Santa Clara University
Internet of Things
RESEARCH LAB
SIOTLAB

Internet of Things Research Lab
Department of Computer Science and Engineering
Santa Clara University

Santa Clara University
School of Engineering

Securing Smart Homes via Software-Defined Networking and Low-Cost Traffic Classification

Authors: Holden Gordon, Christopher Batula, Bhagyashri Tushir, Behnam Dezfouli, Yuhong Liu

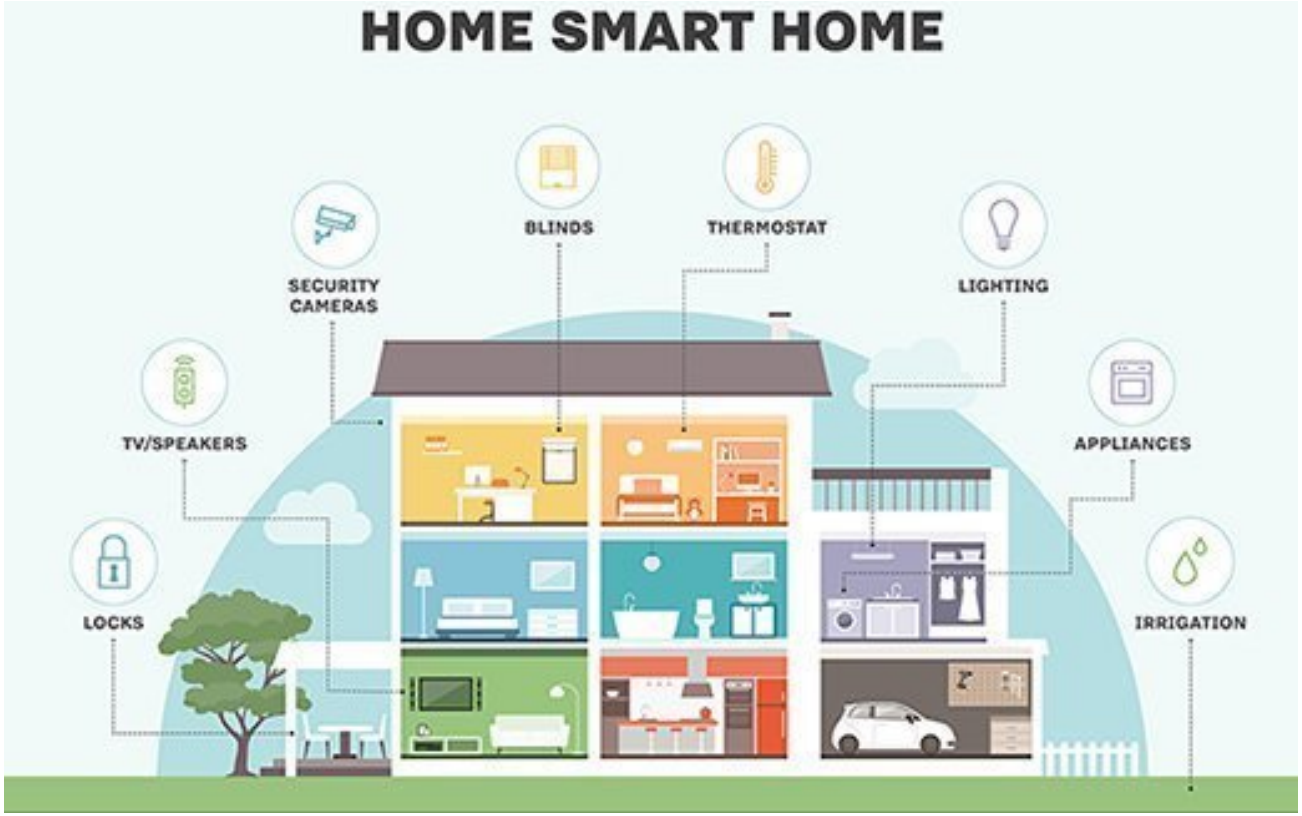
