Internet of Things: Frameworks and resilience

John L. Manferdelli
johnmanferdelli@hotmail.com

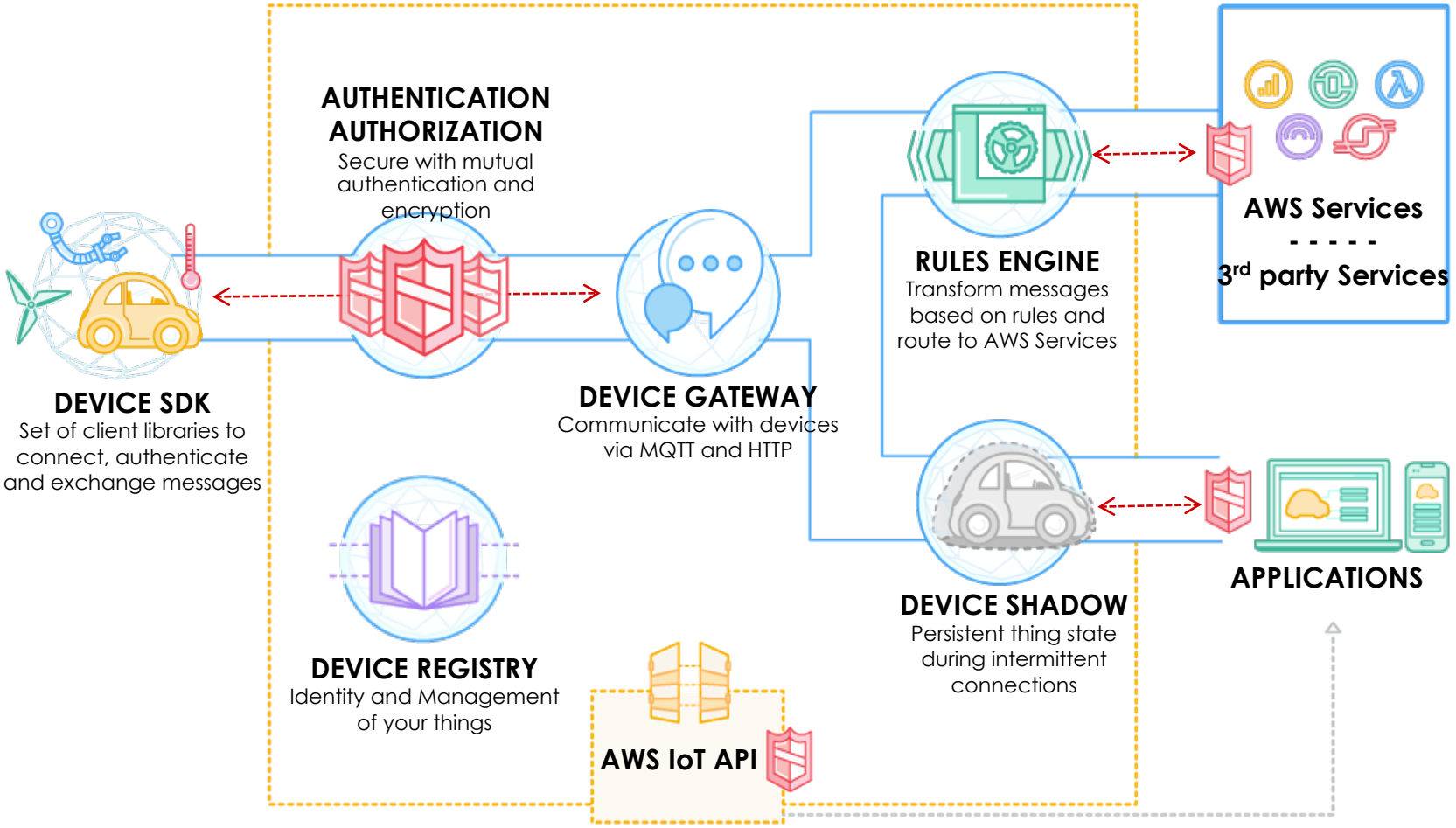
April 6, 2020, 13:00

IoT Device Management

- Managing IoT
  - Provisioning
  - Updates
  - Surveillance and risk assessment
- Resilience a cost risk models
- Agility, diversity and replacement
- Supply chain risk and assessment
- Software and configuration assurance
- Privacy and situational awareness

