Downlink Jamming and its effects on LoRaWAN

Moheed Ali Kayani, CNAM Paris,
Cedric Lab - ROC Team

Supervisor:

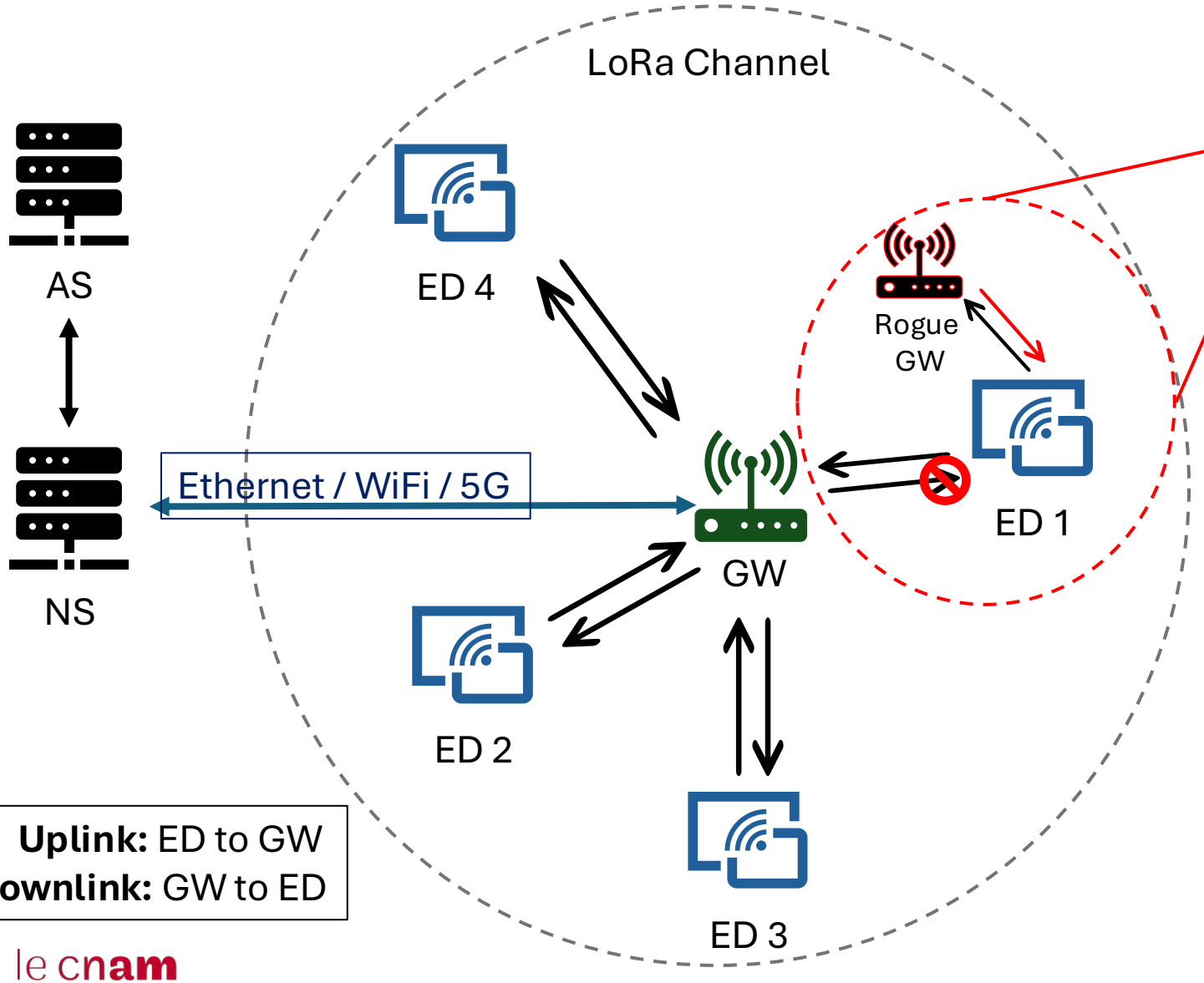
- Vania Conan, CNAM Paris, CEDRIC Lab
- Stéphane Rovedakis, CNAM Paris, CEDRIC Lab
- Alessandro Aimi, University of Bologna, Italy

le cnam cedric EA4629

Presentation Outline

1) Introduction
2) LoRaWAN - Background
3) LoRaWAN - Attacks
4) Proposed Attack
5) Experimental Validation
6) Attack Limitations
7) Conclusion and perspectives

Downlink Jamming Attack



Uplink: ED to GW
Downlink: GW to ED

A rogue gateway placed in **close proximity** to an End Device hijacks downlinks communications by **injecting forged packets** to **jam legitimate downlinks**, causing:

1) **Energy Drain** — Transmission energy spikes
2) **Throughput Collapse** — Goodput degrades for the targeted ED
3) **Traffic Congestion** — Downlink pressure on the legitimate gateway increases for the targeted ED
4) **Uplink Packet Loss** — Uplink drop rate undermining network reliability

Effects on ED,

Network

le cnam cedric EA4629

LPWAN, LoRa and LoRaWAN

LPWAN

- **Bridge:** Connects short-range and cellular networks.
- **Long Range:** 5km to 40km coverage.
- **Low Power:** 10+ year battery life.
- **Efficiency:** Optimized for small, infrequent payloads.

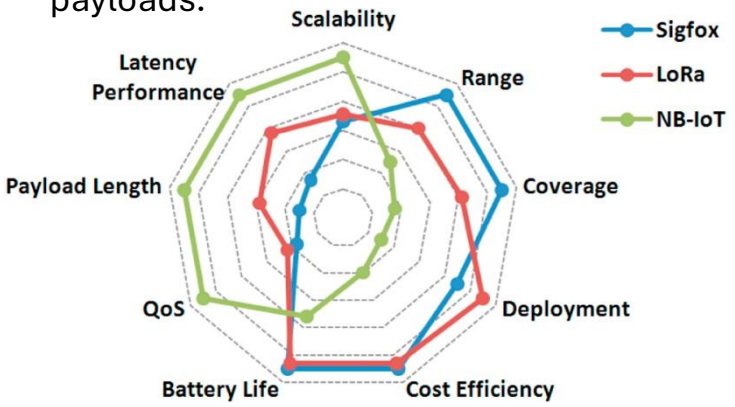


Fig 1: LPWAN technologies [1]

LoRa (Physical)

- **CSS Modulation:** Chirp spread spectrum technique for robust, long-range communication
- **Flexibility:** Scalable SF7-SF12 spreading factors.
- **Bandwidth:** Trade-offs between range and rate.
- **ISM Bands:** Unlicensed EU 868 operation.

