
UNLEASH YOUR SMARTHOME DEVICES: VACUUM CLEANING ROBOT HACKING

WHY IS MY VACUUM AS
POWERFUL AS MY SMARTPHONE

DENNIS GIESE AND DANIEL WEGEMER

Post presentation remarks 27.12. 21:00

- Rooting is now possible without opening the device
- Contact: dustcloud@1338-1.org

Why Xiaomi

“Xiaomi’s ‘Mi Ecosystem’ has 50 million connected devices” [1]

„[...] revenue from its smart hardware ecosystem exceeded 15 billion yuan” (1.9 billion €) [2]

Most important: **The stuff is cheap**


[1] <https://techcrunch.com/2017/01/11/xiaomi-2016-to-2017/>

[2] <https://www.reuters.com/article/us-xiaomi-outlook/chinas-xiaomi-targets-2017-sales-of-14-5-billion-after-2016-overhaul-idUSKBN14W0LZ>

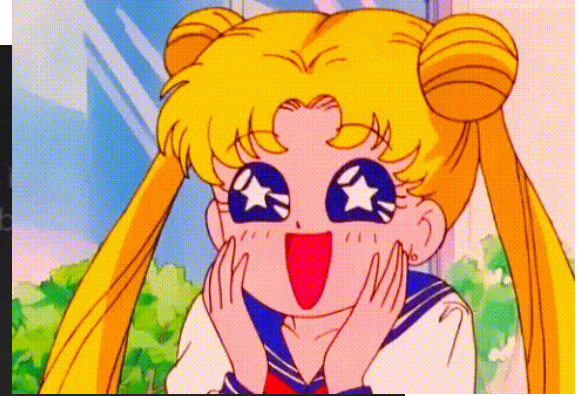
Why Vacuum Robots?

Three Processors

To provide more location stability there are three dedicated processors to track its movements in real-time, calculate the location and determine the b

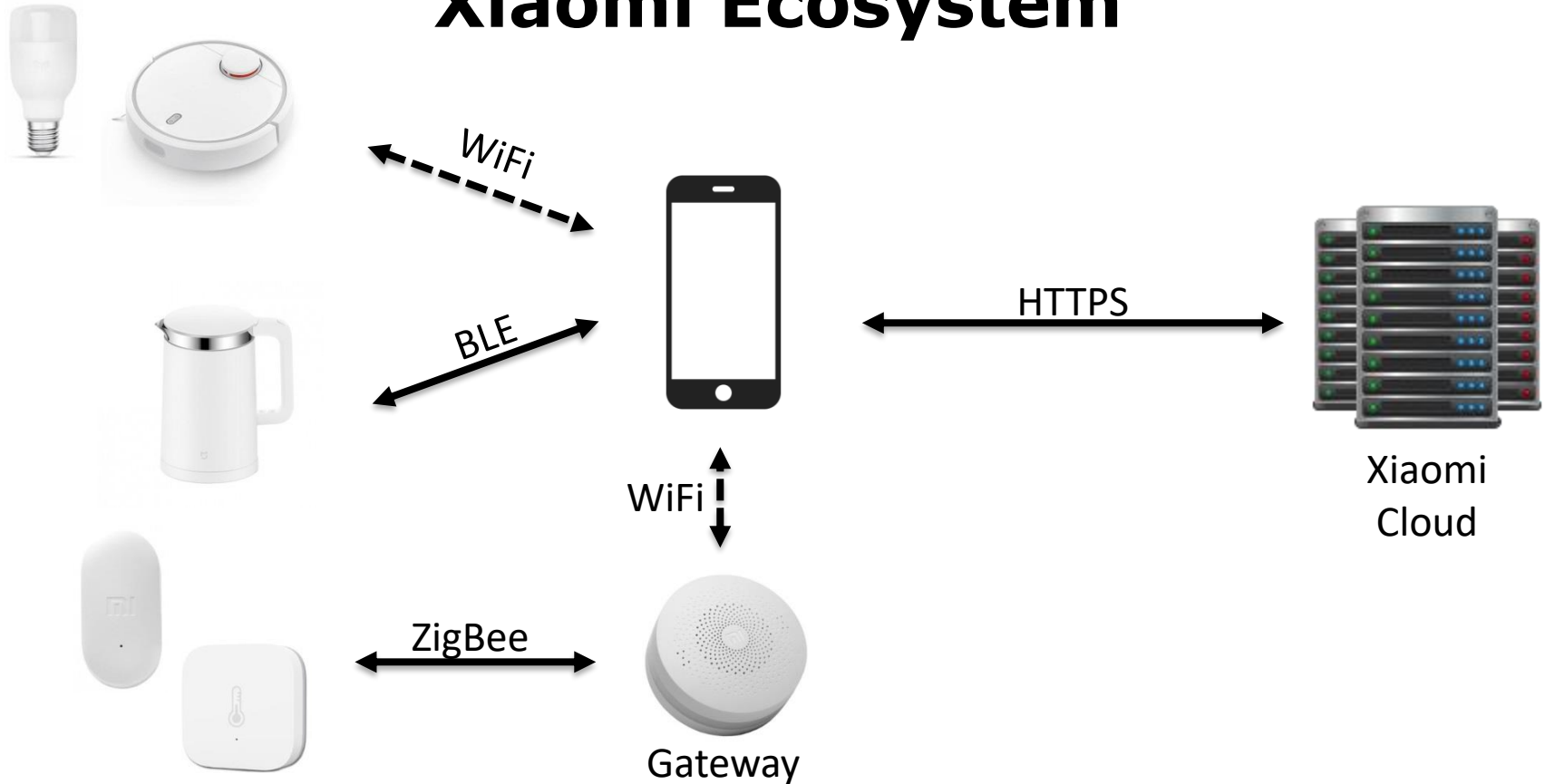


The image displays three microprocessors against a dark background with circuit patterns. On the left is an Allwinner R16 processor with the 'AW' logo and 'ALLWINNER TECH' text. In the center is a Texas Instruments S320 F28026DAS processor with the 'ti' logo and 'G4' branding. On the right is an STMicroelectronics STM32F103 VET6 processor with the 'ST' logo and 'ARM' branding.

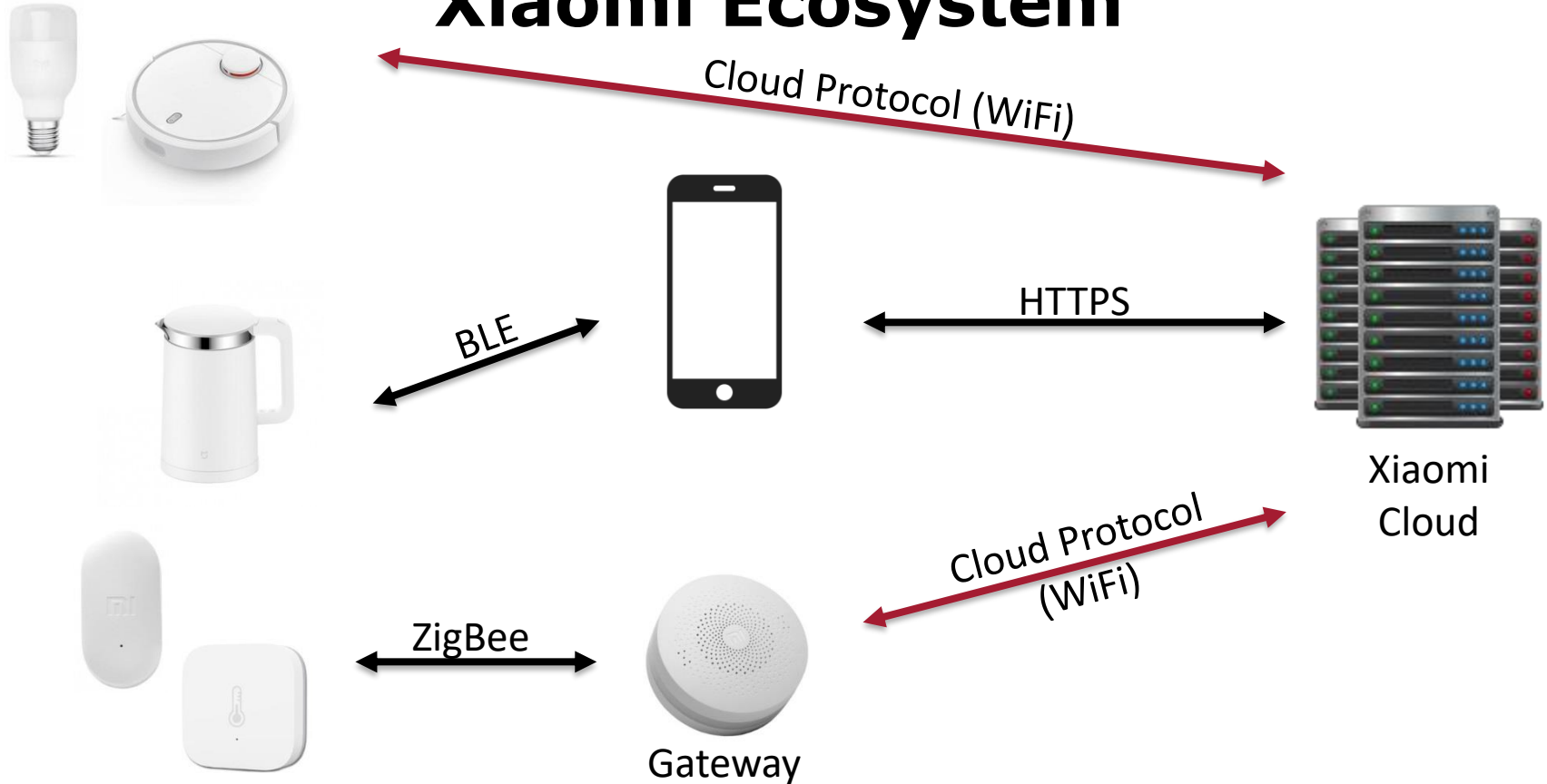


Source: Xiaomi advertisement

Xiaomi Ecosystem



Xiaomi Ecosystem



Device Overview



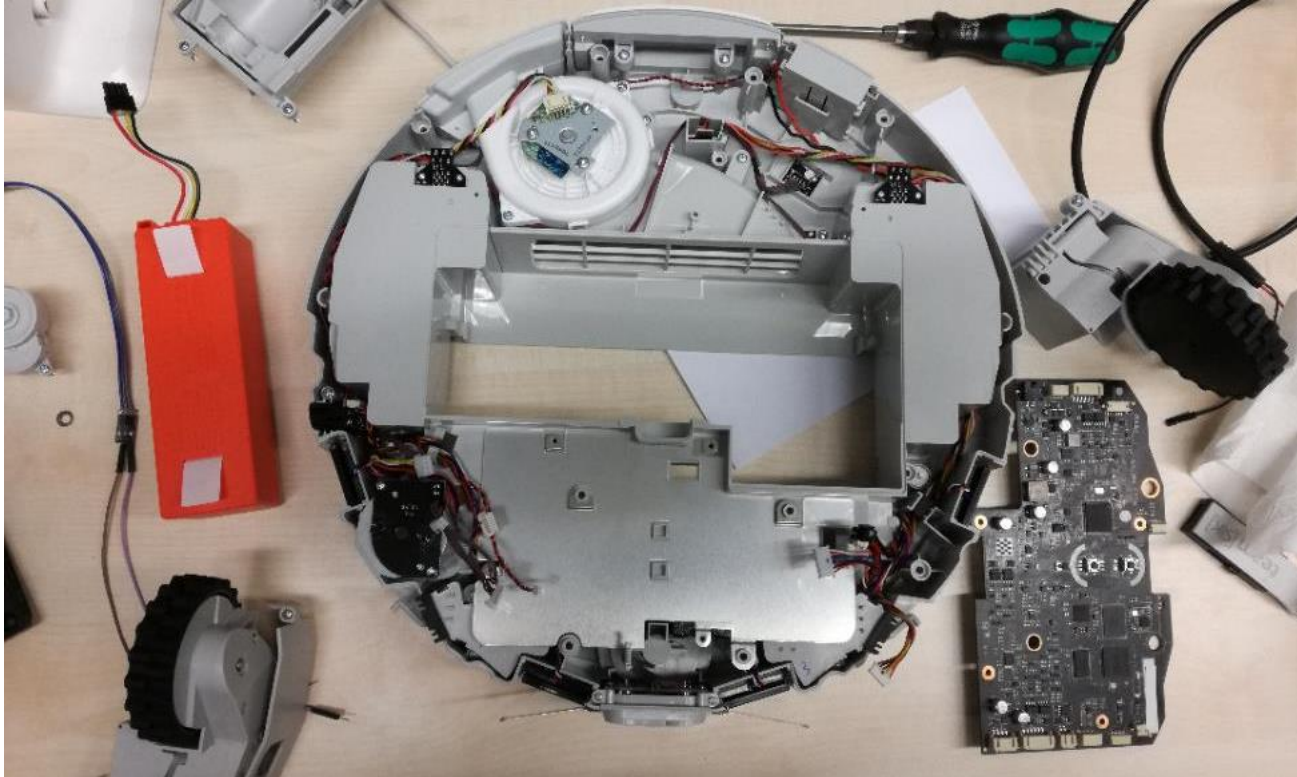
Source: Xiaomi advertisement

Rooting: Challenges

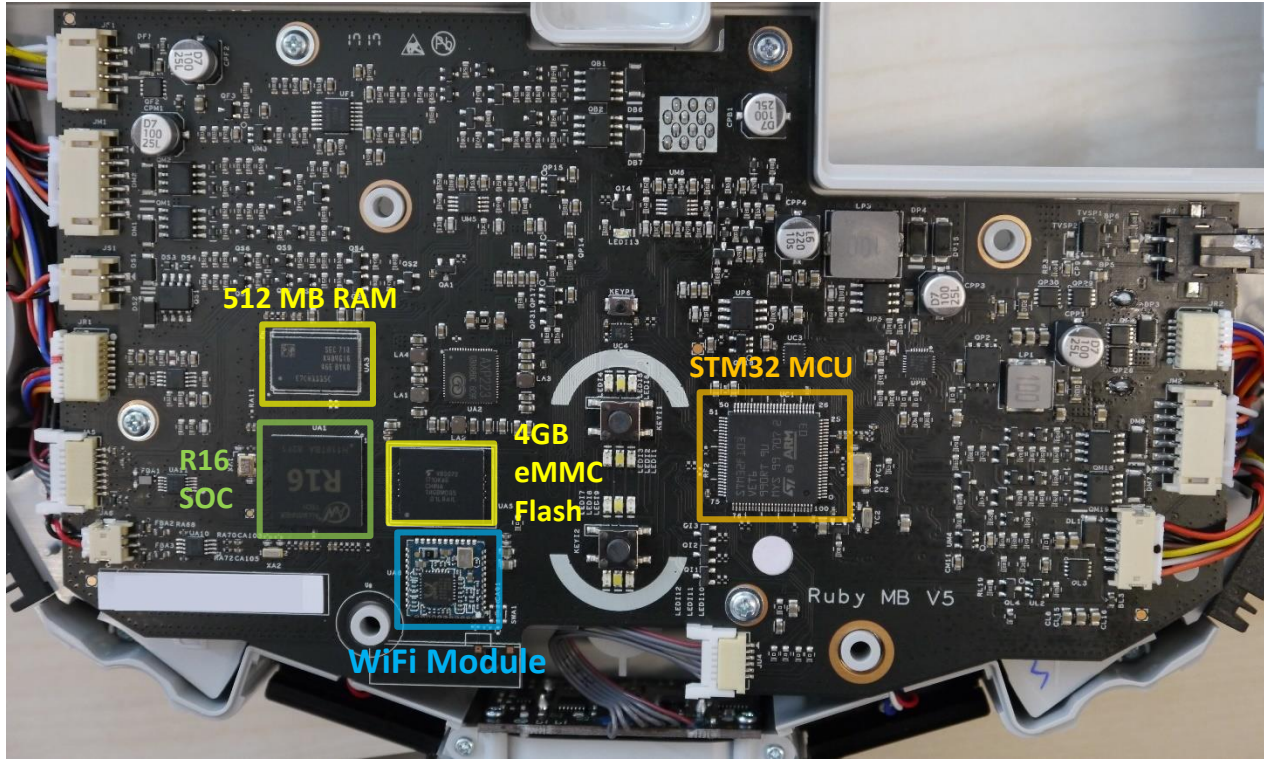
- Hardware Access
 - Micro USB Port ? **X**
 - Serial Connection on PCB ? **X**
- Network Based
 - Portscan ? **X**
 - Sniff Network traffic ? **X**