Frameworks: AWS

AWS IoT


AUTHENTICATION
AUTHORIZATION
Secure with mutual authentication and encryption
DEVICE SDK
Set of client libraries to connect, authenticate and exchange messages
DEVICE GATEWAY
Communicate with devices via MQTT and HTTP
RULES ENGINE
Transform messages based on rules and route to AWS Services
AWS Services
- - - - -
3rd party Services
DEVICE SHADOW
Persistent thing state during intermittent connections
APPLICATIONS
DEVICE REGISTRY
Identity and Management of your things
AWS IoT API

AWS IoT Components

- **Message broker**
  - A secure relay between users (subscribers and publishers)
  - Protocols: MQTT, HTTP REST interface
- **Rules engine**
  - Rules directing data to other AWS services such as Amazon S3, Amazon DynamoDB, and AWS Lambda
- **Thing Registry** (Device Registry)
  - Virtual devices in the cloud, corresponding to physical things
  - Up to three custom attributes for a thing.
  - Association of certificates and MQTT client IDs with a thing

Frameworks: Azure sphere

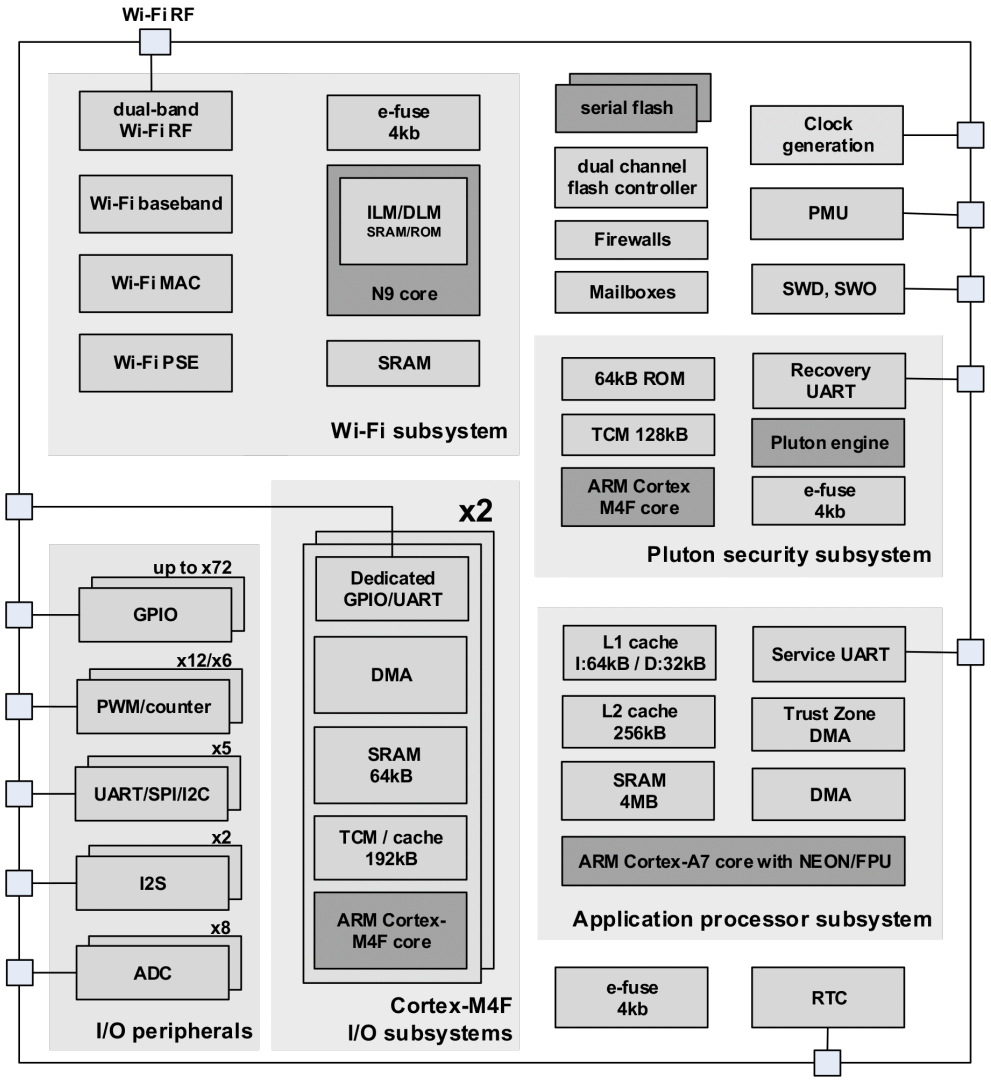
Azure Sphere Introduction

- Microsoft description is here.
- Basic concepts
  - Azure cloud backend service: data collection, device health
  - Authenticated boot
  - Update process
  - Managed exclusion

