Zigbee Dataset for Smart Home and Security Analysis

Eric Song, Merivale High School
Xiaodong Lin, Prof. IEEE Fellow, University of Guelph

Abstract

This project aims to generate smart home IoT datasets (especially Zigbee traffic data) in order to support research on smart home IoT network and device profiling, behaviour modelling, characterization, and security analysis. The Zigbee traffic data is captured in a real house with two Zigbee networks containing over 25 Zigbee devices which monitor the daily activities inside the house. The captured Ethernet traffic data from Home Assistant also contains the status data of several non-Zigbee IoT devices such as printers, a smart thermostat, and entertainment devices. The smart home is built with a Raspberry Pi and Home Assistant. The data collection, as well as the attacks, were done with the help of Wireshark, Killerbee, and ApiMote v4 Beta.

Smart Home and Zigbee network

Two Zigbee networks are set up in the house. They are called “Home Assistant Zigbee Network” and “XiaoMi Zigbee Network”:

Home Assistant Zigbee Network (Running on Raspberry Pi):

Gateway:

SONOFF Zigbee USB dongle, NWK: 0x0000
PAN ID: 0x34b6

Zigbee Nodes:

Door open/close sensor: first floor front hallway door; NWK: 0x2c30
Door open/close sensor: first floor back door; NWK: 0x4482
Door open/close sensor: first floor office; NWK:0x7c90
Door open/close sensor: second floor office; NWK:0x6087
Motion sensor: basement; NWK:0x3a47
Motion sensor: first floor family room; NWK:0x3008
Motion sensor: first floor living room; NWK:0x0c58
Motion sensor: basement movie room; NWK:0x0f71
Motion sensor: first floor office; NWK:0x0b33
Power outlet with light: first floor family room; NWK:0x8d81
Power outlet with light: first floor living room; NWK:0x9f09
Power outlet with dehumidifier: basement; NWK:0x88bf
Neo alarm: basement; NWK:0xc05a

Automation:

- Family room light control: The family room motion sensor controls the family room power outlet which powers a light. The light turns on when motion in the family room is detected, and turns off when no motion is detected from 8:30 pm to 5:00 am.
- Living room light control: The living room motion sensor controls the living room power outlet which powers a light. The light turns on when motion in the living room is detected, and turns off when no motion is detected from 8:30 pm to 5:00 am.

- Dehumidifier control: The measured humidity level from MyEcobee controls the basement power outlet which powers a dehumidifier. Humidity above 55% triggers the dehumidifier to turn on and humidity below 50% triggers the dehumidifier to turn off.
- Alarm control: A Neo alarm is triggered when the basement front and back windows are opened.

XiaoMi Zigbee Network:

Gateway:

XiaoMi Zigbee Gateway: 0x0000
PAN ID: 0x2d89

Zigbee Nodes:

