A LoRaWAN Security Assessment Testbench

Tristan Claverie, José Lopes-Esteves

Agence nationale de la sécurité des systèmes d'information

June, 17, 2019

Lab

National Cybersecurity Agency of France (ANSSI), Wireless Security Lab :

- Radiocommunication protocols
- Electromagnetic Security (TEMPEST, IEMI, ...)
- Signal processing
- Simulations, measurements
- Embedded systems

Radiocommunication protocols in the IoT

- LoRaWAN
- Sigfox
- NarrowBand-IoT (NB-IoT)
- Zigbee
- Z-Wave
- Bluetooth-related (Classic, Low Energy, Mesh)
- ...

Outline

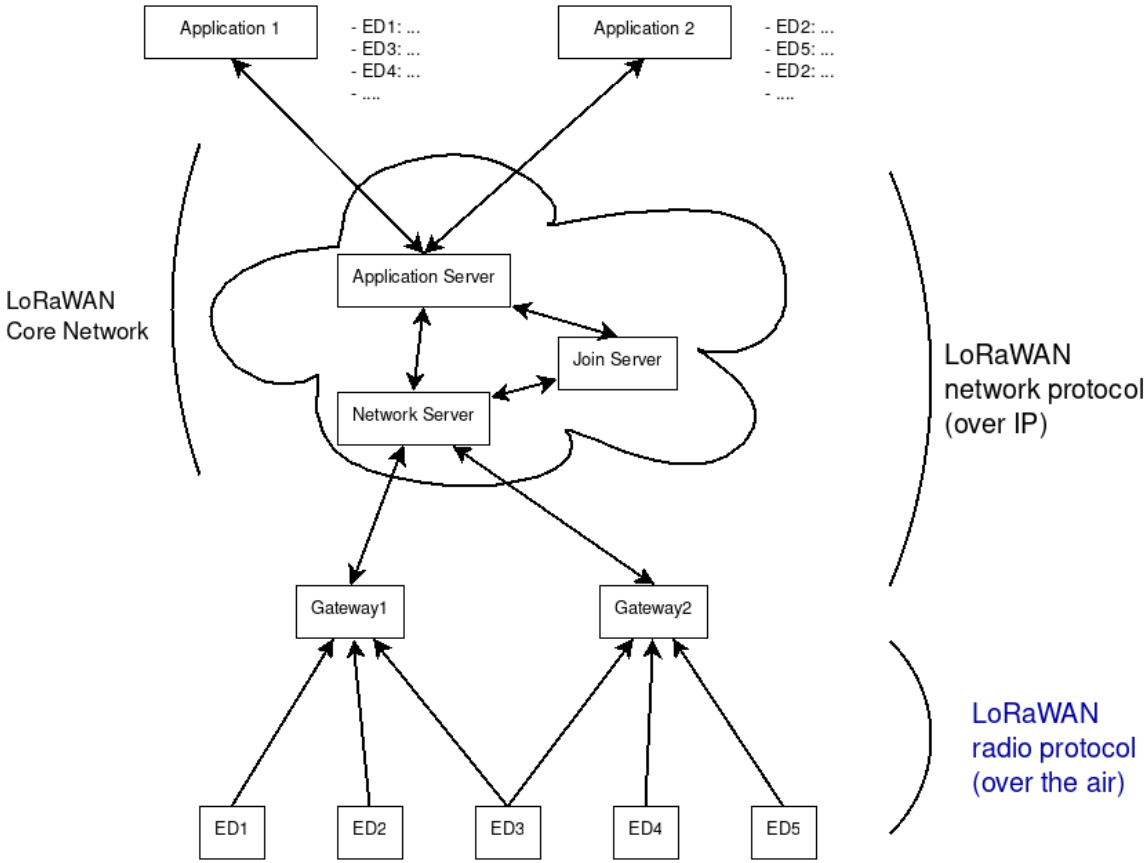
- LoRaWAN in 5 minutes
- Security-related Previous Work
- Working with LoRaWAN
- Experimental Setup
- Case study : Replay or decrypt
- Conclusion