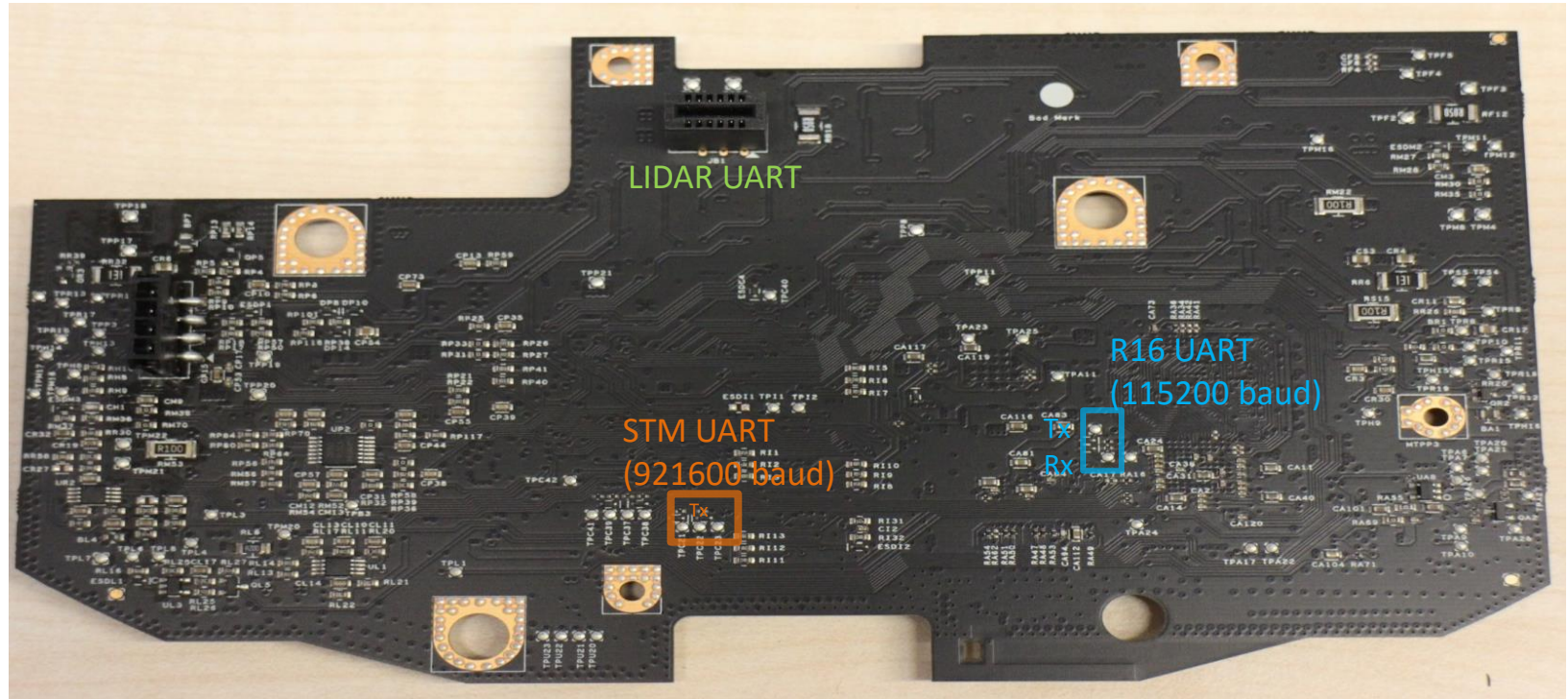
Teardown



Frontside layout mainboard



Backside layout mainboard



Rooting

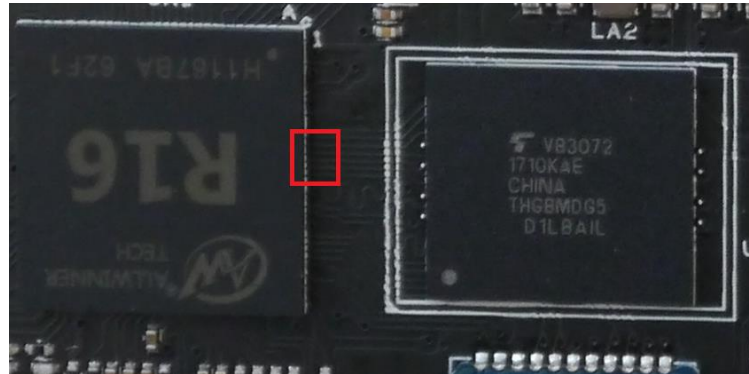
Our weapon of choice:



Rooting

Initial Idea:

- Shortcut the MMC data lines
- SoC falls back to FEL mode
- Load + Execute tool in RAM
 - via USB connector
 - Dump MMC flash
 - Modify image
 - Rewrite image to flash



Source: wikicommons

Software

- Ubuntu 14.04.3 LTS (Kernel 3.4.xxx)
 - Mostly untouched, patched on a regular base
- Player 3.10-svn
 - Open-Source Cross-platform robot device interface & server
- Xiaomi proprietary software (/opt/rockrobo)
 - AppProxy
 - RoboController
 - Miiio_Client
 - Custom addb-version
- iptables firewall enabled
 - Blocks Port 22 (SSHd) + Port 6665 (player)

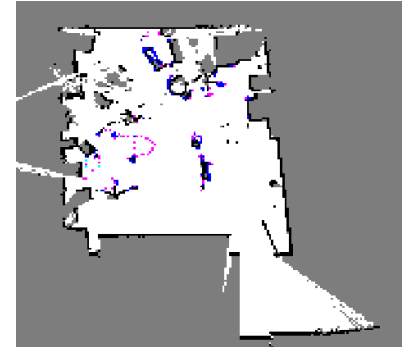
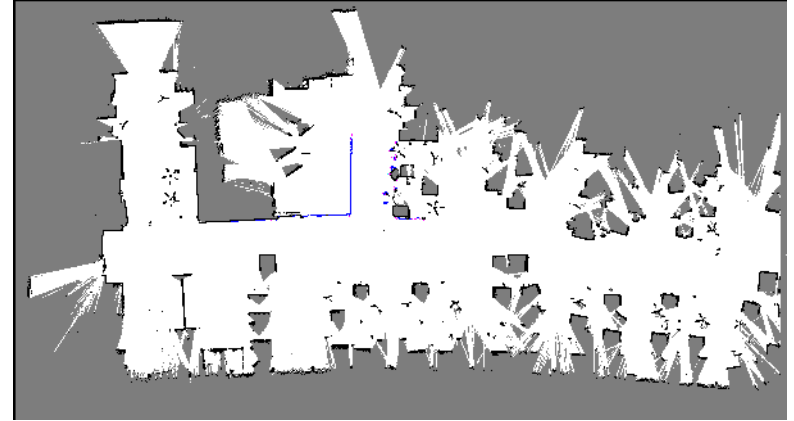


Available data on device

- Data
 - Logfiles (syslogs, duration, area, ssid, passwd)
 - “/usr/sbin/tcpdump -i any -s 0 -c 2000 -w”
 - Multiple MBytes/day
 - Maps
- Data is uploaded to cloud
- Factory reset
 - Restores recovery to system
 - does not delete data
 - Maps, Logs still exist

Available data on device

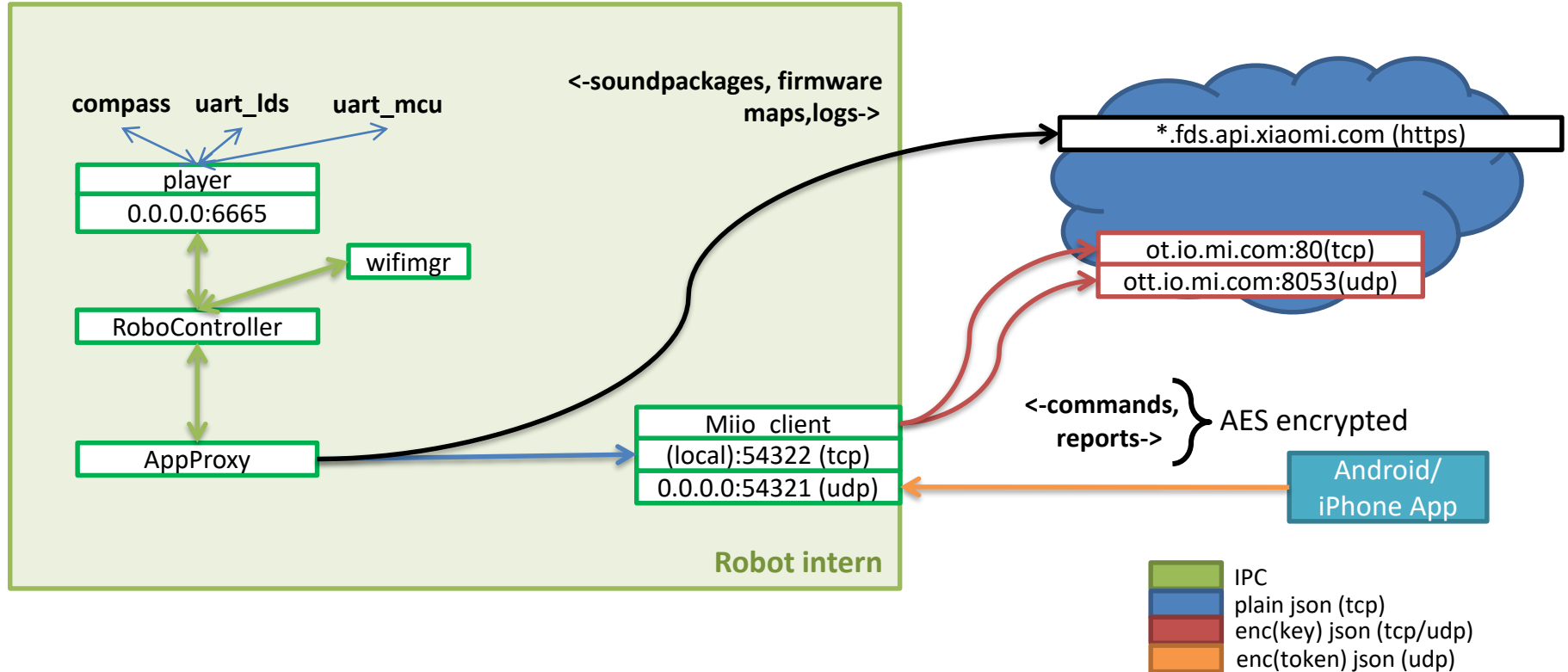
- Maps
 - Created by player
 - 1024px * 1024px
 - 1px = 5cm



Configurations

- DeviceID
 - Unique per device
- Keys
 - Cloudkey (16 byte alpha-numeric)
 - Is used for cloud communication
 - Static, is not changed by update or provisioning
 - Token (16 byte alpha-numeric)
 - Is used for app communication
 - Dynamic, is generated at provisioning (connecting to new WiFi)

Communication relations



Update process

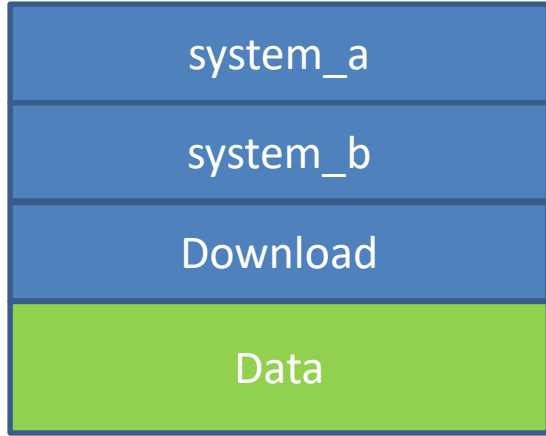


```
milO.ota {"mode":"normal", "install":"1",  
"app_url":"https://[URL]/v11_[version].pkg",  
"file_md5":"[md5]", "proc":"dnld install"}
```

1. encrypted packet with pkg info



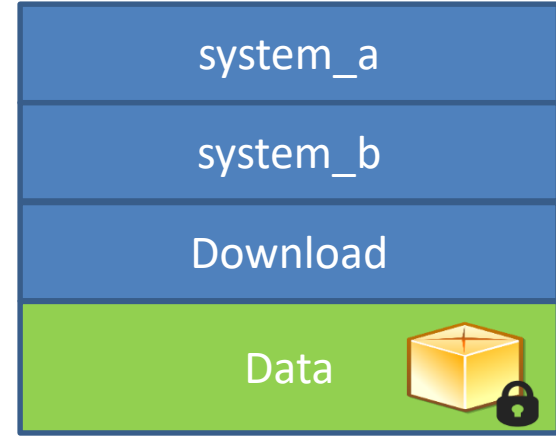
Update process



2. Download [app_url]



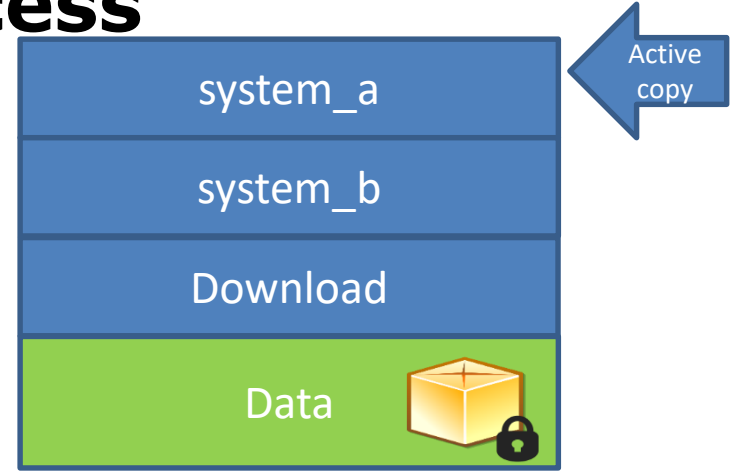
Update process



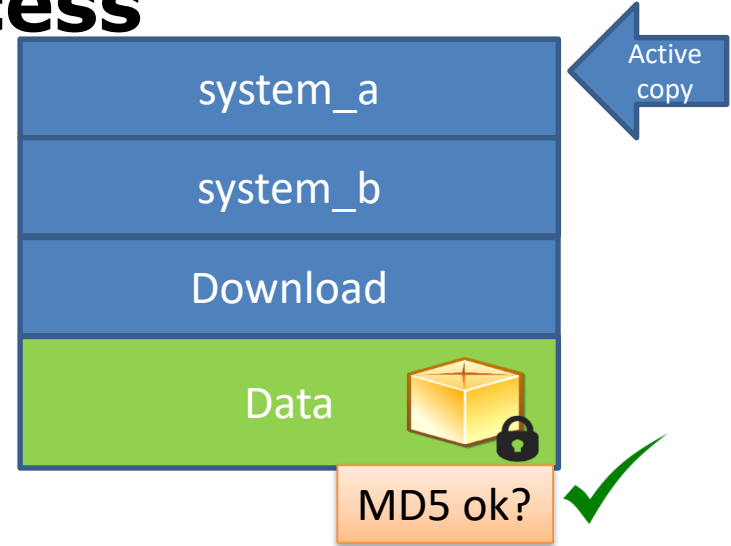
2. Download [app_url]