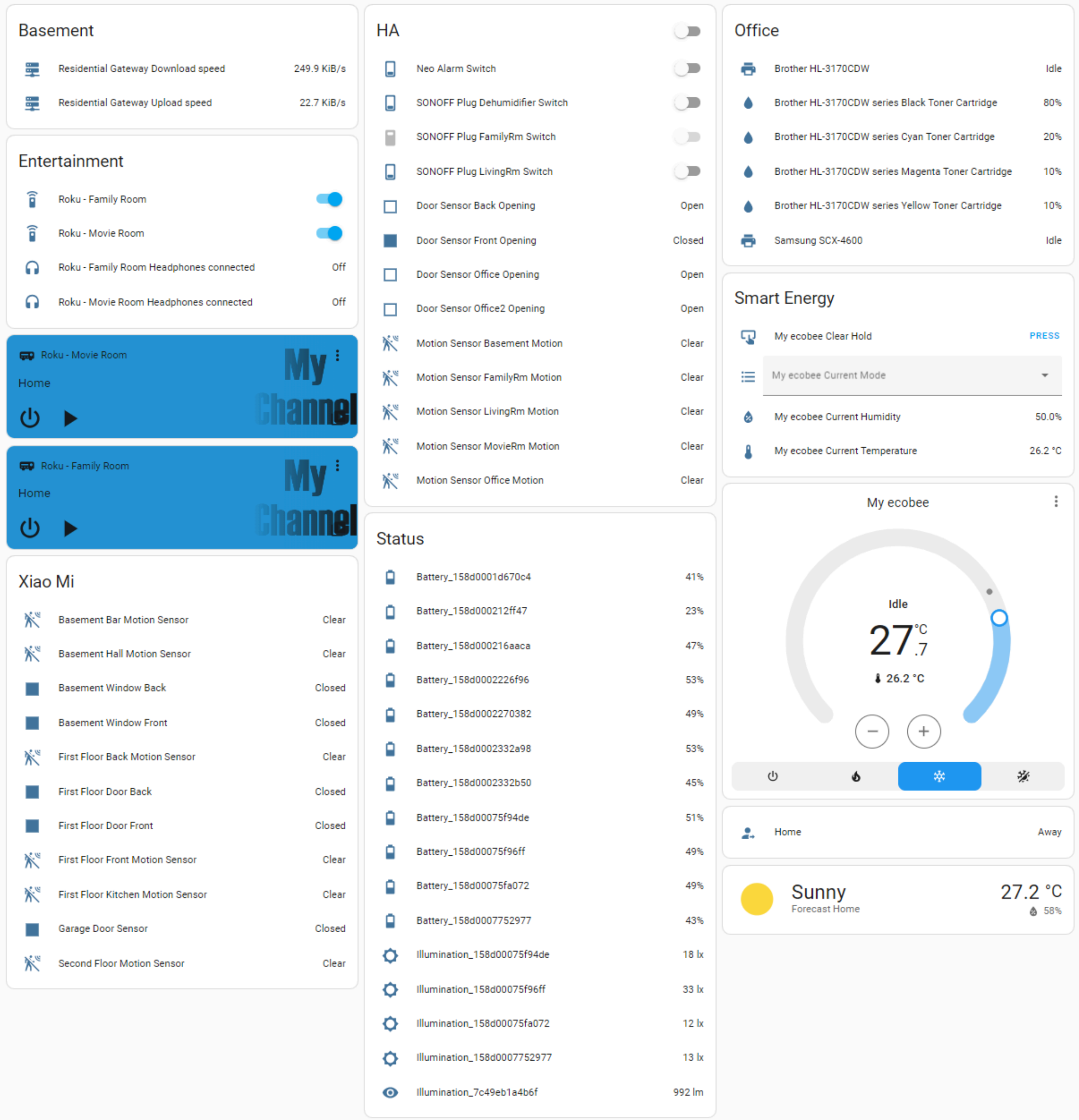
Door open/close sensor: first floor front door; NWK: 0x0b95
Door open/close sensor: first floor back door; NWK:0x4219
Door open/close sensor: garage door; NWK:0x61af
Door open/close sensor: basement front window; NWK:0x8d41
Door open/close sensor: basement back window; NWK:0x0cf0
Motion sensor: basement bar; NWK:0x71e3
Motion sensor: basement centre; NWK:0x0c4a
Motion sensor: first floor front; NWK:0xbbd9
Motion sensor: first floor back; NWK:0x566a
Motion sensor: first floor kitchen; NWK:0x44ac
Motion sensor: second floor hallway; NWK:0x853b

Automation:

- Night light control: The second floor hallway motion sensor controls the night light integrated to the Mi gateway. The night light turns on when motion in the hall is detected, and turns off after three minutes of inactivity from 8:30 pm to 5:00 am.
- Alarm control: Once the Mi gateway is alarmed, all motion and door sensors will trigger an alarm.

Home Assistant Integration:

In addition to the XiaoMi Zigbee network, several other IoT devices such as Brother and Samsung printers, the Ecobee smart thermostat, and Roku entertainment devices are integrated into Home Assistant as shown in Figure 1.



Basement

Residential Gateway Download speed	249.9 KiB/s
Residential Gateway Upload speed	22.7 KiB/s

Entertainment

Roku - Family Room	
Roku - Movie Room	
Roku - Family Room Headphones connected	Off
Roku - Movie Room Headphones connected	Off

Roku - Movie Room
Home

Roku - Family Room
Home

Xiao Mi

Basement Bar Motion Sensor	Clear
Basement Hall Motion Sensor	Clear
Basement Window Back	Closed
Basement Window Front	Closed
First Floor Back Motion Sensor	Clear
First Floor Door Back	Closed
First Floor Door Front	Closed
First Floor Front Motion Sensor	Clear
First Floor Kitchen Motion Sensor	Clear
Garage Door Sensor	Closed
Second Floor Motion Sensor	Clear

HA

Neo Alarm Switch	
SONOFF Plug Dehumidifier Switch	
SONOFF Plug FamilyRm Switch	
SONOFF Plug LivingRm Switch	
Door Sensor Back Opening	Open
Door Sensor Front Opening	Closed
Door Sensor Office Opening	Open
Door Sensor Office2 Opening	Open
Motion Sensor Basement Motion	Clear
Motion Sensor FamilyRm Motion	Clear
Motion Sensor LivingRm Motion	Clear
Motion Sensor MovieRm Motion	Clear
Motion Sensor Office Motion	Clear

Status

Battery_158d0001d670c4	41%
Battery_158d000212ff47	23%
Battery_158d000216aaca	47%
Battery_158d0002226f96	53%
Battery_158d0002270382	49%
Battery_158d0002332a98	53%
Battery_158d0002332b50	45%
Battery_158d00075f94de	51%
Battery_158d00075f96ff	49%
Battery_158d00075fa072	49%
Battery_158d0007752977	43%
Illumination_158d00075f94de	18 lx
Illumination_158d00075f96ff	33 lx
Illumination_158d00075fa072	12 lx
Illumination_158d0007752977	13 lx
Illumination_7c49eb1a4b6f	992 lm

Office

Brother HL-3170CDW	Idle
Brother HL-3170CDW series Black Toner Cartridge	80%
Brother HL-3170CDW series Cyan Toner Cartridge	20%
Brother HL-3170CDW series Magenta Toner Cartridge	10%
Brother HL-3170CDW series Yellow Toner Cartridge	10%
Samsung SCX-4600	Idle

Smart Energy

My ecobee Clear Hold	PRESS
My ecobee Current Mode	
My ecobee Current Humidity	50.0%
My ecobee Current Temperature	26.2 °C

My ecobee

Idle
27.7 °C
26.2 °C

Home	Away

Sunny 27.2 °C
Forecast Home 58%

Figure 1. IoT devices integrated into Home Assistant.

The IP address related to IoT devices shown in Figure 1 is listed below:

Table 1. List of IoT Devices with IP address

IoT Device	IP Address
Samsung SCS-4600 printer	192.168.1.113

Brother HL-3170CDW printer	192.168.1.152
My ecobee thermostat	192.168.1.86
Raspberry Pi	192.168.1.84
Roku - Family Room	192.168.1.131
Roku - Movie Room	192.168.1.124

Instructions

Data collection points are shown in Figure 2, where the Zigbee sniffer uses Wireshark, Killerbee, and ApiMote v4 Beta:

- Home Assistant Zigbee network sniffer: Zigbee channel 15
- XiaoMi Zigbee network sniffer: Zigbee channel 25
- Ethernet Packet sniffer

A Zigbee replay attack is performed with Killerbee and ApiMote v4 Beta on Zigbee channel 15.

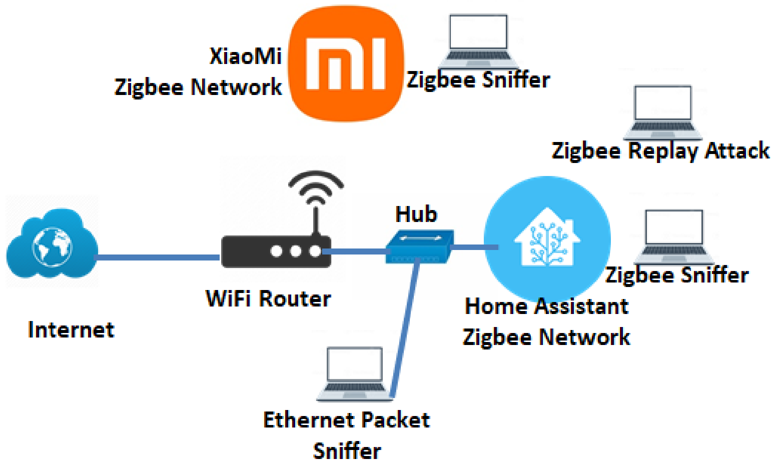


Figure 2. IoT network traffic collection points.

The dataset contains four parts:

- Home Assistant Zigbee network traffic: on Zigbee channel 15 with PAN ID 0x34b6, containing 25 days Zigbee traffic;
- XiaoMi Zigbee network traffic: on Zigbee channel 25 with PAN ID 0x2d89, containing 25 days Zigbee traffic;

- Zigbee replay attack: this dataset contains the replay source pcap file, the sniffed pcap file, and the Ethernet pcap file on Home Assistant, all of which are on Zigbee Channel 15 and collected during the replay attack;
- IoT Ethernet traffic: on Home Assistant, containing 25 days Ethernet IP traffic.

Ethical considerations: the owner and residents of the house have consented to both the collection and release of all data collected for the dataset for public research.