COMPSAC July 2021

Agenda

Santa Clara University
Internet of Things
RESEARCH LAB
SIOTLAB

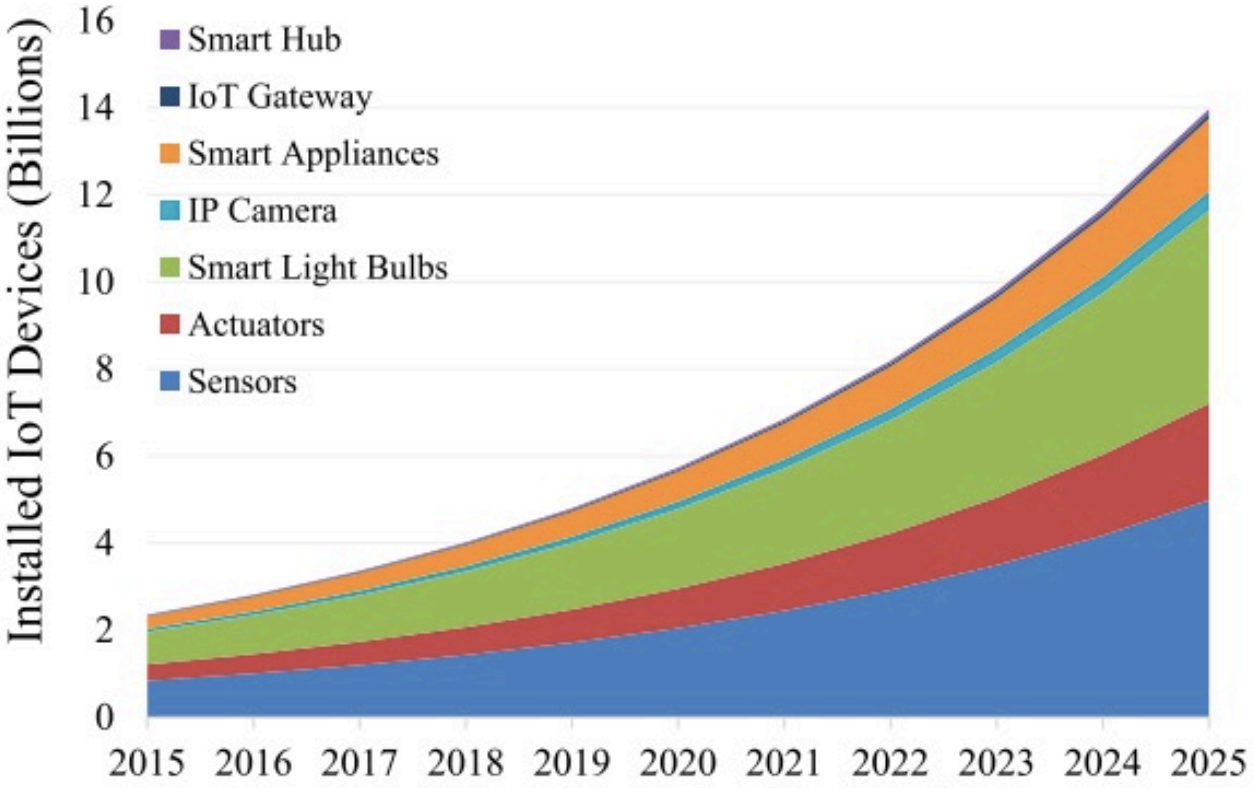
- Smart home and smart home security
- Proposed testing environment
- Proposed features
- Result and discussions

Smart Home Definition



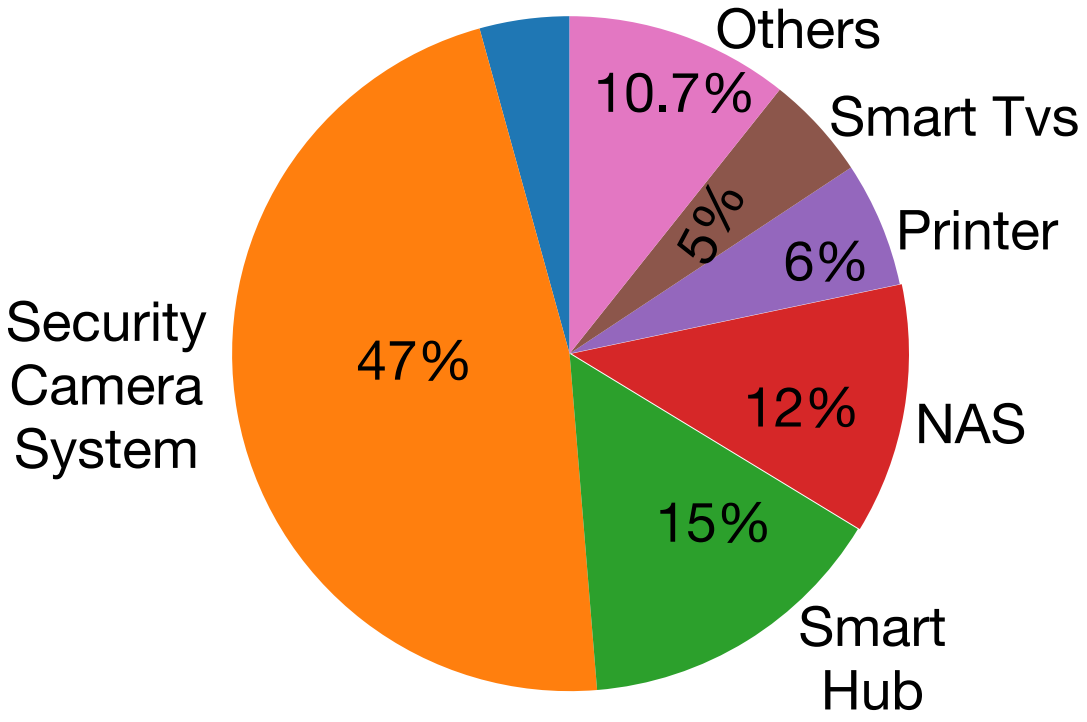
- Smart homes — house with wired and wireless interconnected devices.
- Provide services — voice assistants, security cameras etc.

