Enabling firmware updates over LPWAN

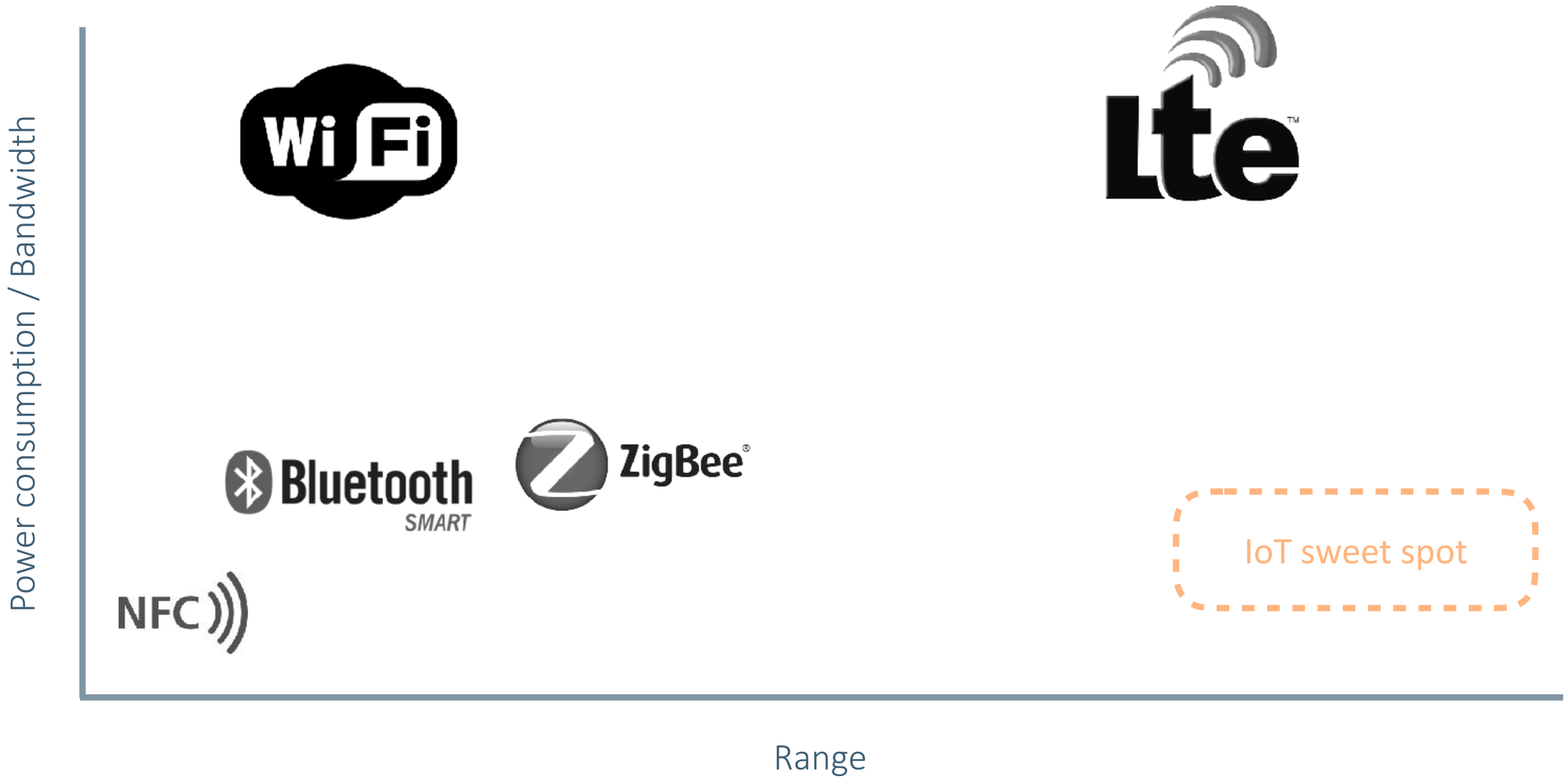
Jan Jongboom | Developer Evangelist | Arm

Arm TechCon 2017


NM-AIST
Data Science 2017 (DSA 2017) - Summer School & Workshop
17th - 21st July, 2017 at NM-AIST, Arusha
PULSE LAB KAMPALA
The University Of Sheffield
ARMmbed
twas
MOUSER

