

A close-up photograph of a man with dark hair and a beard, wearing a dark t-shirt. He is looking down at a tablet device he is holding in his hands. The background is blurred, showing what appears to be a modern interior space.

arm

Enabling firmware updates over LPWAN

Jan Jongboom | Developer Evangelist | Arm

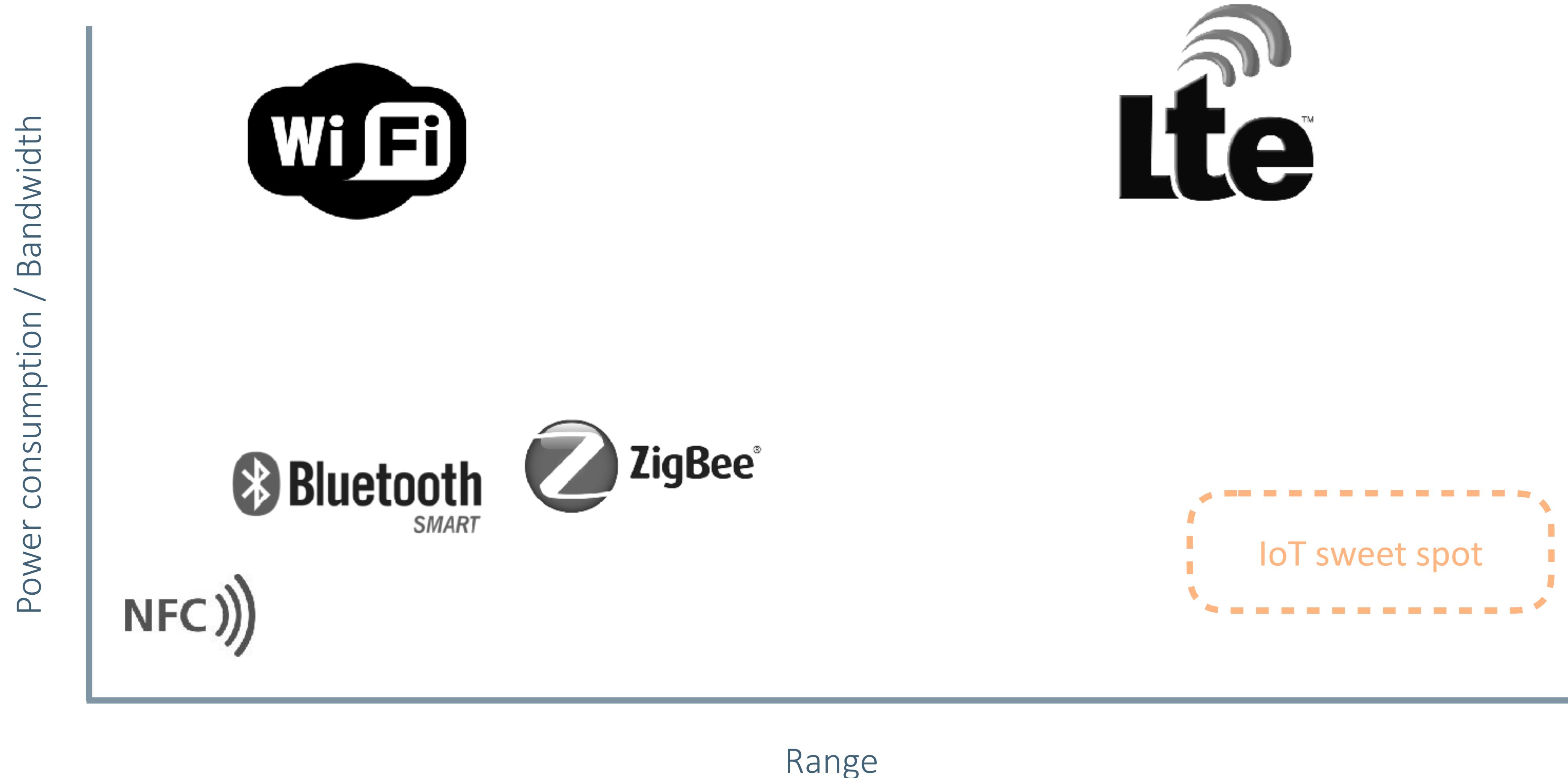




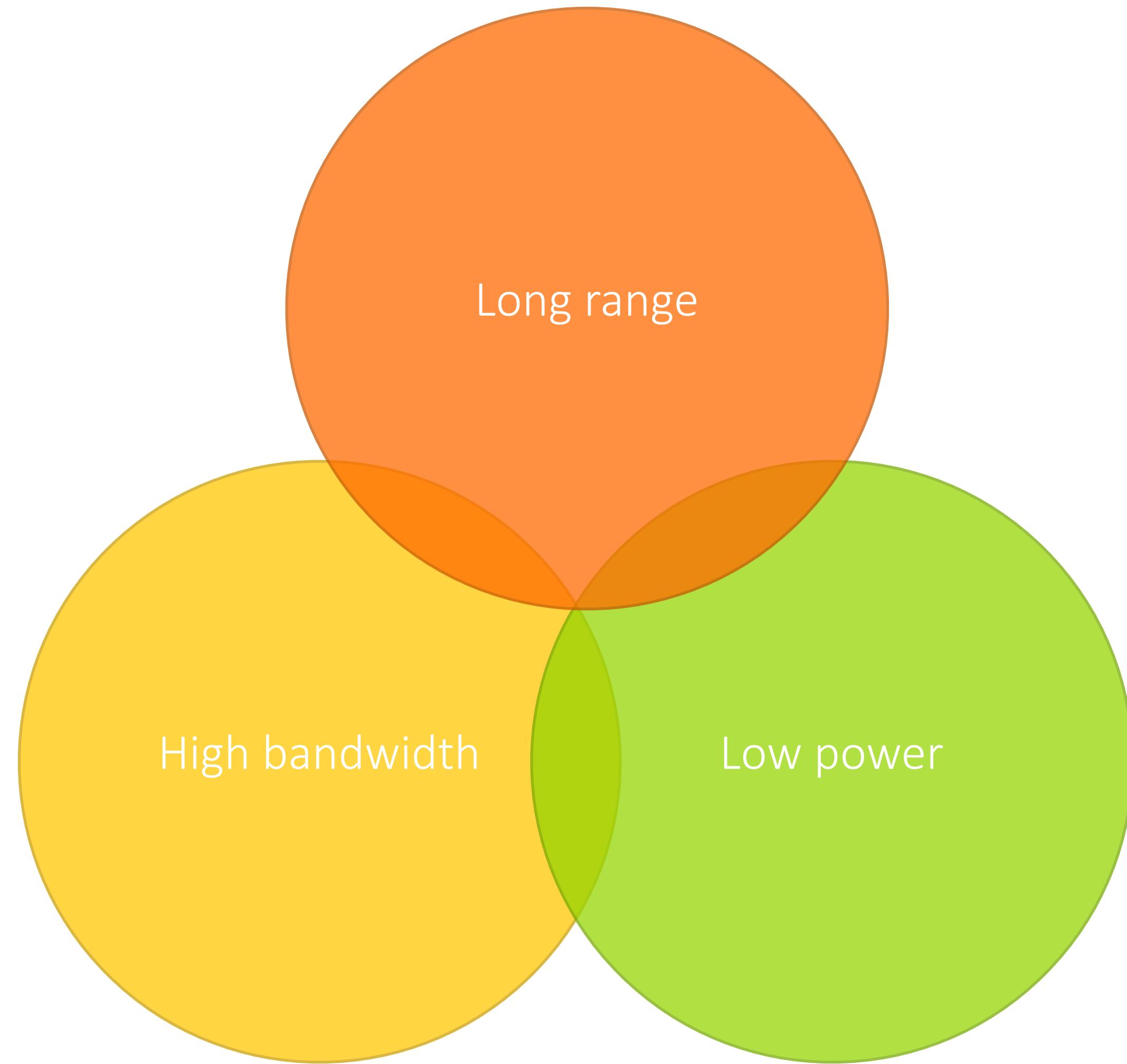
Ra



The case for LPWANs



Pick two



Many choices, same characteristics

LoRaWAN can achieve a 15 km range at power consumption levels low enough to enable 10-year battery life.

LoRaWAN

[...] works over a long distance (between 5 and 40km in open field) and is ultra low-power, with a battery life of 10 to 20 years.