Smart Home IoT devices growth



The number of interconnected smart home devices will reach 72 billion (approx) by 2025.

Smart Home Devices Security



IoT Devices — attractive to hackers.

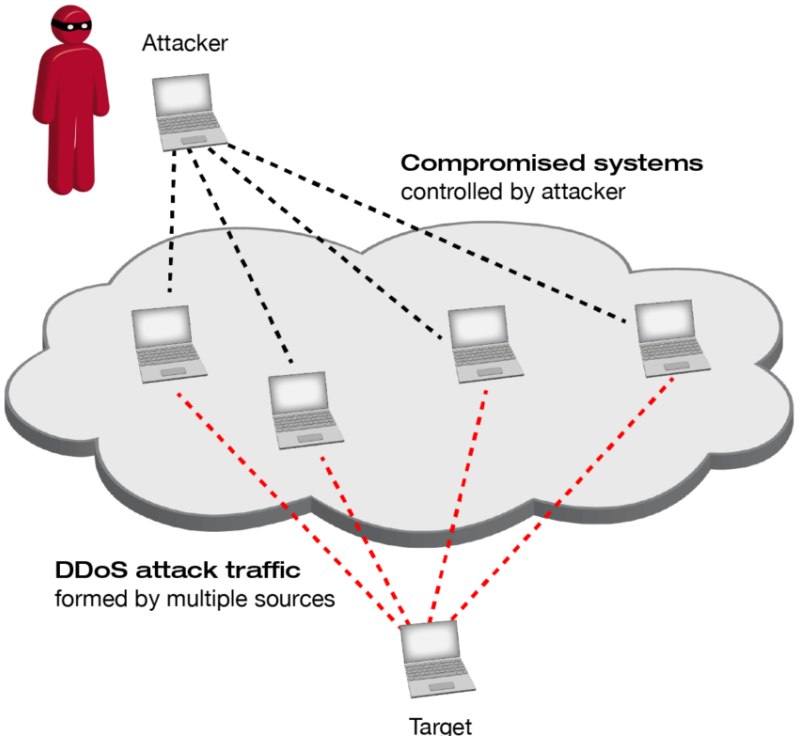
Attacks on Smart Home Devices

- IoT devices are vulnerable to various attacks:
  - *distributed Denial of Service attacks (DDoS),*
  - network scan attacks,
  - SQL injections,
  - zero-day attack and,
  - ransomware attacks

- Reasons:
  - heterogeneity of IoT devices.
  - low storage and computation resources.
  - generate massive data.

Santa Clara University
Internet of Things
RESEARCH LAB
SIOTLAB

DDoS Attacks



- DDoS attacks — target service disruption.
- DDoS attacks — disconnects IoT devices from Access Point.

Software-Defined Networking

- Traditional system inadequate. Why?
  - high volume of data.
  - large amount of connected IoT devices.

- Solution — Software-Defined Networking (SDN):
  - centralize network management,
  - provide flow-based statistics,
  - helps developing flexible solutions.

- SDN and Machine Learning —
  - helps intelligent decisions making.
  - Enhance smart home security via — IoT device classification and DDoS detection.