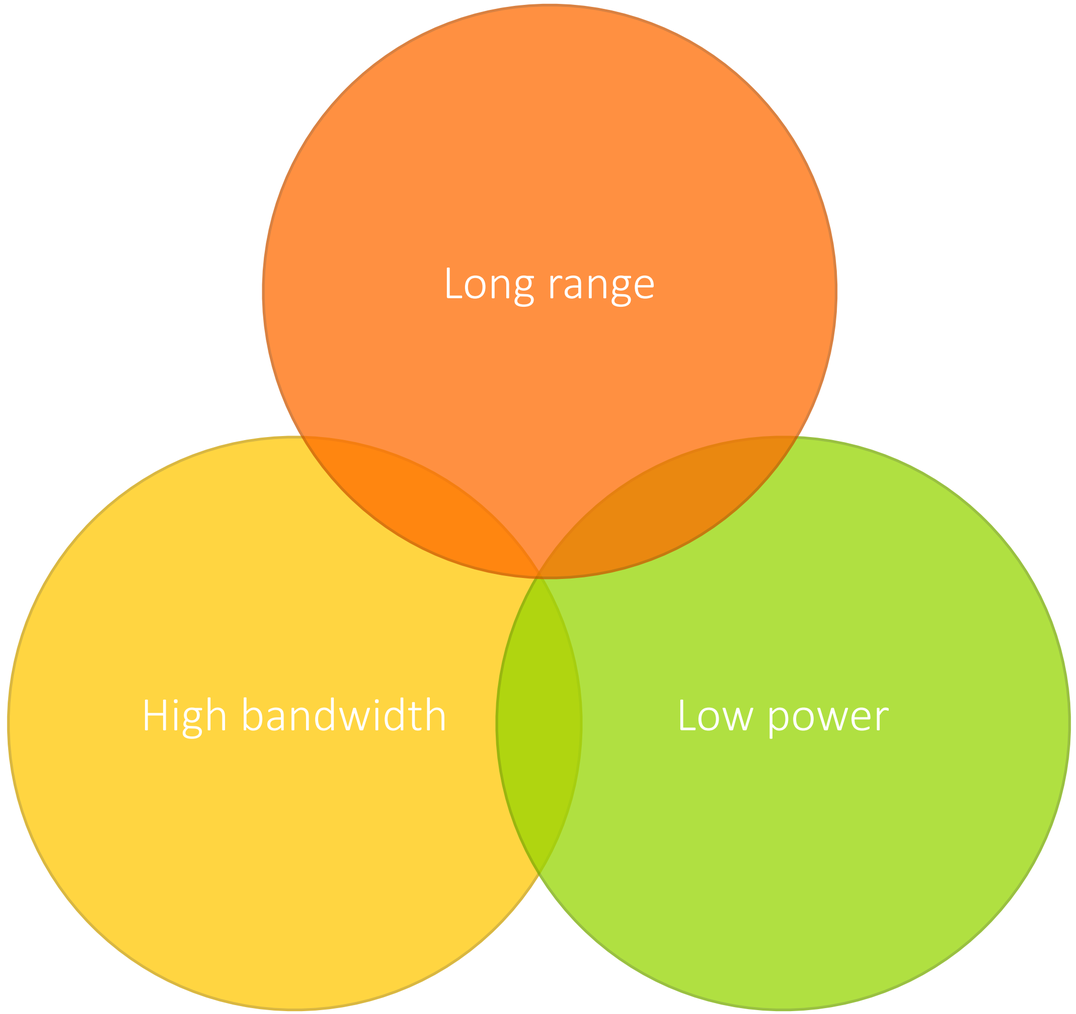

LoRa™
LoRa Alliance
THE THINGS NETWORK & ARM

The case for LPWANs



arm

Pick two



arm

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

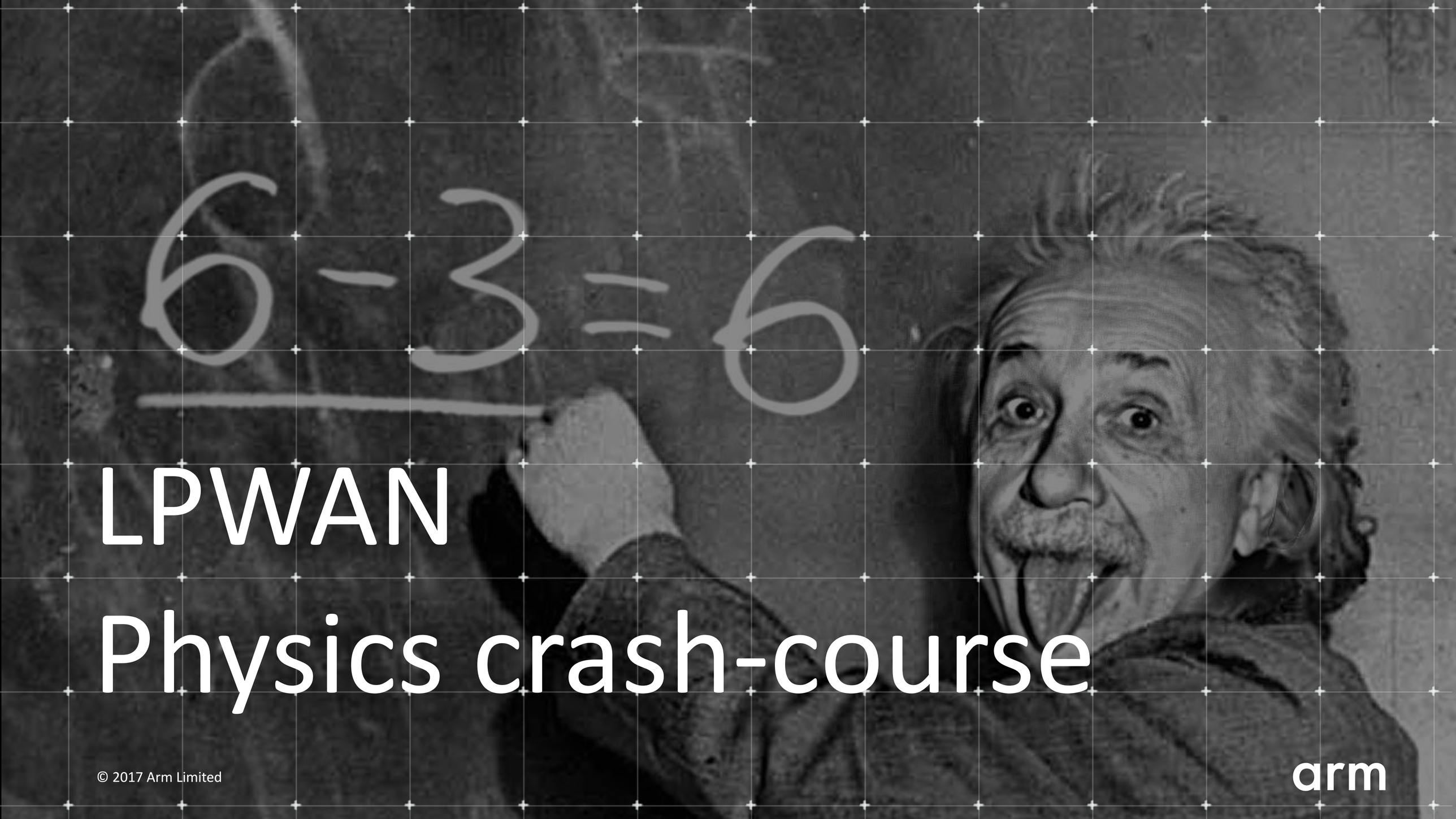
First cellular NB-IoT module combines easy, affordable, global connectivity with over 10 years' battery life for low data rate IoT applications.

