Passive Activity Classification of Smart Home Assistants

Kwon Nung Choi
309252806
Master of Philosophy

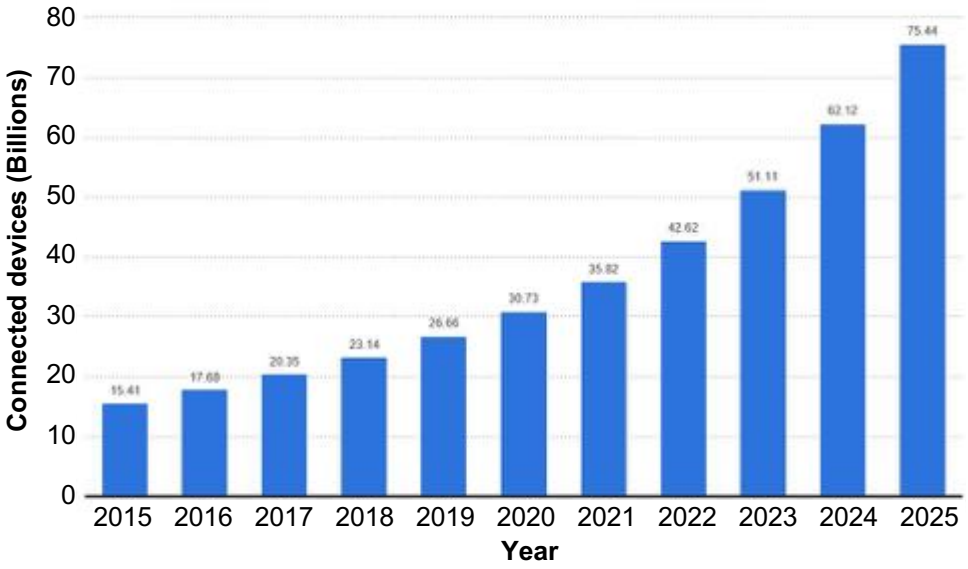
Supervisor
Dr. Kanchana Thilakarathna

Introduction

- Internet of Things (IoT) are growing in popularity
  - Active IoTs numbering 26.66 billion in 2019
  - Projected to reach 75 billion by 2025

- IoT has revolutionised smart home technology
  - Voice assistants have become an increasing necessity for seamless control of diverse IoTs

- Vast majority of smart home IoT devices are WiFi based



(Source: Forbes, 2017)

Motivation

- Home WiFi networks are secure, but…
  - Information are leaked through side-channels
  - Can passively sniff WiFi traffic using wireless capture devices

    e.g. AirPcap

Literature Review

Personal Information

- Infer information about illnesses, medications, family income, and investment details
  - ✓ Passive observation of WiFi frames
  - ✗ Must be on the network layer