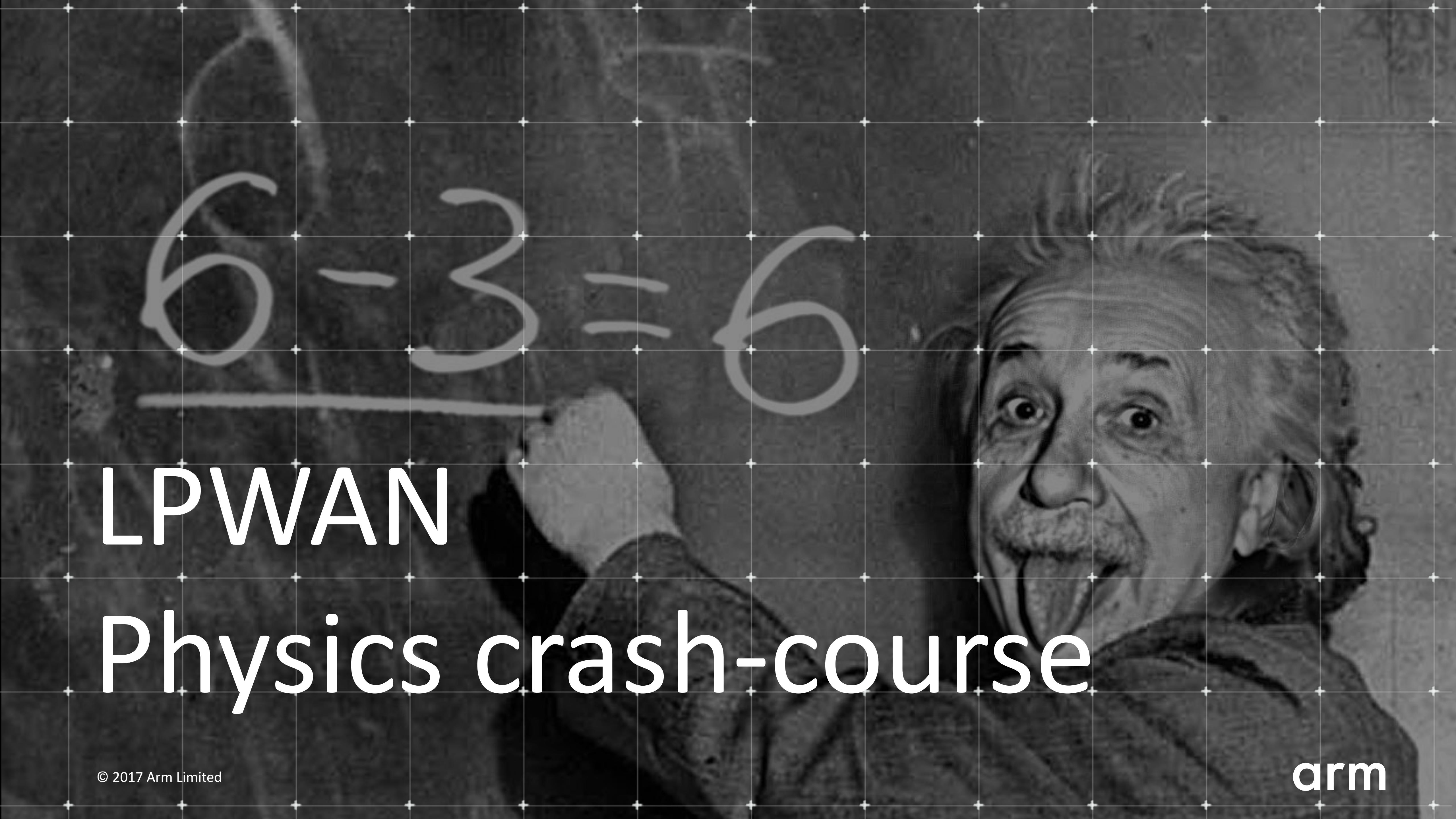
Sigfox

First cellular NB-IoT module combines easy, affordable, global connectivity with over 10 years' battery life for low data rate IoT applications.

NB-IoT

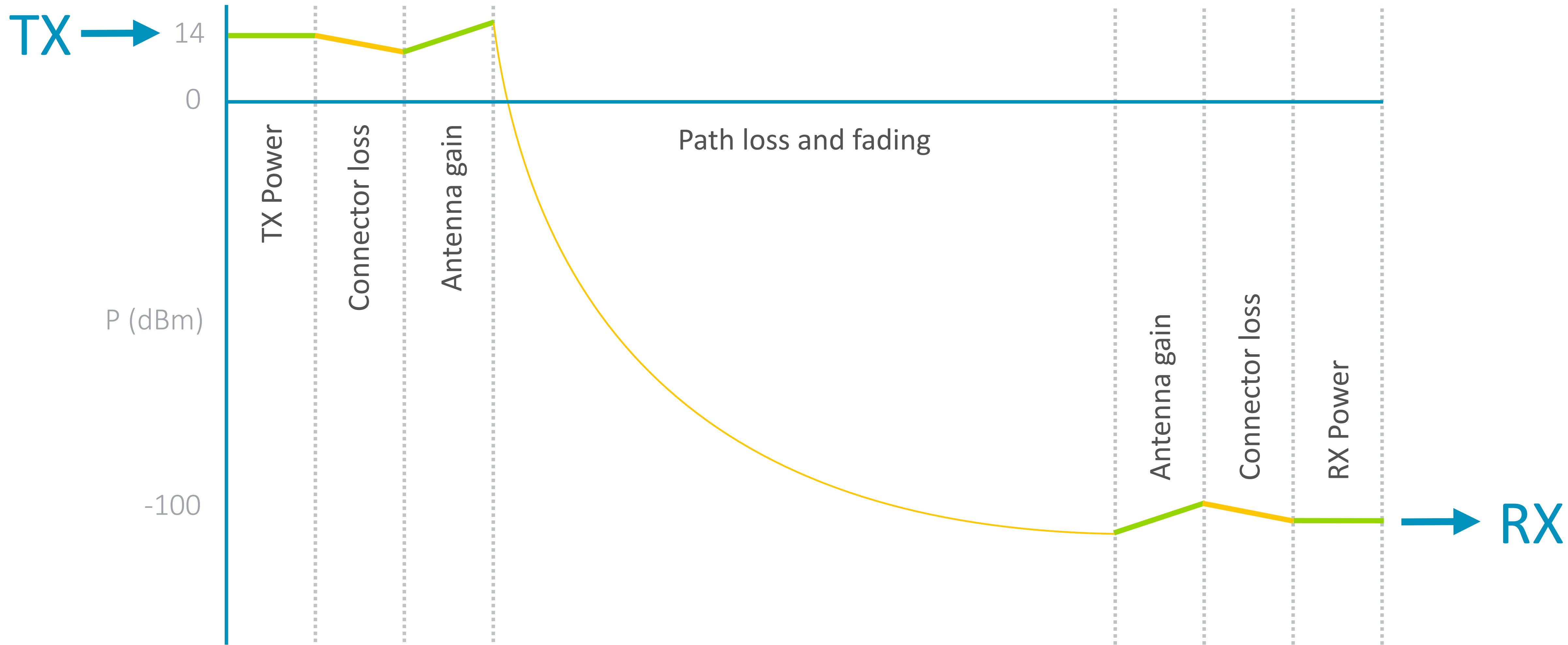
[...] free M2M / IoT communication using low power (10 years battery life) and cost-efficient hardware (\$2 hardware) offering a range of 5 to 10 km.