Contribution

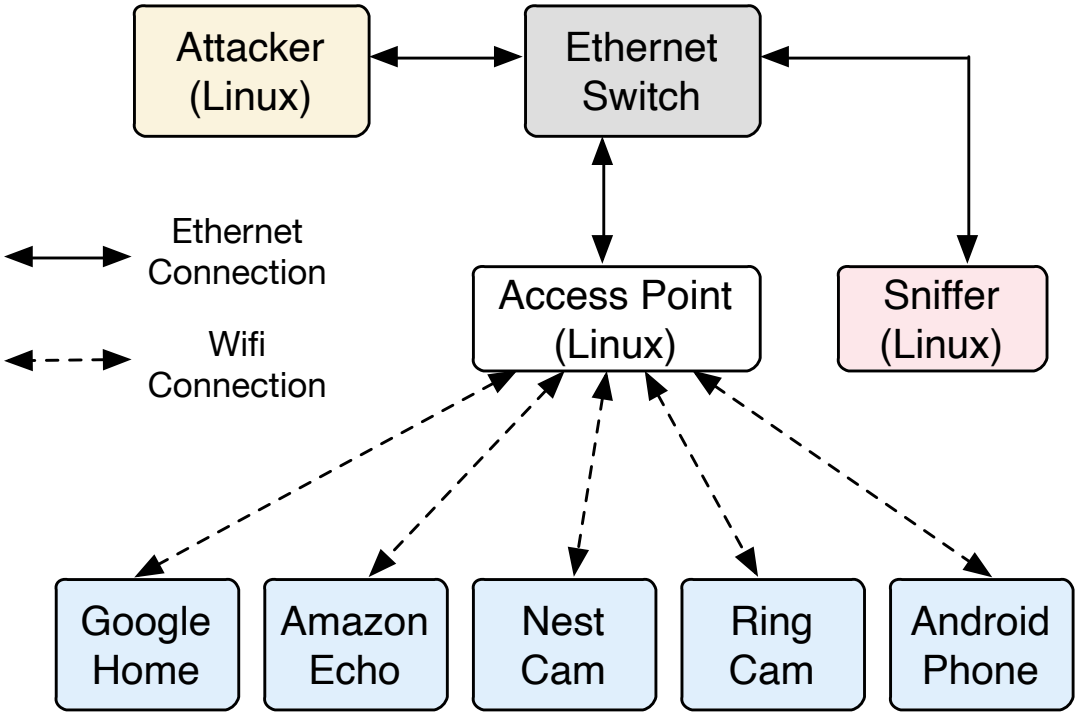
- *Our work focus on SDN based low cost IoT device classification and DDoS detection.*

Contribution —

- novel SDN-based architecture using GNS3 network simulator.
- deployable on low-cost edge system.
- minimum set of flow-based features for both device classification and DDoS detection.
- utilize non-cumulative statistics to reduce controller and switch communication overhead.

Proposed Testing Environment

Smart Home network



Smart Home network for benign and DDoS data collection

Proposed Testing Environment

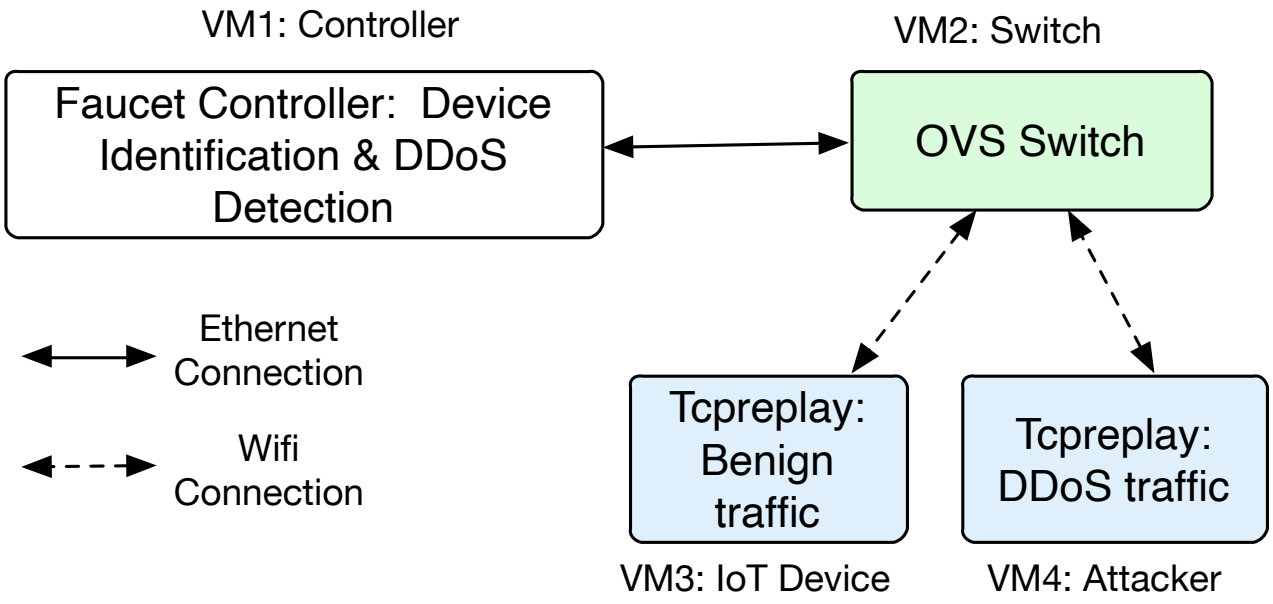
Datasets used

- To confirm the robustness of machine learning models —
  - used 3 datasets: SIOTLAB (our lab), UNSW dataset, combined dataset (SIOTLAB and UNSW)

