs
- 3 Attack circuit types





Impact: Amazon Echo



Exploitability: Amazon Echo, Belkin WeMo

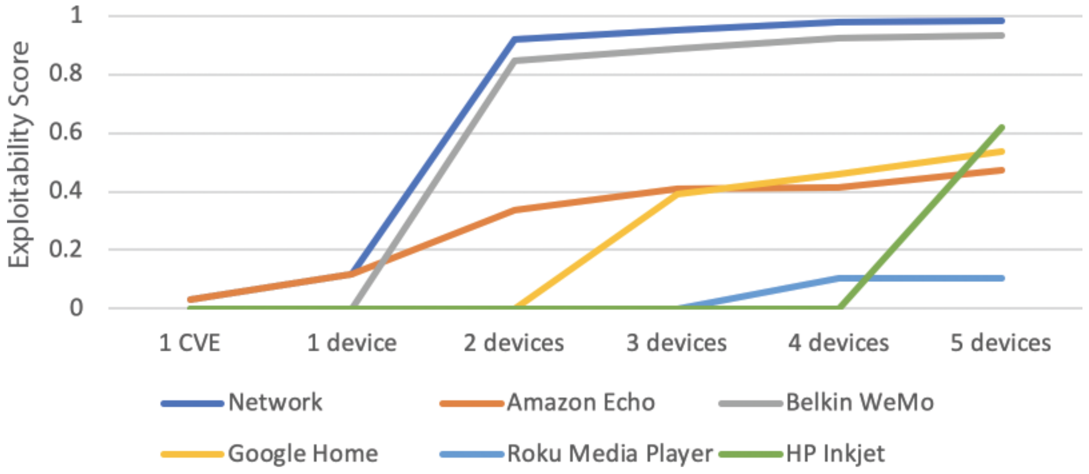
Prototype Results

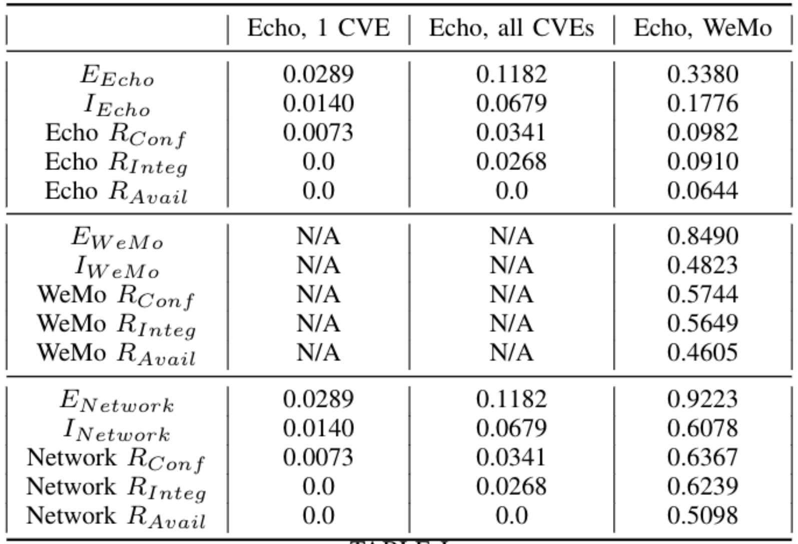
- Tested with five devices with activity metrics

- Initial results are a proof-of-concept for the scoring methods

- Data seems intuitive: compromised devices introduced -> higher exploitability score for other devices and network

- Similar results for impact score





	Echo, 1 CVE	Echo, all CVEs	Echo, WeMo
E_{Echo}	0.0289	0.1182	0.3380
I_{Echo}	0.0140	0.0679	0.1776
Echo R_{Conf}	0.0073	0.0341	0.0982
Echo R_{Integ}	0.0	0.0268	0.0910
Echo R_{Avail}	0.0	0.0	0.0644
E_{WeMo}	N/A	N/A	0.8490
I_{WeMo}	N/A	N/A	0.4823
WeMo R_{Conf}	N/A	N/A	0.5744
WeMo R_{Integ}	N/A	N/A	0.5649
WeMo R_{Avail}	N/A	N/A	0.4605
$E_{Network}$	0.0289	0.1182	0.9223
$I_{Network}$	0.0140	0.0679	0.6078
Network R_{Conf}	0.0073	0.0341	0.6367
Network R_{Integ}	0.0	0.0268	0.6239
Network R_{Avail}	0.0	0.0	0.5098

TABLE I
DEVICE AND NETWORK SCORES FOR DIFFERENT NETWORK SETTINGS.

Future Work

- Testing of system at larger scale, refinement of constants
- Subgraphs for each device representing the program dependence graph
- Sequence models for NLP/NLU: I/O edges

Thank you!

joshp007@stanford.edu