Weightless-P

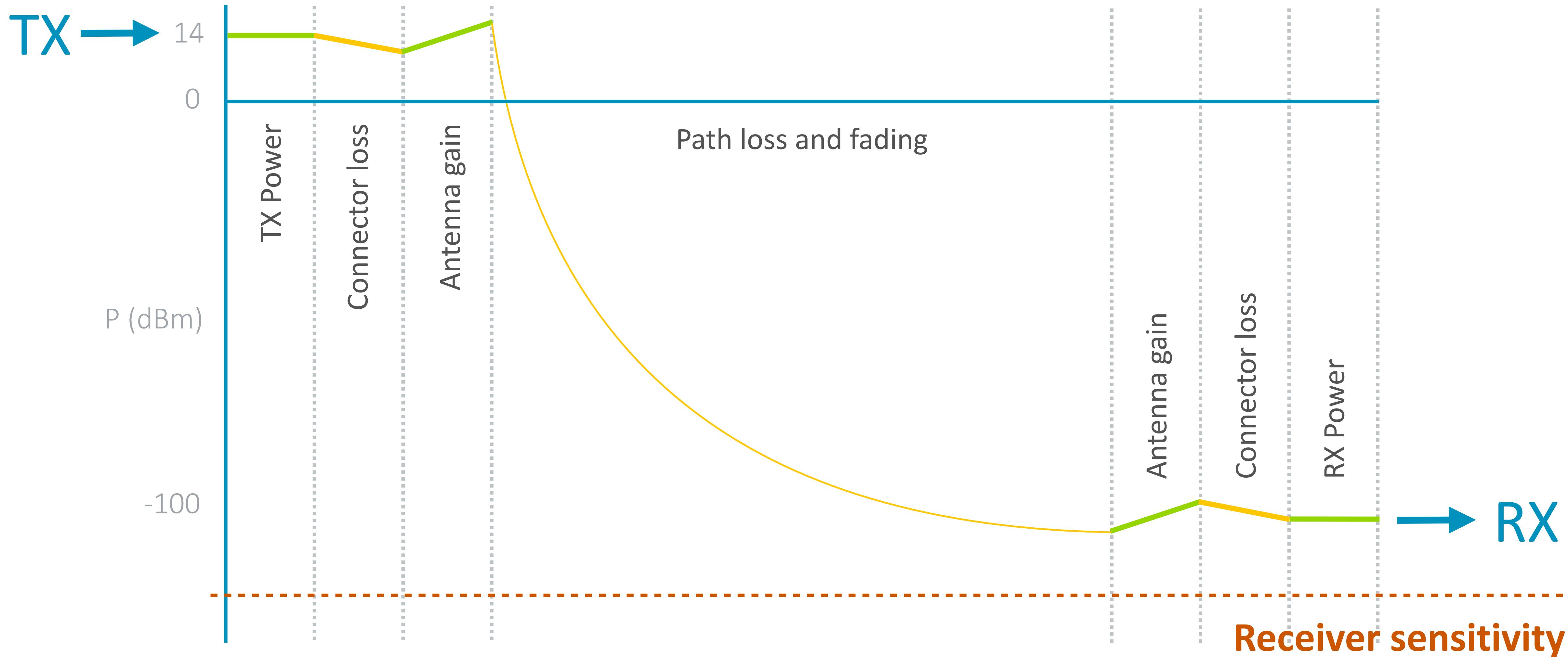


LPWAN Physics crash-course

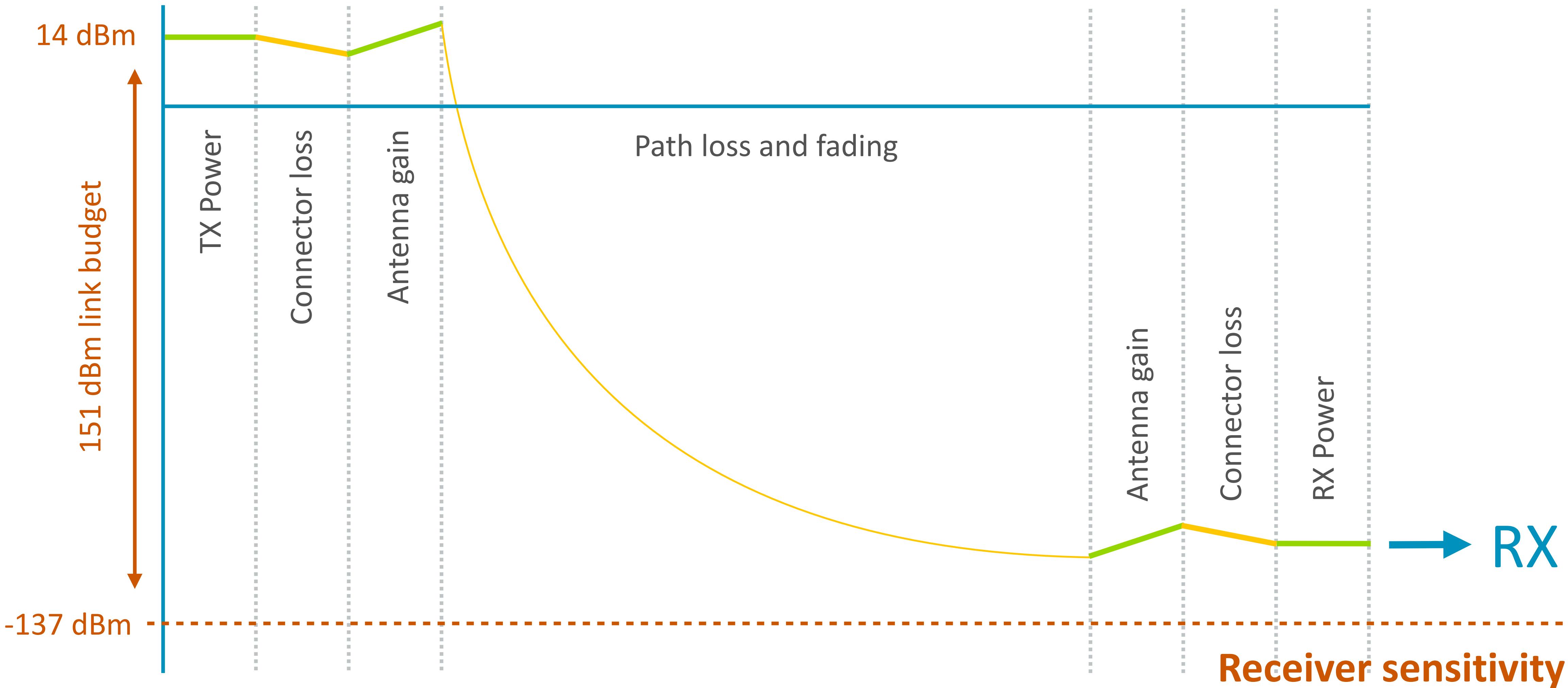
High link budget



High link budget



High link budget



Link budget

	TX Power	RX Sensitivity	Link budget
Wi-Fi	20.5 dBm	-75 dBm	95.5 dBm
Unlicensed LPWAN	14 dBm	-137 dBm	151 dBm
Licensed LPWAN	23 dBm	-129 dBm	152 dBm

$$FSPL = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r$$

Theoretical maximum in free space

2.4 GHz, with 95.5 dBm link budget:

550 meters

915 MHz, with 151 dBm link budget:

850,000 meters

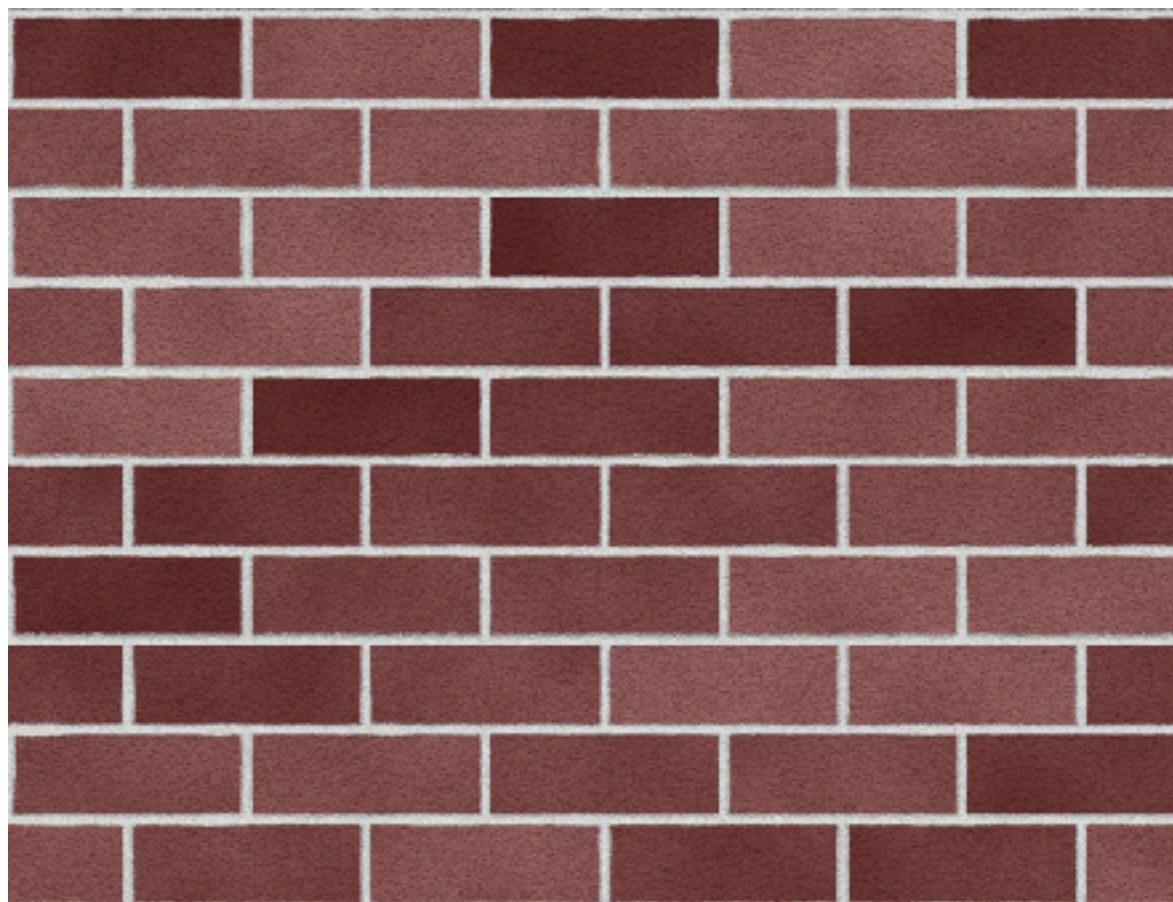
**Ground breaking world record! LoRaWAN
packet received at 702 km (436 miles) distance**