Device Category	Device
Switches /Triggers	WeMo Motion Sensor, TP Link Plug, Chromecast, Amazon Alexa, Nest Home Alert System
Camera Systems	Ring Cam, Nest Cam, Samsung Cam, Chromecast
IoT Hub Devices	Amazon Echo, IFix, Huebulb, iHome, Google Home

Proposed Testing Environment

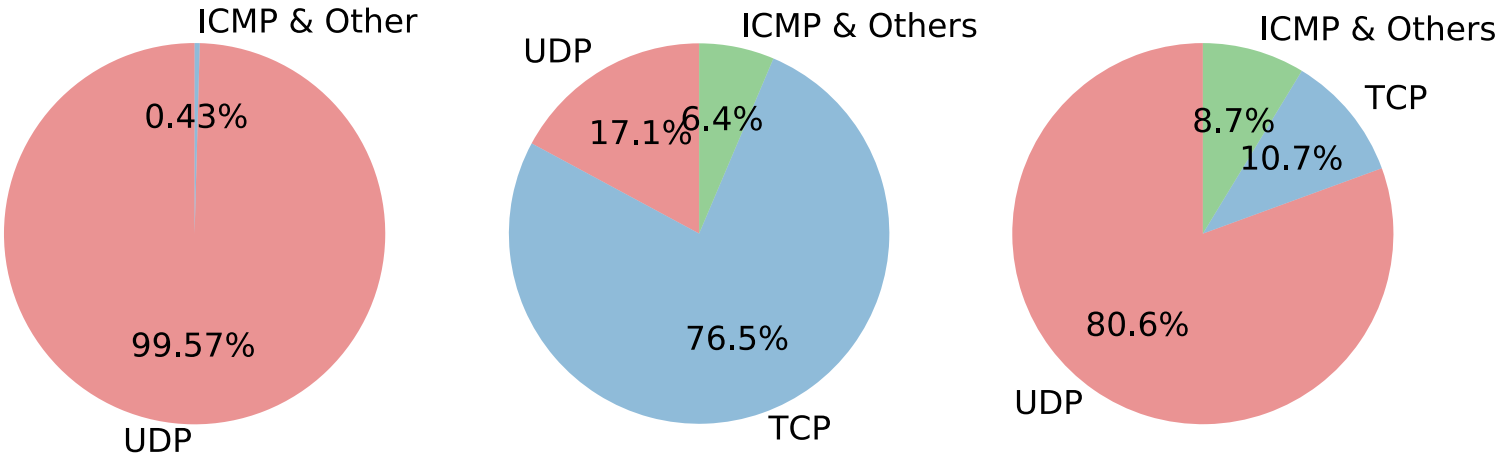
GNS3 Environment



Virtual SDN-based smart home environment using GNS3 simulator

Proposed Testing Environment

Proposed Flow-based Features