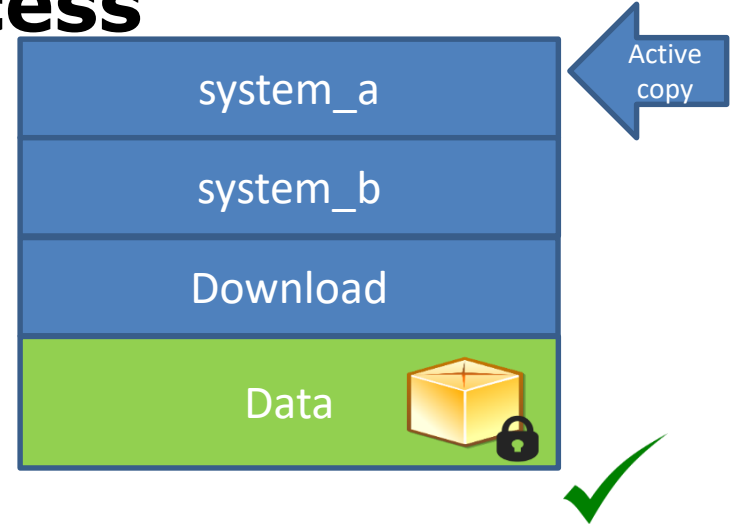
Update process



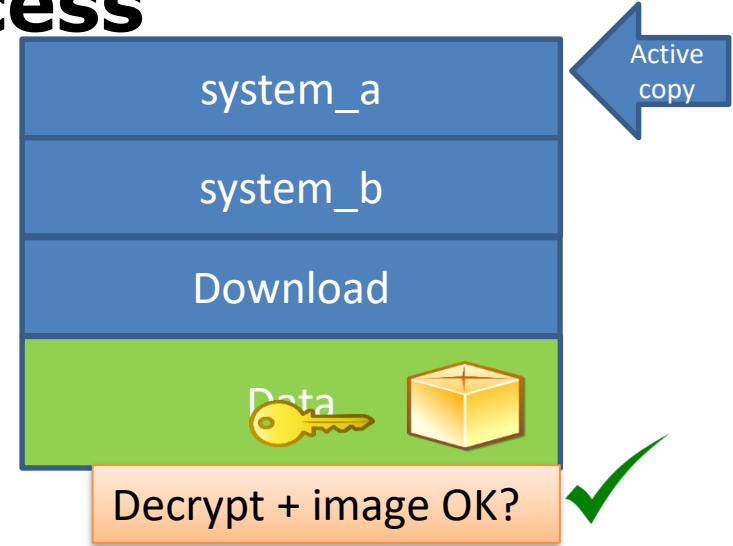
Update process



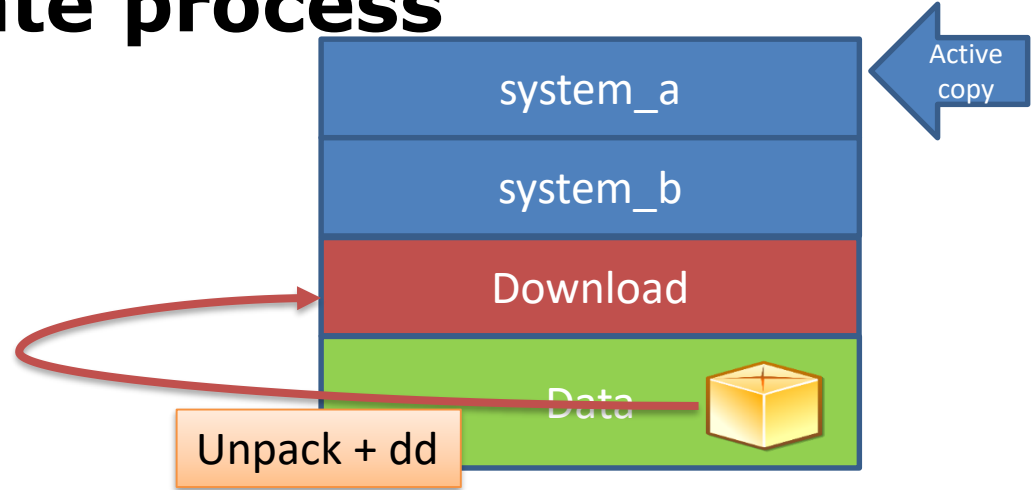
Update process



Update process



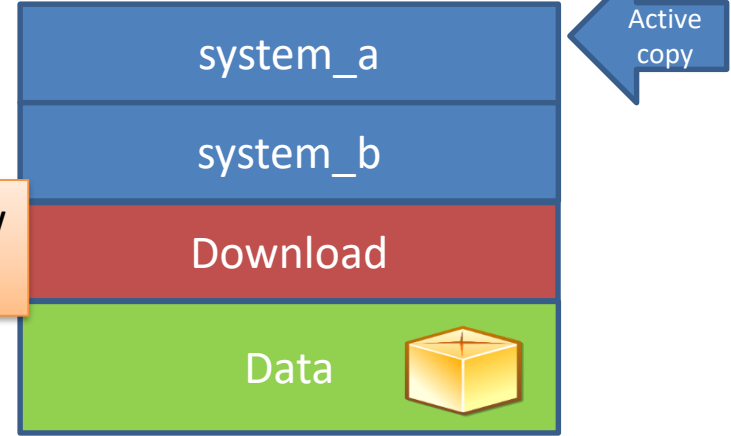
Update process



Update process



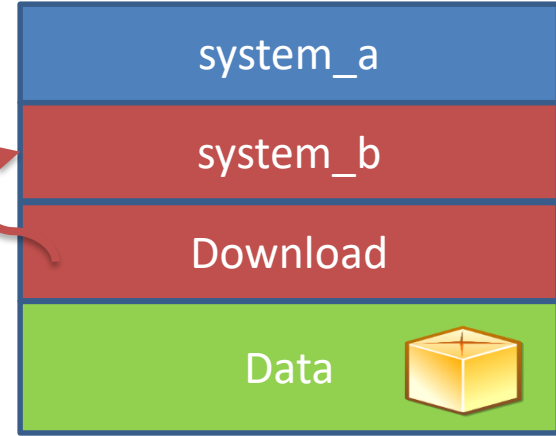
Update root pw
in /etc/shadow



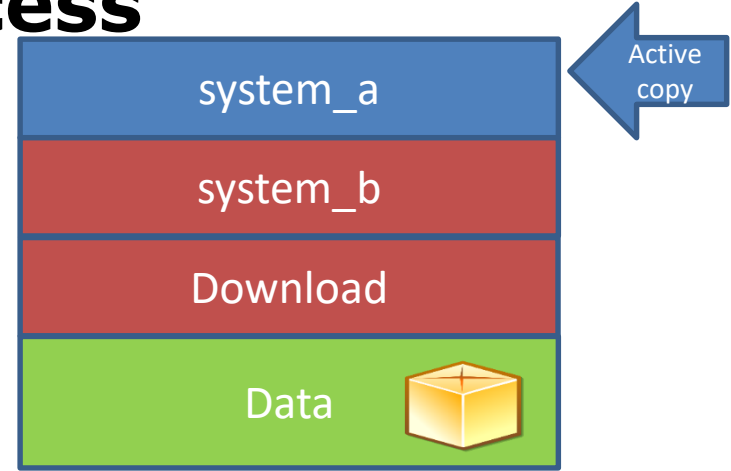
Update process



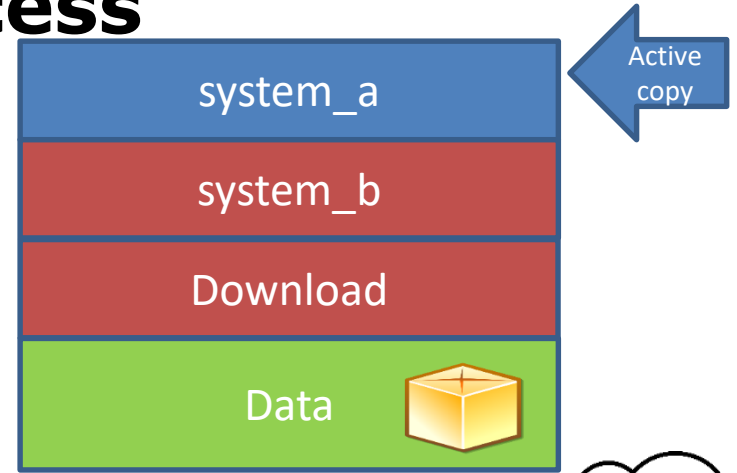
dd



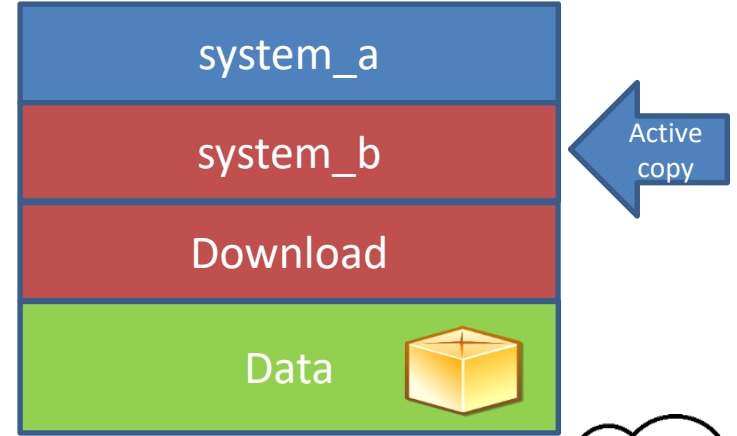
Update process



Update process



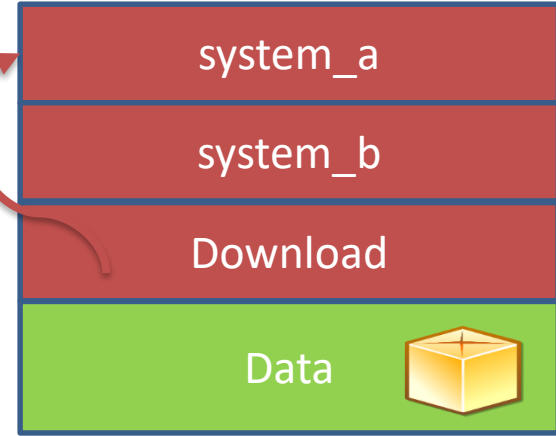
Update process



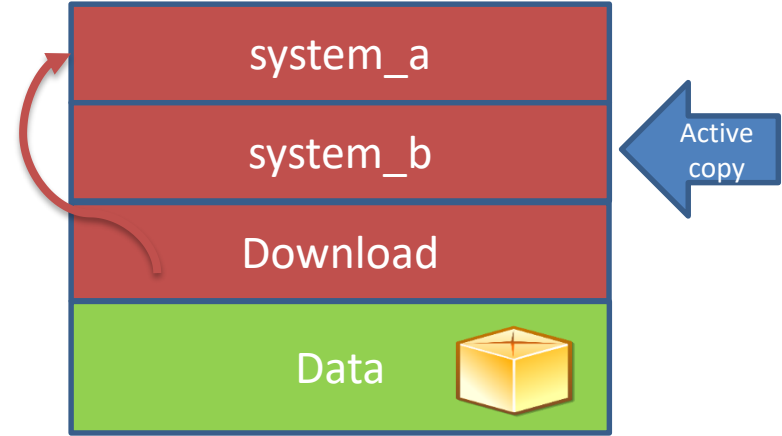
Update process



dd



Update process



Firmware updates

- Full and partial images
 - Encrypted tar.gz archives
 - Full image contains disk.img
 - 512 Mbyte ext4-filesystem
- Encryption
 - Static password: “rockrobo”
 - Ccrypt [256-bit Rijndael encryption (AES)]
- Integrity
 - MD5 provided by cloud

Lets root remotely

- Preparation
 - Rebuild Firmware
 - Include authorized_keys
 - Remove iptables rule for sshd
- Send „milO.ota“ command to vacuum
 - Encrypted with token
 - From app or unprovisioned state
 - Pointing to own http server

root@rockrobo: ~

```
login as: root
Authenticating with public key "rsa-key-gami" from agent
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.4.39 armv7l)

* Documentation:  https://help.ubuntu.com/
Last login: Thu Dec 14 01:43:59 2017 from 192.168.8.67
root@rockrobo:~#
```

root@rockrobo: ~

```
root@rockrobo:~# apt-get update
Ign http://us.ports.ubuntu.com trusty InRelease
Get:1 http://us.ports.ubuntu.com trusty-updates InRelease [65.9 kB]
Get:2 http://us.ports.ubuntu.com trusty-security InRelease [65.9 kB]
Hit http://us.ports.ubuntu.com trusty Release.gpg
Hit http://us.ports.ubuntu.com trusty Release
Hit http://ppa.launchpad.net trusty InRelease
Get:3 http://us.ports.ubuntu.com trusty-updates/main Sources [409 kB]
Get:4 http://us.ports.ubuntu.com trusty-updates/restricted Sources [6322 B]
Get:5 http://us.ports.ubuntu.com trusty-updates/main armhf Packages [875 kB]
Hit http://ppa.launchpad.net trusty/main armhf Packages
Get:6 http://us.ports.ubuntu.com trusty-updates/restricted armhf Packages [8931 B]
Get:7 http://us.ports.ubuntu.com trusty-updates/main Translation-en [516 kB]
Hit http://ppa.launchpad.net trusty/main Translation-en
Get:8 http://us.ports.ubuntu.com trusty-updates/restricted Translation-en [4031 B]
Get:9 http://us.ports.ubuntu.com trusty-security/main Sources [147 kB]
Get:10 http://us.ports.ubuntu.com trusty-security/restricted Sources [4931 B]
Get:11 http://us.ports.ubuntu.com trusty-security/main armhf Packages [575 kB]
Get:12 http://us.ports.ubuntu.com trusty-security/restricted armhf Packages [8931 B]
Get:13 http://us.ports.ubuntu.com trusty-security/main Translation-en [375 kB]
Get:14 http://us.ports.ubuntu.com trusty-security/restricted Translation-en [354
```