MT3620

- MT3620 development board is first implementation. Documentation is here.
  - ARM Cortex A7 core @500MHz , 4MB RAM
  - ARM Cortex M4 core @200MHz , 64KB RAM with FPU
  - ADC, I2S, and PWM peripheral interfaces (GPIO, I2C [1MHz], SPI [40MHz] and UART [3Mbps])
  - Wi-Fi 802.11a/b/g/n
  - RTC with clock selection and battery backup
  - Pluton Security system, hardware RNG
  - Visual Studio IDE, Windows required
  - Azure Sphere OS
    - Application containers compartmentalize code for agility, robustness, and security.
    - On-chip connectivity services secure your connection to the cloud and provide access to the Azure Sphere Security Service.
    - Custom Linux kernel.
    - A security monitor guards integrity and access to critical resources.

MT3620



- Some features not yet implemented in development environment.

IoT protocols

MQTT

- MQTT is a messaging broker system, documentation is here.
- Clients can publish (Pub) messages and subscribe (Sub) to topics.
  - Clients can both publish and subscribe.
  - A broker communicates with clients.

IoT Security design

Development, curation and test

- x

Configuration, software and boot

- x

Monitoring

- x

Redundancy

- x

Supply Chain

- x

Top ten vulnerabilities

1. Weak, guessable passwords (poor authentication)
2. Insecure network services (poor configuration/software)
3. Insecure APIs and service (poor software security)
4. Lack of update
5. Insecure, outdated components (hardware and software)
6. Poor privacy protection for data stored on devices
7. Insecure data storage and transfer
8. Lack of device management
9. Insecure default settings (poor configuration)
10. Lack of physical hardening (including physical security)

Refernce: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Todo

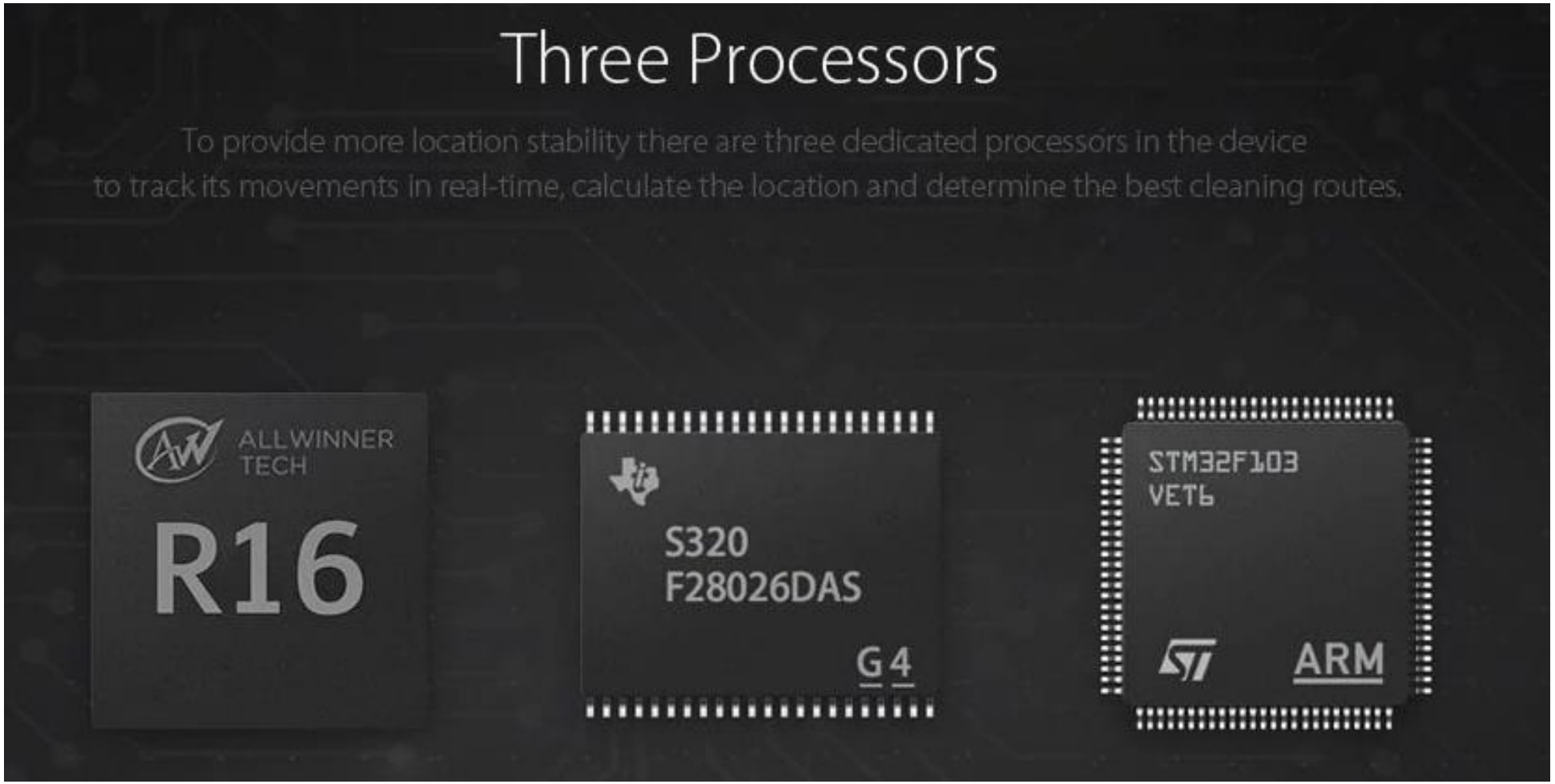
- Busybox
- REST/Json
- Mesh
- Contrast with industrial control