1. LoRaWAN in 5 minutes

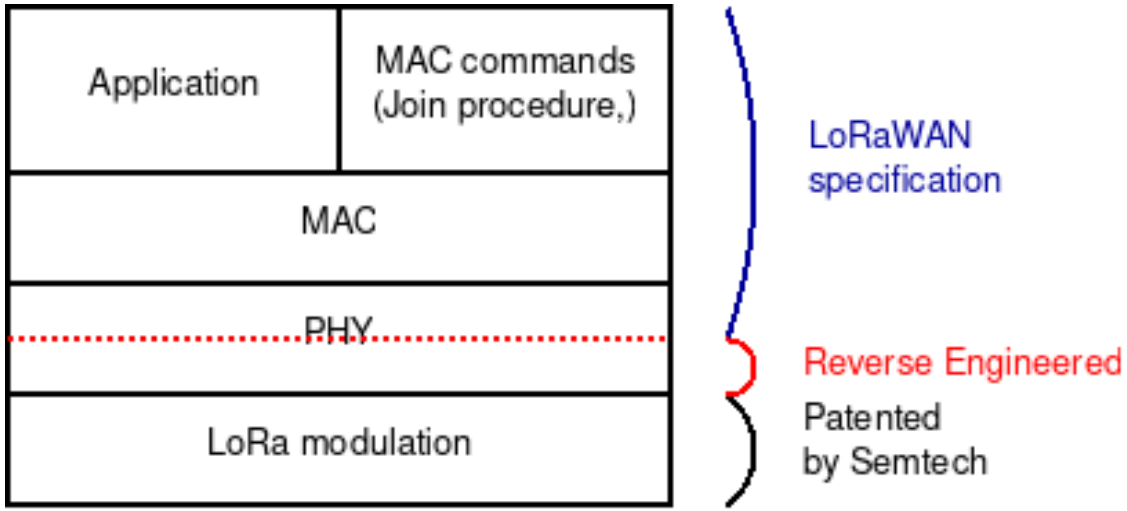
LoRaWAN : Introduction

- Part of the Low-Power Wide Area Network protocol family ;
- Open specifications, some existing open source implementations ;
- Mainly used for one-way communications : smart metering ;
- Developed and specified by the LoRa Alliance[2] ;
- Based on the LoRa (Long Range) modulation patented by Semtech ;
- Version 1.0 of the protocol in 2015, version 1.1 in 2017.