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

arm

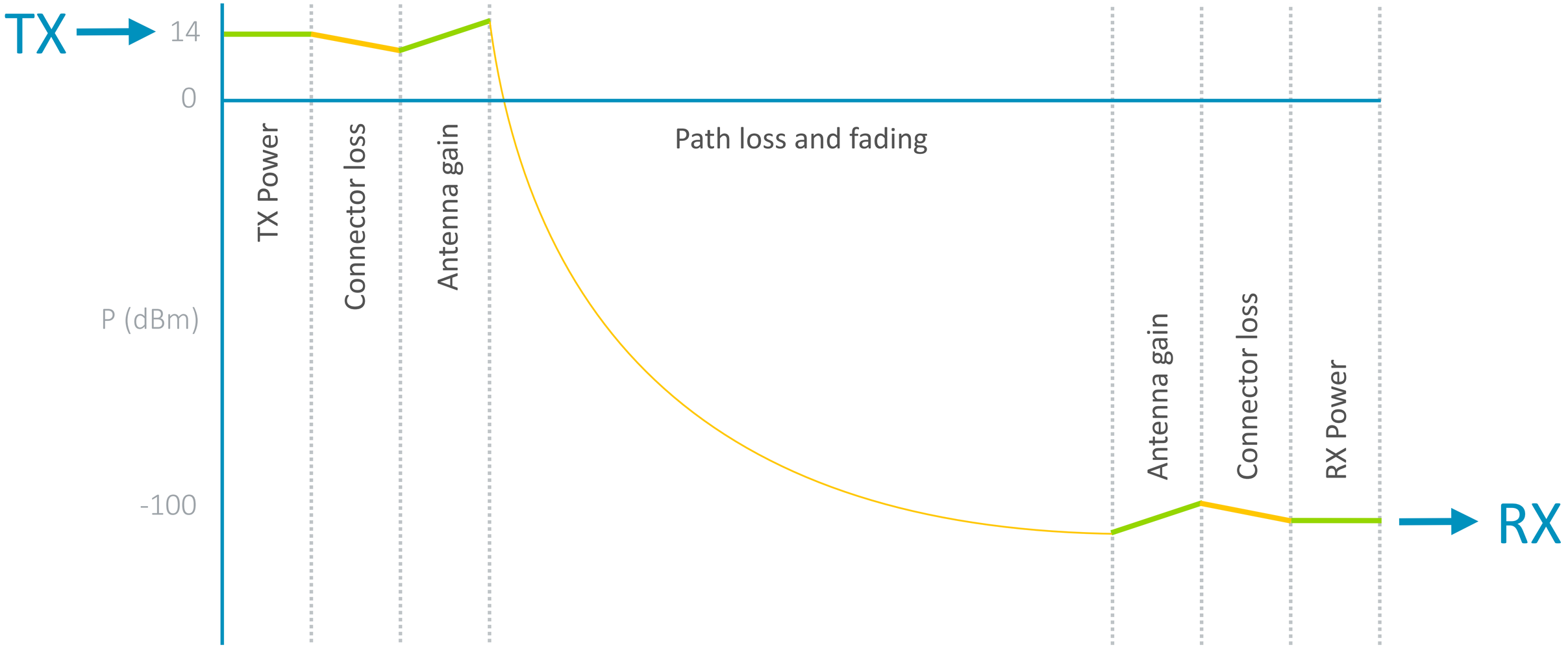


LPWAN
Physics crash-course

arm

Derived from work by Thomas Telkamp

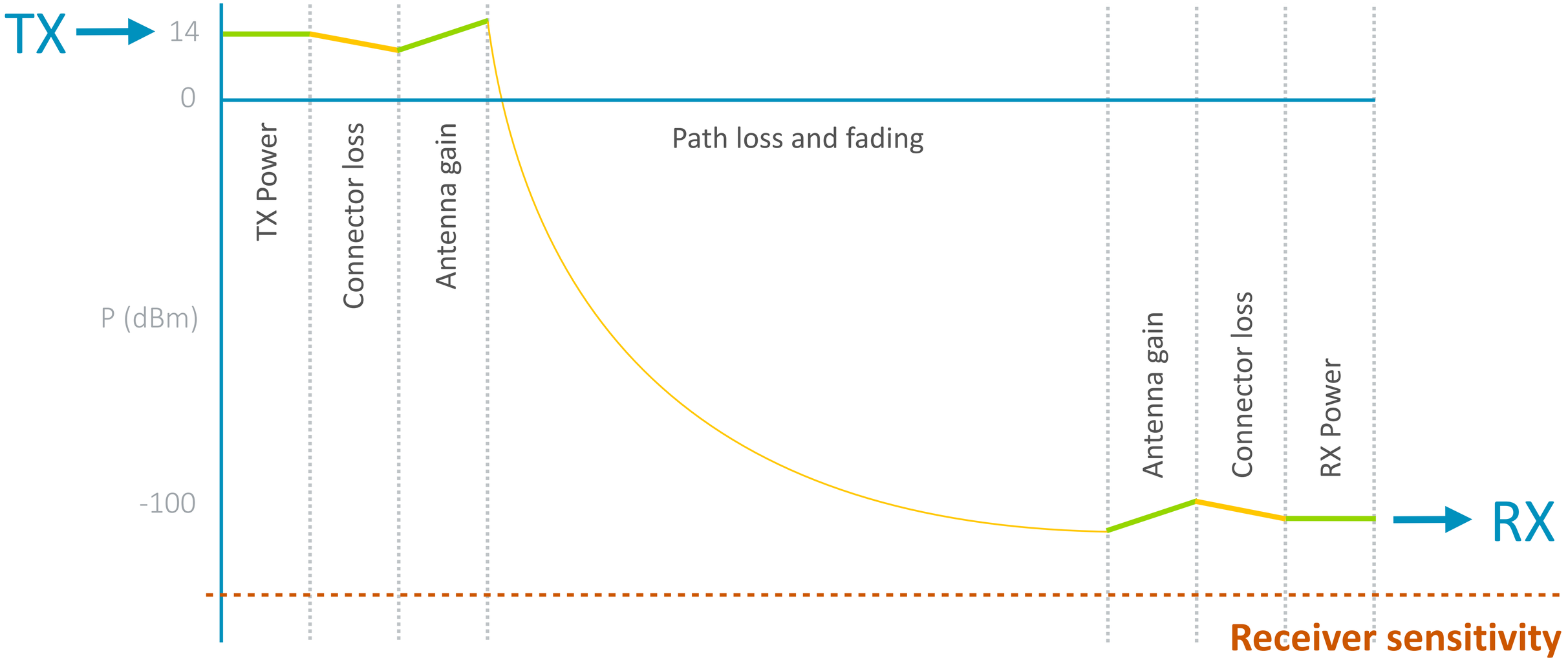
High link budget



arm

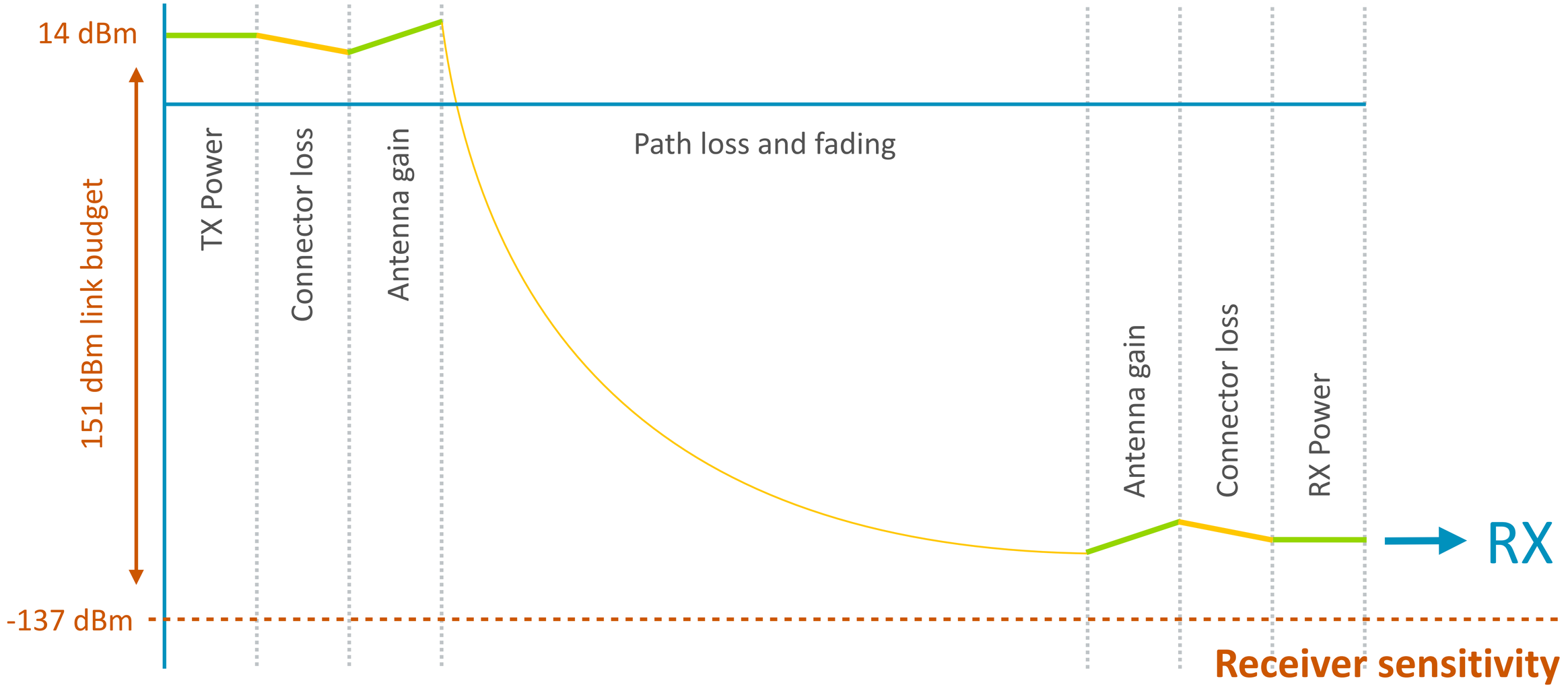
Derived from work by Thomas Telkamp

High link budget



arm

High link budget



arm

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**

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

arm

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