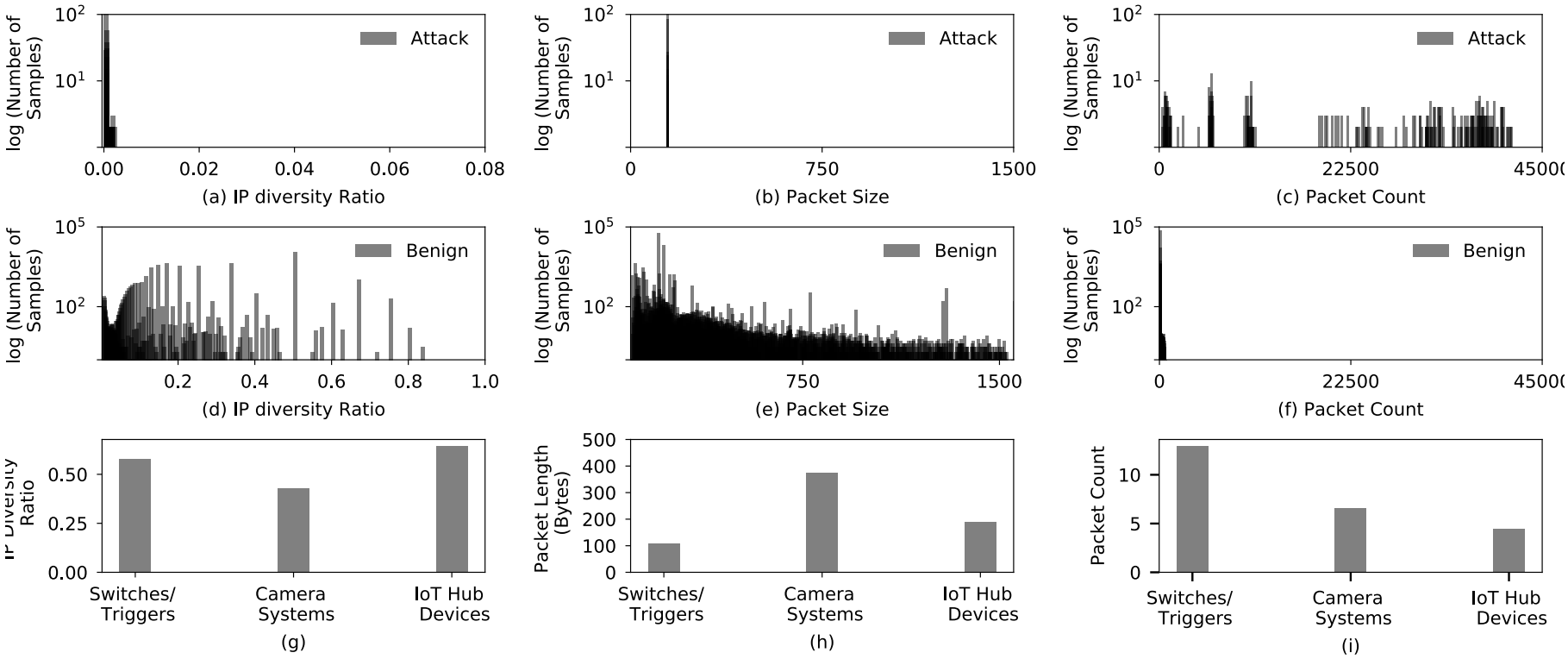


(a) Switches/Triggers (b) Camera Systems (c) IoT Hub Devices

The distinct difference between the distribution of TCP, UDP, ICMP, and other flows among device types enables us to successfully classify devices

Proposed Testing Environment

Proposed Flow-based Features

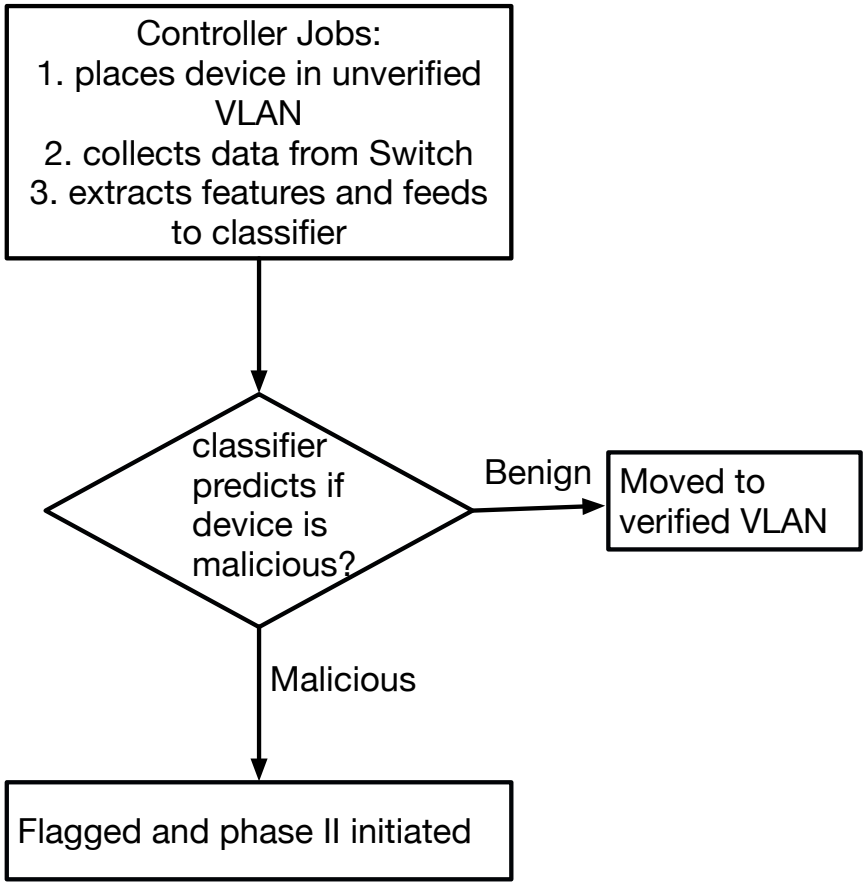


The higher shift in IP diversity ratio, packet size, and packet count allows us to classify devices and identify DDoS attacks with accuracy of 95%.