LoRaWAN : Architecture



LoRaWAN : Radio Protocol Stack



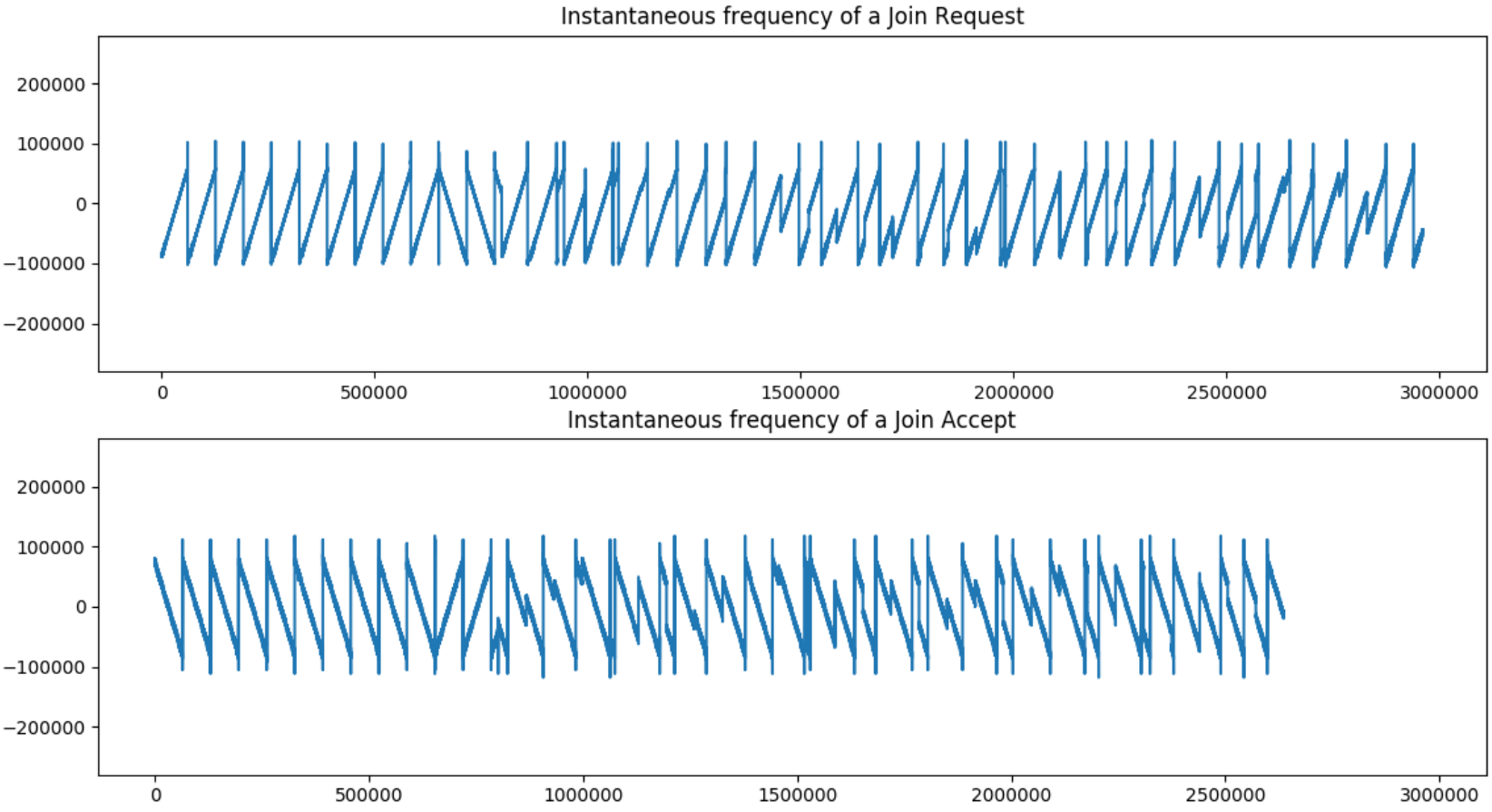
LoRa :