arm

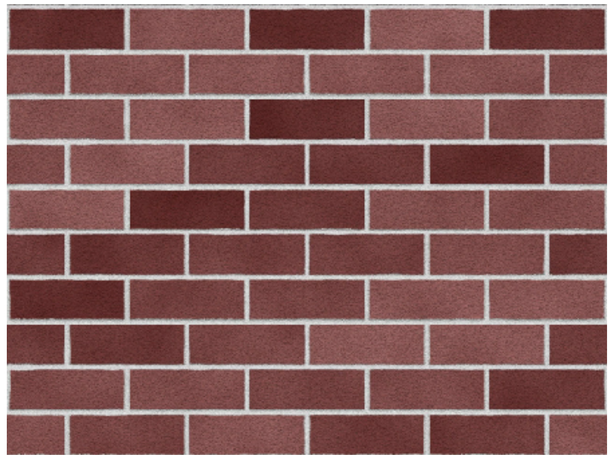
THE THINGS NETWORK COMMUNITIES LABS LEARN FORUM SHOP Hi armmbed

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

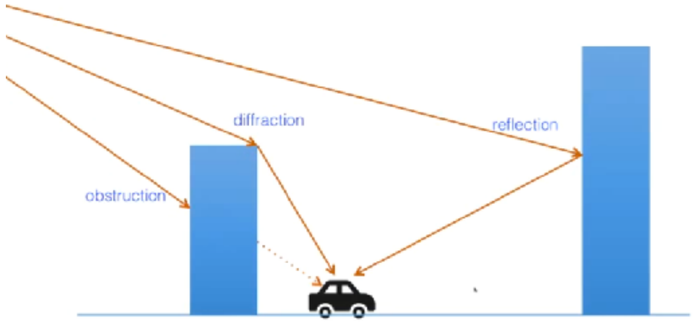
THE THINGS NETWORK

arm

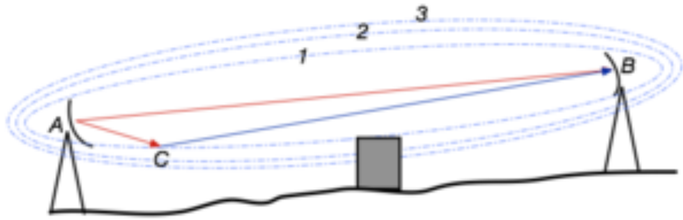
Unfortunately... we don't live in free space



Attenuation



Reflection and diffraction



Fresnel zone

arm

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**

Picture by Moyan Brenn: https://commons.wikimedia.org/wiki/File:Tokyo_(16043023330).jpg