An IoT Lab

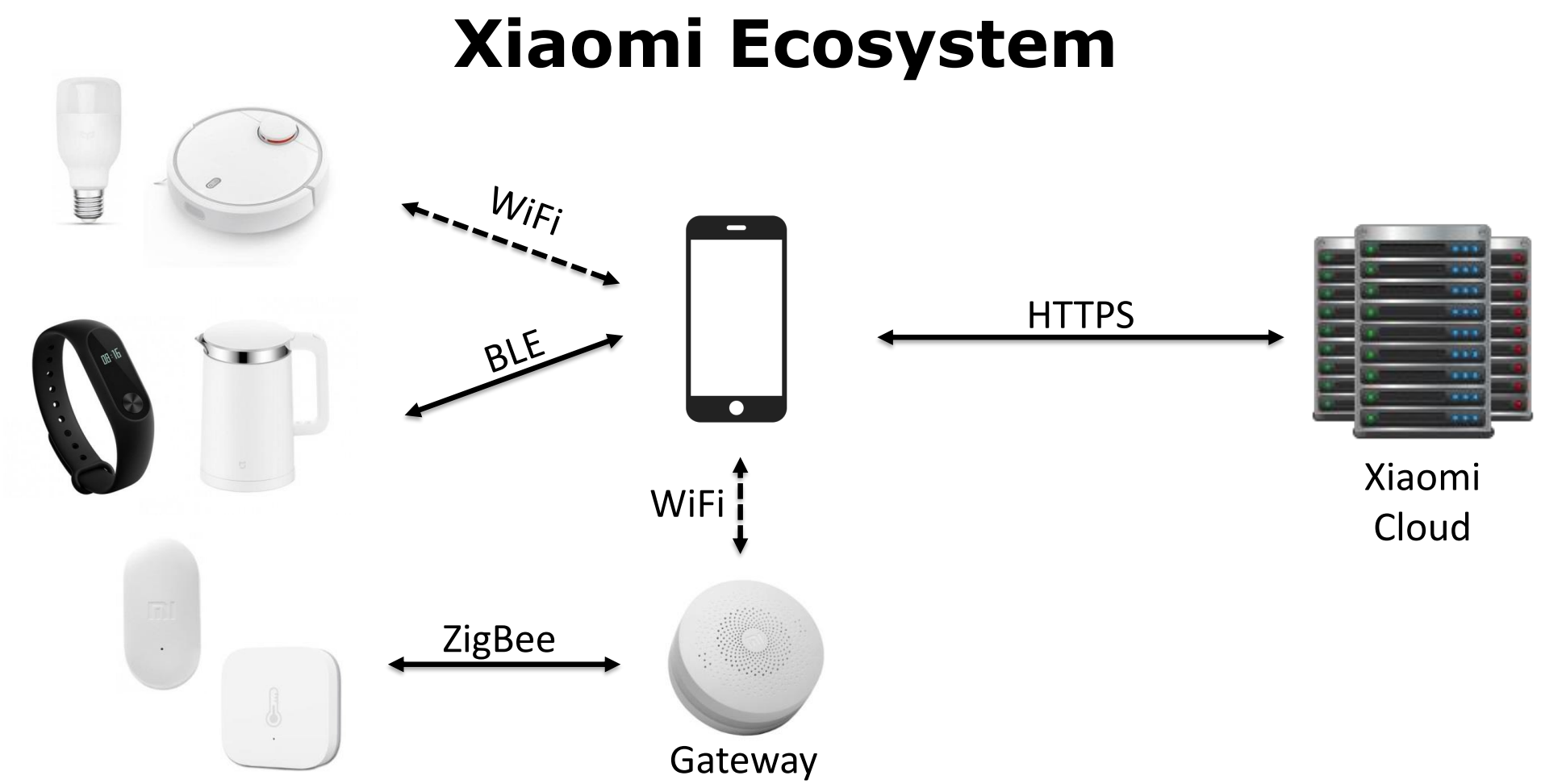
Typical IoT devices and their cost

- Vacuum Cleaning Robot Gen2: ~ 400$
- Smart Home Gateway: ~25$
- Sensors: ~5-14$
- Wifi-Lightbulbs: ~6-12$

Commercial processors



Typical ecosystem



App to cloud communication

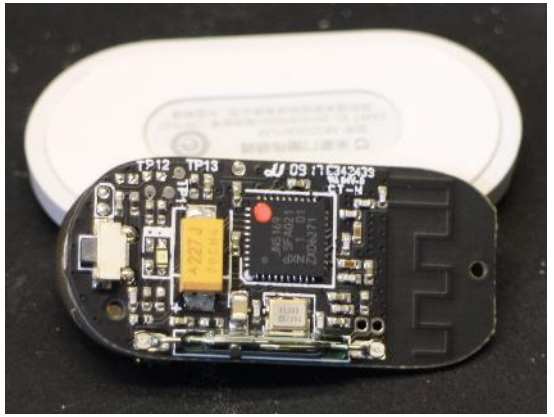
- REQ: api.io.mi.com/home/device_list method:POST params:[]
- RES: {"message":"ok","result":{"list":[{"did":"65981234","token":“a bc...zzz","name":"Mi