Proposed Secure Home Architecture

Phase I

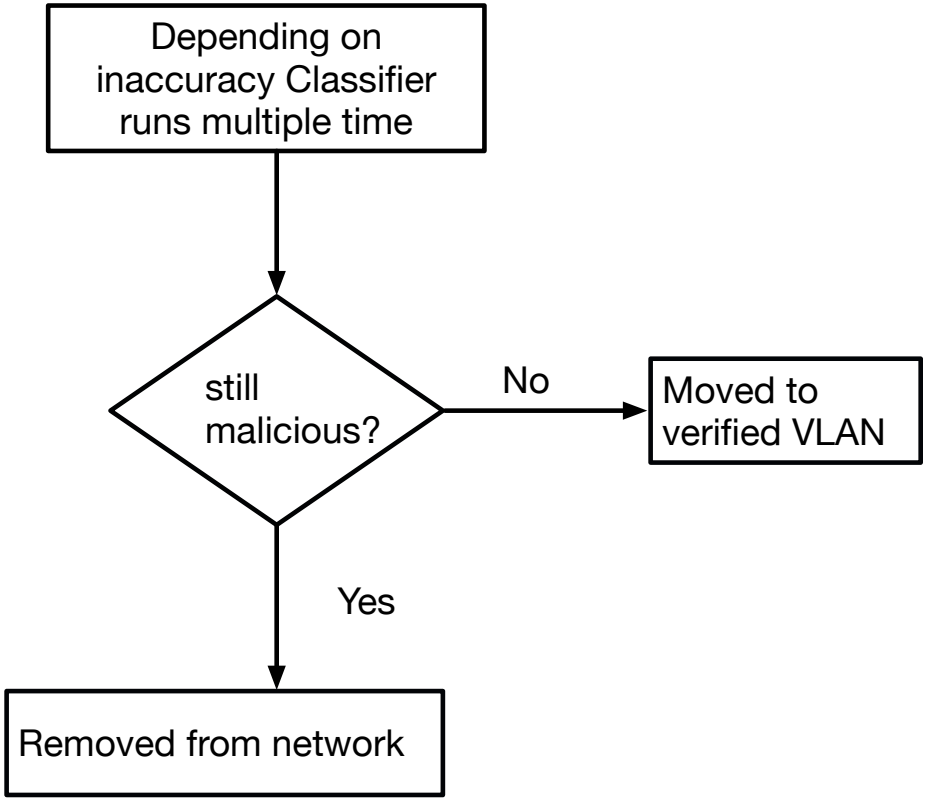
Proposed architecture has two phases —



Phase I

Proposed Secure Home Architecture

Phase II



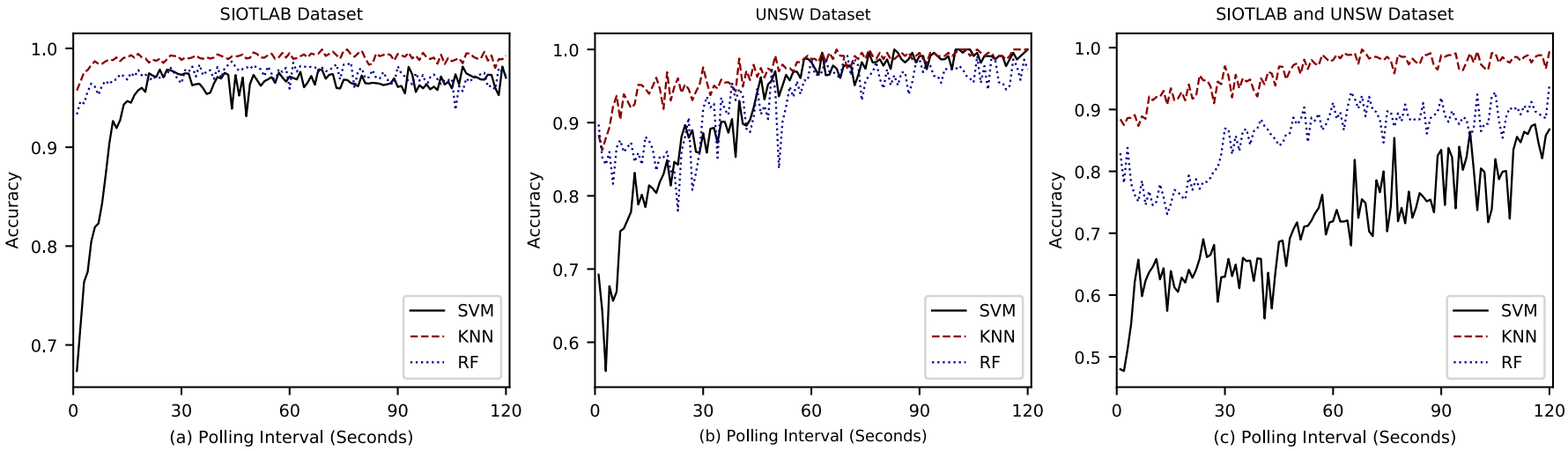
Phase II

Machine learning algorithms

- Machine Learning algorithms used —
  - K-Nearest Neighbors algorithm (KNN)
  - Support Vector Machine with linear kernel (LK-SVM)
  - Random Forest using Gini impurities (RF)
- Hyperparameters are default.
- Split data into 75% train and 25% test data.
- Classes are balanced.