arm

Aggressive sleeping

https://www.flickr.com/photos/aaronjacobs/64368770

arm

Transmit as little as possible

No gateway pinning

No keep-alive

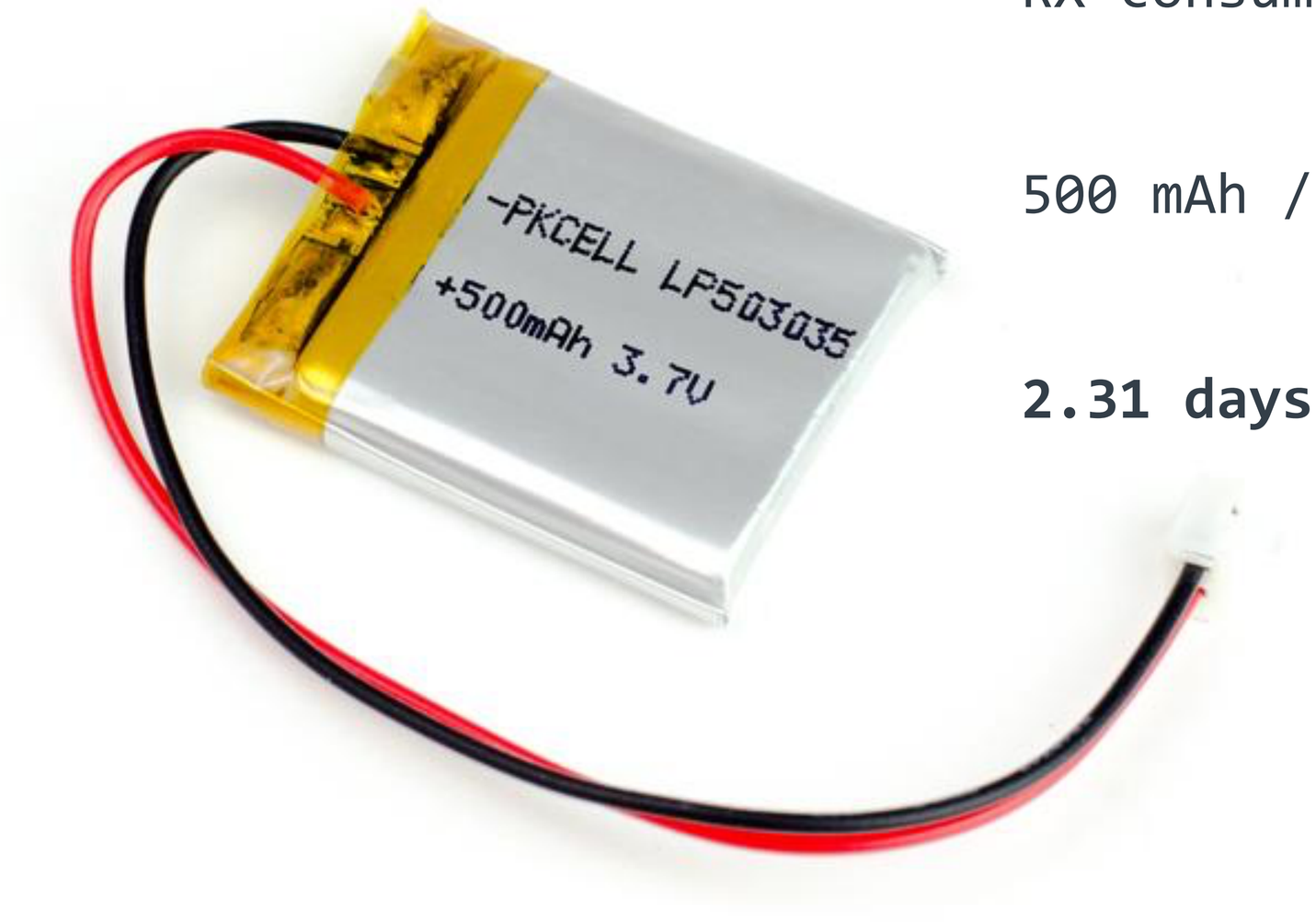
NB-IoT: 200 mW

Sigfox: 25 mW

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

arm

Listen as little as possible



RX consumption: 9 mA

500 mAh / 9 mA / 24h = 2.31 days

2.31 days !== 10 years

arm

Relaying data back to device

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

arm

Relaying data back to device

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

LoRaWAN Class B, LTE-M EdRX

arm

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

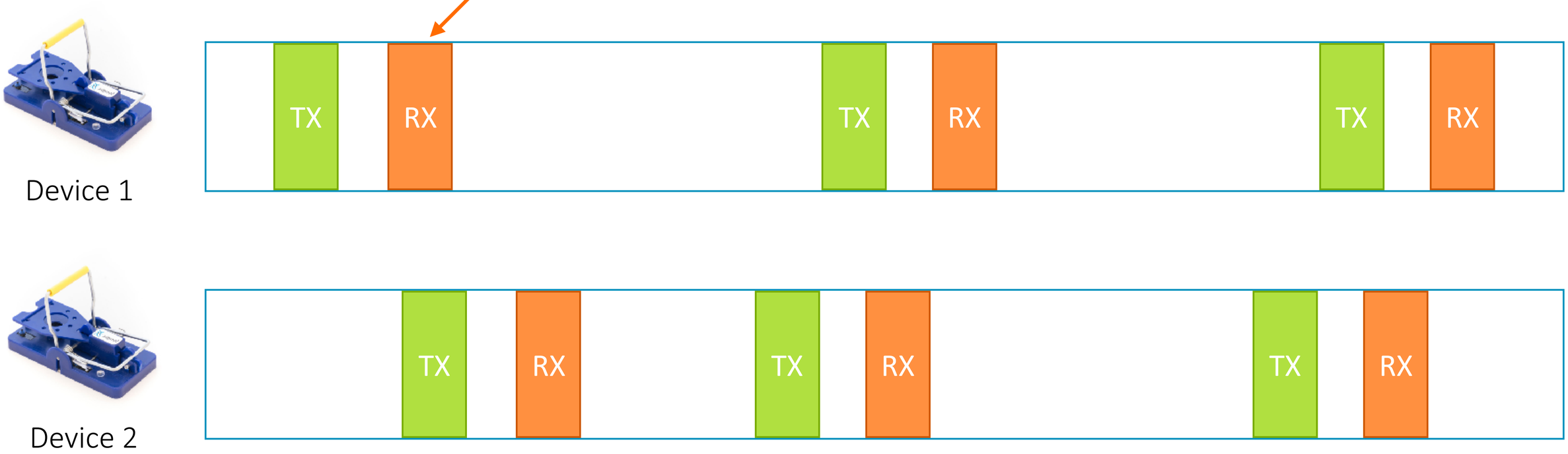
Every byte counts!

arm

How to

arm

Naive approach

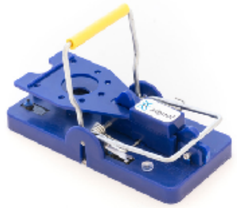


Very inefficient!