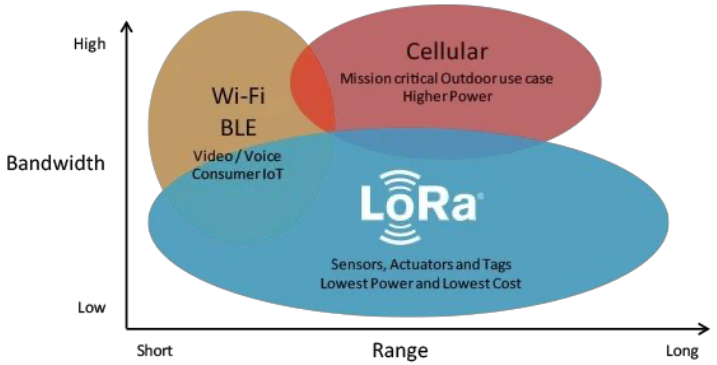


Fig 2: BW vs Range [2]

LoRaWAN (Protocol)

- **Network Topology:** Uses a **Star-of-Stars architecture** where gateways relay data to servers, and performs **deduplication** to process only one instance of redundant packets.
- **Transmission Control:** Have Adaptive Data Rate (ADR) to optimize capacity, and Duty Cycle limits to ensure fair spectrum usage per regional regulations.
- **Messaging Modes:** Offers Bi-Directional communication with both **Unconfirmed** (low power) and **Confirmed** (requires ACK) traffic modes.
- **Device & Security:** Manages power via Class A, B, and C profiles, secured by AES-128 multi-layered encryption.
- **Downlink Timing:** Devices open two specific **RX Windows** after every uplink to enable remote control and OTA updates.

[1] Mekki et al., "A comparative study of LPWAN technologies for large-scale IoT deployment". *ICT Express, 2019*
[2] https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

LoRaWAN Bit rate, ToA and Energy Consumption

Bit Rate

- **Bit Rate** decreases by a factor of **~ 22x** from SF7 to SF12

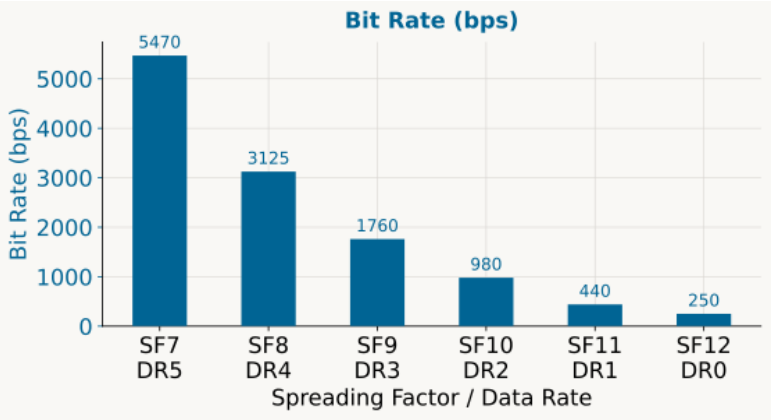


Fig 3: LoRA Bit Rate

Time on Air

- **ToA** increases by a factor of **~ 23x** from SF7 to SF12 [3]

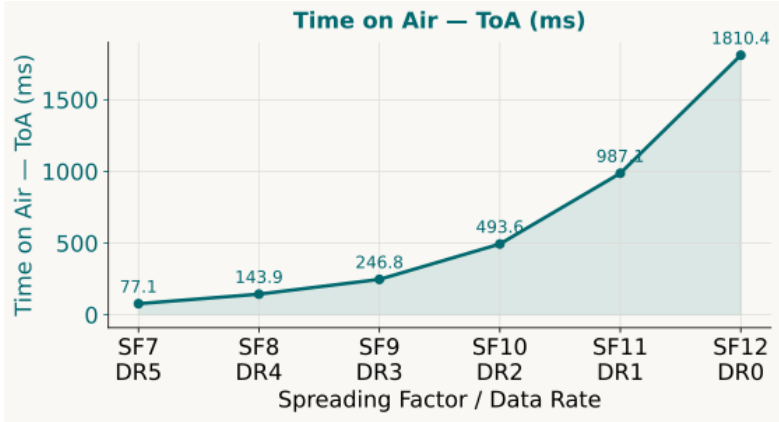


Fig 4: LoRa Time on air (ToA) per SF (BW = 125 KHZ, CR = 4/5, 35-BYTE FRAME: 13-BYTE MAC Header + 22-BYTE application payload)

Tx Energy Consumption

- **E_Tx** increases by a factor of **~ 23x** from SF7 to SF12. computed as [4]:
  - $E_{TX} = I_{TX} \times V \times T_{ToA}$ with $I_{TX} = 83$ mA, $V = 3.3$ V

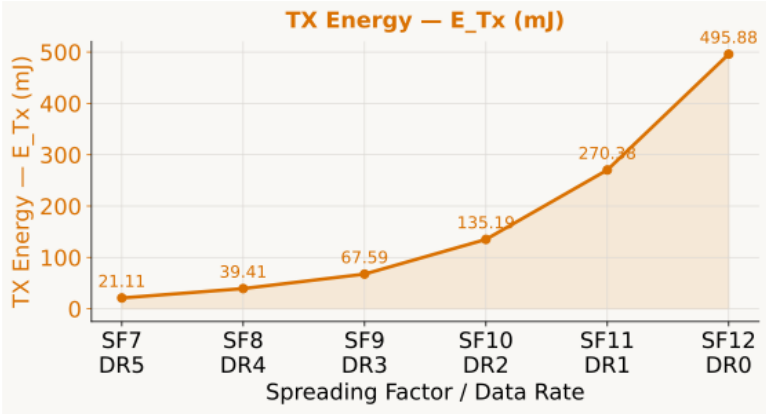


Fig 5: LoRa TX Energy per SF (BW = 125 KHZ, CR = 4/5, 35-BYTE FRAME: 13-BYTE MAC Header + 22-BYTE application payload)

[3] https://www.thethingsnetwork.org/airtime-calculator
[4] Casals et al., "Modeling the energy performance of LoRaWAN," Sensors, 2017

Class A: RX Windows, Downlink Validation & DevAddr Exposure

- **RX1** opens **1s** post-uplink — same channel and data rate (DR) as uplink and
- **RX2** opens **2s** post-uplink — fixed channel & DR (default: 869.525 MHz / SF12 / BW125)
- If a valid downlink is received in RX1, **RX2 is skipped** to conserve energy
- Upon receiving a frame in RX1, the ED first checks **DevAddr** — no match means immediate discard and open the RX2
- If DevAddr matches, the ED verifies the **MIC** using NwkSKey; failure results in silent discard and open the RX2
- Discarding or not receving the downlink in both the receive windows triggers the **ADR backoff procedure**

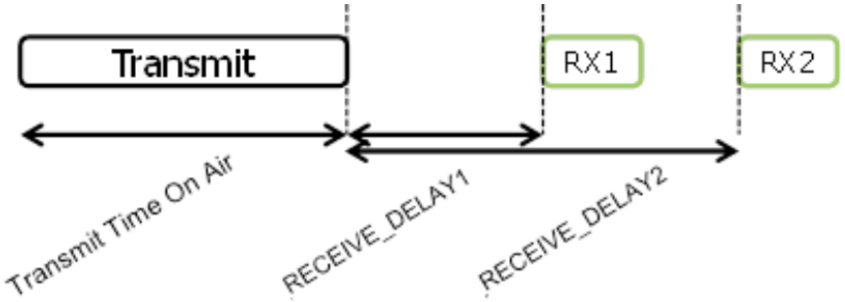


Fig. 5: Receive windows

Preamble	PHY Header	PHY CRC	MAC Header	MAC Payload			MIC	CRC
				Headers	FPort	Payload 🔒		
n Symbols	Optional	Optional	1 Byte	7 Bytes	1 Byte	n encrypted Bytes	4 Bytes	Optional