Result and Discussion

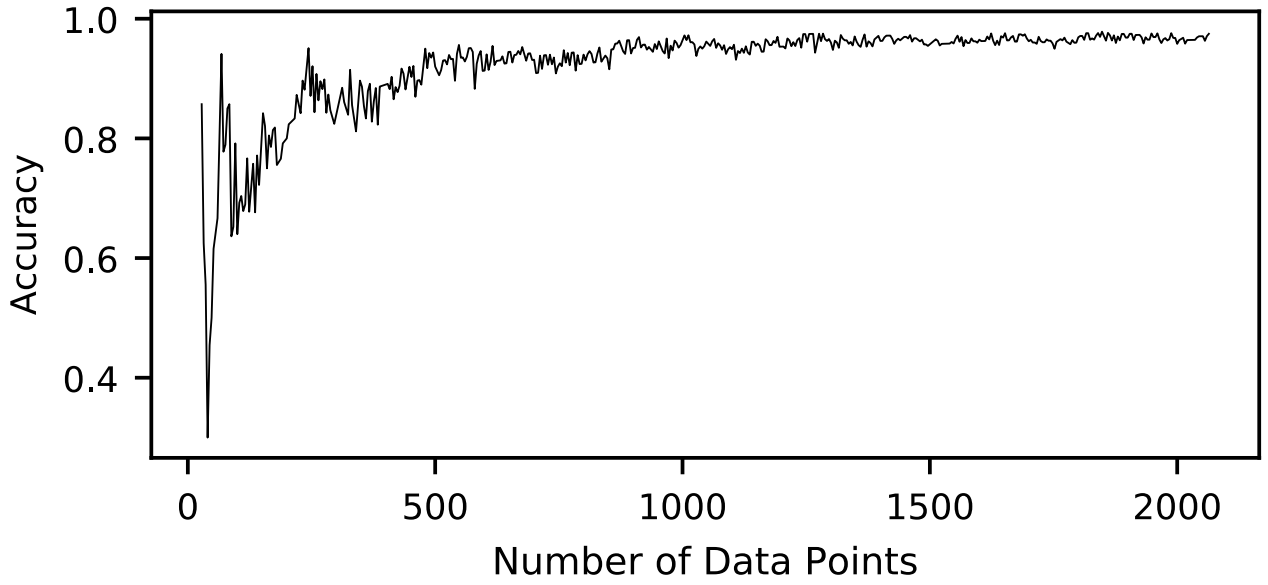
Machine learning algorithms performance



Accuracy of KNN, RF, and LK-SVM for SIOTLAB dataset, UNSW's dataset, and a combination of both datasets improves with increase in polling interval

Result and Discussion

Optimal polling interval



For combined dataset KNN shows 95% accuracy for 1820 data points, meeting the low memory requirement for IoT devices with high accuracy

Result and Discussion

Comparison with existing work

Existing work	Accuracy	Detection type	Dataset	Storage	Latency	Feature Count
[1]	97.5%	DDoS	UNSW	Yes	Yes	30
[2]	91.2%	Classification	Tor & Custom	No	Yes	6
[3]	96.37%	Classification	3 dataset	No	No	87
[4]	87.8%	Classification	Custom	No	Yes	15
[5]	99.8	DDoS	KD99	No	No	41
[6]	99.8%	DDoS	Custom	No	No	11
Proposed	99.9%	Classification & DDoS	Custom & UNSW	Yes	Yes	6

References

[1] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman, "Detecting volumetric attacks on IoT devices via sdn-based monitoring of mud activity," *in Proceedings of the 2019 ACM Symposium on SDN Research , 2019, pp. 36–48.*

[2] A. I. Owusu and A. Nayak, "An intelligent traffic classification in sdn-iot: A machine learning approach," *in 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom),2020, pp. 1–6.*

[3] M. Reza, M. J. Sobouti, S. Raouf, and R. Javidan, "Network traffic classification using machine learning techniques over software defined networks," *International Journal of Advanced Computer Science and Applications , vol. 8, 01 2017.*

[4] J. Xu, J. Wang, Q. Qi, H. Sun, and B. He, "Deep neural networks for application awareness in sdn-based network," *in 2018 IEEE 28th International Workshop on Machine Learning for Signal Processing (MLSP) , 2018, pp. 1–6.*

[5] L. Yang and H. Zhao, "Ddos attack identification and defense using sdn based on machine learning method," *in 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN) , 2018, pp. 174–178.*

[6] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," *pp. 29–35, 2018*

Thank you!

Q & A