arm

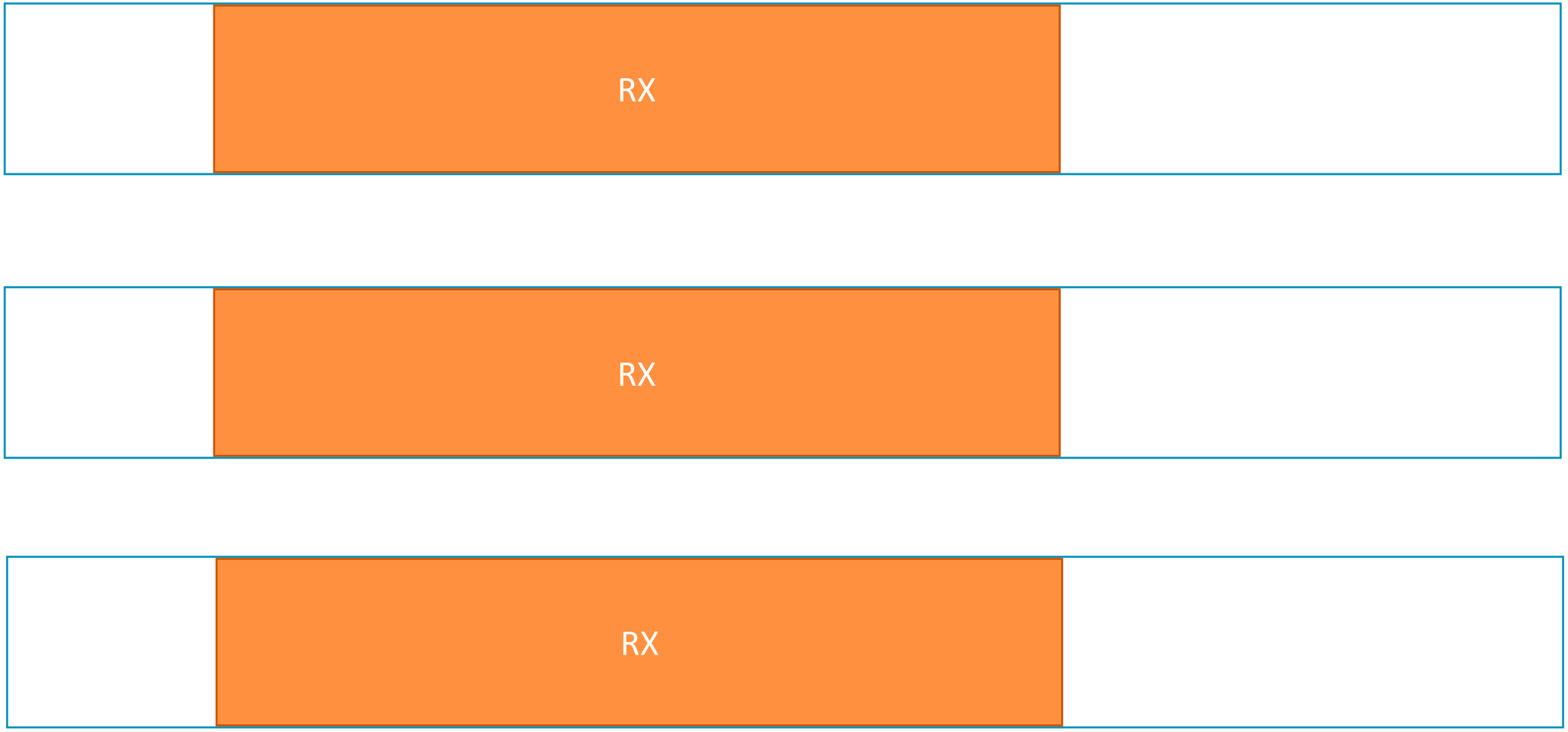
Better approach

Device 1



Device 2

Device N



arm

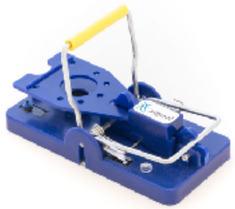
But... how do we do this?

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

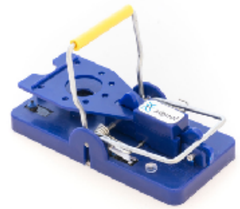

```
Device Address: 0xCF32AB09
Multicast Key:  9310E28FA291...
```



arm

Setting up the device


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

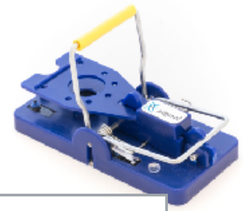


arm

Starting multicast session

```
Frequency:      924.525 MHz
Data rate:      220 bytes / sec

Time to start:  812 sec after UL event 13
```

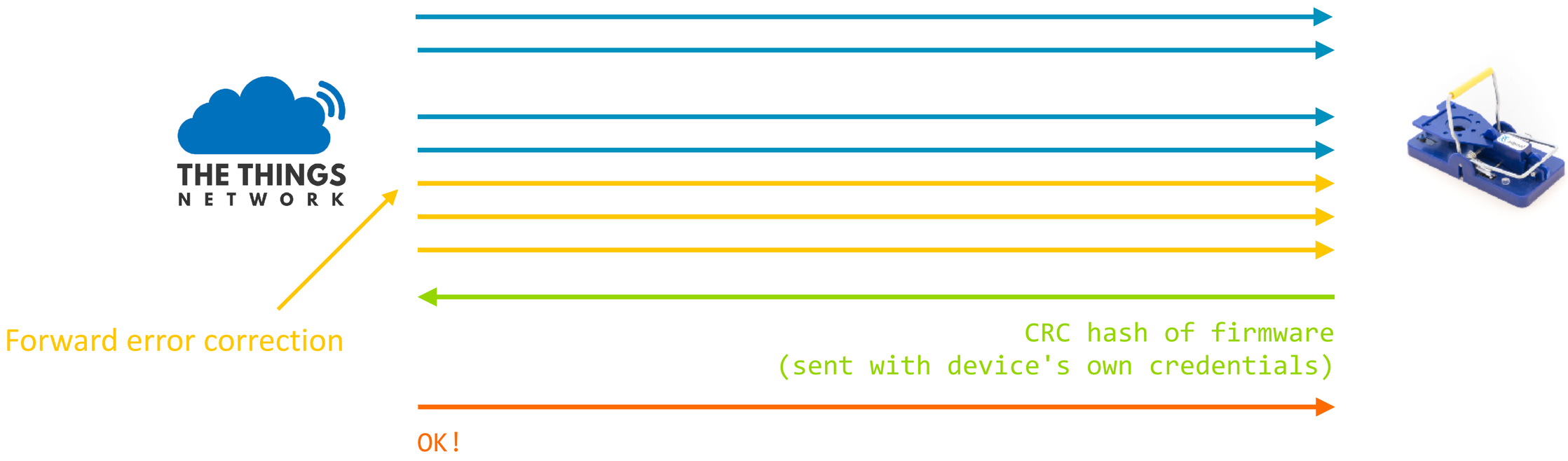


ULCounter	RTC
15	781
14	704
13	623
12	491
...	