Fig. 6: LoRaWAN frame structure. DevAddr, FCnt, and radio metadata are transmitted in the clear. FRMPayload is encrypted with AppSKey; the MIC is computed using NwkSKey

Adaptive Data Rate (ADR)

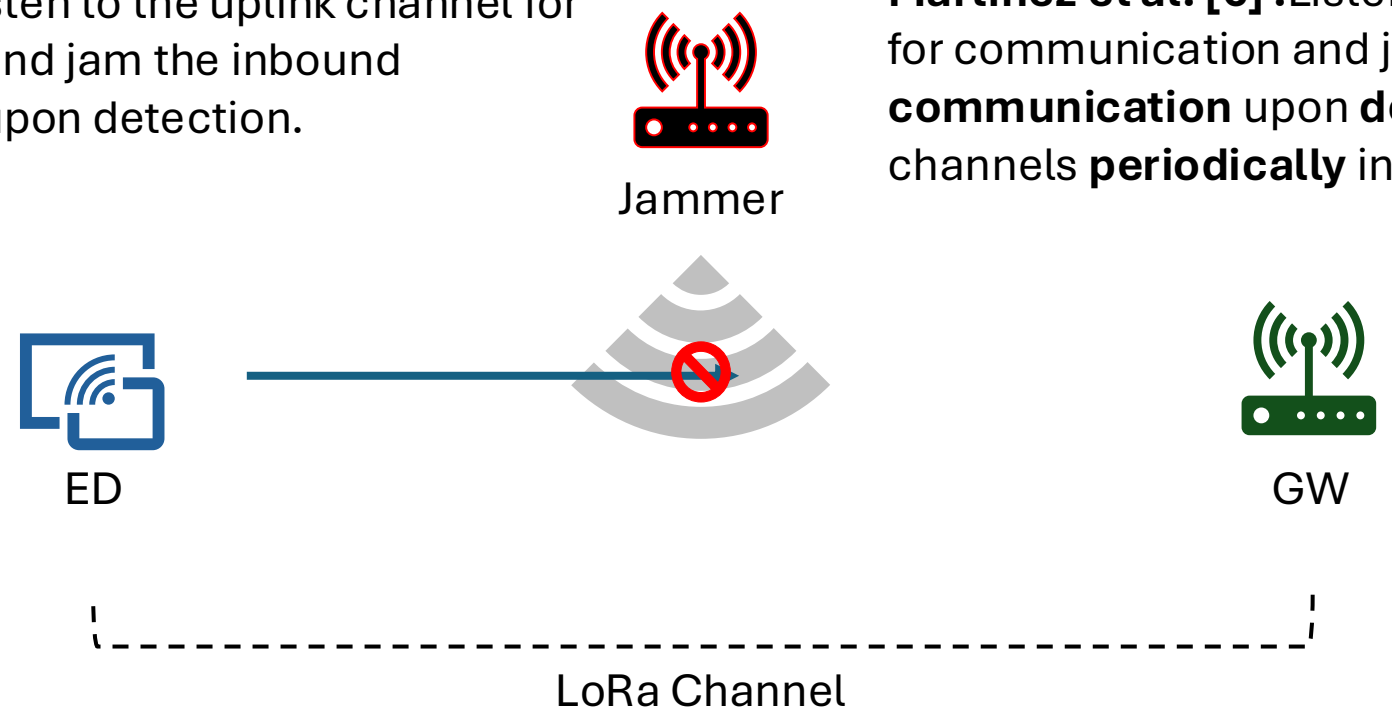
Controls the SF, Tx, Freqs and nbTrans of the ED		
Step #	**ADR Network-Server (Optimization)**	**ADR Backoff - ED side (Recovery)**
1	**Monitor:** Track channel SNR/quality.	**Detect:** Increment `ADRACKCNT` after no downlink received.
2	**Analyze:** Calculate SNR margin.	**Trigger:** Set `ADRACKReq` bit to 1.
3	**Optimize:** Adjust SF & Tx power for efficiency.	**Power Up:** Set Tx power to max (14 dB).
4	**Re-evaluate:** Calculate margin per 20 UL packets.	**Scale:** Increase SF step-by-step (up to SF12).
5	**Adjust:** control Freq, `nbTrans`, and Tx power.	**Reset:** Revert to default Freqs and `nbTrans=1`.

LoRaWAN - Attacks (1/5): Uplink Jamming

Aras et al. [5]: Listen to the uplink channel for communication and jam the inbound communication upon detection.

Martinez et al. [6] : Listen to the uplink channel for communication and jam the **inbound communication** upon **detection** or **jam** all the channels **periodically** in a loop.

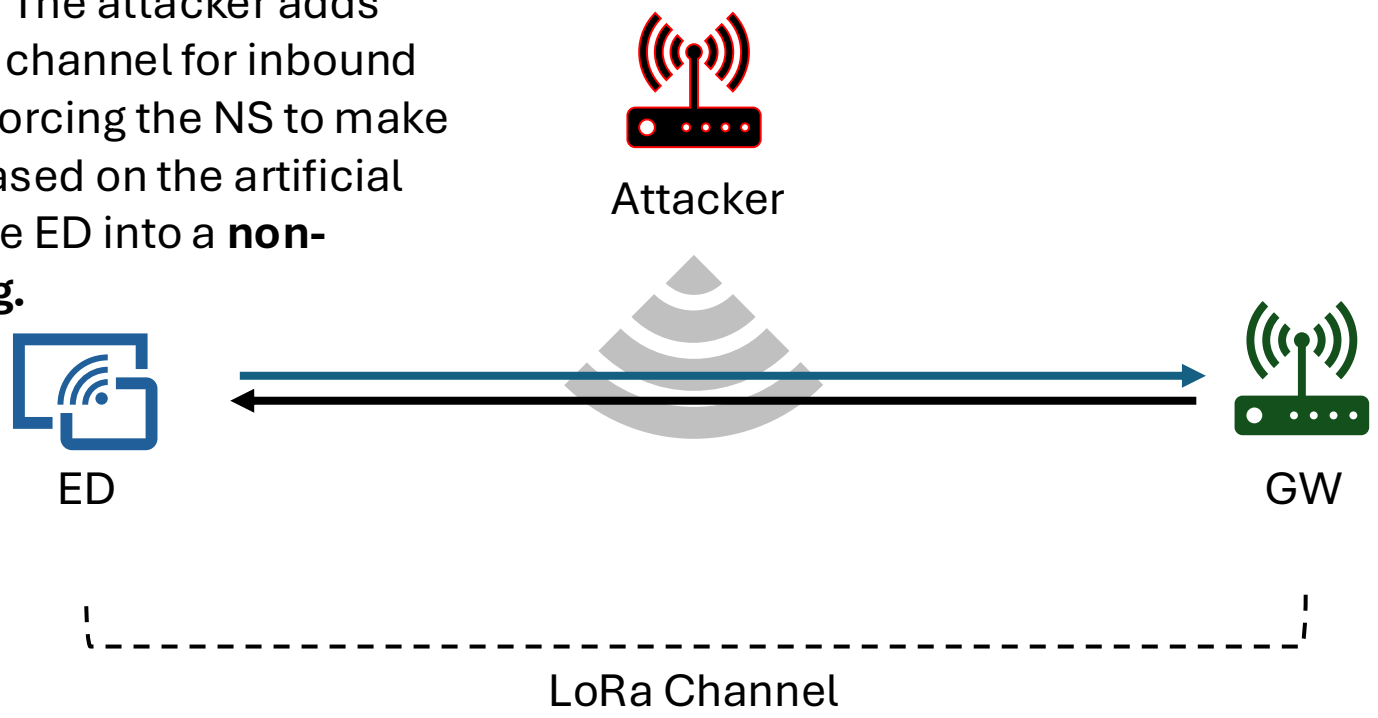
Dossa et al. [7]: Listen to the uplink channel for **chirps** and jam the **inbound** communication **upon detection**.