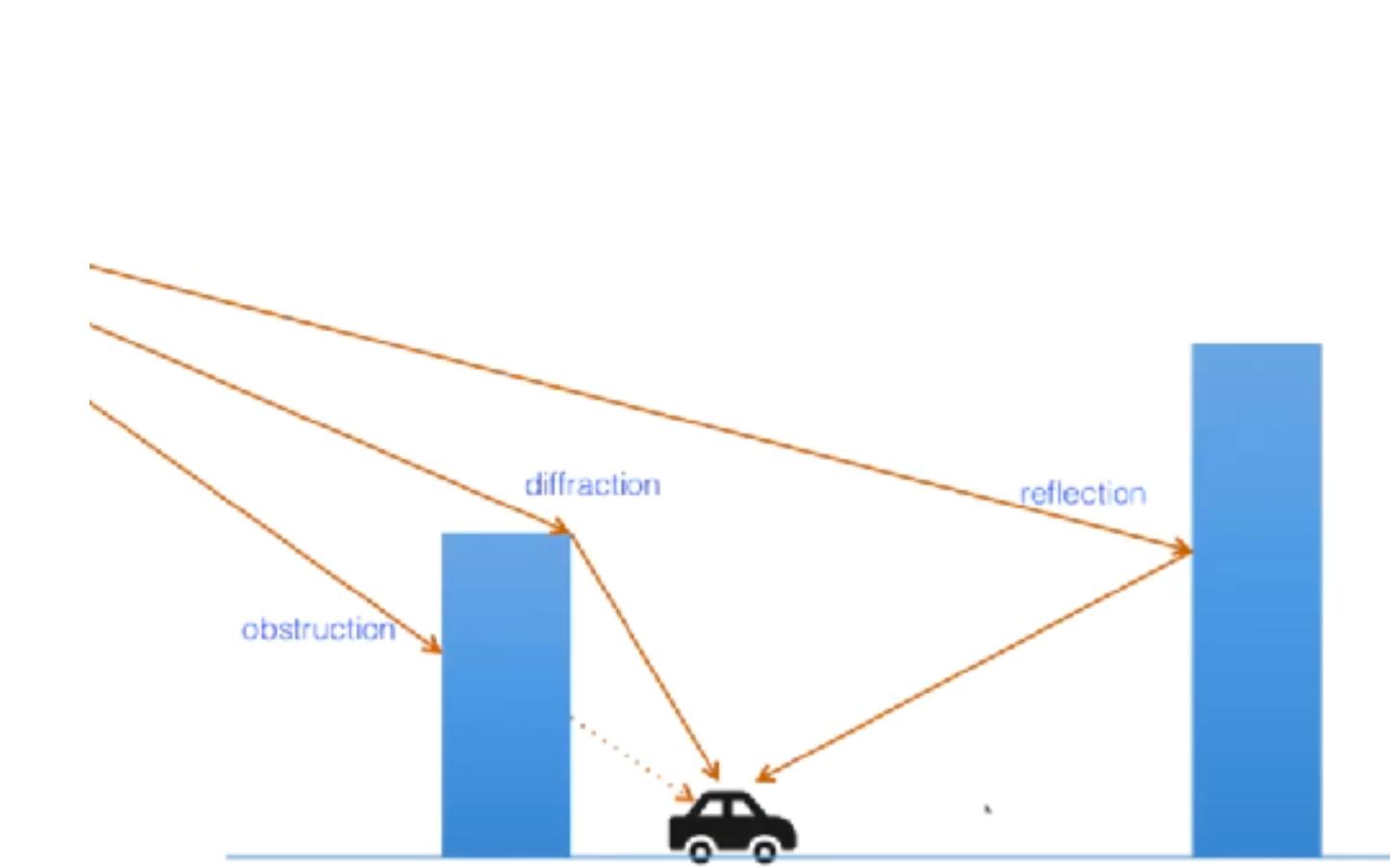
**THE THINGS
NETWORK**



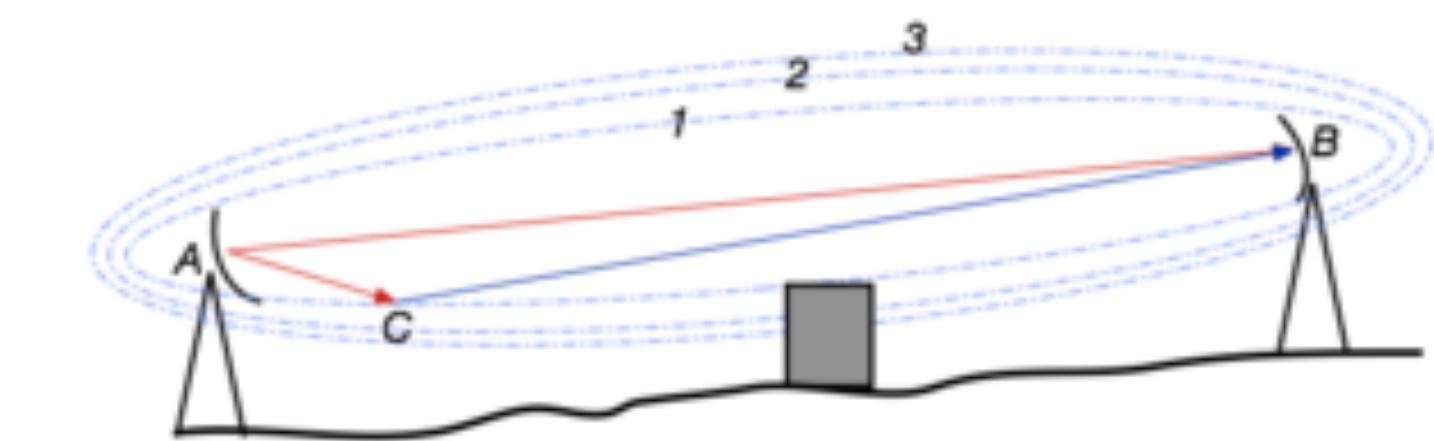
Unfortunately... we don't live in free space



Attenuation



Reflection and diffraction



Fresnel zone

Hata model

Based on Tokyo - model for calculating realistic path loss

	TX height	RX height	Range
Large city (250 bps)	0.1 m	40 m	4 km
Large city (1,760 bps)	0.1 m	40 m	2.5 km
Suburb (250 bps)	0.1 m	40 m	9 km
Suburb (250 bps)	1 m	100 m	13 km

A photograph of a woman sleeping aggressively. She has long brown hair and is wearing a dark green zip-up hoodie. Her mouth is wide open, showing her teeth, and her tongue is slightly out. She is lying on her side, facing right. In the background, there is a white chair and a blue object, possibly a book or a folder, on a surface.