Dealing with low QoS

arm

Dealing with low QoS



http://www.inference.phy.cam.ac.uk/mackay/gallager/papers/ldpc.pdf

arm

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
EU868 DR3 (SF9, 125 KHz)	336	51	559 ms.	**3m36s**
US915 DR11 (SF9, 500 KHz)	170	25	262 ms.	**2m09s**

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

arm

Security

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

arm

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

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

arm

Caveats

http://www.totalprosports.com/wp-content/uploads/2013/04/first-pitch-fail-baseball-fail-gifs.gif

arm

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

arm

Spectrum regulations in EU

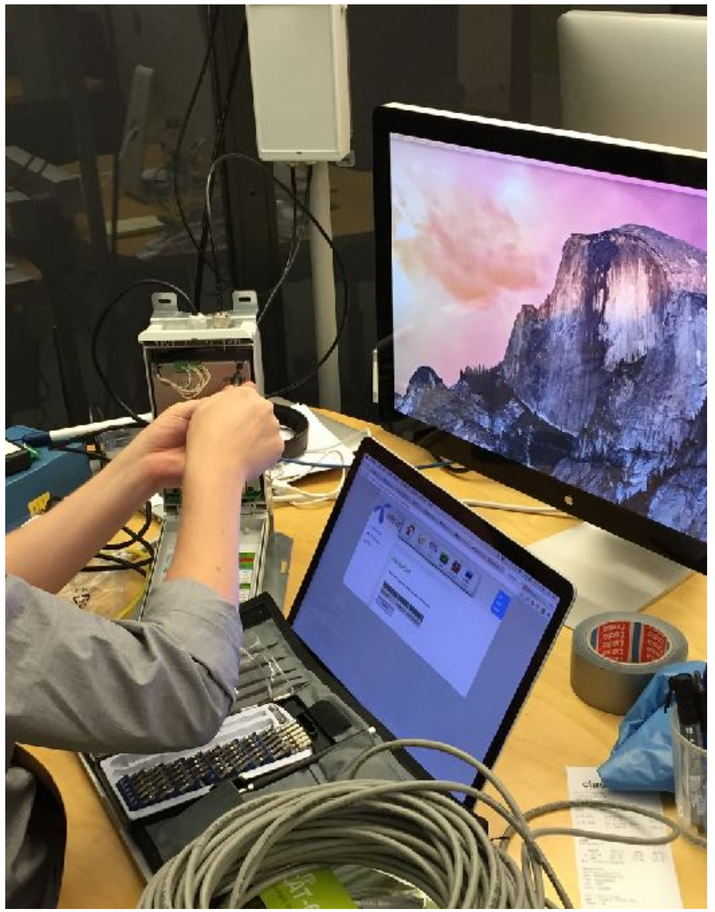
Unlicensed does not mean unregulated

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

arm

Applicability for non-LoRa networks

https://en.wikipedia.org/wiki/Computer_network#/media/File:Internet_map_1024.jpg

arm

Multicast

RX is cheaper than TX

Many LPWANs use same principle as LoRaWAN

Might not be needed in licensed spectrum

arm

The Sigfox issue

Designed as TX only, modulation needs SDR

RX added at later point, simple modulation scheme

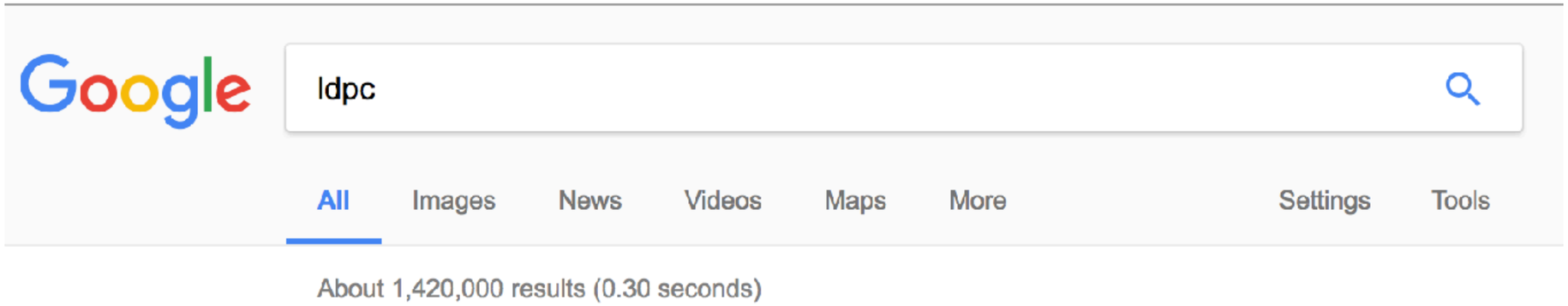
Link budget to device is way lower (20 dBm)