[5] Aras *et al.*, "Selective jamming of LoRaWAN using commodity hardware," *MobiQuitousMobiQuitous*, 2017.
[6] Martinez et al., "On the performance evaluation of LoRaWAN under jamming," WMNC, 2019
[7] Dossa *et al.*, "Impact of reactive jamming attacks on LoRaWAN," *PIMRC*, 2025

LoRaWAN - Attacks (2/5): ADR Manipulation

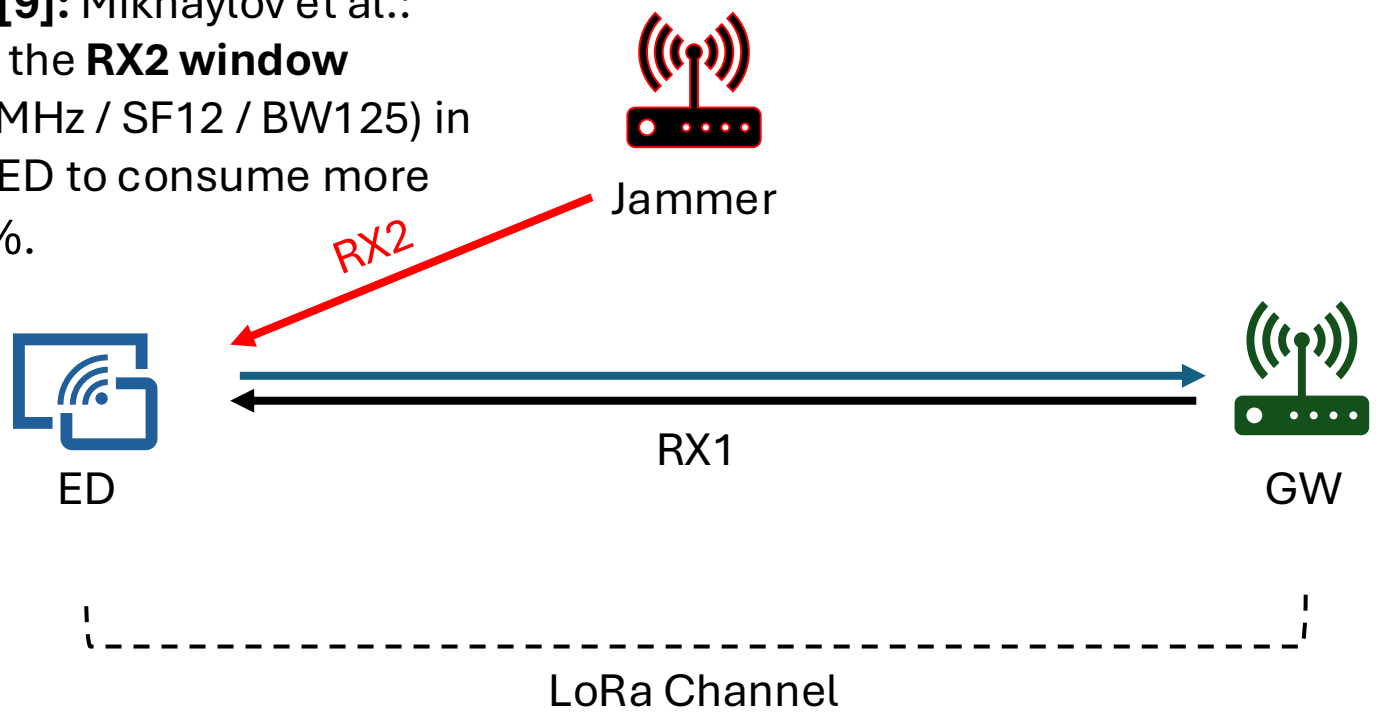
BlackoutADR [8]: The attacker adds **noise** to the LoRa channel for inbound communication, forcing the NS to make **ADR decisions** based on the artificial noise and push the ED into a **non-optimised setting.**



[8] Hidawi et al., "BlackoutADR: Exploiting adaptive data rate vulnerabilities in LoRaWAN-based FANETs," J. Netw. Comput. Appl., 2026

LoRaWAN - Attacks (3/5): Energy Attack

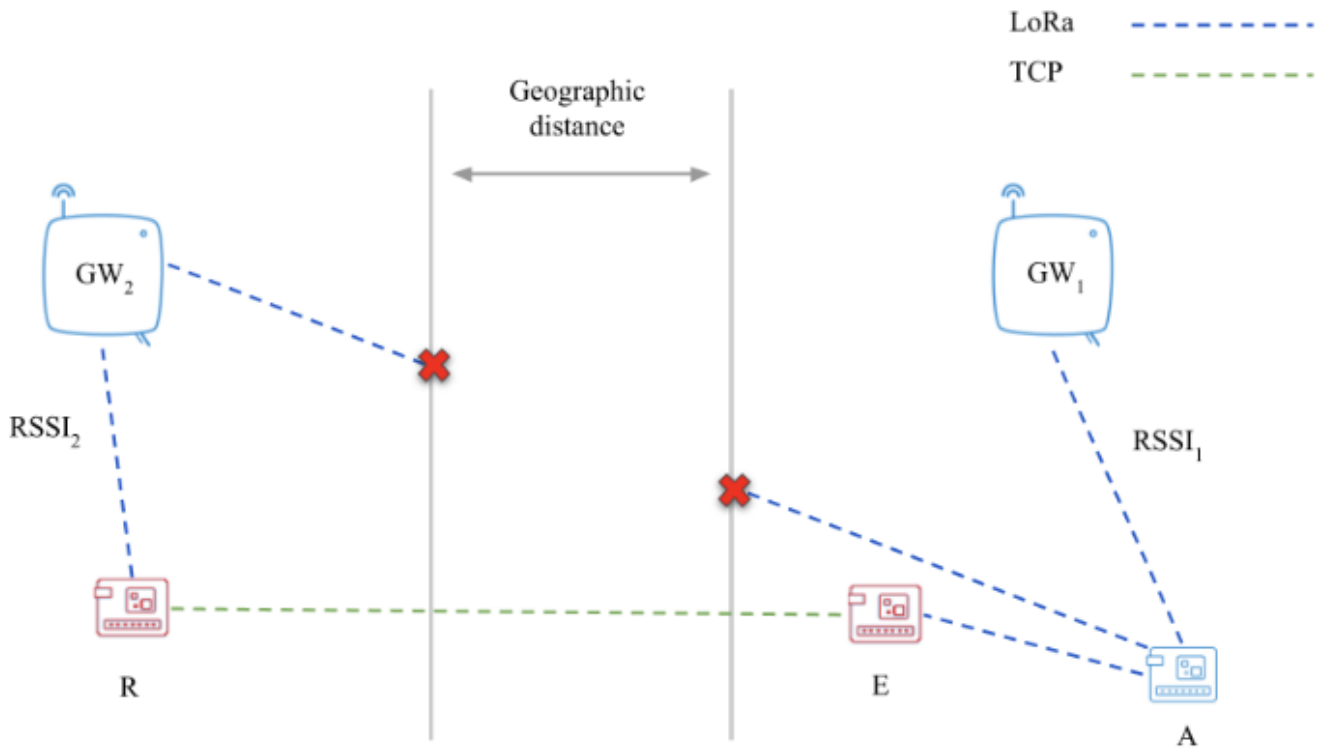
Milkhayloc et al. [9]: Mikhaylov et al.: The attacker jams the **RX2 window** (default: 869.525 MHz / SF12 / BW125) in order to force the ED to consume more energy up to 576%.