Aggressive
sleeping

Transmit as little as possible

No gateway pinning

No keep-alive

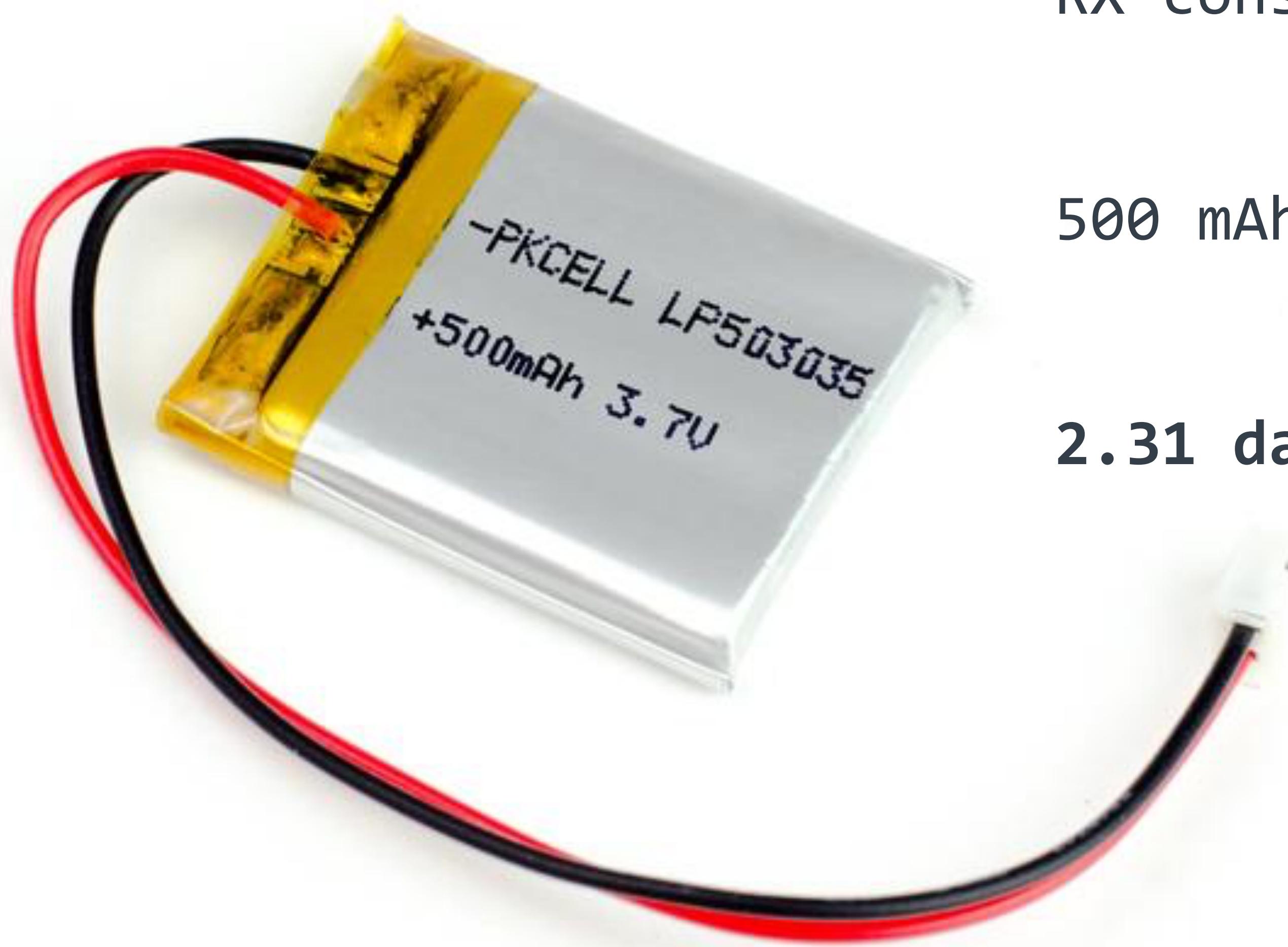
NB-IoT: 200 mW

Sigfox: 25 mW



<https://www.flickr.com/photos/pheezy/5875298232>

Listen as little as possible



RX consumption: 9 mA

$$500 \text{ mAh} / 9 \text{ mA} / 24\text{h} = 2.31 \text{ days}$$

2.31 days != 10 years

Relaying data back to device

LoRaWAN Class A, LTE-M Power Save Mode, Sigfox

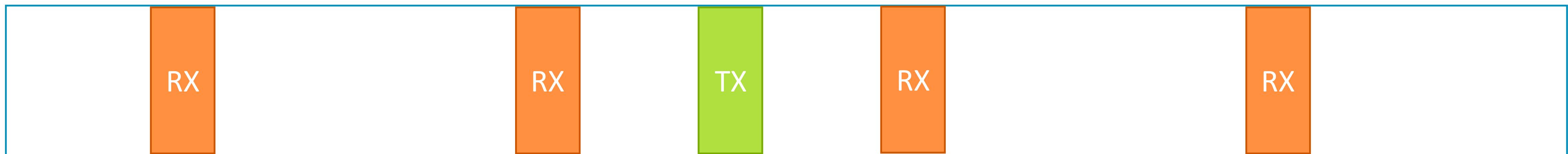


Relaying data back to device

LoRaWAN Class A, LTE-M Power Save Mode, Sigfox



LoRaWAN Class B, LTE-M EdRX



Tiny packets

No IP routing in packets

Security in message, not in transport layer

No TLS handshakes (6 messages, 6.5K data)

Small 13-14 byte header

Every byte counts!

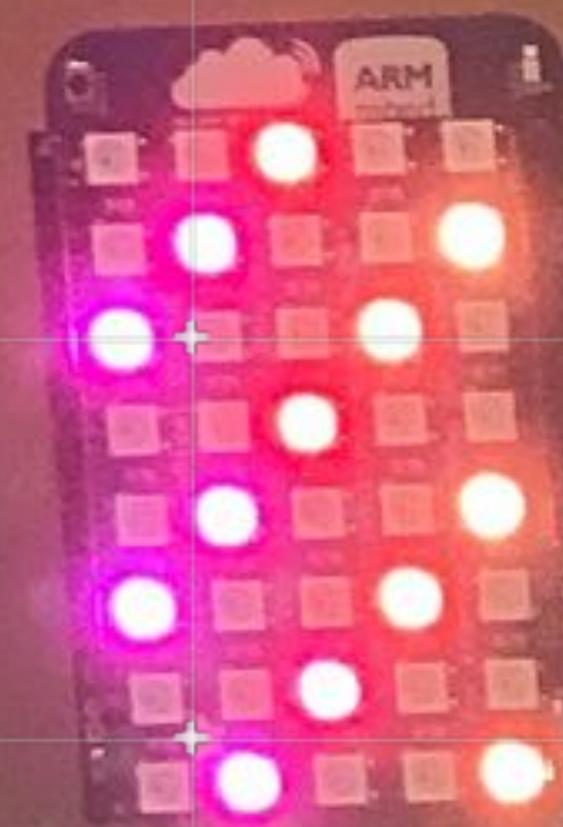


How to

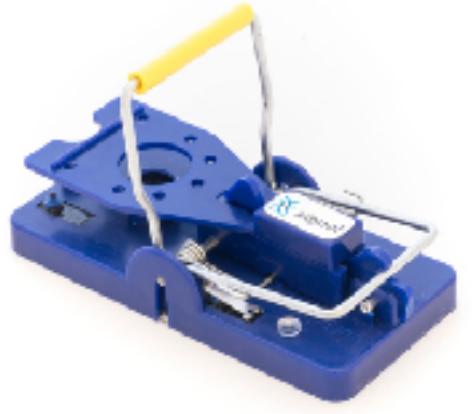
FIRMWARE UPDATES

BY THE THINGS NETWORK & ARM

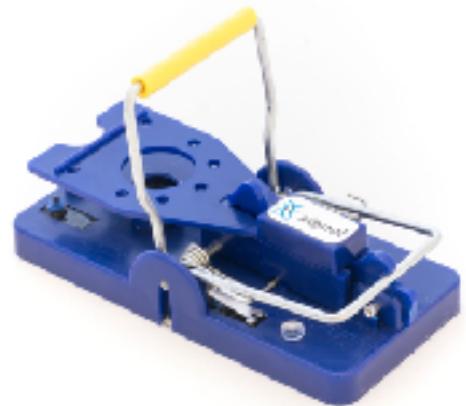
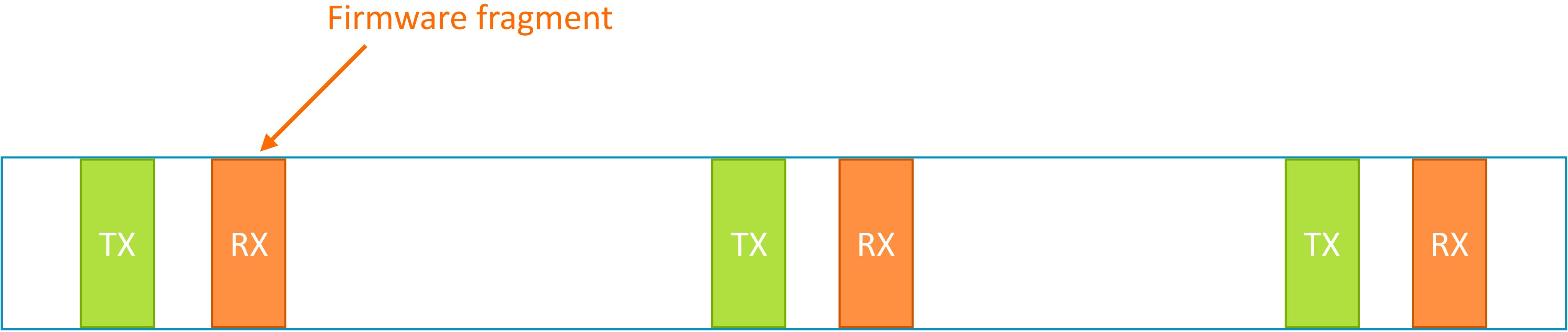
OVER
LORAWAN



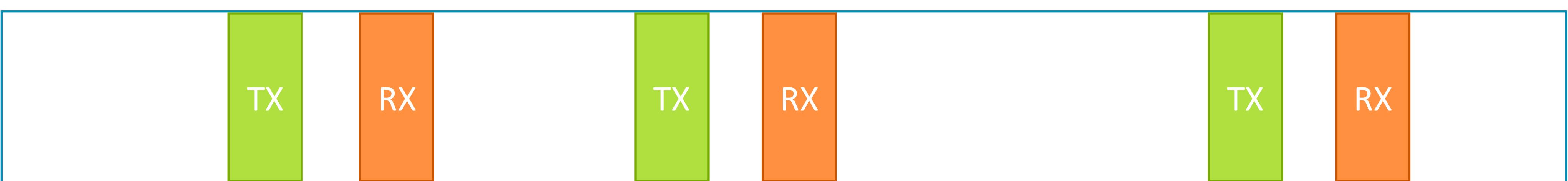
Naive approach



Device 1

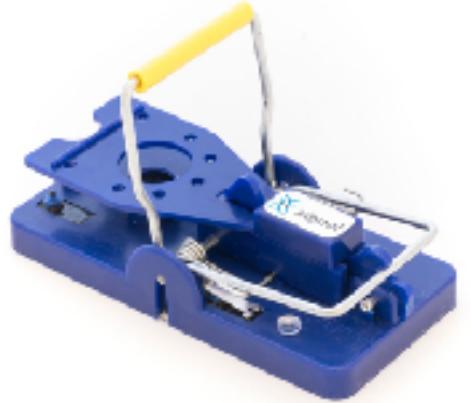


Device 2

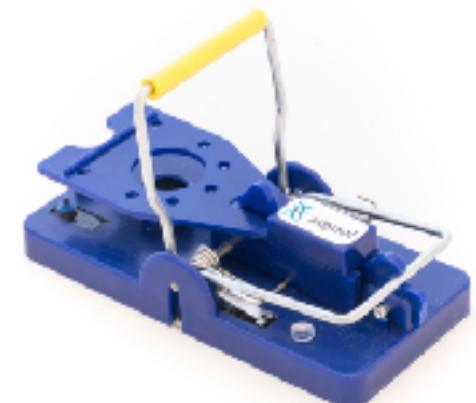


Very inefficient!