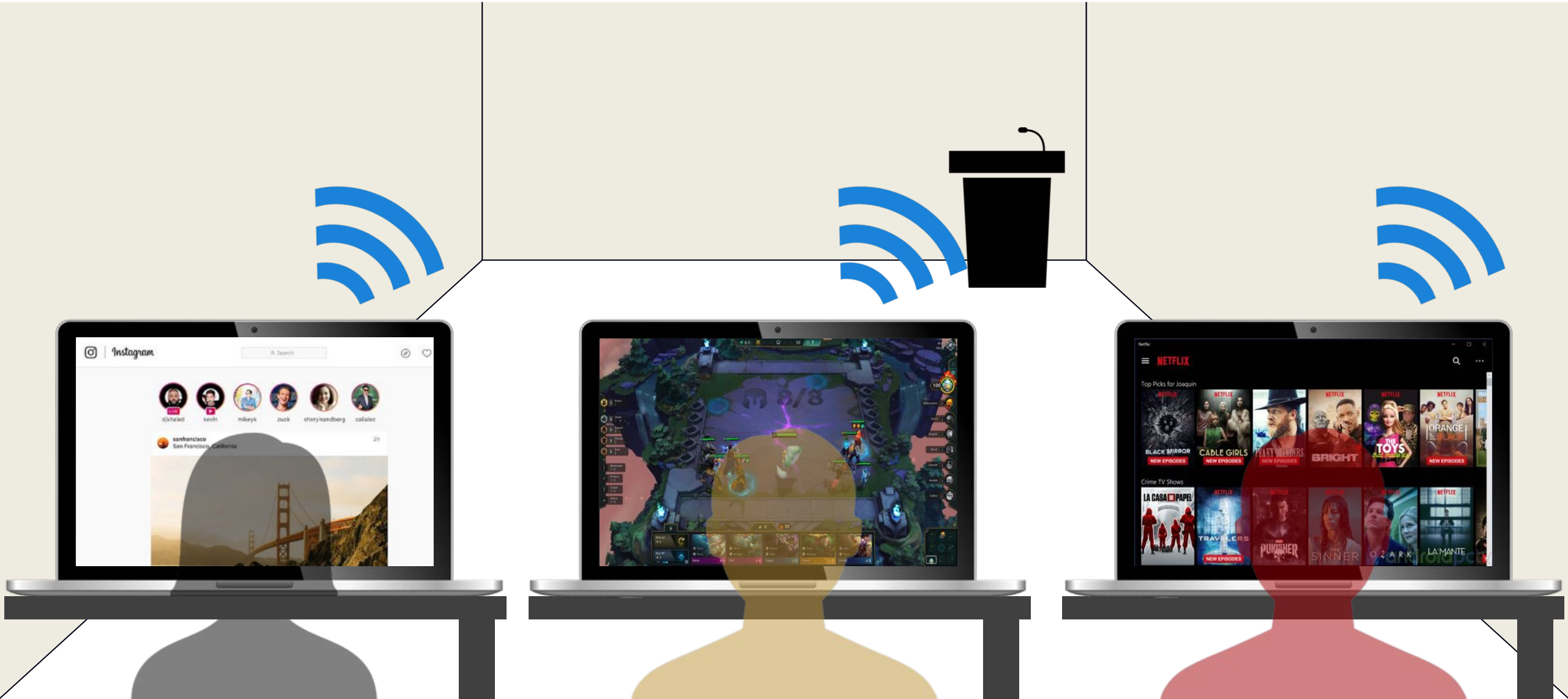
Content Information

- Identify which video is being streamed by a Youtube user
  - ✓ Fingerprinting passive WiFi traffic
  - ✗ Must be on the network layer

Device Information

- Identify IoT devices and IoT activities
  - ✓ Passive observation of WiFi frames
  - ✓ Even when end-to-end encryption is used
  - ✗ Can only tell whether active or not, rather than identifying activity type