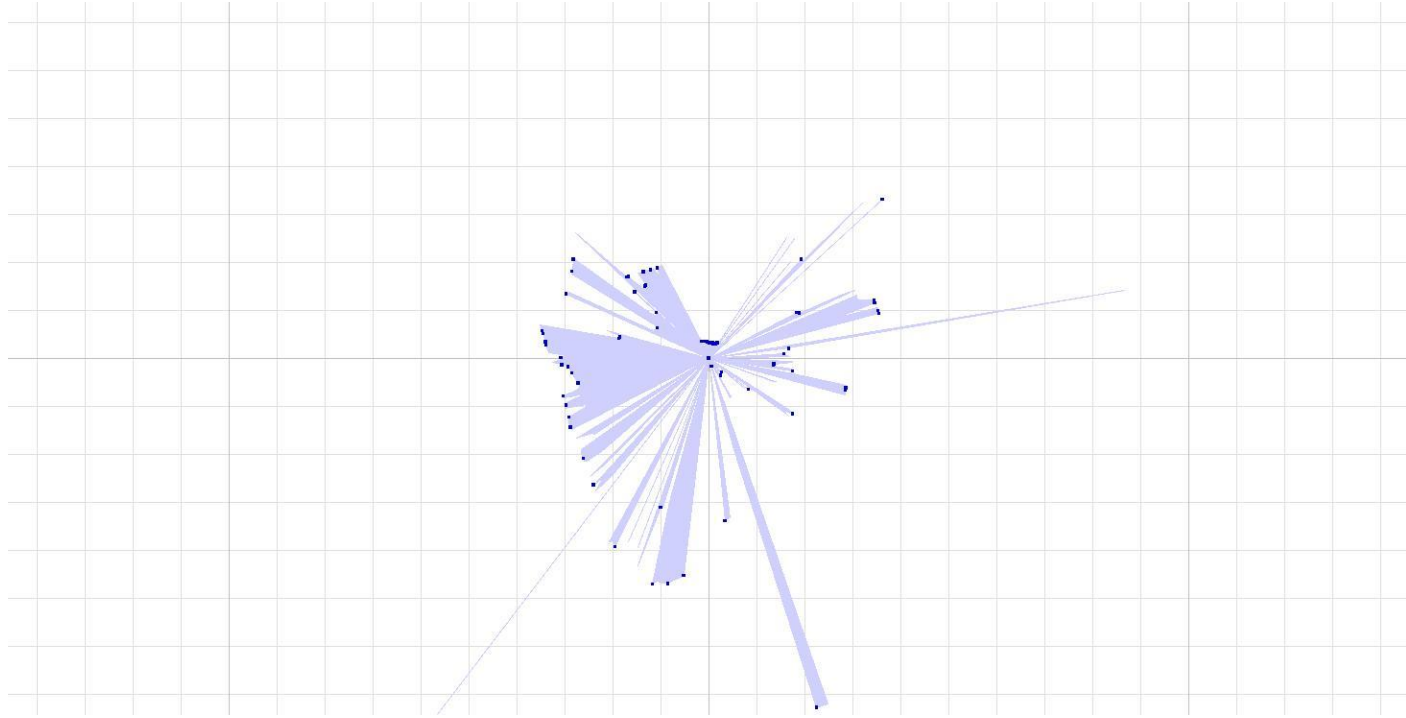
```

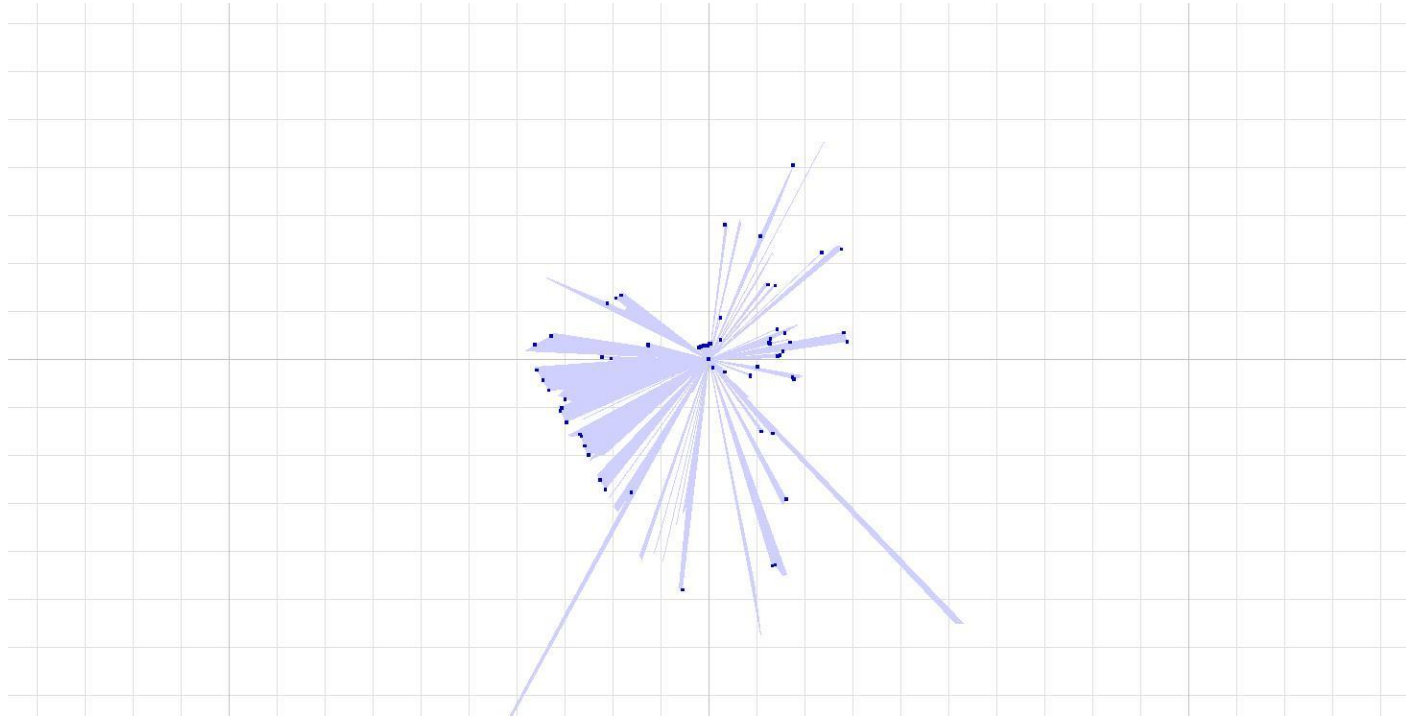
1  [|||||          7.4%]      Tasks: 39, 46 thr; 1 running
2  [|||           7.7%]      Load average: 1.23 1.18 1.21
3  [|||           7.2%]      Uptime: 21:51:32
4  [|||||         11.1%]
Mem[|||||||||||||207/498MB]
Swp[              0/0MB]

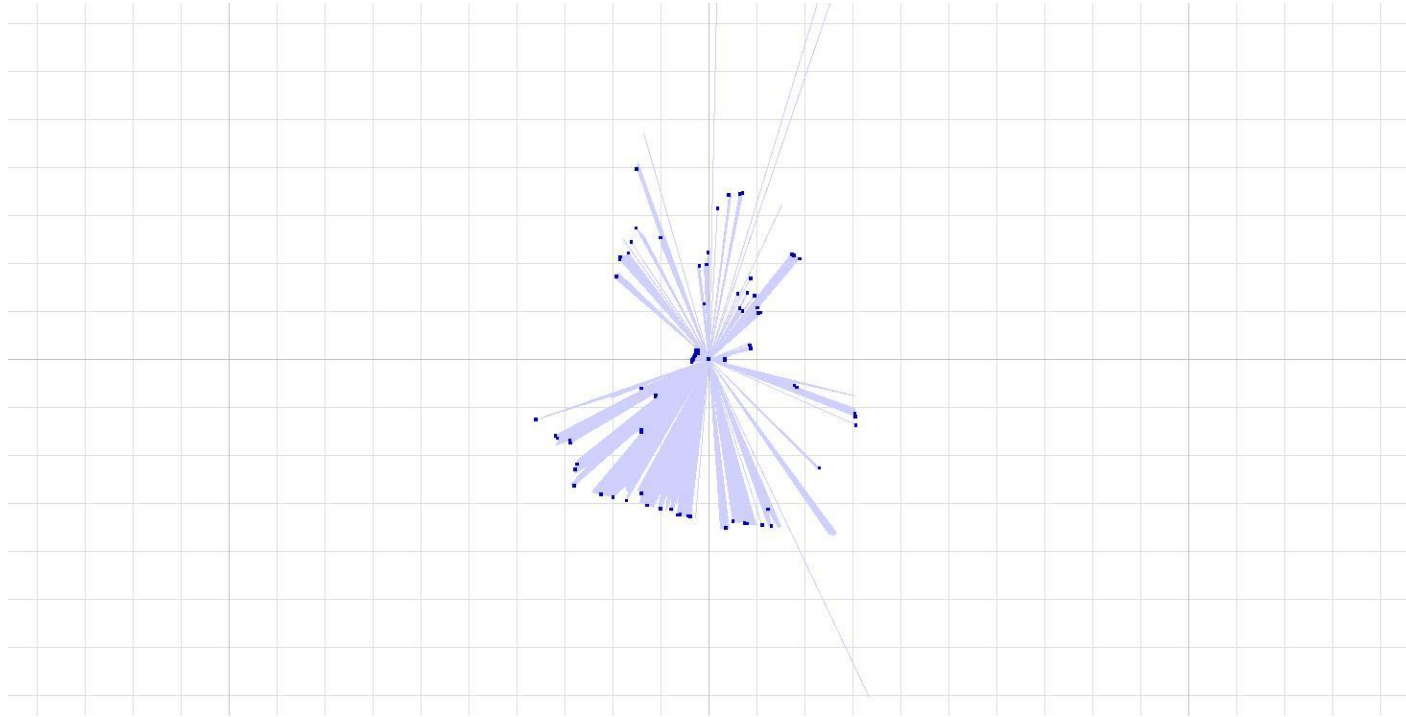
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
922	root	0	-20	329M	97900	6168	S	5.9	19.2	1h05:03	player /opt/rockr
27788	root	20	0	2724	1324	932	R	3.9	0.3	0:00.45	htop
940	root	0	-20	329M	97900	6168	S	2.0	19.2	22:22.18	player /opt/rockr
947	root	0	-20	329M	97900	6168	S	1.3	19.2	15:59.31	player /opt/rockr
535	root	20	0	2452	1276	992	S	1.3	0.2	6:00.78	/bin/bash /usr/bi
719	root	0	-20	40184	37692	3996	S	0.7	7.4	9:15.19	WatchDoge /opt/ro
939	root	0	-20	329M	97900	6168	S	0.7	19.2	11:03.31	player /opt/rockr
948	root	0	-20	329M	97900	6168	S	0.7	19.2	7:09.43	player /opt/rockr
951	root	0	-20	329M	97900	6168	S	0.7	19.2	2:28.84	player /opt/rockr
881	root	0	-20	2552	1096	776	S	0.0	0.2	4:27.87	top -H -d 15 -b
938	root	0	-20	329M	97900	6168	S	0.0	19.2	4:09.65	player /opt/rockr