[9] Mikhaylov et al., "Energy attack in LoRaWAN: Experimental validation," ARES, 2019

LoRaWAN - Attacks (4/5): Hijacking Downlink Path

- Locatelli et al. [10] showed that downlink path hijacking can silence an ED without physical-layer jamming.
- The attack uses a **sniffer-replayer** pair to **replay** captured uplinks.
- These uplinks are forwarded to an **out-of-range GW** with artificially **stronger** signal quality.
- As a result, the Network Server keeps **selecting** the unreachable GW for downlinks.

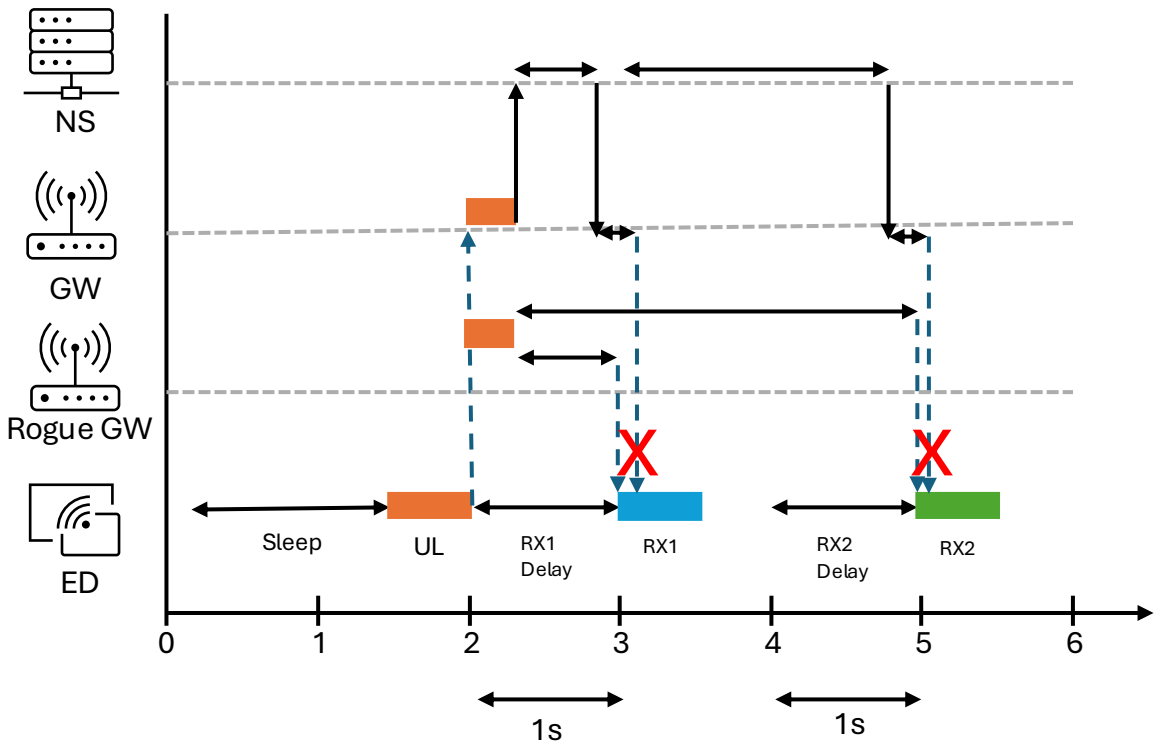


[10] Locatelli et al ., “Hijacking downlink path selection in LoRaWAN,” in Proc. 2021 IEEE Global Commun. Conf. (GLOBECOM), 2021, pp. 1–6.

LoRaWAN - Attacks (5/5)

Work	Attack Vector	Disruption	RX Windows Exploitation	ADR Manipulation	Network Goodput	Battery Depletion
Aras et al. [5]	Selective preamble jamming	Uplink	✗	✗	⋙	✗
Martinez et al. [6]	Channel-aware / oblivious jamming	Uplink	✗	✗	⋙	✗
Dossa et al. [7]	Reactive chirp jamming	Uplink	✗	✗	⋙	✗
BlackoutADR [8]	PHY noise injection (GW-side)	Uplink	✗	✓	⋙	✓
Milkhayloc et al. [9]	RX2 channel jamming	Downlink	✓	✗	✗	✓
Locatelli et al. [10]	Downlink Path hijacking	Downlink	✓	✗	✗	✗
This work	**Forged downlink (RX1/RX)**	**Downlink**	✓	✓	⋙	✓

Downlink Jamming Attack



1. ED sends an uplink; GW forwards it to the NS.
2. NS schedules the legitimate downlink in RX1 or RX2.
3. A nearby Rogue Gateway forges an downlink using the **UL parameters**.
4. The ED discards the forged frame but miss the legitimate one, which trigger **ADR backoff.**

RX2 case

- If the network server reschedules the downlink in RX2, the attacker can target RX2.
- Since RX2 uses region-defined default parameters unless **reconfigured**.

Experimental Validation

Simulation Parameters

Validation of Attack

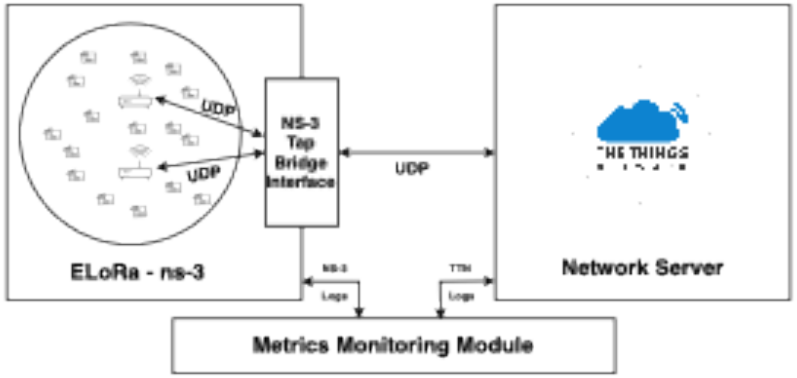
Effect of Attacked End Device

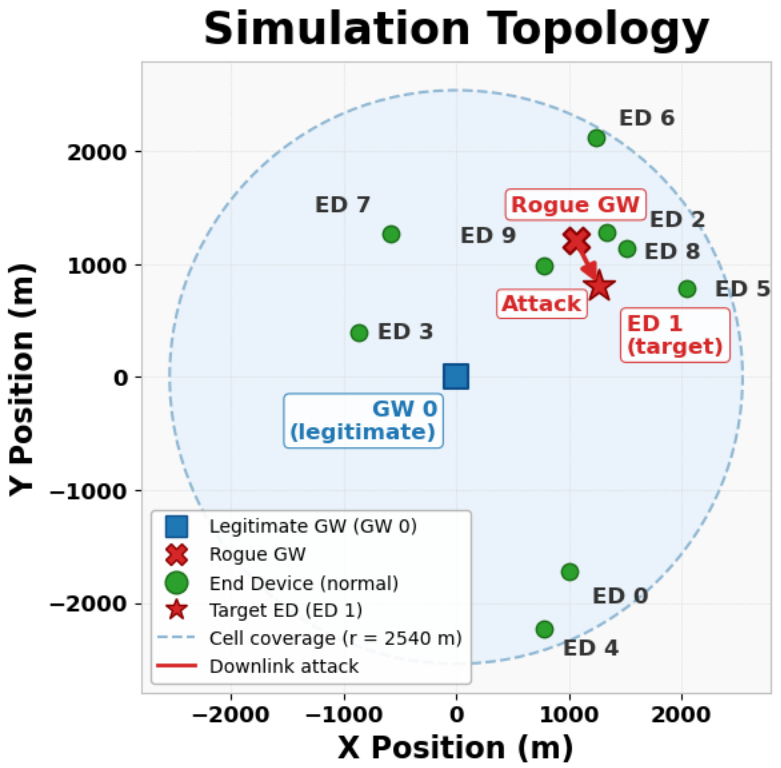
Effect on the Legitimate GW and Network Server

Simulation Parameters

We use ELoRa (ns-3) [11], [12] with The Things Stack for evaluation, and the parameter settings are summarized below:

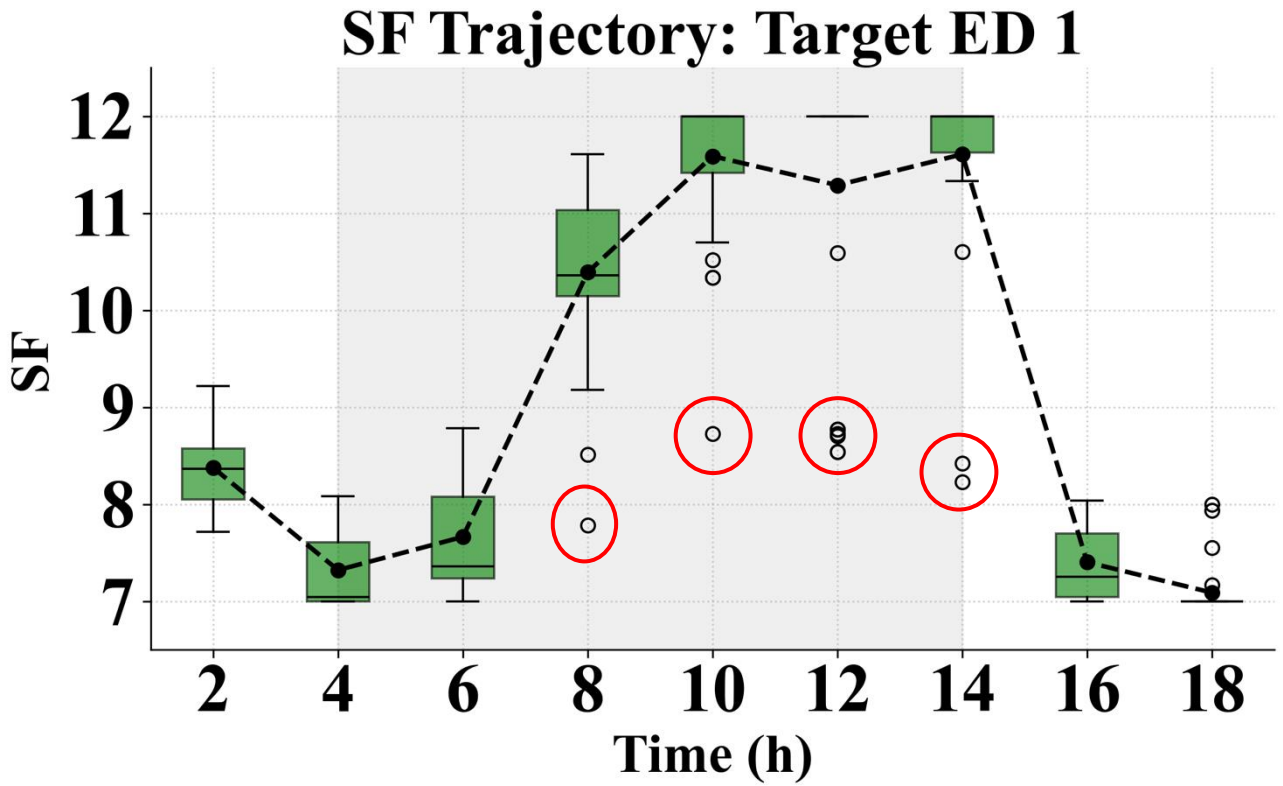
Parameter	Value / Description
EDs & GW	10 (1 under attack) & 1 GW
Rogue GW	1
Duration	18 h (4 h init, 10 h attack, 4 h recovery) **(wall-clock)**
Initial ED Configuration	SF12, 3 default channels, 14 dBm TX power
Traffic Pattern	22-byte uplink every 60 seconds per ED
Channel Model	Okumura-Hata + Rayleigh + CROCE SIR
Features	ADR + LoRaWAN MAC security
Runs	30 Randomize





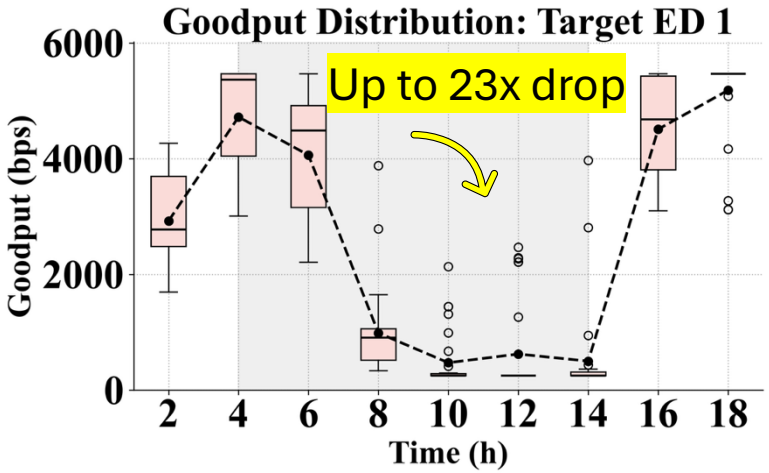
Results: SF Trajectory

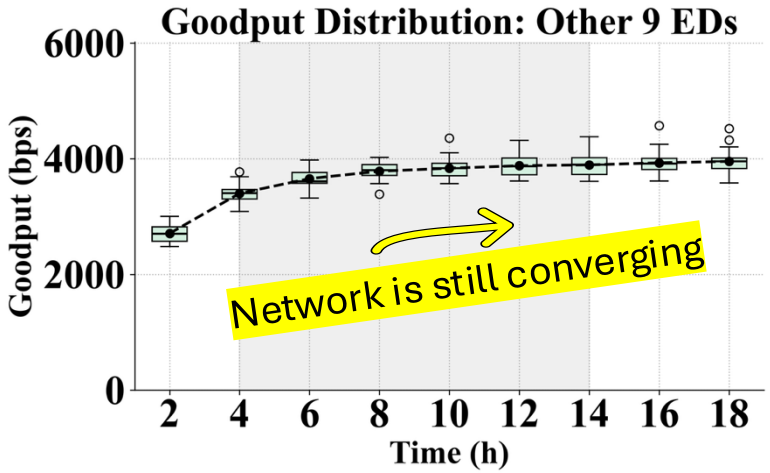
- During this period, the target ED's SF increases sharply because the attack triggers the **ADR Backoff**.
- After the attack ends, the SF drops again as the network recovers.
- The **outliers** visible here will be discussed further in the **limitations section**.

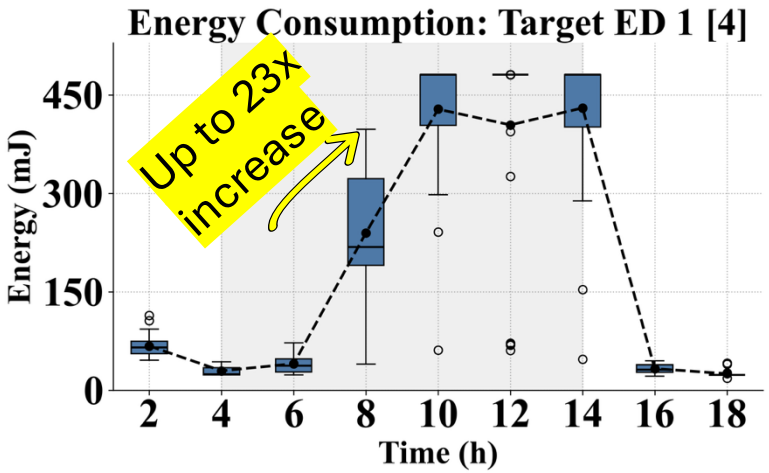


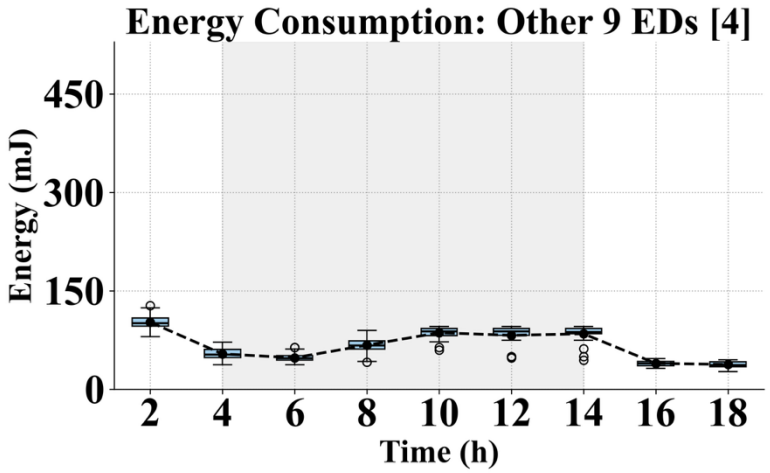
The **Grey shaded region** indicates the attack period.

Results: Goodput & Tx Energy consumption









Results: Effect of legitimate GW & NS

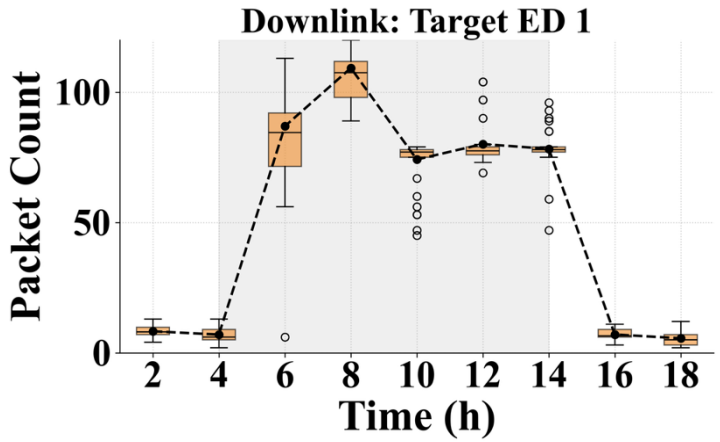


Fig 7: Number of downlink packets sent to the target ED.

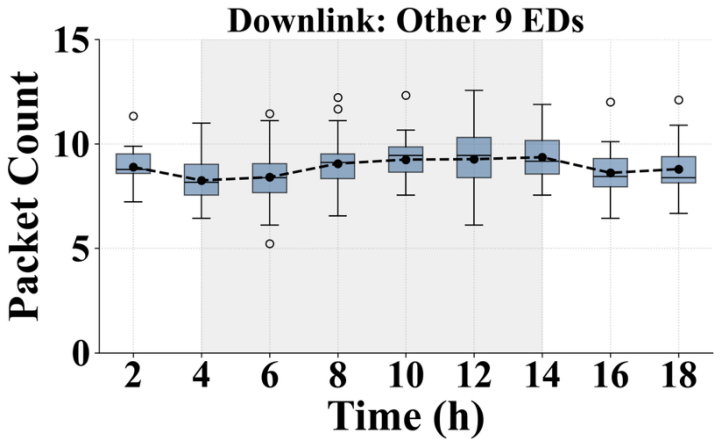


Fig 8: Avg. number of downlink packets sent to non-target EDs.

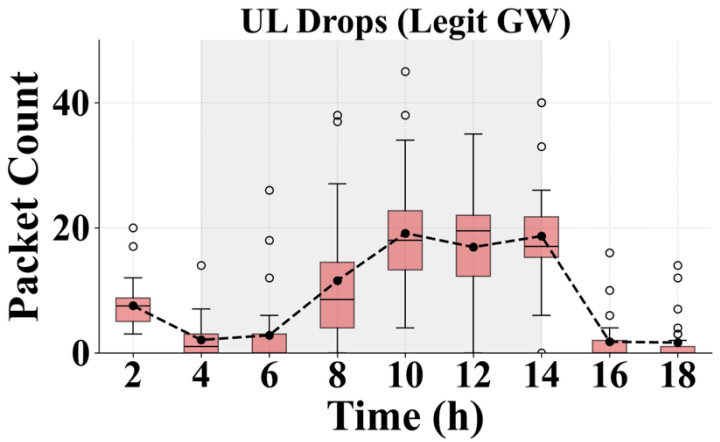


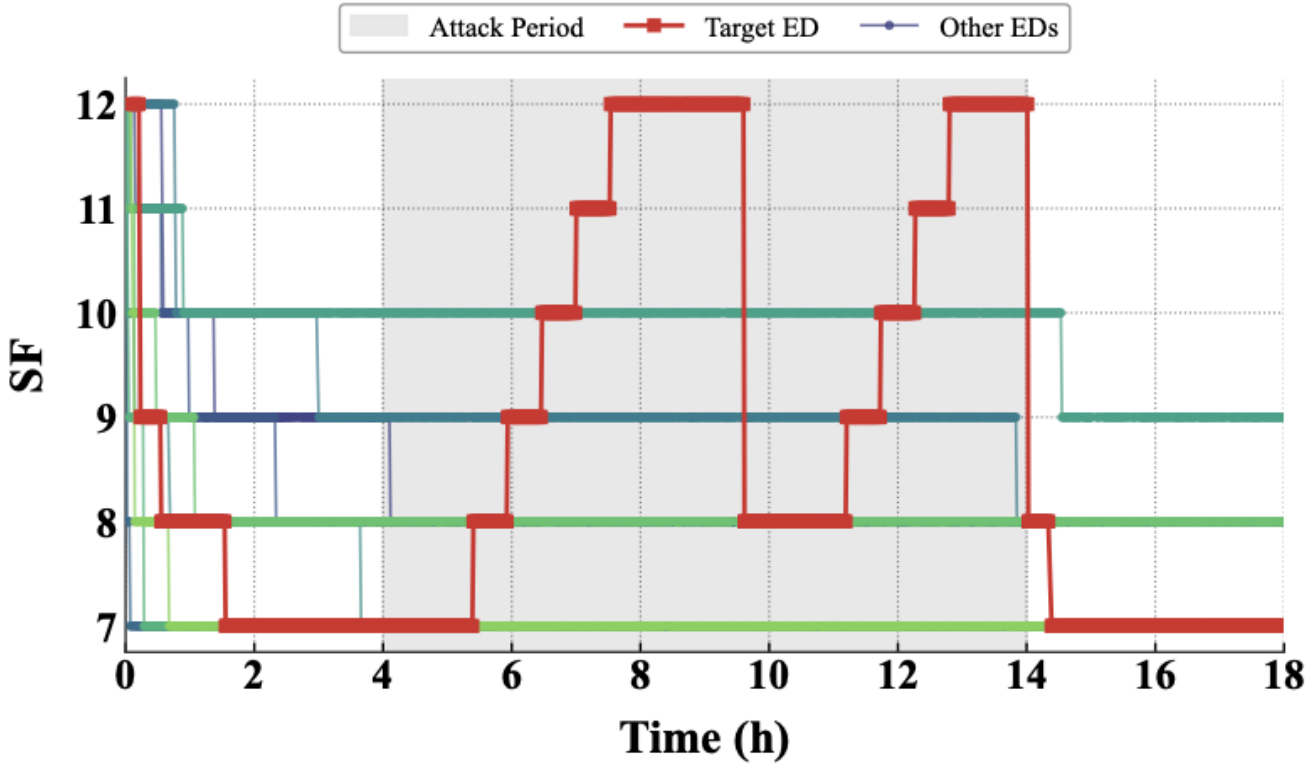
Fig 9: Packet loss caused by downlink frame transmission at the legitimate GW.

- The attack drives **downlink traffic** (for attacked ED) up by about **20x** and **UL drops** up by about **4x**

Note: UL drops **increase** because gateways are **half-duplex** and scheduling **prioritizes downlink** transmissions, which **reduces** uplink **reception opportunities** [12], [13].

Attack Limitations

- In 7/30 runs **(23.3%),** partial recovery was observed because channel conditions caused the attacker to **miss** a **target uplink**, interrupting the **ADR backoff** sequence.
- When this happens, the ADRACKCNT state may be **reset** after a legitimate downlink or successful recovery event.
- As a result, the target device can regain the intended ADR progression and **partially recover**.
- This shows that attack persistence depends on continuously **observing the victim uplinks** and controlling the receive windows.



Conclusion & Perspectives

- LoRaWAN Class A receive windows are a practical attack surface for **selective downlink jamming.**
- A rogue gateway can **block** legitimate downlink responses without **continuous** uplink jamming or **network-server access**.
- The attack triggers **ADR backoff**, increasing spreading factor, time on air, and energy consumption.
- It can degrades neighboring devices **goodput** by **increasing** downlink pressure.
- Future work will focus on **protocol-aware defenses**, anomaly detection at gateway and network-server levels, larger topologies, alternative NS implementations, and **statistical or ML-based detection.**

Thank You

Acknowledgment

This work was supported in part by the French ANR under the INTELLIGENTSIA project (grant no.ANR-20-CE25-0011), in part by the IE6 project, and in part by Orange through the ME/CT collaboration.

Questions?

Moheed Ali Kayani | Ph.D. Student | CNAM, Paris

Email: moheed-ali.kayani@cnam.fr

Linkedin: https://www.linkedin.com/in/moheed-ali-kayani/

le cnam
cedric EA4629

References

[1] Mekki *et al.*, “A comparative study of LPWAN technologies for large-scale IoT deployment,” *ICT Express*, 2019.image.jpg

[2] The Things Network, “What is LoRaWAN?”image.jpg

[3] The Things Network, “Airtime Calculator.”image.jpg

[4] Casals *et al.*, “Modeling the energy performance of LoRaWAN,” *Sensors*, 2017.

[5] Aras *et al.*, “Selective jamming of LoRaWAN using commodity hardware,” *MobiQuitous*, 2017.techscience

[6] Martinez *et al.*, “On the performance evaluation of LoRaWAN under jamming,” *WMNC*, 2019.journals.sagepub
Dossa *et al.*, “Impact of reactive jamming attacks on LoRaWAN: A theoretical and experimental study,” *PIMRC*, 2025.ar5iv.labs.arxiv

[7] Hidawi *et al.*, “BlackoutADR: Exploiting adaptive data rate vulnerabilities in LoRaWAN-based FANETs,” *JNCA*, 2026.webthesis.biblio.polito

[8] Mikhaylov *et al.*, “Energy attack in LoRaWAN: Experimental validation,” *ARES*, 2019.lora-alliance

[9] Locatelli *et al.*, “Hijacking downlink path selection in LoRaWAN,” *GLOBECOM*, 2021.ewsn

[10] Aimi *et al.*, “ELoRa: End-to-end emulation of massive IoT LoRaWAN infrastructures,” *NOMS*, 2023.hal

[12] Hernandez et al., “Downlink scheduling in LoRaWAN: ChirpStack vs The Things Stack”. LATINCOM, 2024

[13] Caillouet *et al.*, “The impact of downlink scheduling policy on the capacity of LoRaWAN,” *GLOBECOM*, 2024.