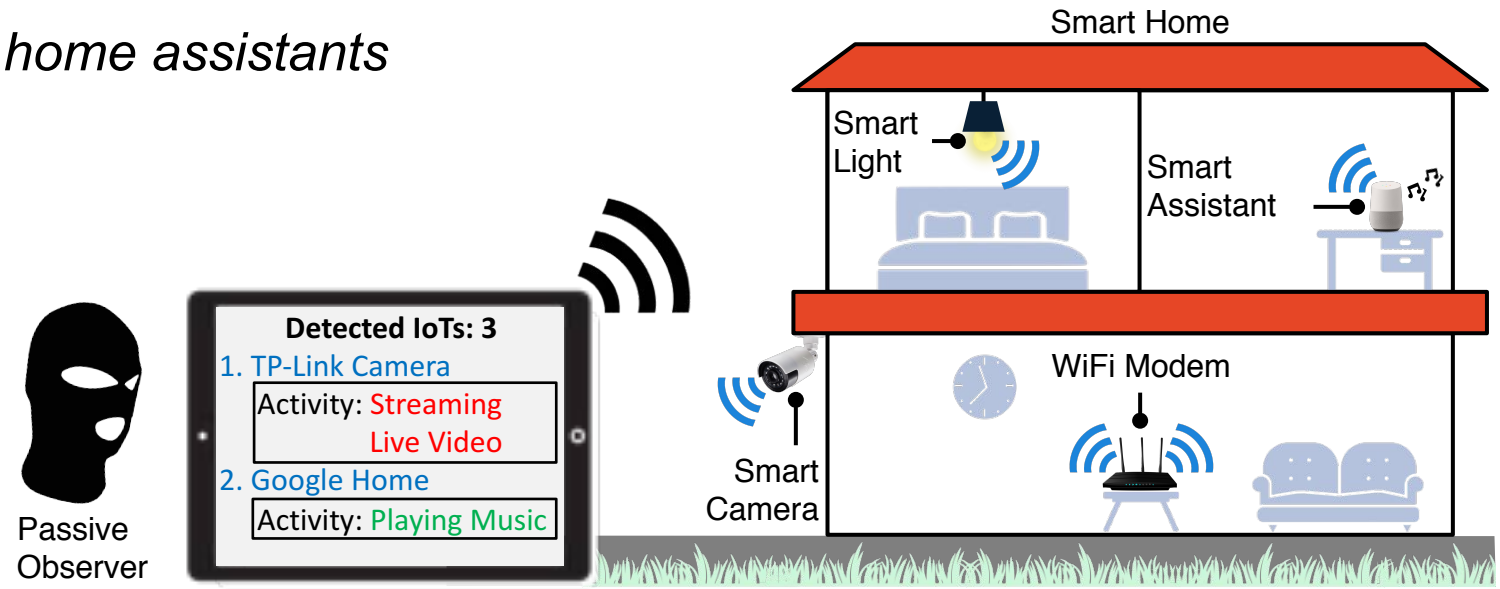
Literature Review



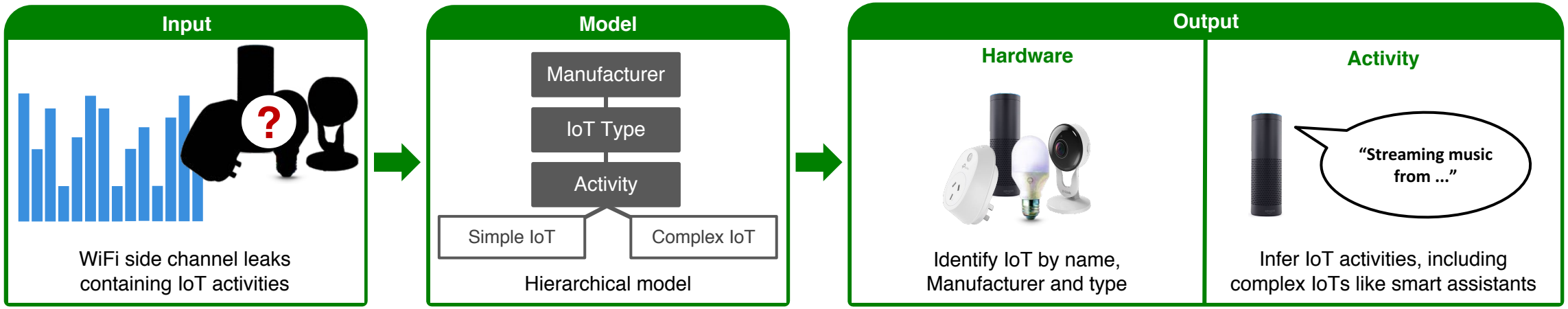
Research Objective

Without being on the network layer…

- Identify IoT devices
- Identify device-human interaction types
  - Simple IoT sensors *e.g. air quality sensor*
  - Complex IoT devices *e.g. smart home assistants*