520	syslog	20	0	30472	1352	828	S	0.0	0.3	0:11.07	rsyslogd
882	root	0	-20	2540	1068	776	S	0.0	0.2	8:15.61	top -d 5 -b
27798	root	0	-20	2564	1400	1004	S	0.0	0.3	0:00.06	/bin/bash /opt/ro

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit







Gain independence

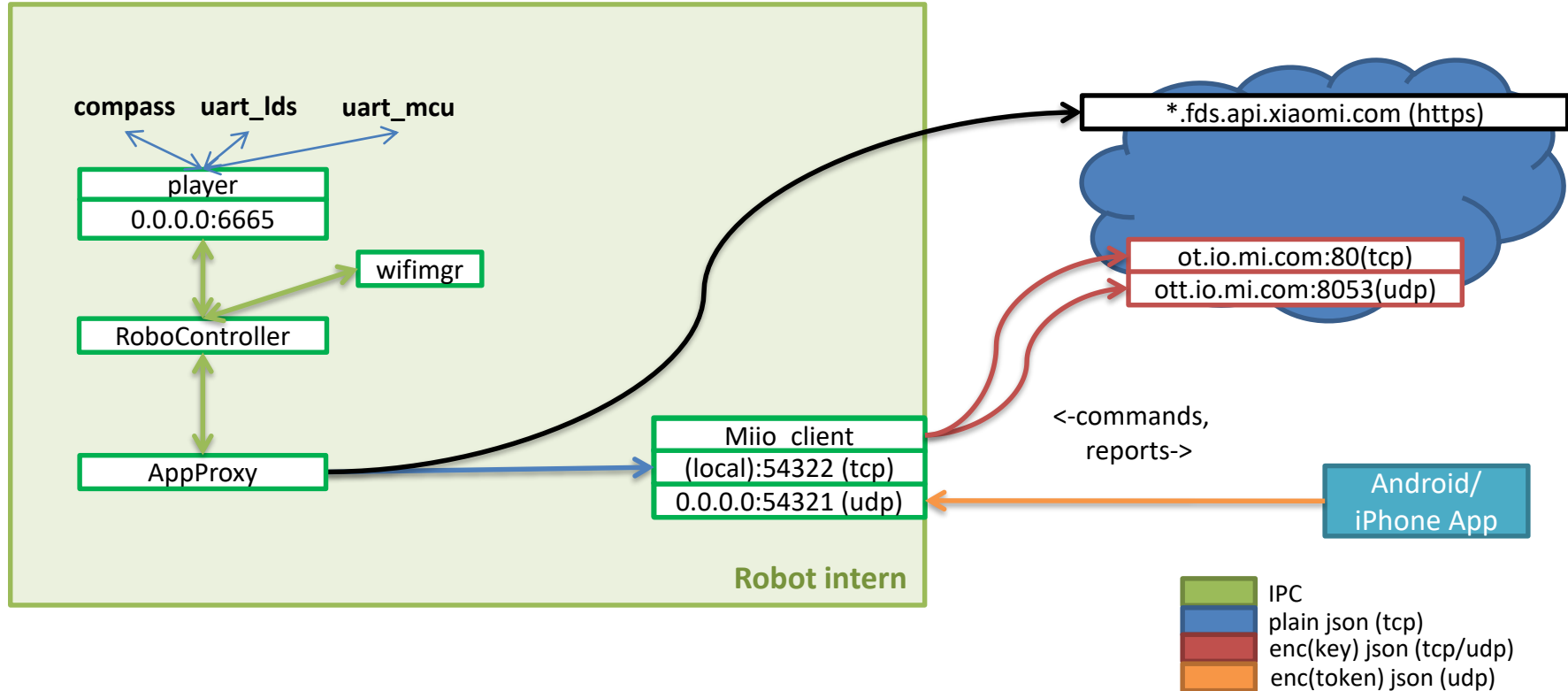


Source: 20th Century Fox

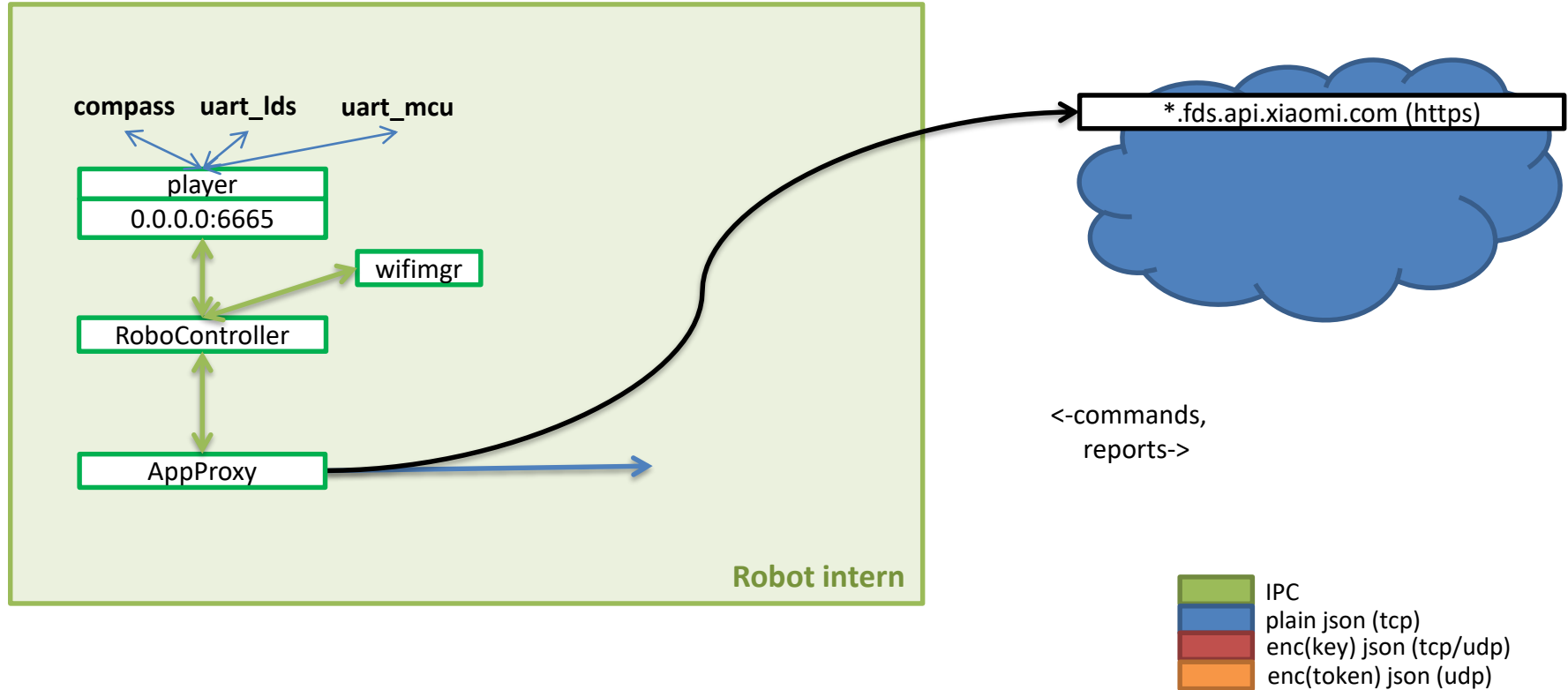
Two methods:

- **Replacing** the cloud interface
- **Proxy** cloud communication

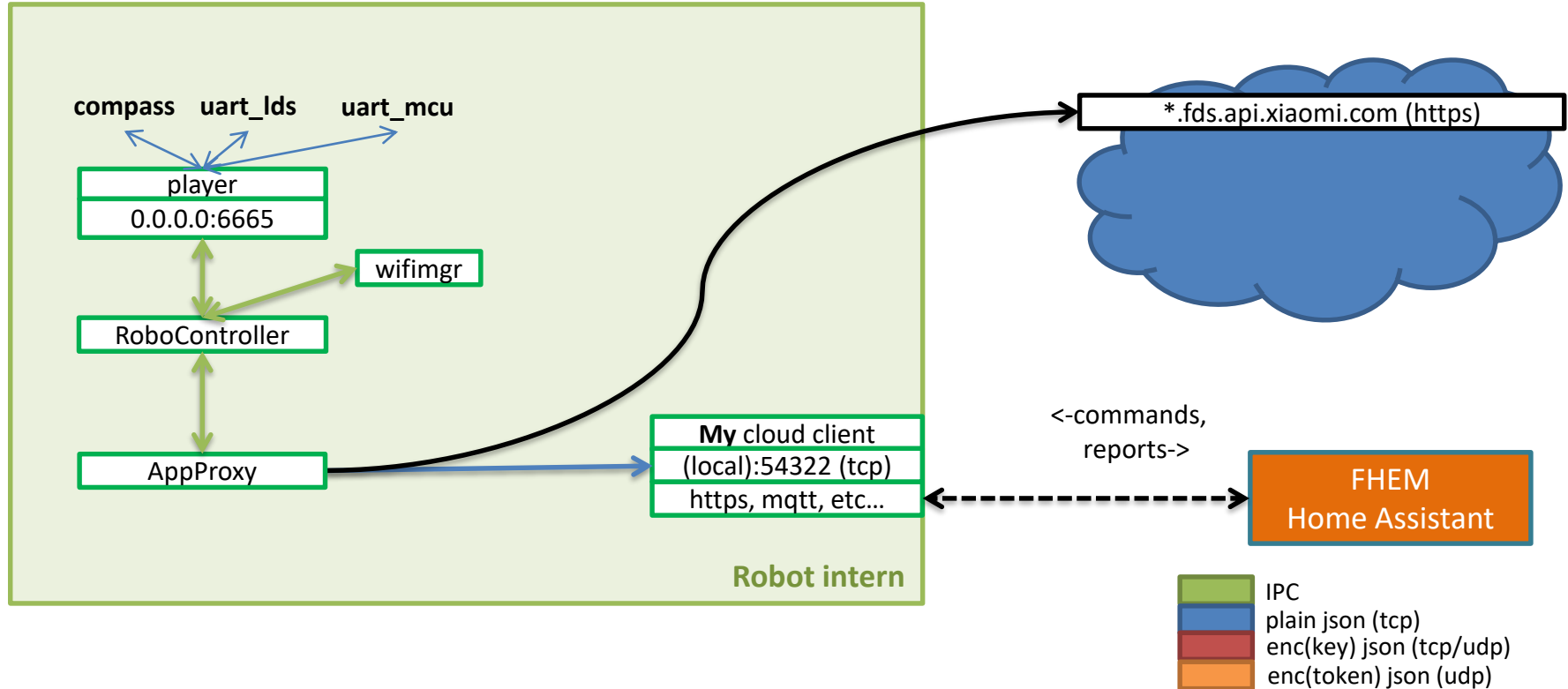
Replacing the cloud interface



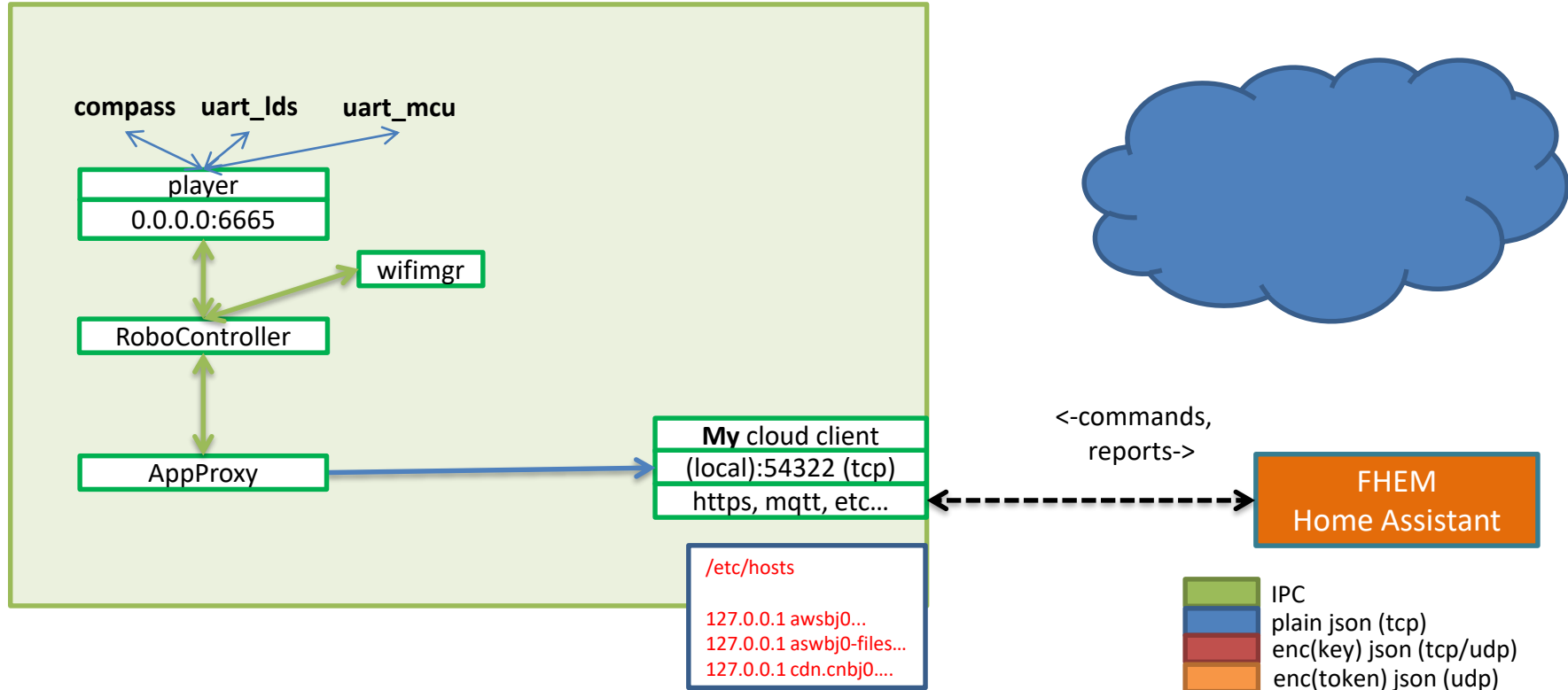
Replacing the cloud interface



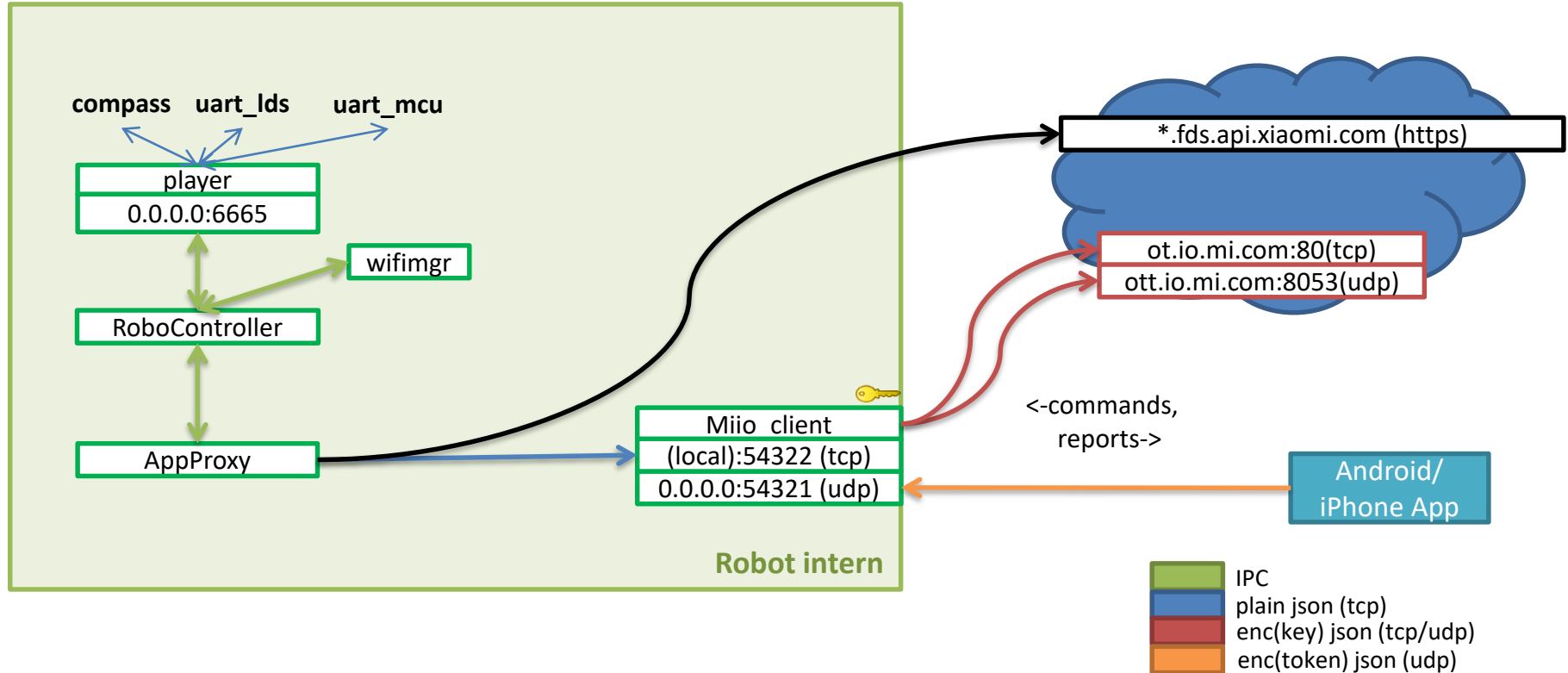
Replacing the cloud interface



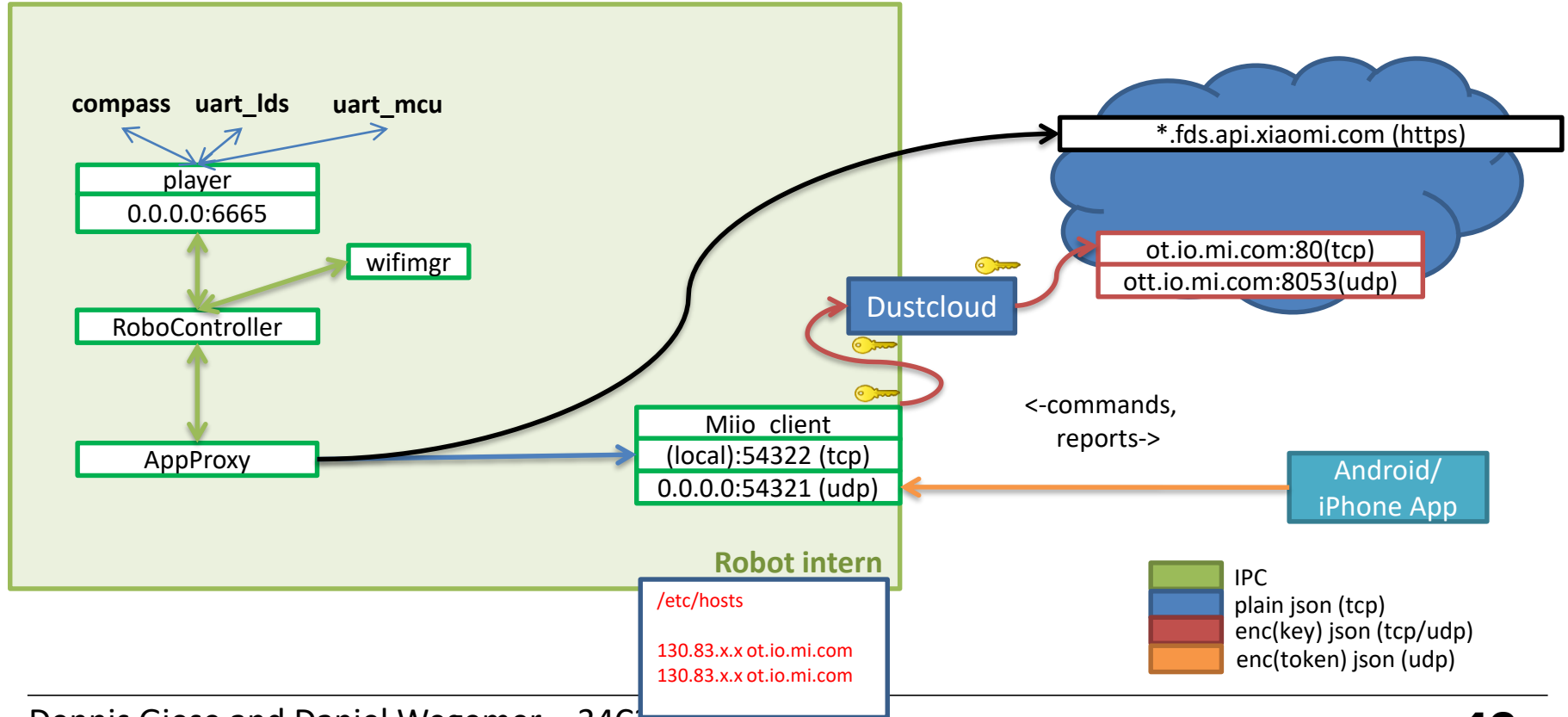
Replacing the cloud interface



Proxy cloud communication



Proxy cloud communication



Usecases

- Home automation server
- Webradio
- Fileserver
 - with integrated UPS
- ~~Bitcoin mining~~



FHEM

Save config

Unsorted

 Everything

Logfile

Commandref

Remote doc

Edit files

Select style

Event monitor

DeviceOverview

[this.vacuum](#) Docked start pause charge

set this.vacuum fan_power 60