Forward error correction

Applicable to every LPWAN

Removes delivery guarantee in link layer

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



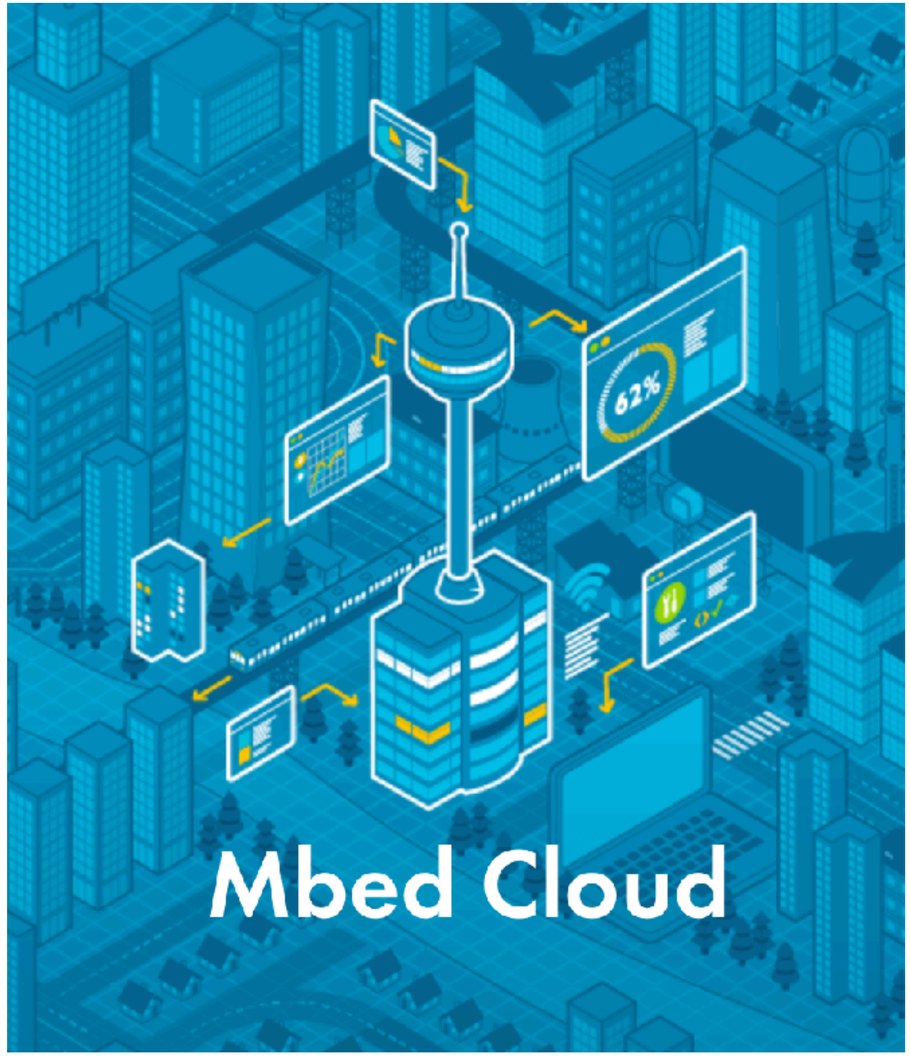
arm

Firmware update service

Re-usable for any protocol

Must-have for any IoT device

For IP devices: Mbed Cloud



arm

Current state

arm

Reference implementation

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

LoRaWAN 1.02

mbed OS 5.5

Network server by The Things Network

arm

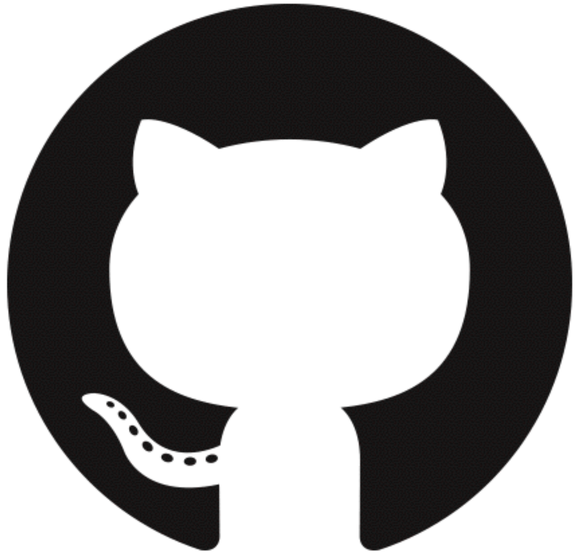
Client + bootloader

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

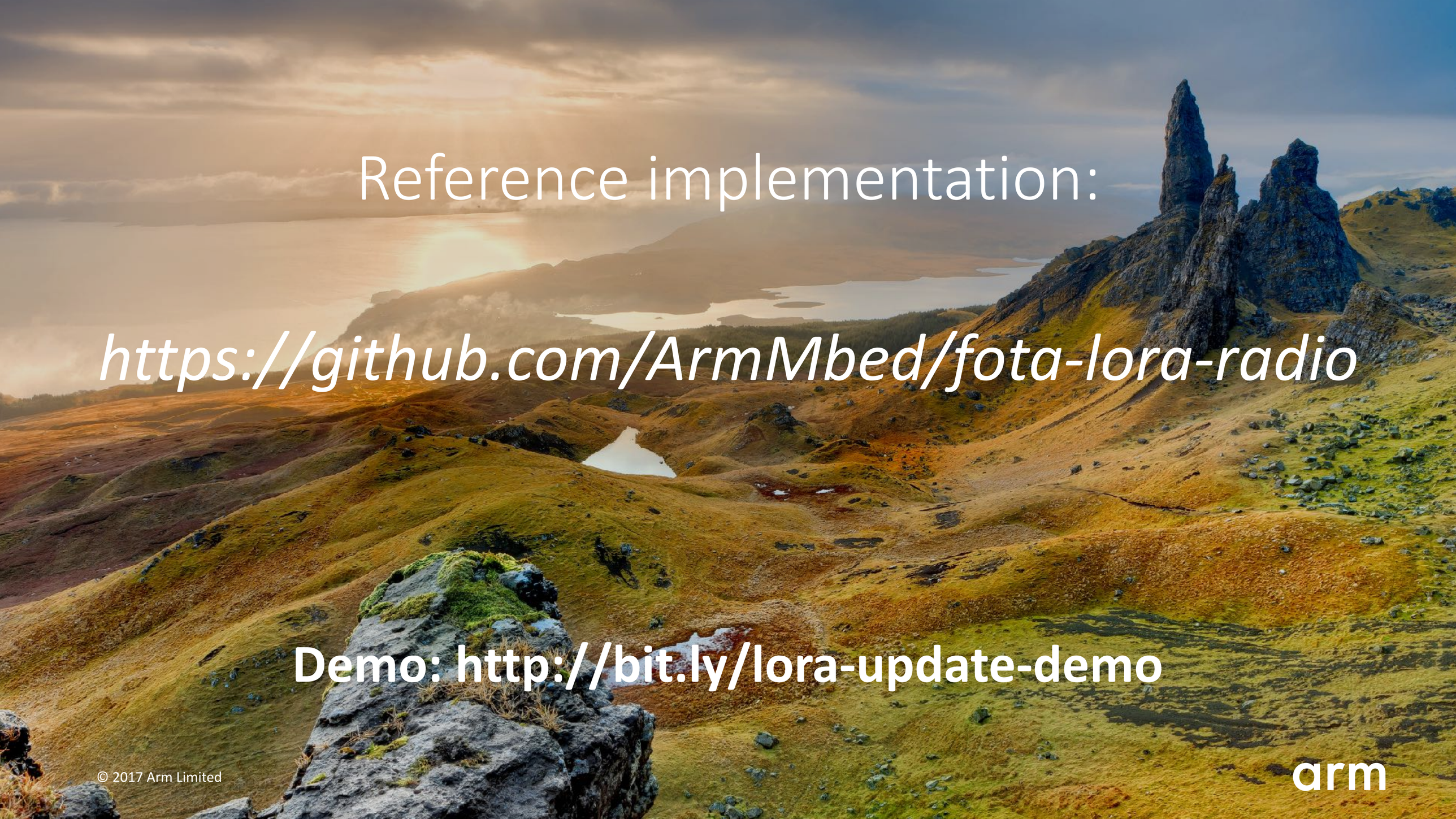
LoRa Alliance meeting last week

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

Aiming to standardize in next LoRaWAN standard

Specifications are available for LoRa Alliance members

arm



arm

Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!
감사합니다
धन्यवाद

arm

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