Research Method



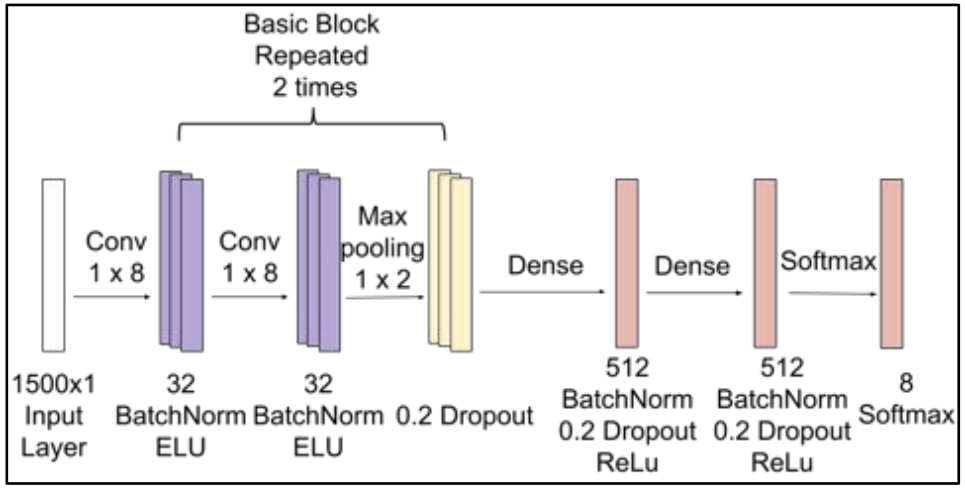
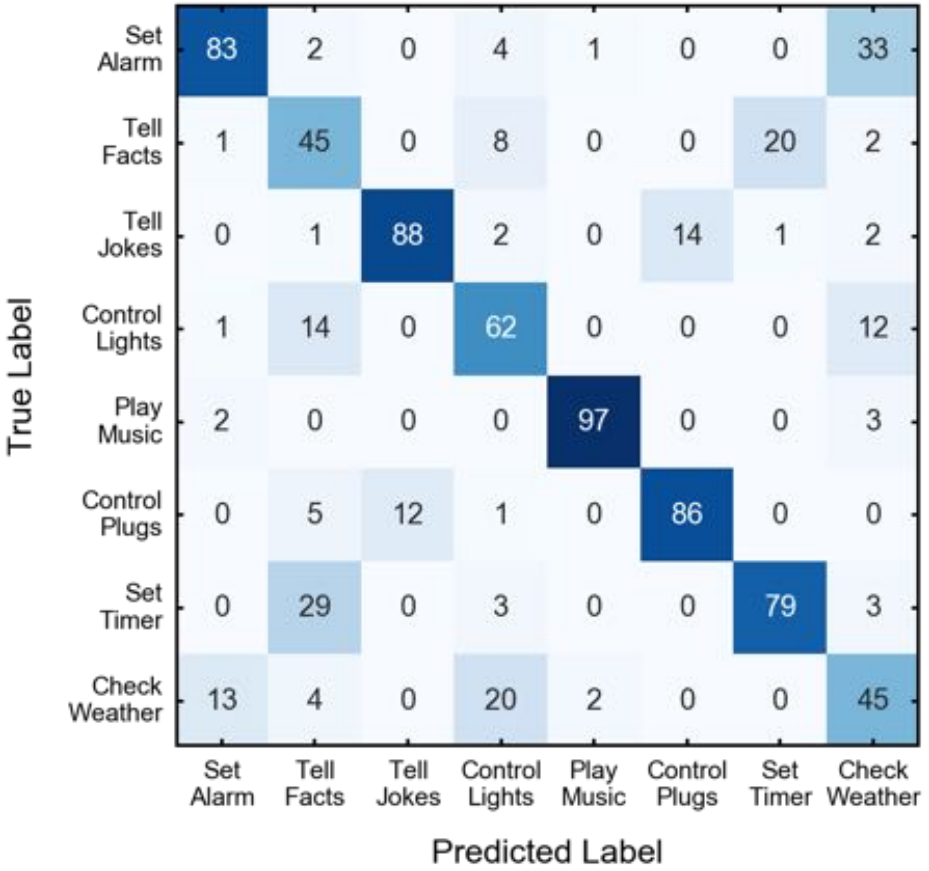


Figure: CNN-based classifier

Results

- All IoT devices correctly identified in terms of model and manufacturer name
- Mean activity classification accuracy of 73.2%
  - Activities like streaming music that have distinctly large frame size and frequency are easier to classify
  - Activities involving simple Internet queries are more difficult due to having patterns similar to local query reliant tasks that do not require communication over the Internet e.g. Setting an alarm



Conclusion & Future Work

- Demonstrated efficacy of classifying IoT devices and their activities
- Increase the classifier generalizability
  - Collect data from multiple locations, under different networks and in different time frames
- Investigate inference capability limits under considerable packet loss

Thank you for listening