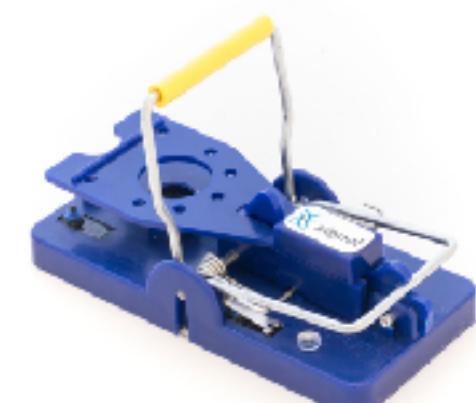
Better approach



Device 1



Device 2



Device N



But... how do we do this?

1. Instruct devices to use a new set of keys (same for everyone).
2. Instruct devices to wake up at the same time.
3. Gateway can transmit to all devices with one message.

Problem: low QoS and uni-directional

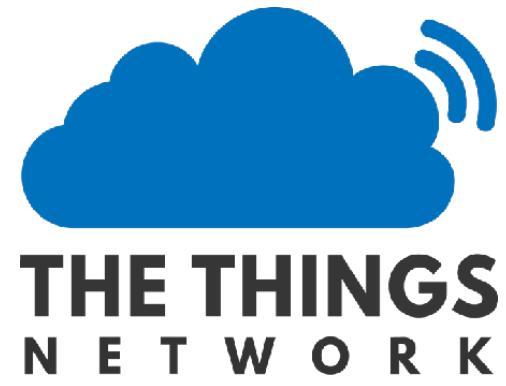
Setting up the device



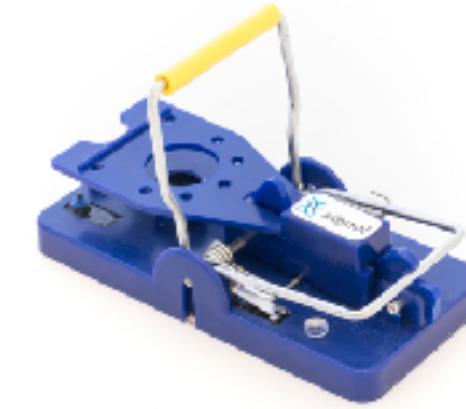
Device Address: 0xCF32AB09
Multicast Key: 9310E28FA291...



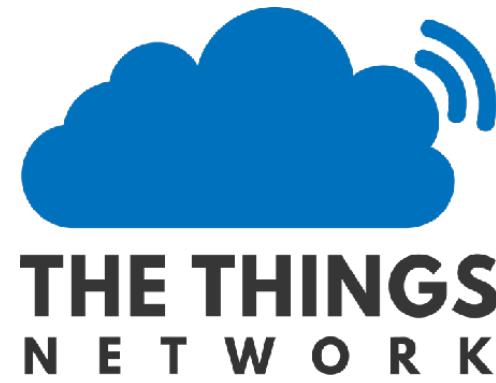
Setting up the device



Packet size: 204 bytes
Packet count: 491
Padding: 16 bytes

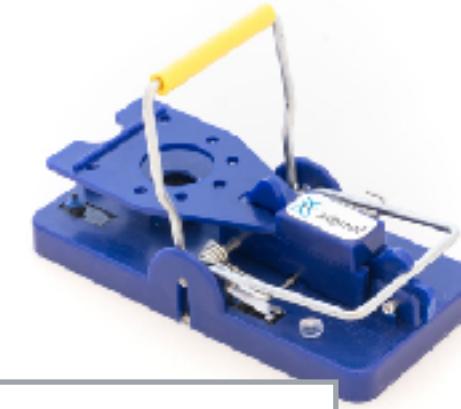


Starting multicast session



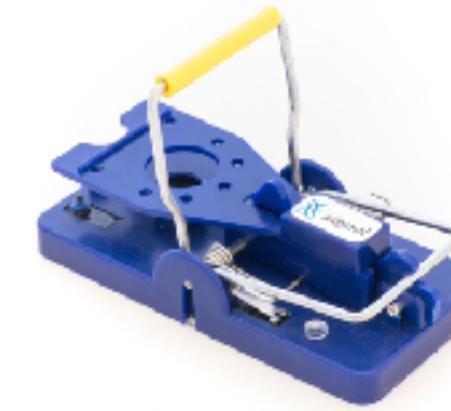
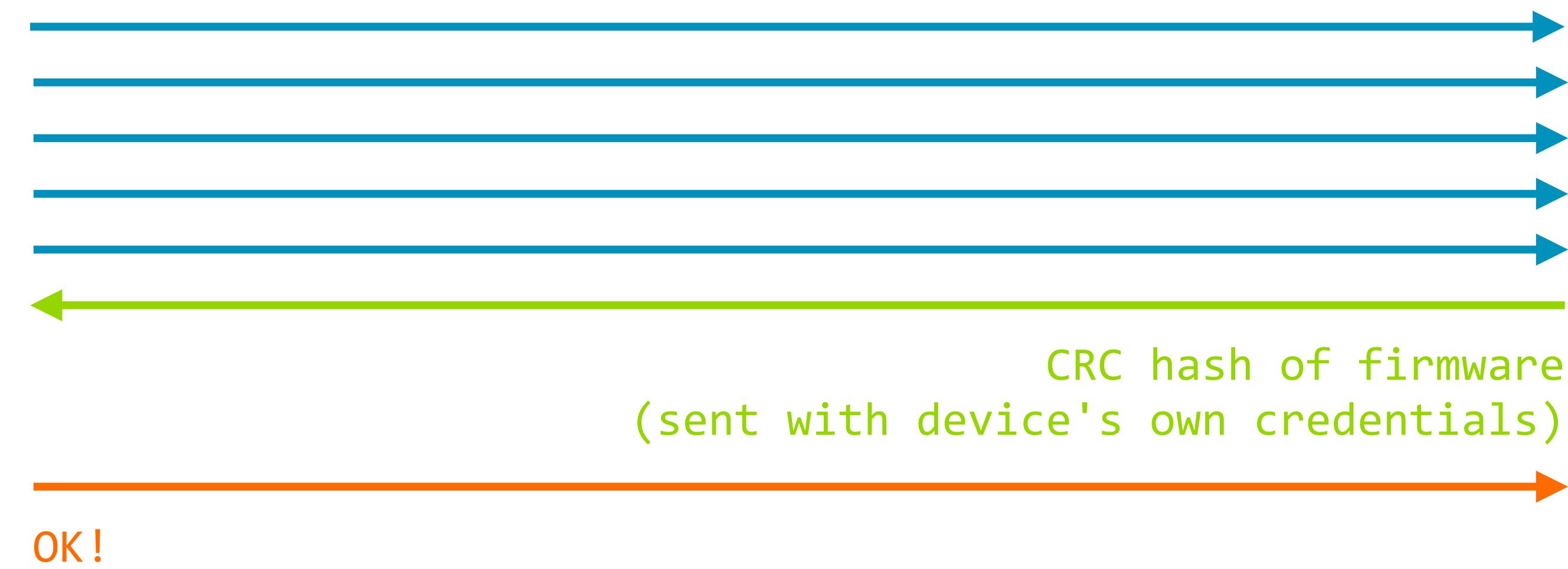
Frequency: 924.525 MHz
Data rate: 220 bytes / sec

Time to start: 812 sec after UL event 13



ULCounter		RTC
15		781
14		704
13		623
12		491
...		