get this.vacuum clean_summary

Internals

DEF	127.0.0.1 656c423233624835384f46374a445177
FD	5
NAME	this.vacuum
NR	20
STATE	connected
TYPE	XiaomiDevice
device_type	unknown
mac	34:CE:00:
model	rockrobo.vacuum.v1
token	656c423233624835384f46374a445177

Readings

battery	ok	2017-12-2
batteryLevel	100	2017-12-2

DLC

- Modified firmware (SSH + FHEM)
- Dustcloud (Cloud emulation)
 - totally broken, insecure code!
- Pictures, Pinouts, and much more

→ www.dontvacuum.me

One word of warning...

- Never leave your devices unprovisioned
 - Someone else can provision it for you
 - Install malicious firmware
 - Snoop on your apartment
- Be careful with used devices
 - e.g. Amazon Marketplace
 - Some malicious software may be installed

Acknowledgements & FAQ

- Secure Mobile Networking (SEEMOO) Labs



- Prof. Guevara Noubir (CCIS, Northeastern University)

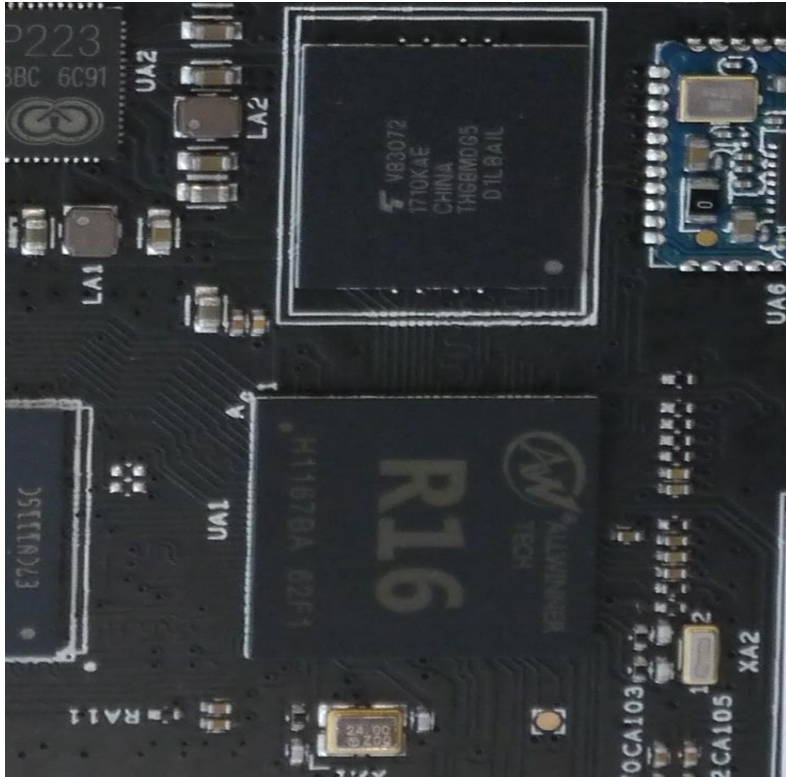


Northeastern University
College of Computer and Information Science



BACKUP

Pin Layout CPU



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
A						MMC Reset	D6	D4	D2	D0		D2	D0	CLK		TX	UART1	
B						D7	D5	D3	D1			D3	D1	CMD		RX		