PlugMini","localip":"192.168.99.123", "mac":"34:CE:00:AA:BB:CC","ssid":"IoT","bssid":"FA:1A:67:CC: DD:EE","model":"chuangmi.plug.m1", "longitude":“-71.0872248","latitude":"42.33794500“, "adminFlag":1,"shareFlag":0,"permitLevel":16,"isOnline":true, "desc":"Power plug on ","rssi":-47}

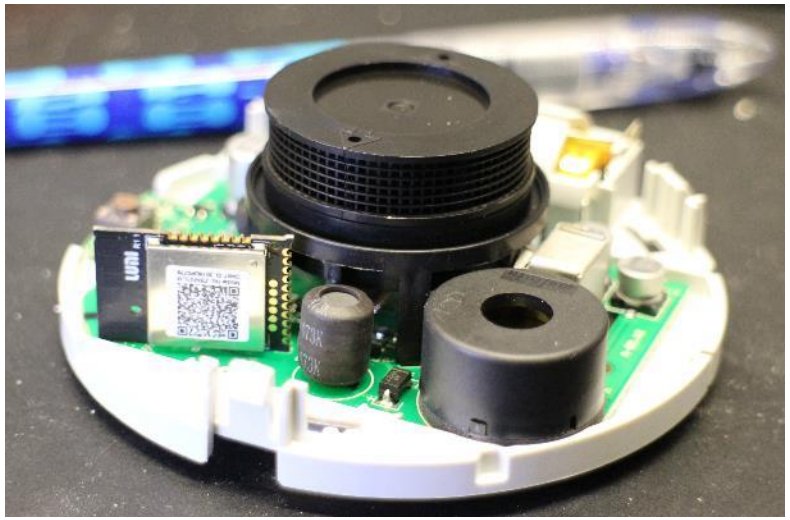
Nexmon patching

Sensors connected via gateway

Zigbee (NXP JN5169) based

- Door Sensor (Reed contact)
- Temperature sensor
- Power Plug
- Motion Sensor
- Button
- Smoke Detector
- Smart Door Lock

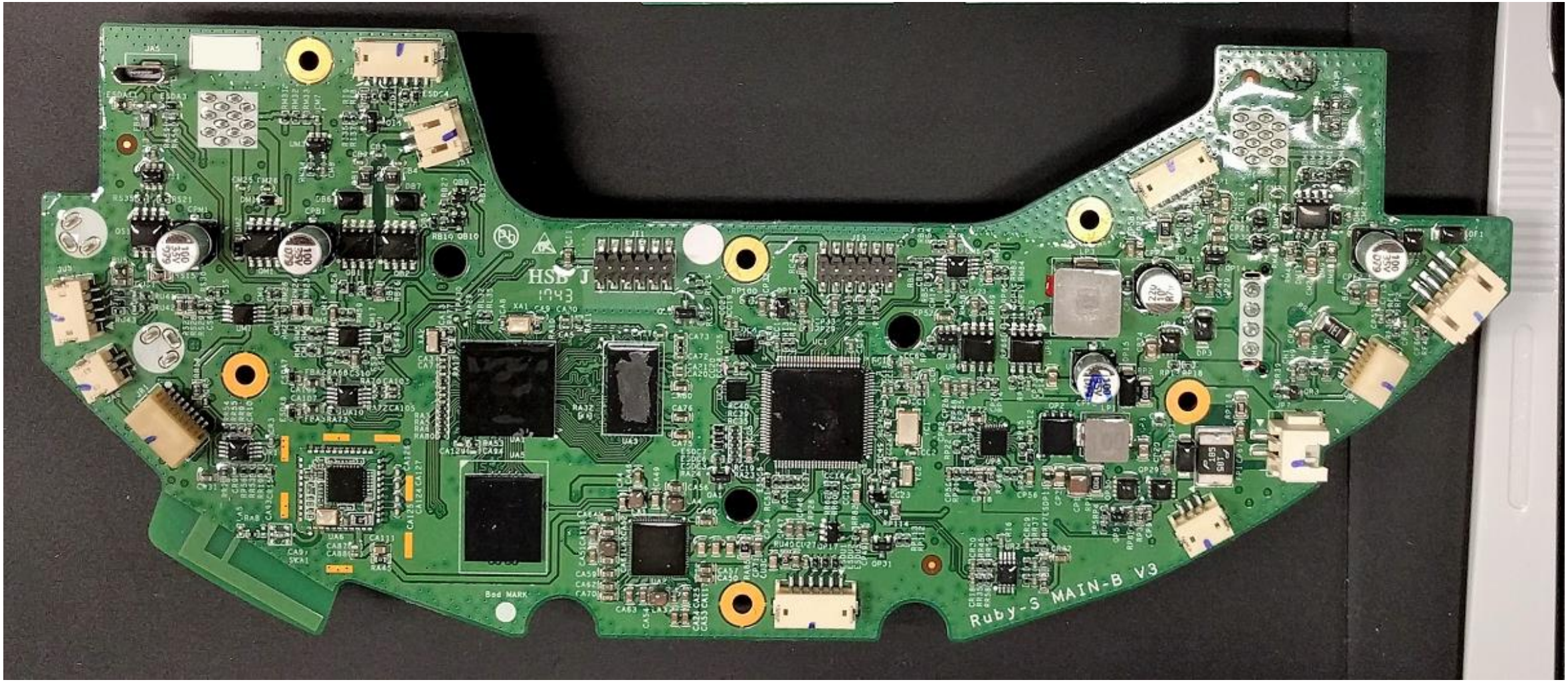




eMMc layout

Label	Content	Size in MByte
boot-res	bitmaps & some wav files	8
env	uboot cmd line	16
app	device.conf (DID, key, MAC), adb.conf, vinda	16
recovery	fallback copy of OS	512
system_a	copy of OS (active by default)	512
system_b	copy of OS (passive by default)	512
Download	temporary unpacked OS update	528
reserve	config + calibration files, blackbox.db	16
UDISK/Data	logs, maps, pcap files	~1900

Xiaomi vacuum



Xiaomi vacuum