Dealing with low QoS



Dealing with low QoS



Speed

220 bytes per second in real world scenario
(2.5KM range in cities)

180KB Firmware size, 30KB with delta updates

Transmission costs **3m30s** @ 10mA current



https://www.reddit.com/r/Eyebleach/comments/68r4rt/tortoise_taxi/

Network capacity required

Incremental update: 36 KB, no round robin, 10% packet loss

	Packets	Correction	Time p/p	Total time
<i>EU868 DR3 (SF9, 125 KHz)</i>	336	51	559 ms.	3m36s
<i>US915 DR11 (SF9, 500 KHz)</i>	170	25	262 ms.	2m09s

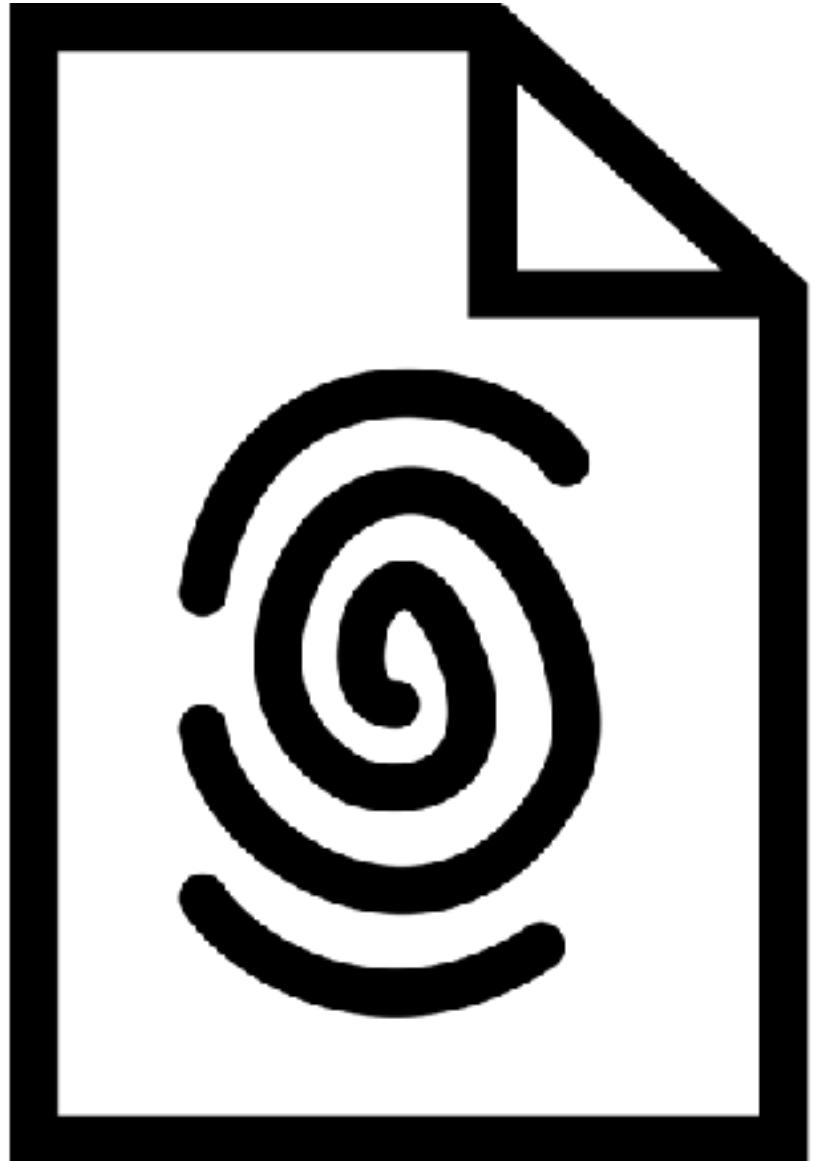
500 mAh battery, 15 mA RX current = **0.18%** of battery per update

Security



Picture by Yuri Samoilov <https://www.flickr.com/photos/yusamoilov/13334048894>

Link layer security is not enough



Firmware manifest

Contains firmware hash

Contains manufacturer and device class ID

Signed with private key

Separate trusted and non-trusted code

arm
TRUSTZONE

(Not yet implemented)

Bootloader support

New in Mbed OS 5.5

Bootloader verifies integrity,
preferably in non-writable flash

Tamper-proof secure element to
protect keys

The screenshot shows the arm MBED website's navigation bar at the top, featuring links for 'Developer Resources', 'Partners', and 'Cloud'. Below the navigation is a secondary menu with 'Hardware', 'Documentation', 'Code', 'Questions', and 'Forum' options, along with 'Log In/Signup' and 'Compiler' links. A blue header bar contains the text 'Blog » Firmware updates on mbed OS 5.5 with FlashIAP'.

Firmware updates on mbed OS 5.5 with FlashIAP

Last updated 12 days ago, by **Jan Jongboom**. [firmware](#), [Firmware Update](#)

The Dutch have a saying: "where people work, mistakes are made." This is a problem if the mistake involves thousands of IoT devices that have a critical bug or a gaping security hole, especially if these devices are on a remote island or baked into concrete. Therefore, every Internet of Things deployment needs to remotely upgrade firmware securely and safely. To help developers build these firmware update capabilities into their devices, we have added new APIs and tools to Arm Mbed OS 5.5.

<https://os.mbed.com/blog/entry/firmware-updates-mbed-5-flashiap/>

Caveats

Network congestion

Sending a lot of data has negative effect on network

Higher data rate is better

RX sensitivity is useless when someone screams next to you

Spread spectrum helps against narrowband interference

Spectrum regulations in EU

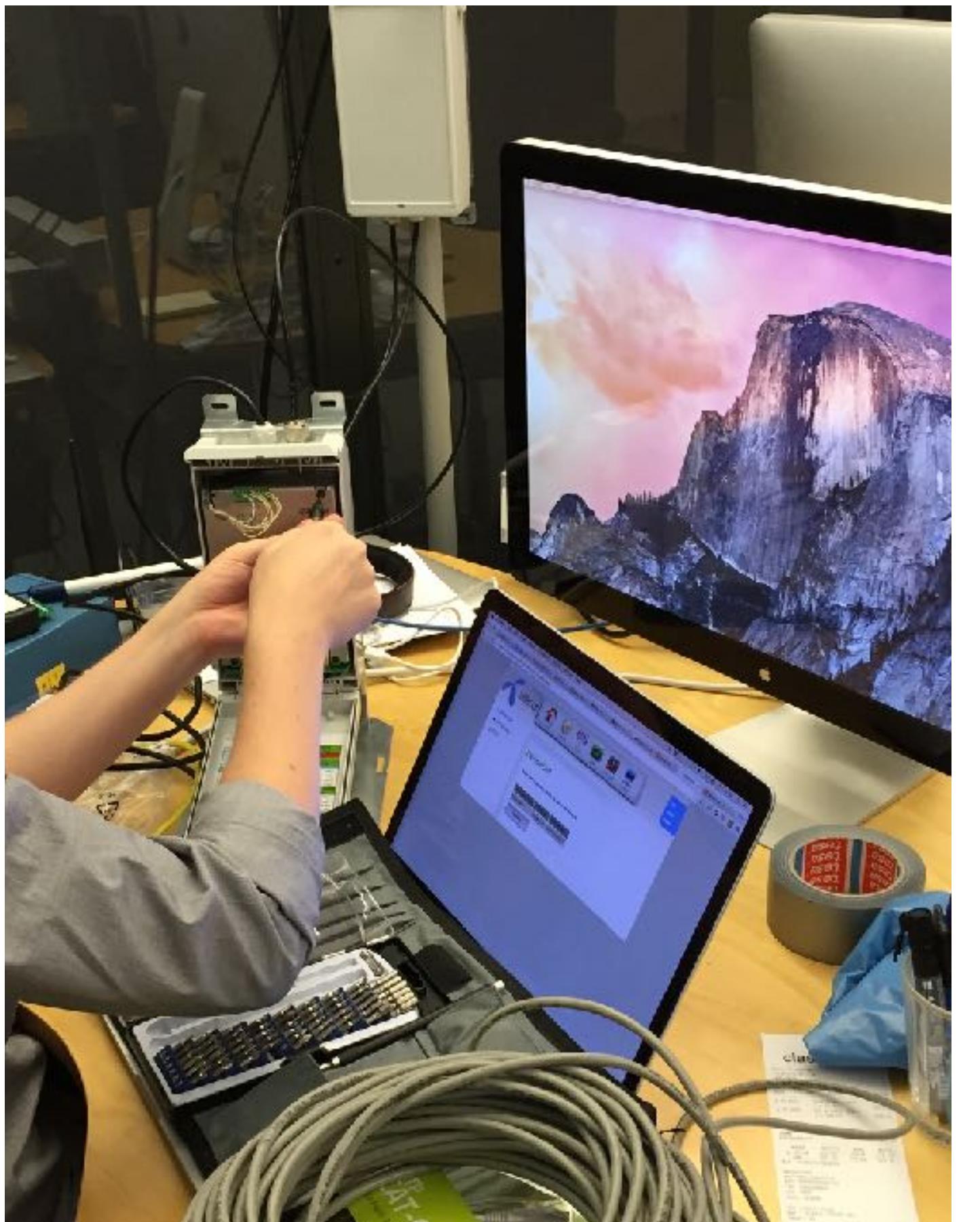
Unlicensed does not mean unregulated

1% duty cycle in 868 MHz band, except at 869.525 MHz

Downside: it's the RX2 channel

Round-robin between gateways

Drive over to site and deploy temporary gateway



US is both better and worse

Better

No duty cycle

Wider channels (500 KHz vs. 125 KHz)