C									CLK			SDA					TWI1	
D						RX	TX		CMD			SCL						
E																		
F																Recov ery	Confir m	UART2
G																RX	TX	
H																Line IN L		
J																LINE IN R		
K																PHO NE IN		
L																PHO NE IN		
M																PHO NE	MIC1 P	
N																PHO NE	MIC2 P	
P																SDA SCK	RESET	RSB0
R																		
T							LCD9	LCD7	LCD5	LCD3	LCD1					USB- DM0	USB- DP0	USB 1
U							LCD8	LCD6	LCD4	LCD2	LCD0	USB DRV				USB- DM1	USB- DP1	USB 2
	DRAM	VCC/VDD	GND							LCD								

Overview sensors

- 2D **LIDAR** SLAM ($5 \times 360^\circ/\text{s}$)
- **Ultrasonic** distance sensor
- multiple **IR** sensors
- 3-axis **Magnetic** Sensor
- 3-axis **accelerometer**
- 3-axis **gyroscope**
- **Bump** sensors



Sound packages

- Contents of /mnt/data/sounds
 - Encrypted tar.gz archives
 - Contains wav-files in specific language or style
- Encryption
 - Static password: “r0ckrobo#23456”
 - Ccrypt [256-bit Rijndael encryption (AES)]
- Integrity
 - MD5 provided by cloud

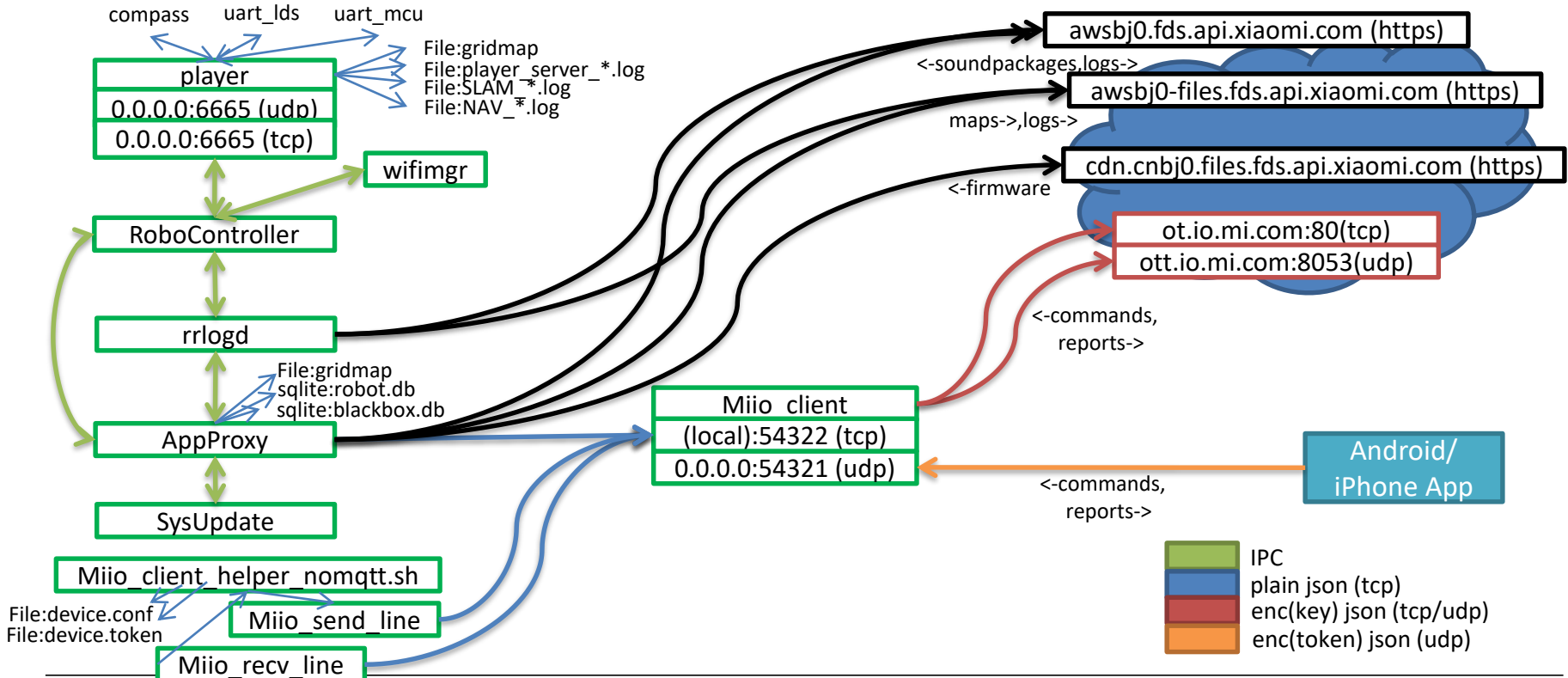
eMMC Layout

Label	Partion nand{}	Size in MByte	Start address
boot-res	a	8	0x00008000
env	b	16	0x0000c000
app	c	16	0x00014000
recovery	d	512	0x0001c000
system_a	e	512	0x0011c000
system_b	f	512	0x0021c000
Download	g	528	0x0031c000
reserve	h	16	0x00424000
UDISK	i	~1900	0x0042c000

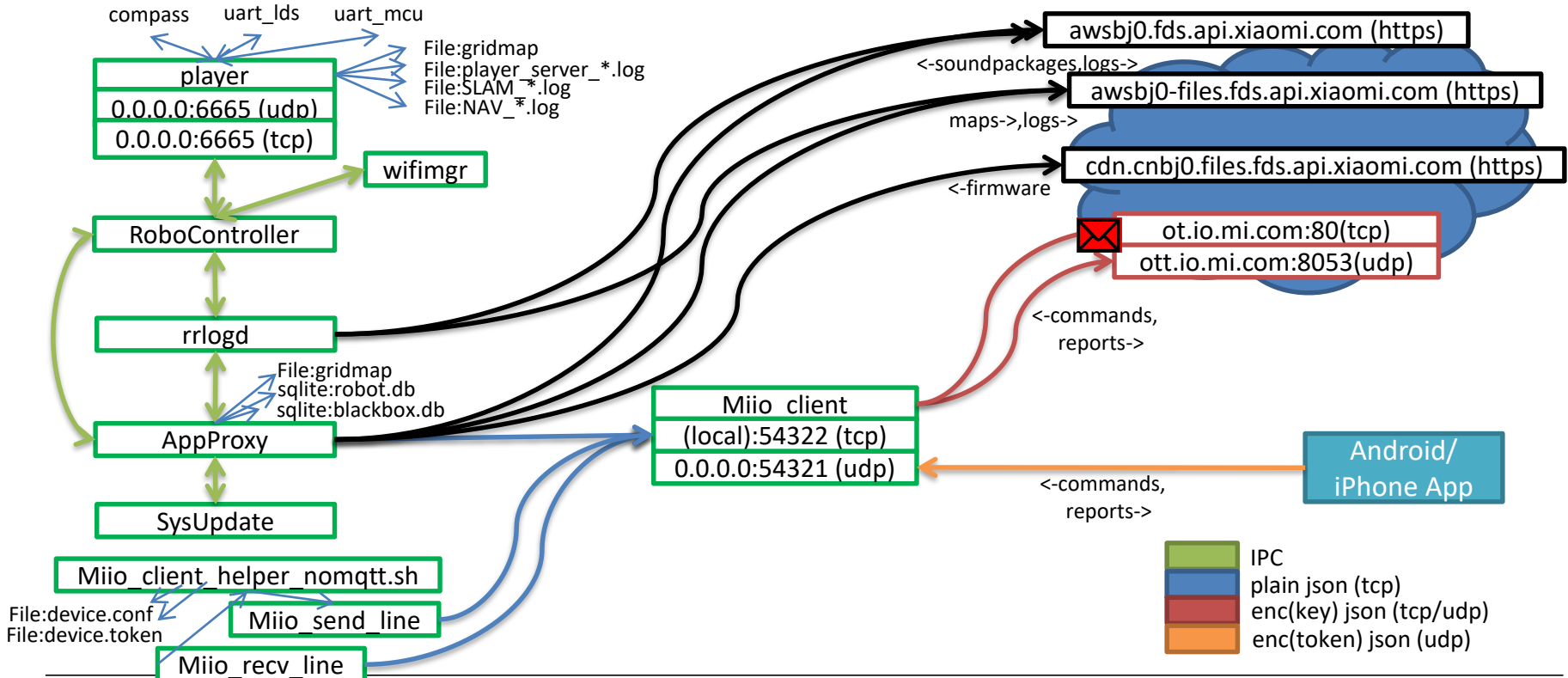
eMMC Layout

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

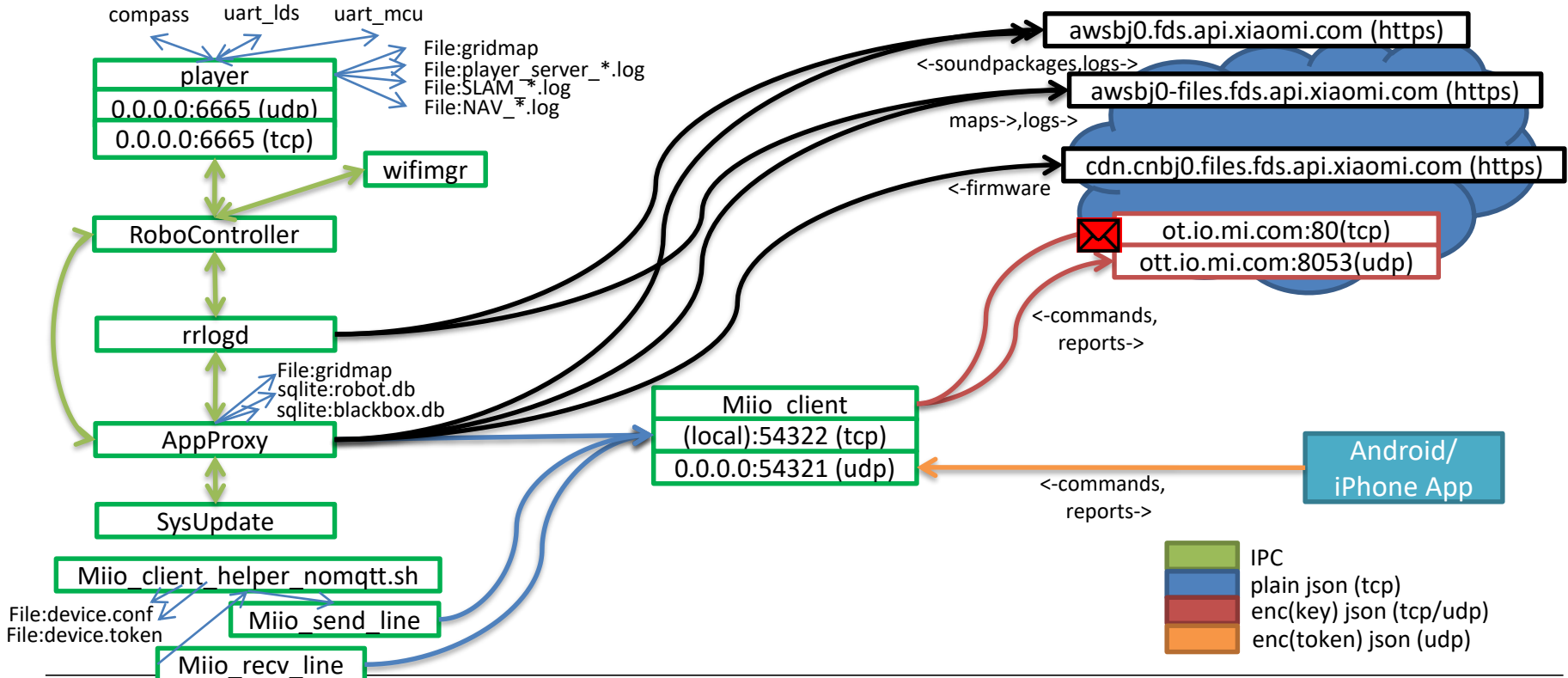
Communication relations



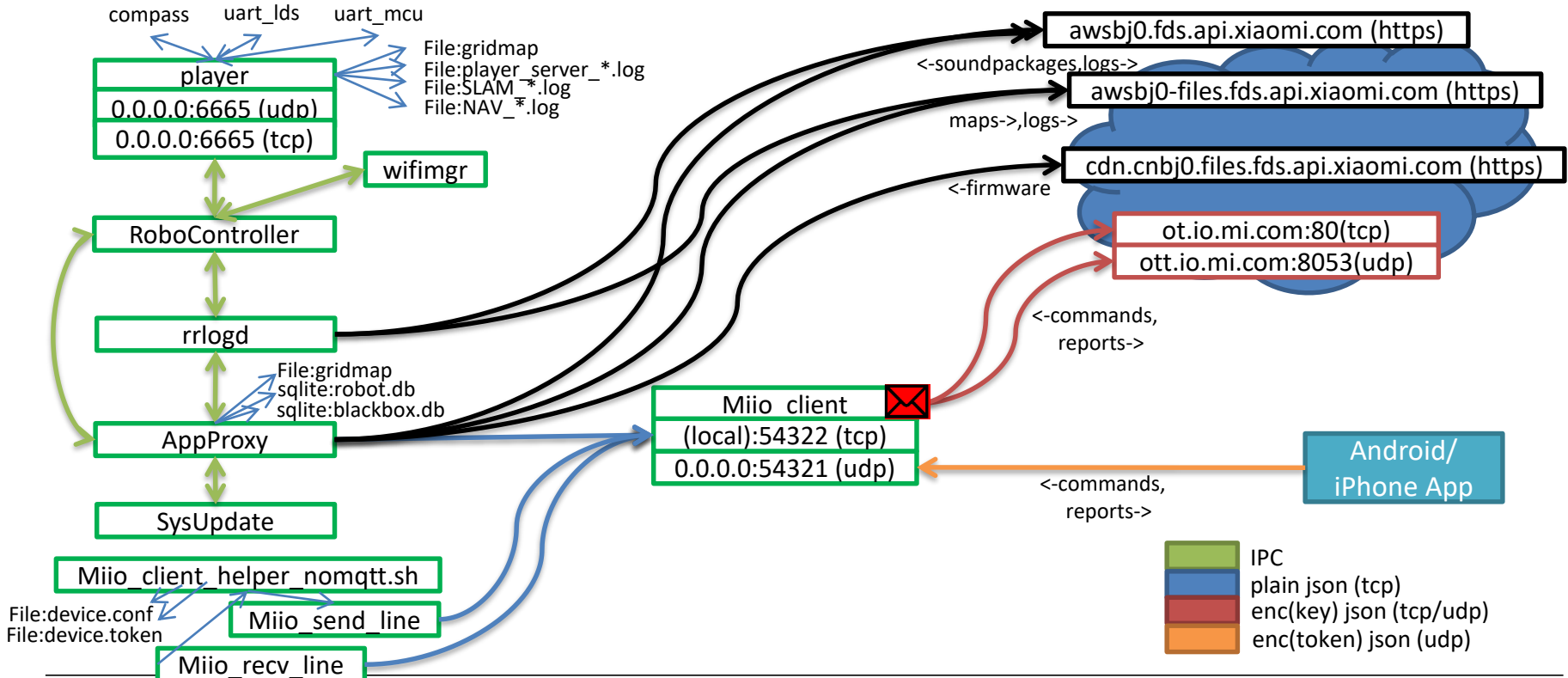
Communication relations



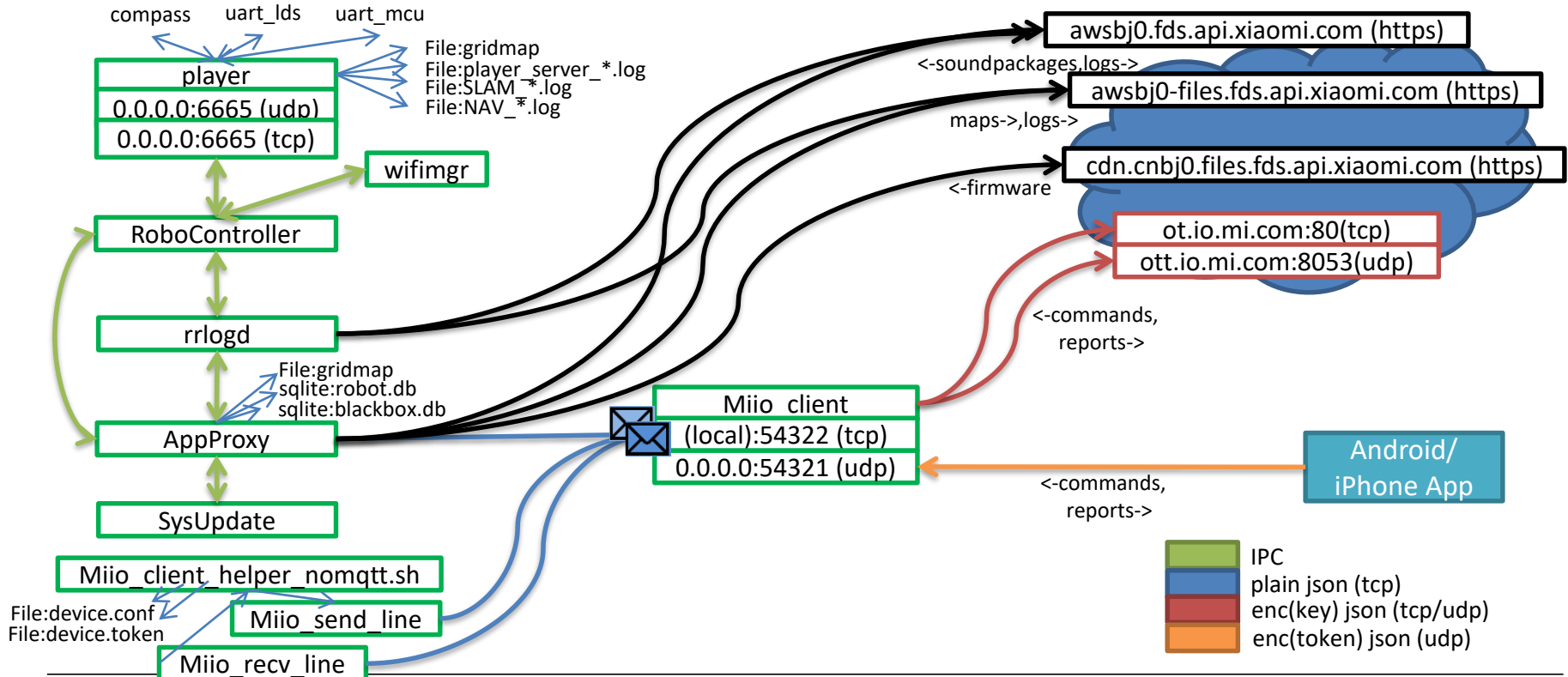
Communication relations



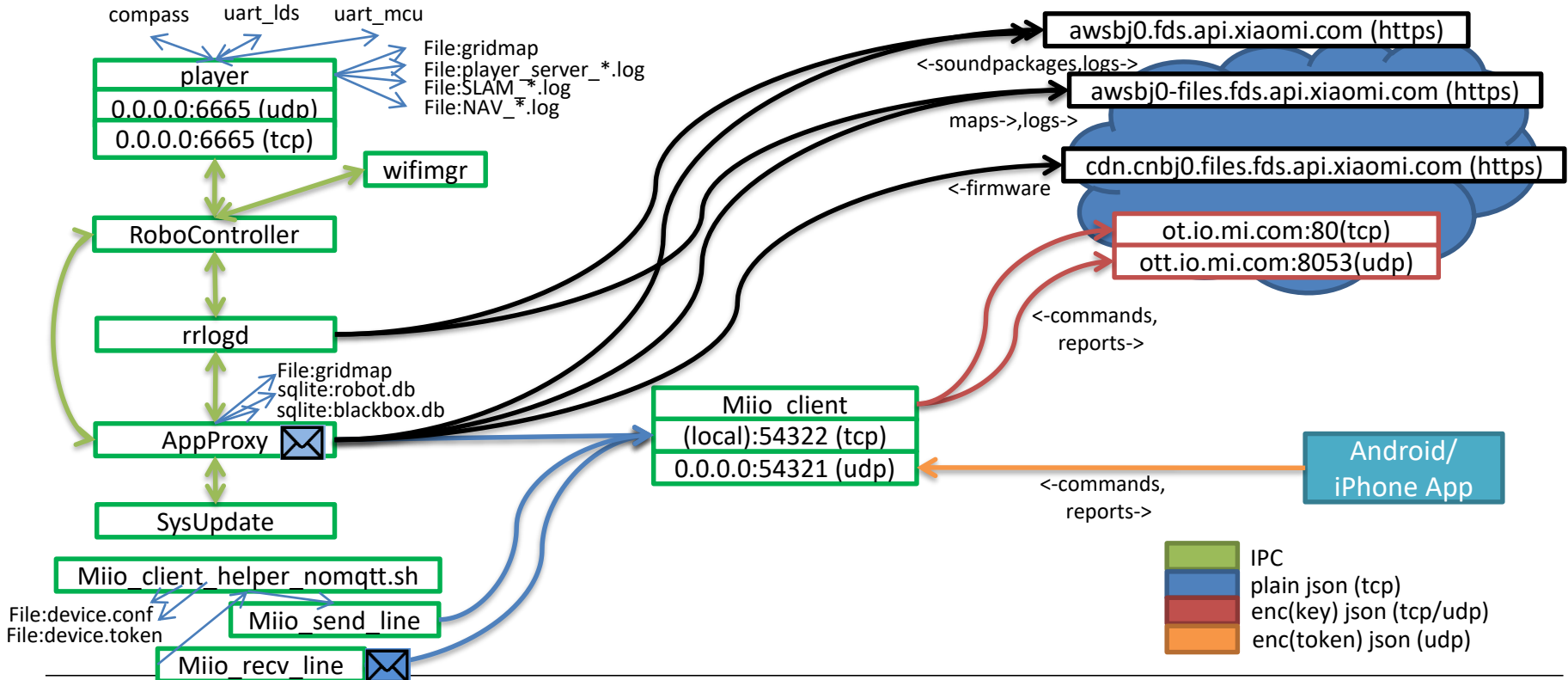
Communication relations



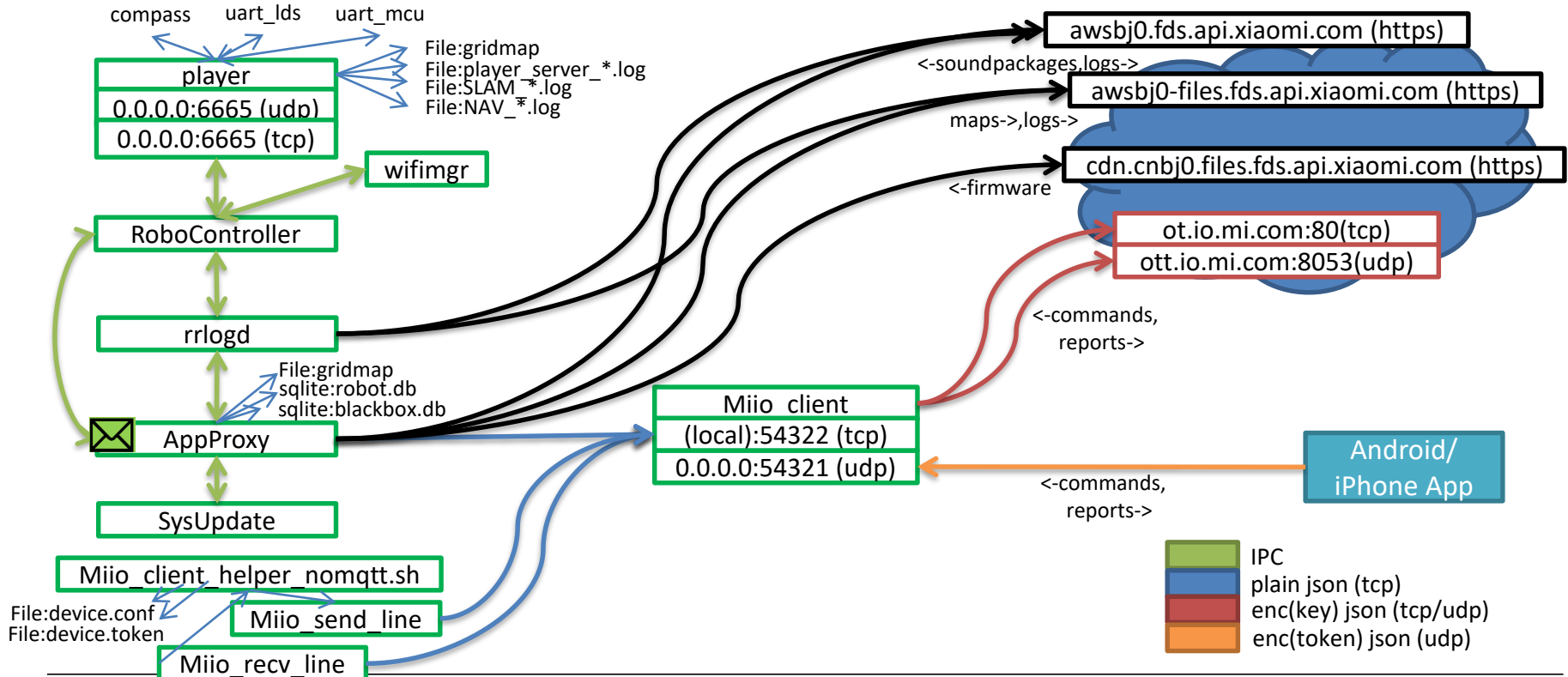
Communication relations



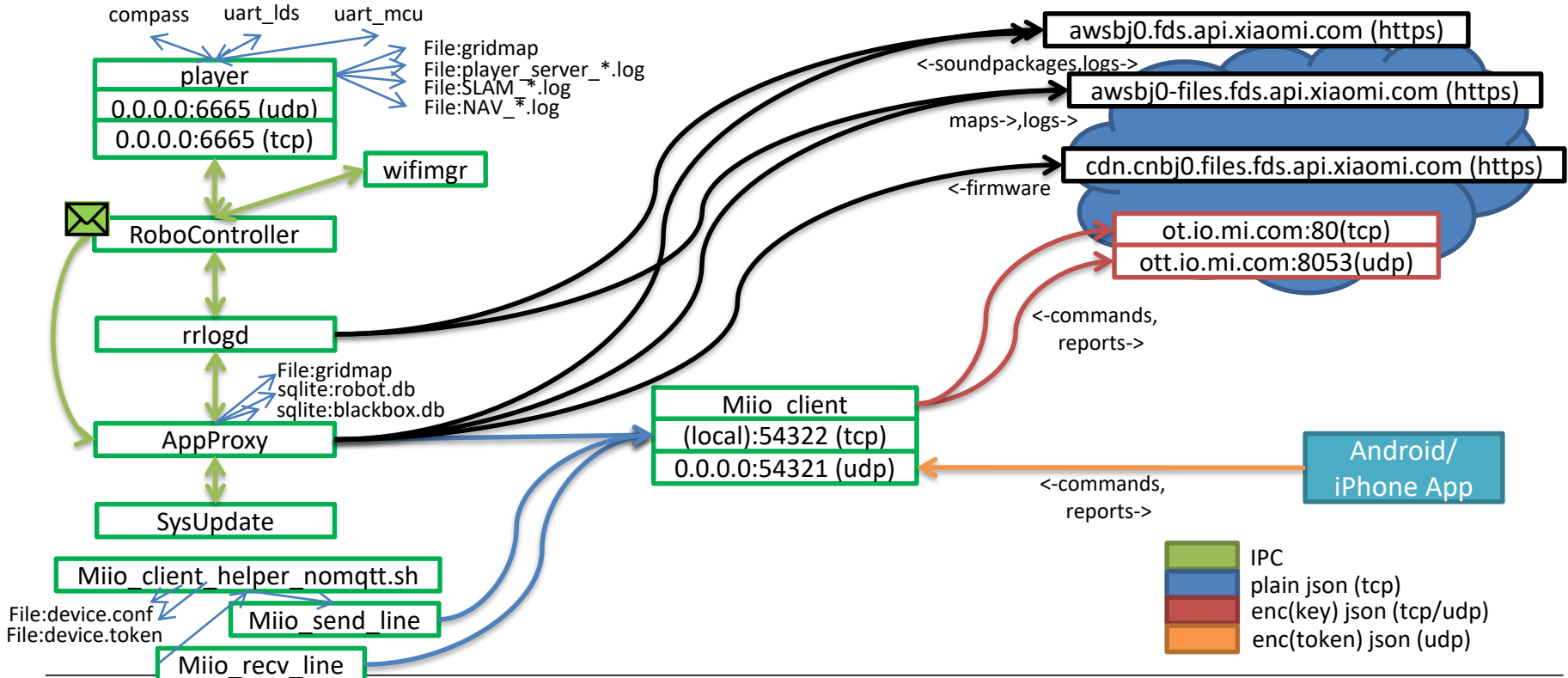
Communication relations



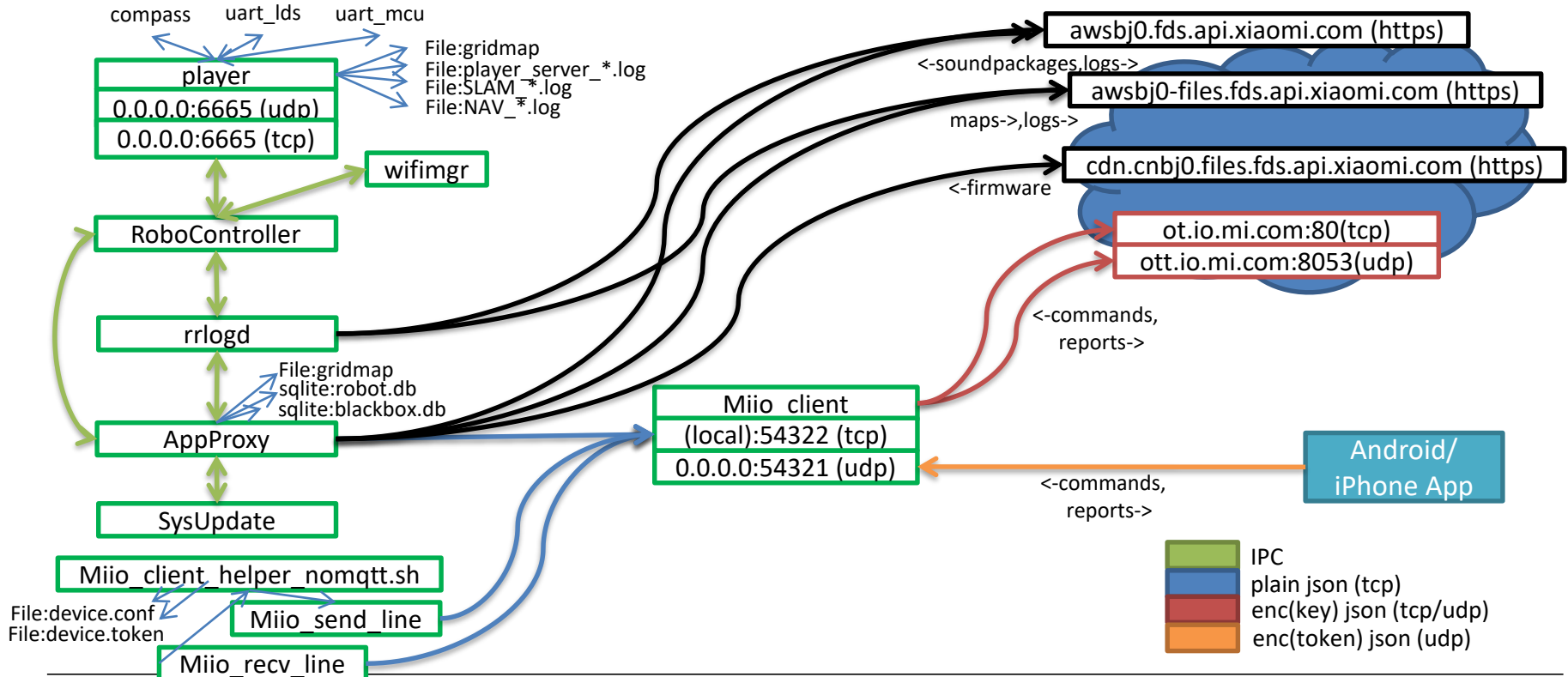
Communication relations



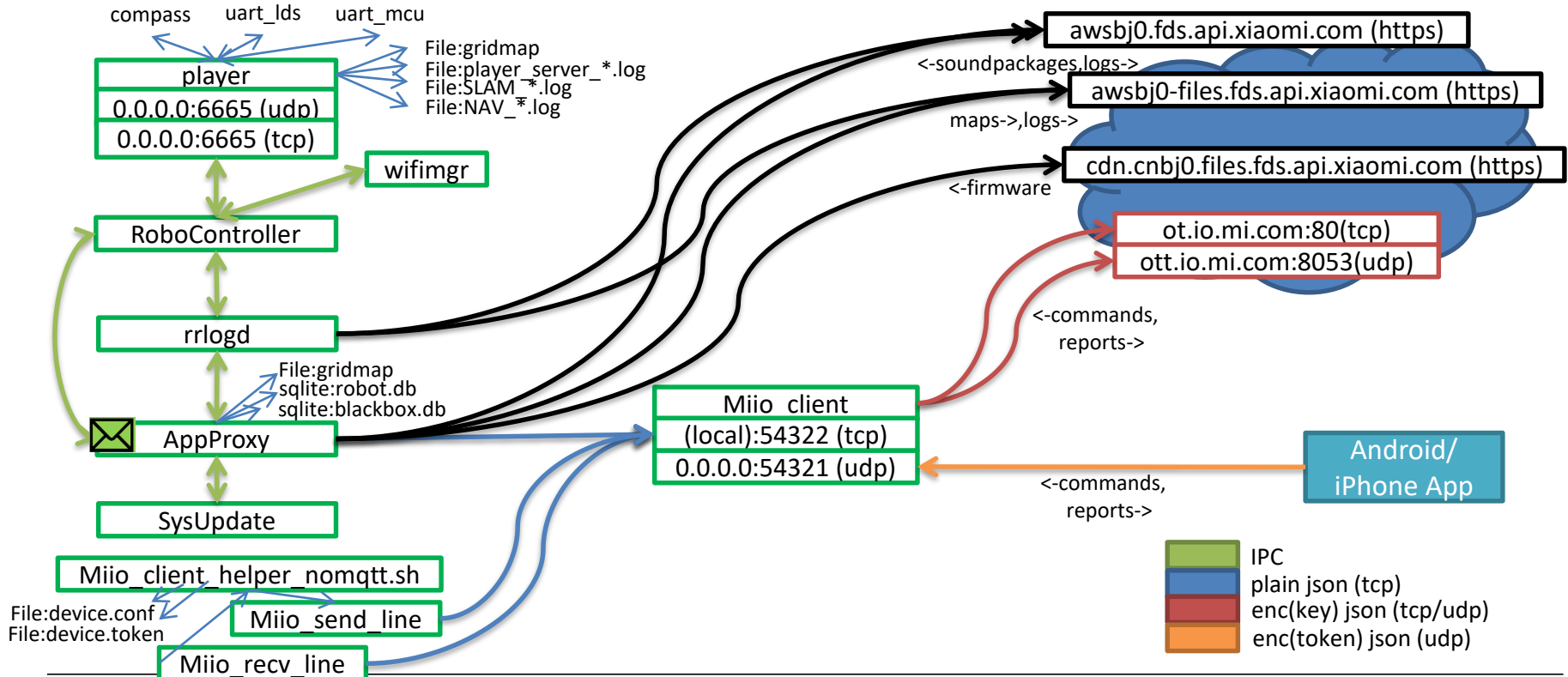
Communication relations



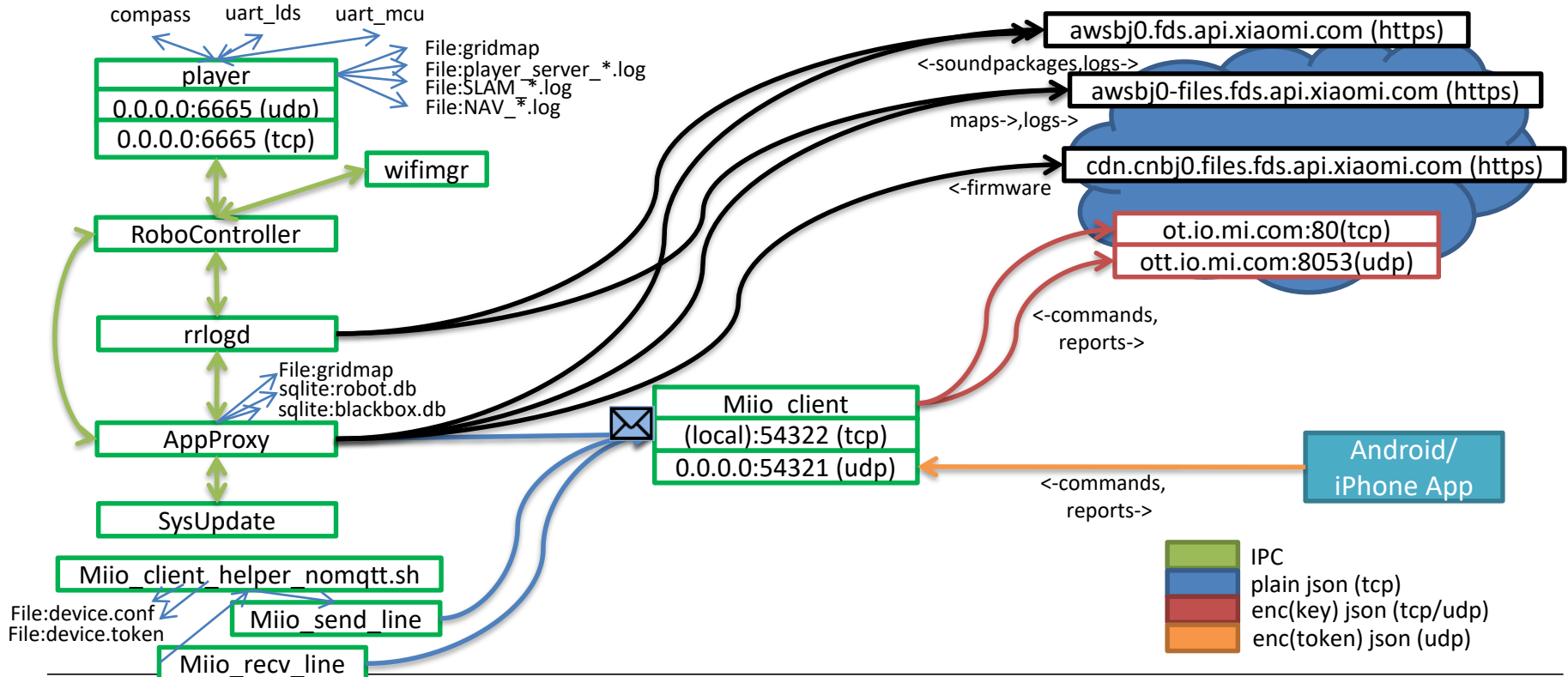
Communication relations



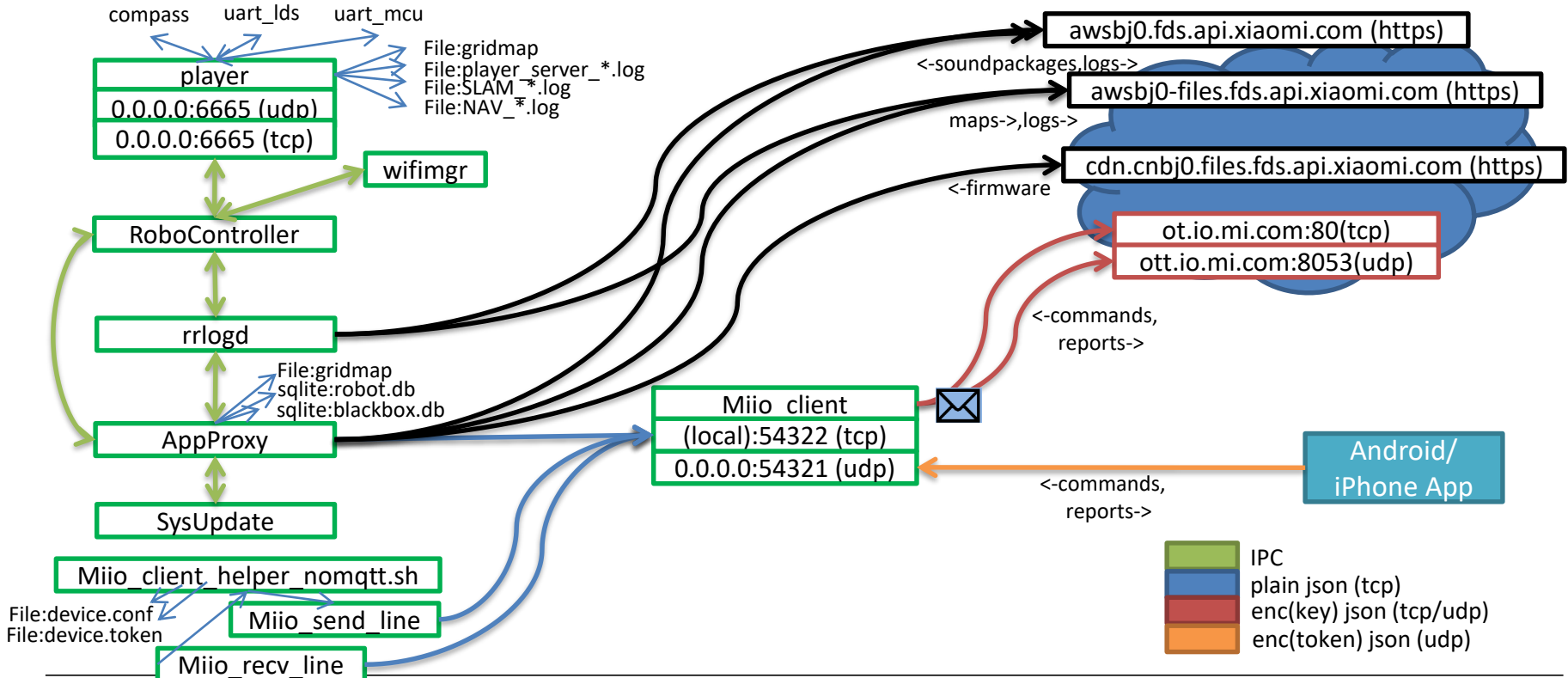
Communication relations



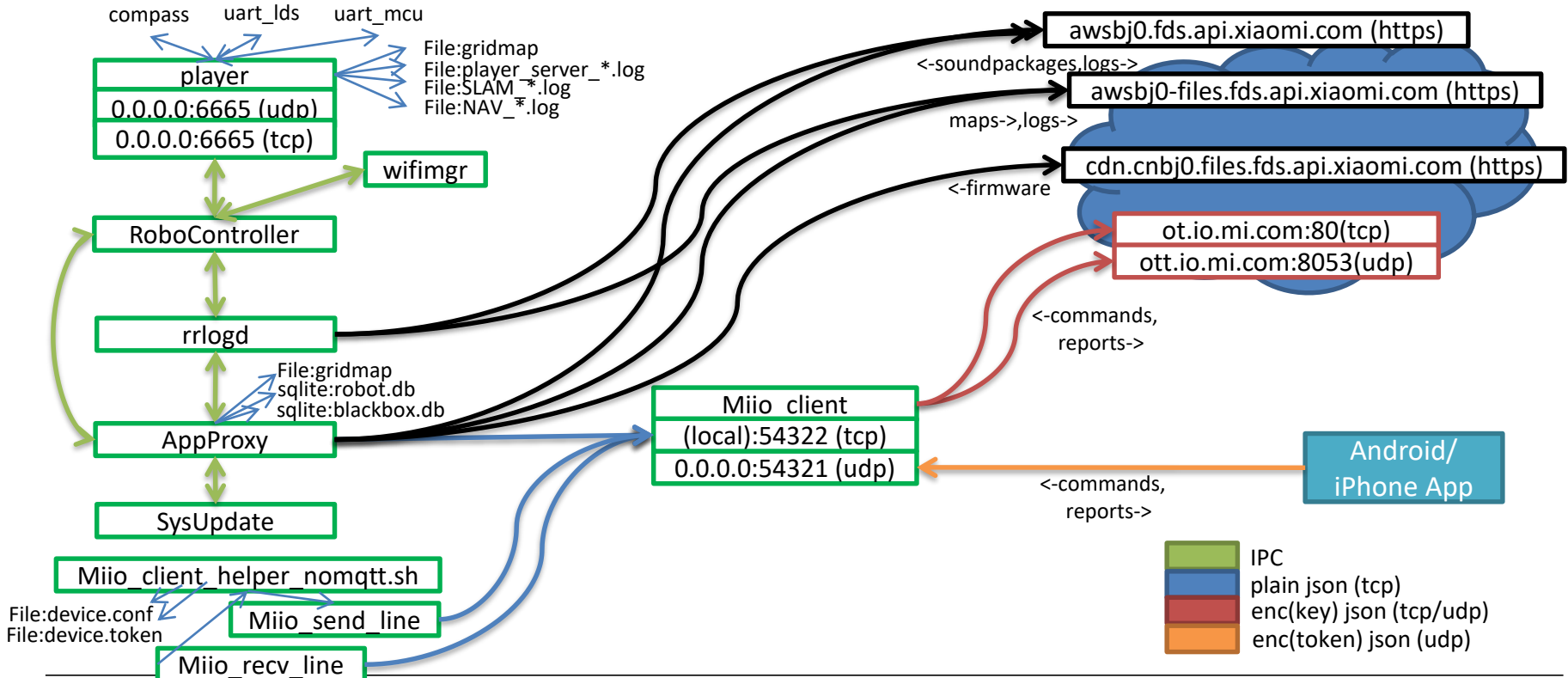
Communication relations



Communication relations



Communication relations



Communication relations