- Spreading factor : 7-12
- Bandwidth : 125, 250, 500kHz

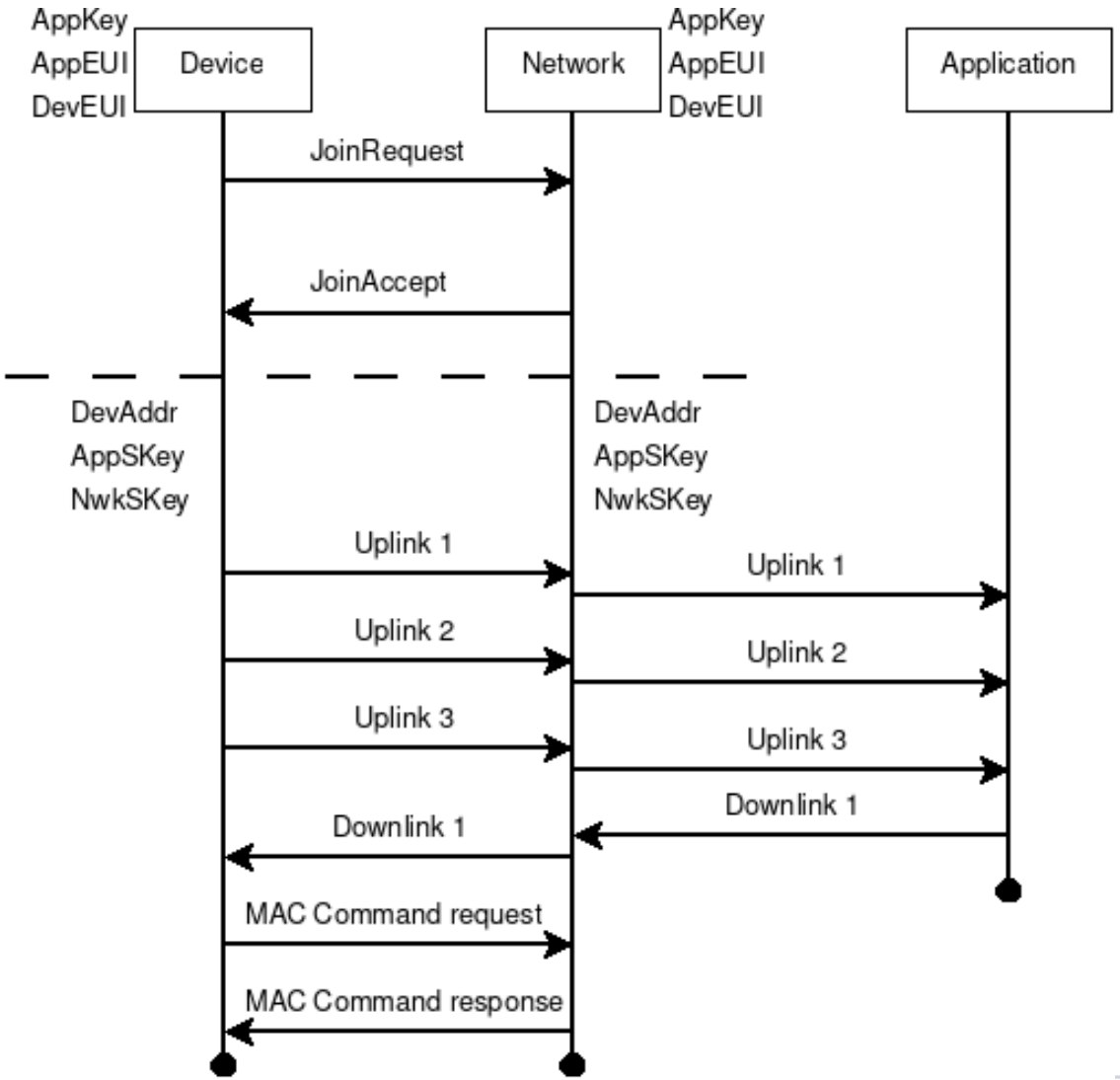
LoRaWAN radio :

- EU : 868/433MHz
- US : 915MHz

LoRaWAN : Uplink and Downlink



LoRaWAN : A complete session (1.0)



2. Security-related Previous Work

Previous Work

Subject	Involves radio	Tests mentioned
Desynchronisation between device and network[4, 17, 13, 10, 11]	yes	yes
Replay or decrypt[4]	yes	no
Gateways can be spoofed[11, 18]	yes	no
Formal analysis of the handshake[7]	yes	n/a
Jamming[3, 5]	yes	yes
Bias RNG using IEMI[17, 6]	yes	yes
Bitflip attacks[14, 9]	no	no

Previous Work : LoRaWAN radio testbenches

L'Hereec et Joulain[10]

- Able to sniff and replay
- Desynchronisation of devices
- Denial of service on the network

Lifschitz[11]

- Sniffing
- Packet dissection

Previous Work : Conclusion

- Lots of attacks involving radio proposed
- Very few practical implementations
- Results presented often lack details
- No information on the experimental setup

$\Rightarrow$ Previous work can't be reproduced and must be reimplemented.

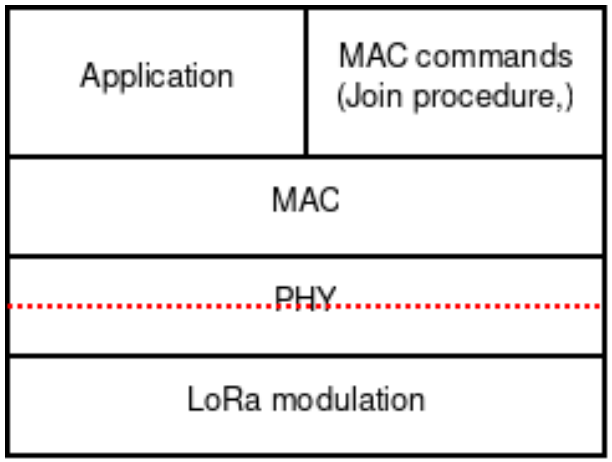
We need to build our own platform to properly study LoRaWAN security.

3. Working with LoRaWAN

Working with LoRaWAN : LoRa modulation

- Patented by Semtech
- Chirp spread spectrum
- Depends on two parameters : spreading factor and bandwidth (+ frequency)
- Modulation is open, coding is not

Working with LoRaWAN : Hardware modules



- LoRaWAN module = LoRa transceiver + LoRaWAN software implementation
- With a transceiver, complete control over MAC layer, configurable PHY layer
- Two kinds of transceivers : end devices (SX12xx) and gateways (SX13xx)

Working with LoRaWAN : Software Defined Radio

- Demodulation by Josh Blum (MyriadRF) [1]
- Reverse engineered by Matt Knight [16] then Pieter Robyns [8]
- $\Rightarrow$ Two gr-lora implementations

rpp0/gr-lora (Pieter Robyns)

- Only open source implementation which does demodulation + decoding
- One block per channel
- Uplink OR downlink for a single block

4. Experimental Setup

Experimental setup : Development kit

- One development kit from Microchip [12] (∼450€) :
  - One LoRaWAN gateway based on the SX1301
  - Two LoRa Mote based on the SX1276
  - A packaged core network
- A complete test network infrastructure
- Transmit arbitrary LoRa MAC frames whith Motes

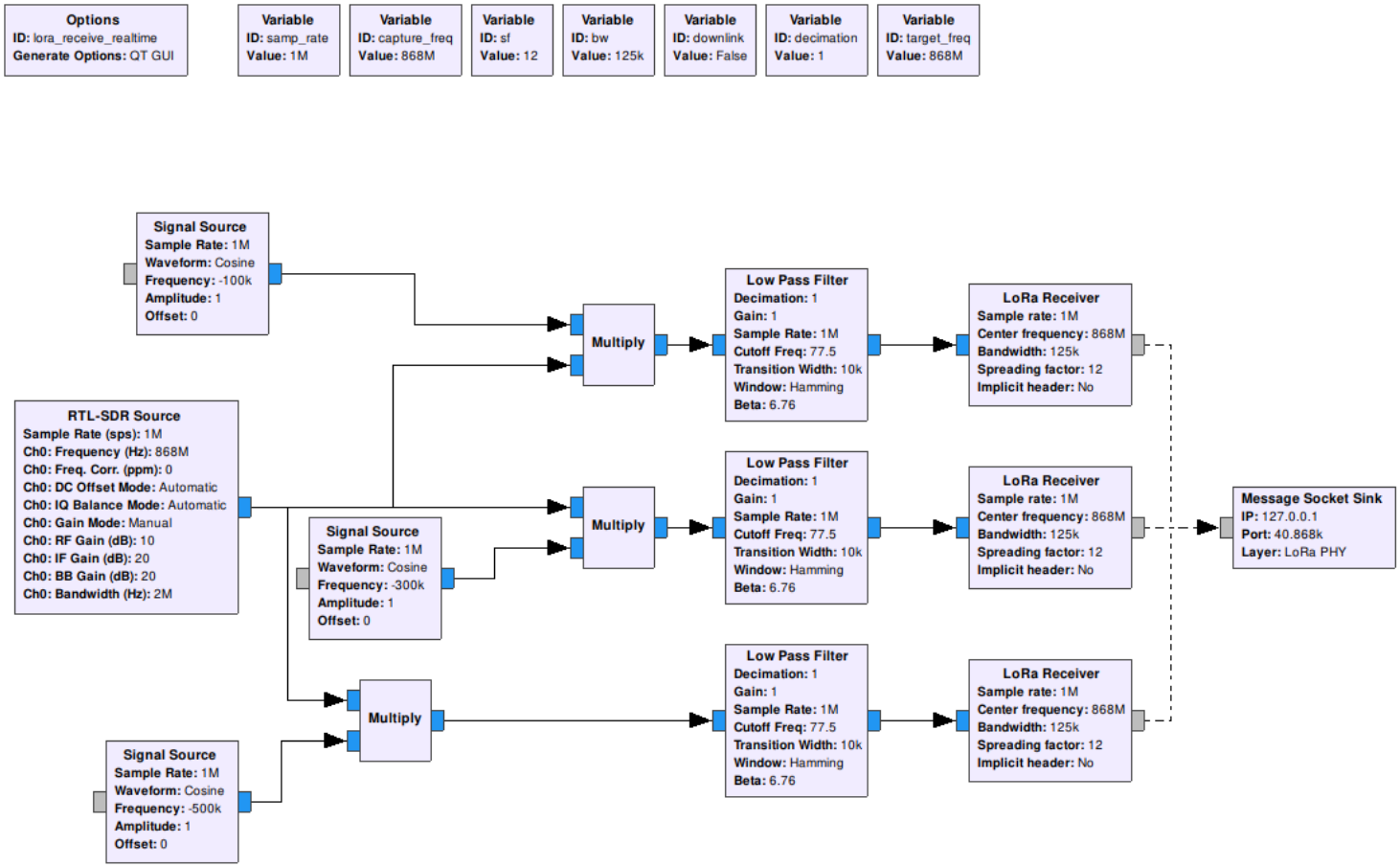
Experimental setup : FiPy

- One Fipy from Pycom [15] (∼50€) :
  - Multi-protocol development board
  - Micropython environment
  - Direct interaction with the LoRa/LoRaWAN module
- Program complex scenarios, starting at the LoRa MAC layer
- Can be turned into a single channel gateway

Experimental setup : RTL-SDR

- One RTL-SDR (∼30€) with GNUradio (gr-lora)
  - Capture signals for further processing
  - Real-time decoding of transmissions
  - Only RX
- gr-lora modified to allow listening uplink AND downlink with a single block
- Debug modules behavior through the waterfall
- Multi-channel decoder

Example : Sniffer (multi-channel decoder) with GNUradio



5. Case study : Replay or decrypt

Replay or decrypt attack : outline

- Published by Avoine/Ferreira [4]
- Partially decrypt some messages, allows replaying others
- No mention of any practical implementation
- Lots of precisions in the paper
- Patched in LoRaWAN 1.1

Replay or decrypt attack : Presentation

- Application layer messages are protected using AES-CCM
- Security of AES-CCM relies on unicity of the security parameters [a]
- Basic idea : force nonce reuse in a JoinRequest/JoinAccept
- => Security parameters ($\sim$ keystream) will be reused

---

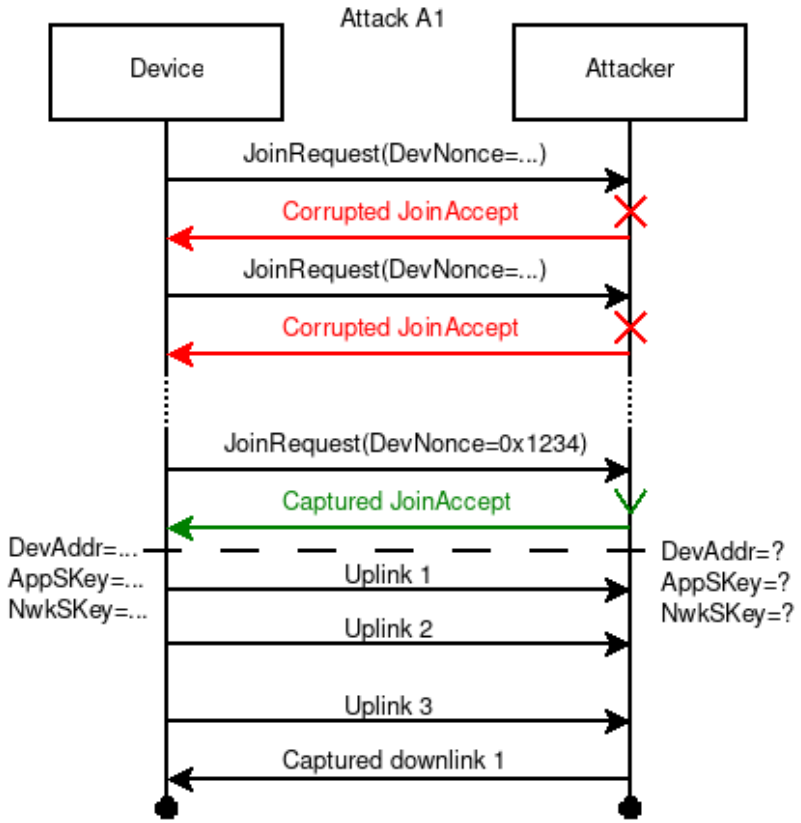
a. **More specifically, on the unicity of the tuple (session key, counter block, B_0)**

Replay or decrypt attack : Impact

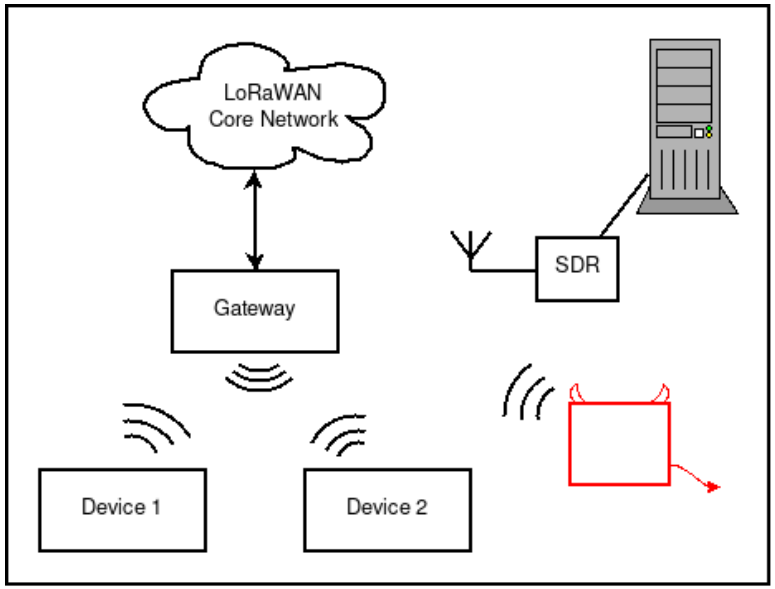
- Two-time pad on messages encrypted under the same keystream
- $c1 \oplus c2 = (m1 \oplus kstr) \oplus (m2 \oplus kstr) = m1 \oplus m2$
- For end device : allows partial decryption of uplink messages and replay of downlink messages (A1)
- For core network : allows partial decryption of downlink messages and replay of uplink messages (A2)

Replay or decrypt attack : Scenario

Captured a complete session:	- JoinRequest(DevNonce=0x1234) - JoinAccept(AppNonce=0x123456)	- Uplink messages - Downlink messages



Replay or decrypt attack : Implementation of A1



- Implemented with the FiPy in about 100 lines of MicroPython
- A first try involved SDR + LoRa Mote, but synchronisation was off.

Replay or decrypt attack : Results

- Took several days to complete, with one join attempt every 10 seconds
- $\Rightarrow$ Matches theoretical expectations
- Instead of actively jamming the JoinAccept, we powered off the fake gateway
- Attack A2 would take longer

Final thoughts : LoRaWAN modules notes/quirks

- LoRa Mote : After one emission, sets frequency to 869.525MHz
- FiPy : LoRaWAN module tends to crash silently
- FiPy : Joining a network tries indefinitely in the background
- LoRa Mote : Joining a network tries once
- LoRa Mote : Receive/Transmit downlink frames with 'iqi' parameter
- FiPy : Receive/Transmit downlink frames with rx_iq/tx_iq

6. Conclusion

Conclusion

Summary

- Up-to-date state of the art about LoRaWAN security
- Described a complete testbench
- Reproducible setup

Results

- Debug the odd behaviors of LoRaWAN stacks
- Easy to use and efficient, even with complex scenarios
- Combination of SDR and hardware proved very useful

Perspectives

- Optimise SDR decoding to enable precise sync
- Experiment with Intentional Electromagnetic Interferences
- Develop detection system
- Develop and share test vectors
- Study commercial devices

Questions

Thanks for listening !

Contact

- tristan.claverie@ssi.gouv.fr
- jose.lopes-esteves@ssi.gouv.fr

Bibliography

[1] Lora-sdr, 2016.
`https://github.com/myriadrf/LoRa-SDR`.

[2] Alliance, L.
Lora alliance, 2019.
`https://lora-alliance.org/`.

[3] Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., and Hughes, D.
Selective Jamming of LoRaWAN Using Commodity Hardware.
In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems : Computing, Networking and Services* (New York, NY, USA, 2017), MobiQuitous 2017, ACM, pp. 363–372.
event-place : Melbourne, VIC, Australia.

[4] Avoine, G., and Ferreira, L.
Rescuing LoRaWAN 1.0.
Tech. Rep. 651, IACR, 2017.

[5] Danish, S. M., Nasir, A., Qureshi, H. K., Ashfaq, A. B., Mumtaz, S., and Rodriguez, J.
Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure.
In *2018 IEEE International Conference on Communications (ICC)* (May 2018), pp. 1–6.

Bibliography (cont.)

[6] Danish, S. M., Qureshi, H. K., and Jangsher, S.
Jamming Attack Analysis of Wireless Power Transfer on LoRaWAN Join Procedure.
In *2018 IEEE Globecom Workshops (GC Wkshps)* (Dec. 2018), pp. 1–6.

[7] Eldefrawy, M., Butun, I., Pereira, N., and Gidlund, M.
Formal security analysis of lorawan.
Computer Networks 148 (2019), 328 – 339.

[8] Knight, M.
gr-lora, 2016.
https://github.com/BastilleResearch/gr-lora.

[9] Lee, J., Hwang, D., Park, J., and Kim, K.-H.
Risk analysis and countermeasure for bit-flipping attack in LoRaWAN.
In *2017 International Conference on Information Networking (ICOIN)* (Da Nang, Jan. 2017), pp. 549–551.

[10] L'Hereec, F., and Joulain, N.
Sécurité LoRaWAN.
In *Computer & Electronics Security applications Rendez-vous (C&ESAR) 2016* (Rennes, France, 2016), pp. 92–108.

Bibliography (cont.)

[11] Lifchitz, R.
Security review of LoRaWAN networks.
In *Hardwear.io* (The Hague, Netherlands, 2016).

[12] Microchip.
Lora technology evaluation kit, 2018.
https://www.microchip.com/DevelopmentTools/ProductDetails/DV164140-1.

[13] Miller, R.
LoRa Security - Building a Secure LoRa Solution.
Whitepaper, MWR Labs, 2016.

[14] Miller, R.
LoRa the explorer : Attacking and Defending LoRa Systems.
In *Syscan 360 Singapore* (Singapore, 2016).

[15] Pycom.
Fipy from pycom, 2019.
https://pycom.io/product/fipy/.

Bibliography (cont.)

[16] Robyns, P.
gr-lora, 2018.
https://github.com/rpp0/gr-lora.

[17] Tomasin, S., Zulian, S., and Vangelista, L.
Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks.
In *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (Mar. 2017), pp. 1–6.

[18] Yang, X., Karampatzakis, E., Doerr, C., and Kuipers, F.
Security Vulnerabilities in LoRaWAN.
In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)* (Apr. 2018), pp. 129–140.