Faster

Worse

400 ms. dwell time

915 MHz band is used for a lot of other stuff, lower QoS



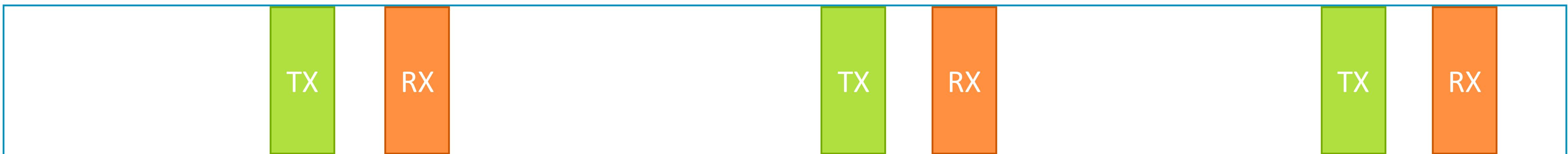
Applicability for non-LoRa networks

Multicast

RX is cheaper than TX

Many LPWANs use same principle as LoRaWAN

Might not be needed in licensed spectrum



The Sigfox issue



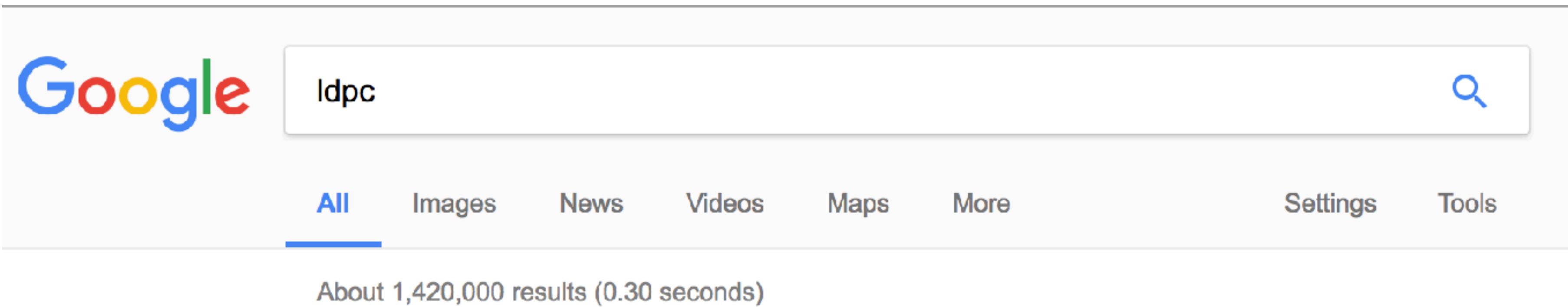
Designed as TX only, modulation needs SDR
RX added at later point, simple modulation scheme
Link budget to device is way lower (20 dBm)

Forward error correction

Applicable to every LPWAN

Removes delivery guarantee in link layer

Also usable in non-LPWAN, f.e. over UDP



Firmware update service

Re-usable for any protocol

Must-have for any IoT device

For IP devices: Mbed Cloud



A photograph of four young women of diverse ethnicities laughing and holding hands in a confetti shower. They are outdoors, surrounded by greenery and colorful confetti. The woman on the far left has dark hair and is wearing a grey top. The woman next to her has long brown hair and is wearing a white top. The woman in the center has short blonde hair and is wearing a white top. The woman on the far right has dark hair and is wearing a grey top. They are all smiling and laughing, creating a joyful and celebratory atmosphere.

Current state

Reference implementation

Multi-Tech xDot (Cortex-M3, 32K RAM)

LoRaWAN 1.02

mbed OS 5.5

Network server by The Things Network



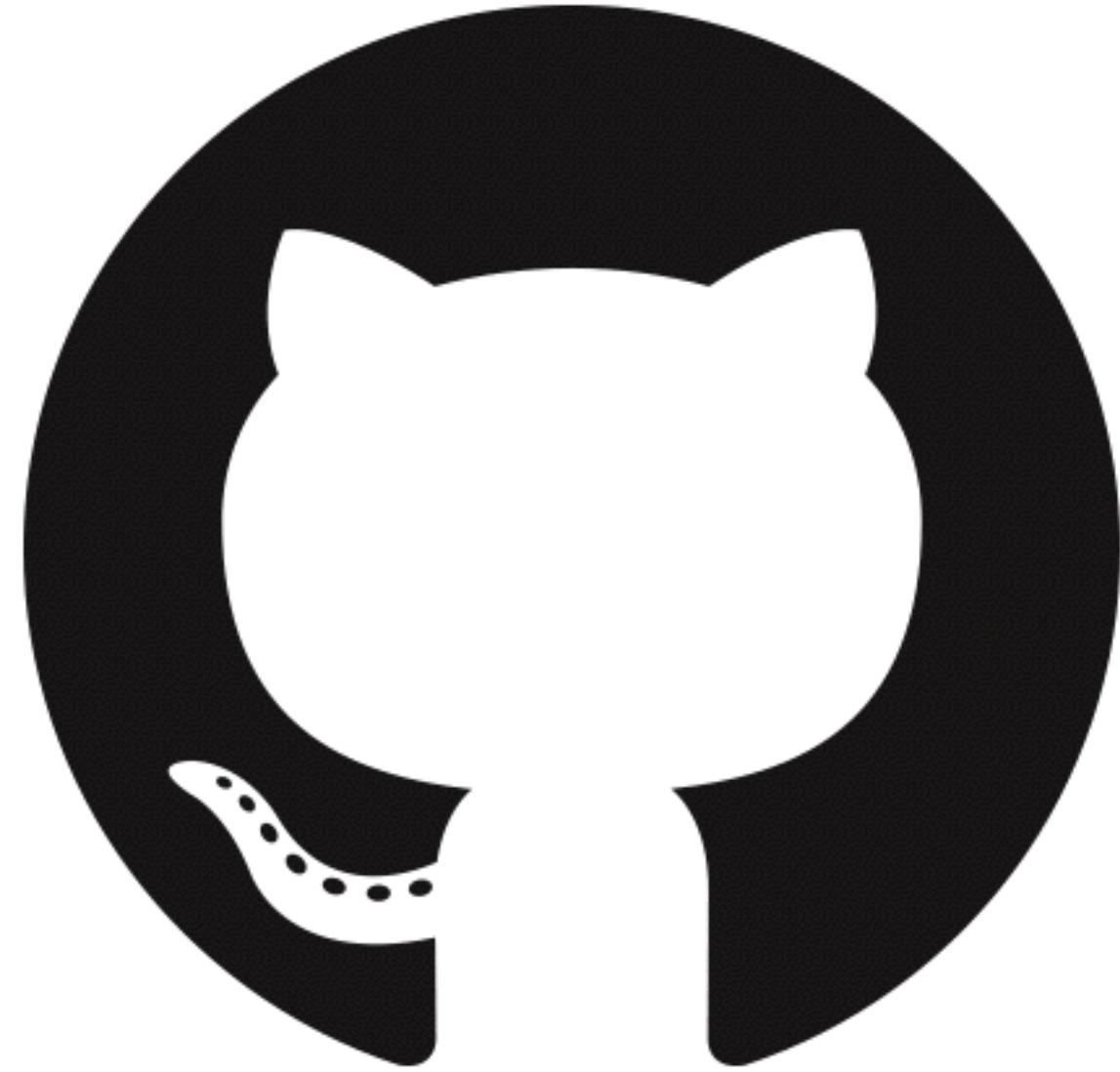
Client + bootloader

Open source

Apache 2.0

Available on GitHub

Very little security!



Secure bootloader and cryptographically secure update service available as licensable IP from Arm.

Forward error correction

C++ library available on GitHub

Uses less than 2K of RAM, flash as storage layer

<https://github.com/janjongboom/mbed-lorawan-frag-lib/>

Standardization work

LoRa Alliance meeting last week

Two specs: 'multicast' and 'data block' specs

Aiming to standardize in next LoRaWAN standard

Specifications are available for LoRa Alliance members

A scenic landscape featuring the Old Man of Storr, a prominent sea stack on the Isle of Skye in Scotland. The foreground shows rugged, grassy hillsides with patches of snow. In the background, a large body of water meets a cloudy sky at sunset, with the sun's light reflecting off the water.

Reference implementation:

<https://github.com/ArmMbed/fota-lora-radio>

Demo: <http://bit.ly/lora-update-demo>

Thank You!

Danke!

Merci!

谢谢!

ありがとう!

Gracias!

Kiitos!

감사합니다

ধন্যবাদ

arm

<http://bit.ly/lora-update-demo>

arm

The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks