AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Decoding the Drone: Live Analysis of Aerial Cybersecurity

Philipp-Sebastian Vogt

IT-SECX 2026
October 02, 2026



Drone Protocols

Overview

Multiple Hobbyist Options

- DJI OcuSync
  - Proprietary and only used in DJI drones
  - Reverse engineered in dji_droneid on Github. -->
- TBS Crossfire
  - Proprietary, comes in RX/TX modules for DIY drones, from 2016
  - Reverse engineered by g3gg0.
- ExpressLRS
  - Open Source, multiple DIY and Buy options, from 2018

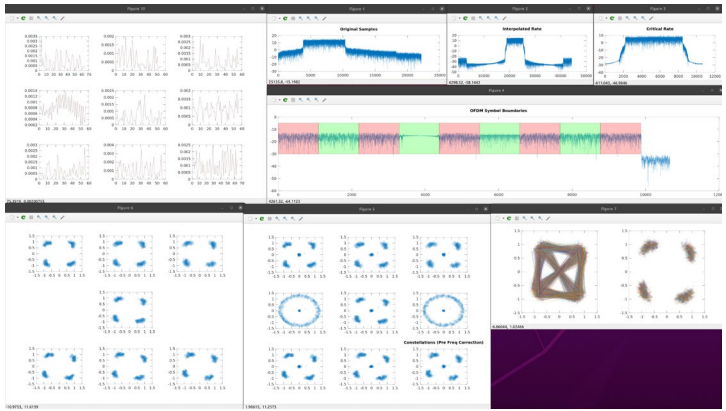


Image Source: (Github dji_droneid, 2022)

Why ExpressLRS?:

"We are working against [such modules], jamming [them], but we can't say that it's 100% perfect. Currently, there isn't a single system in Ukraine that can reliably jam ExpressLRS, especially with its remote antenna amplifying the signal" : Developer from Obriy Miltech. **(Militarnyi, 2024)**

Militarnyi, *"Perspective Market of Ukrainian Short-Range EW Systems"* (2024).

ExpressLRS

Overview

General

- Insecure by design -->
  - But open-source, so modifiable
- LoRa Based

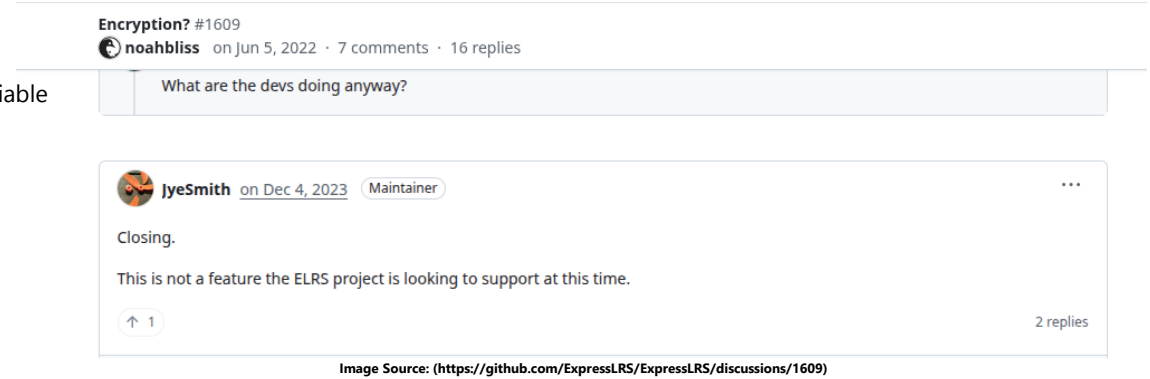


Image Source: (https://github.com/ExpressLRS/ExpressLRS/discussions/1609)

868MHz

- Older
- Lower Bandwidth
- More Robust
- Receivable with an RTLSDR

2.4GHz

- Higher Bandwidth
- Can be coupled in Gemini Mode(Dual Frequency, Dual Antenna)

ExpressLRS 868MHz

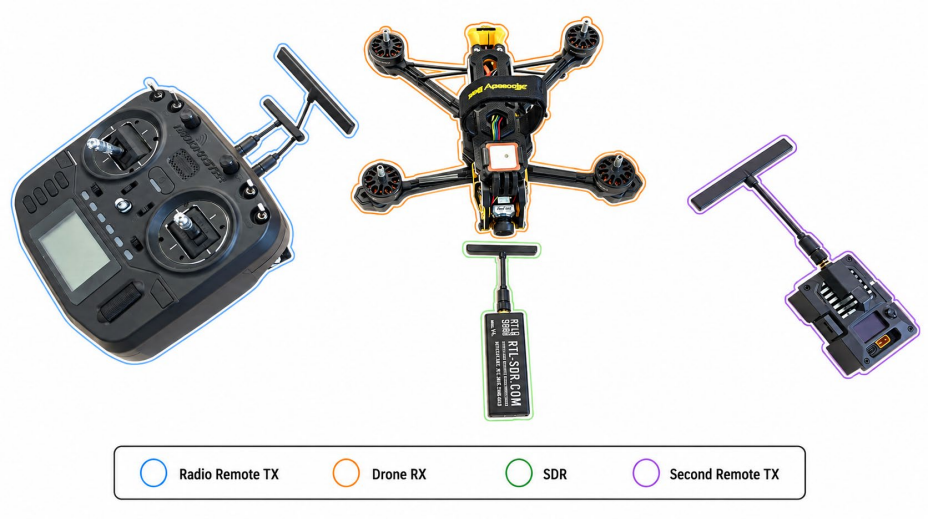
Technical Details

LoRa Parameter

- Based on the SX127x Modules
- LoRa BW 500kHz
- SF 6
- CR 4/7
- Preamble Length 8
- Payload Length 8

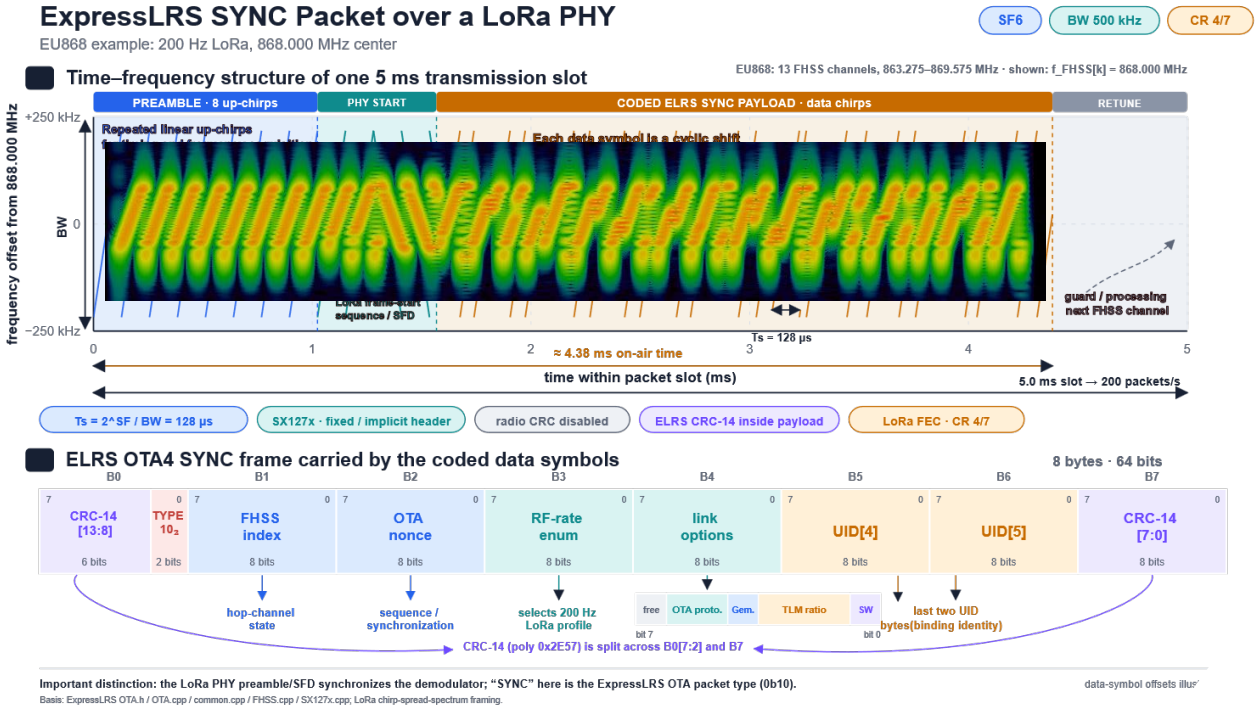
Software

- V2.X had a major "security vulnerability" **(Appleby, 2022)**.
- V3.6.3 can also be exploited.
- V4.X was released Feb 2026 and is also vulnerable.



Appleby, 2022. "Technical Advisory – ExpressLRS vulnerabilities allow for hijack of control link". https://www.nccgroup.com/research/technical-advisory-expresslrs-vulnerabilities-allow-for-hijack-of-control-link/

ELRS OTA STRUCTURE



ExpressLRS Hacking

Hijacking the Control Link

ExpressLRS Sniffer

- Reconstructs drone control packets
- Displays the control visually

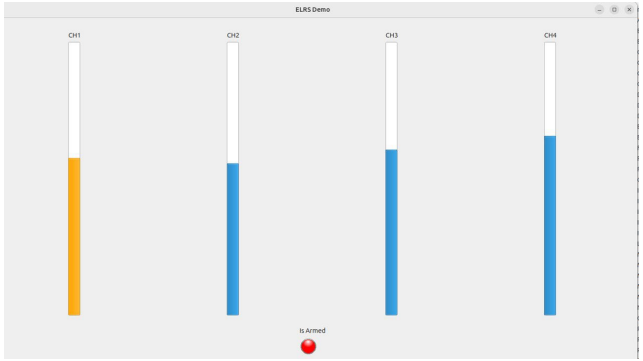
Benefits:

- Inexpensive (~50€) for an SDR-RTL
- Portable -> Windows, Linux, Android

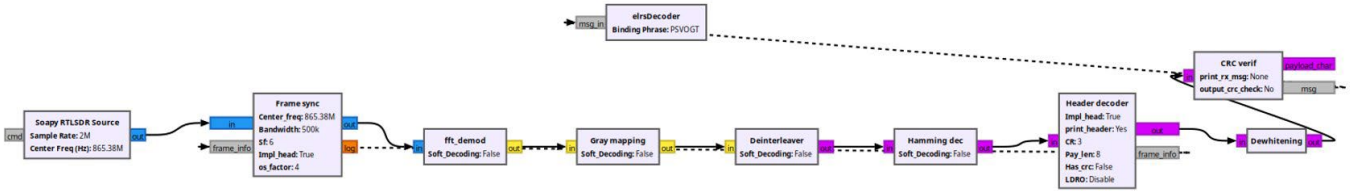
Further work:

- This approach may enable the use of smartphones as distributed sensor nodes for a perimeter detection system.





Demo: Reconstruction of the Drone Uplink



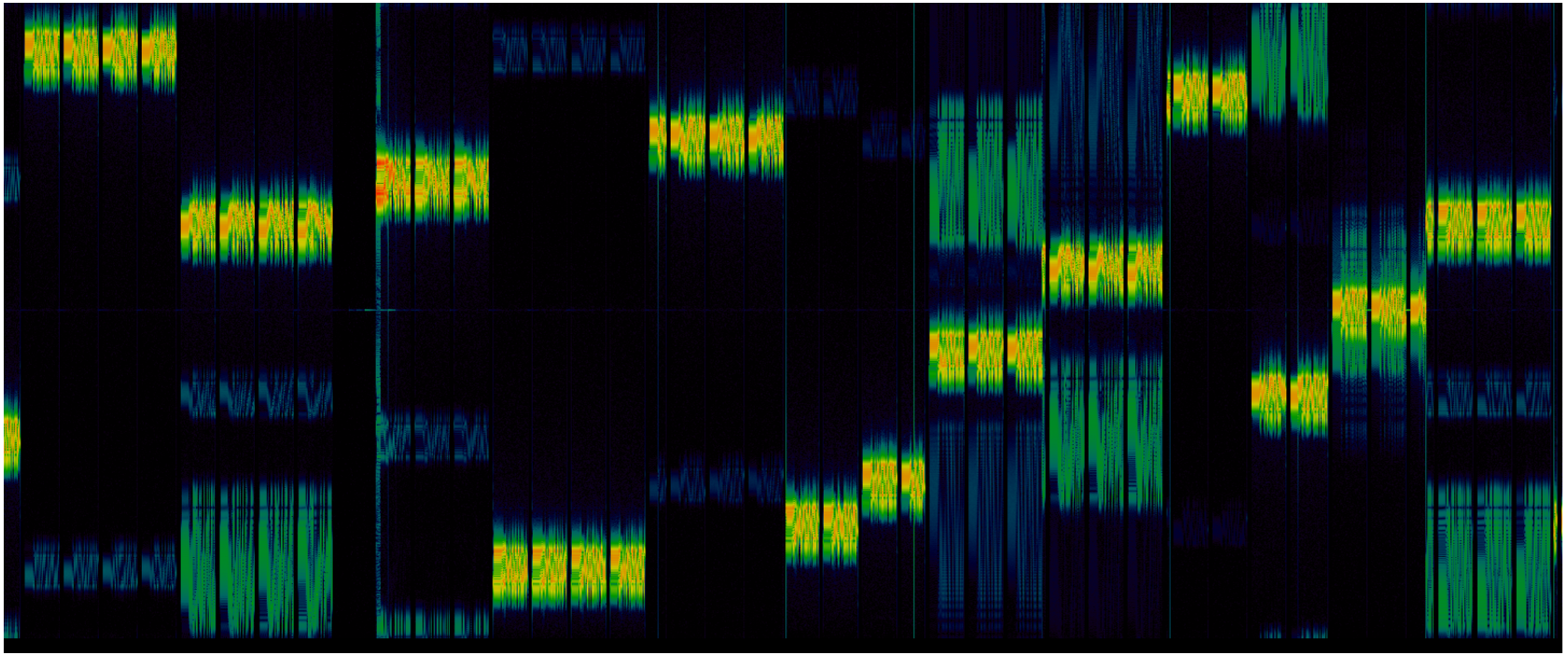
GNU Radio Workflow

Vogt et al., 2026, *"From Passive Capture to Control: Recovering ExpressLRS Link State for Commercial-off-the-Shelf Drone Hijacking"*. Submission in preparation.

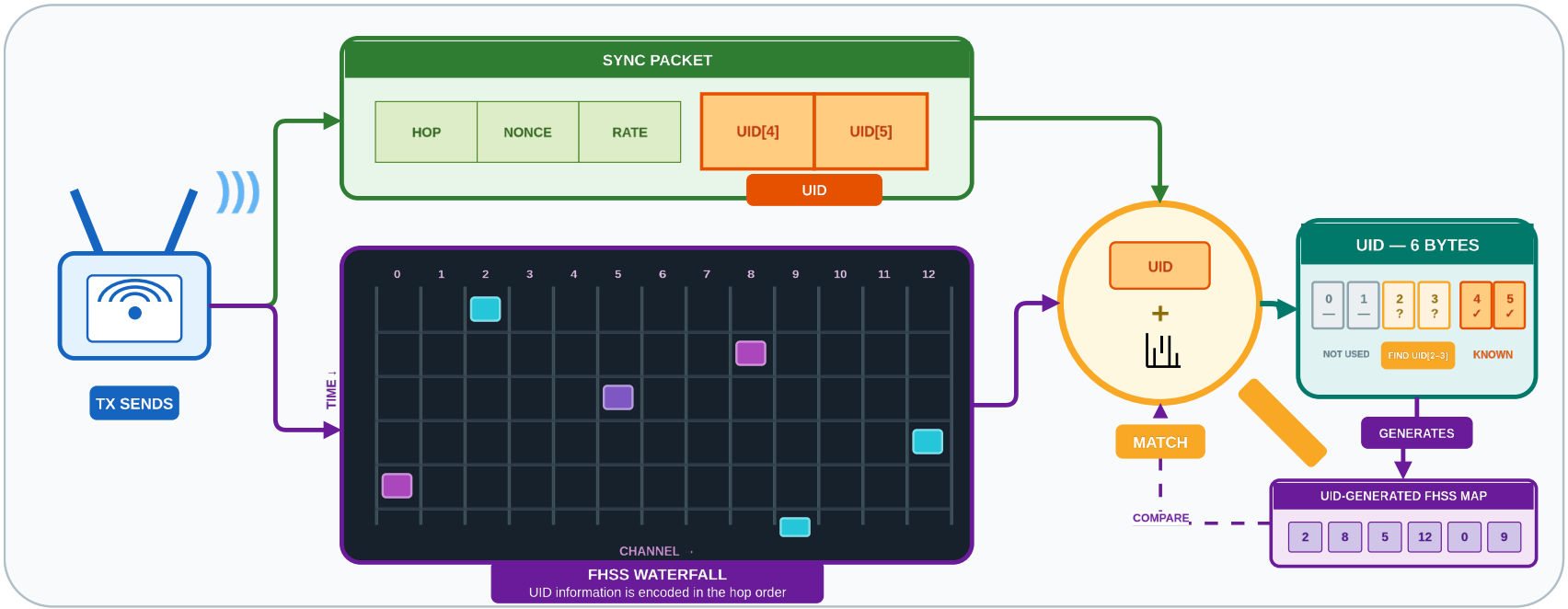
LIVE DEMO

Decoding the RC Channels

ELRS WITH FHSS HOPPING



ELRS SECRET EXTRACTION

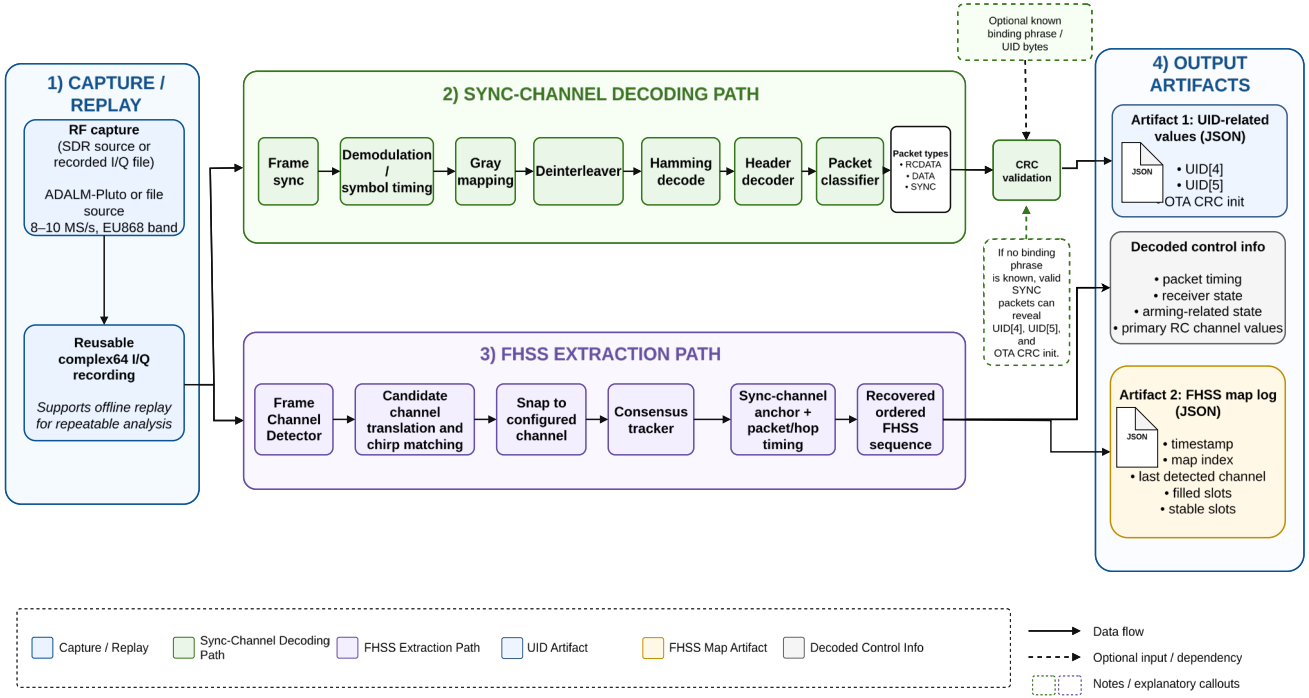


ELRS DECODING PIPELINE

With an **Adalm Pluto SDR**:

A **5 second** recording reveals the UID and therefore allows to clone the remote control -->

This allows to **hijack the drone**.



LIVE DEMO

Decoding UID

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Thank you!

Questions?

IT-SECX 2026

October 02, 2026



Foto: © Johannes Zinner

Philipp-Sebastian Vogt
Philipp.Vogt@ait.ac.at

References

(Appleby, 2022) Appleby, 2022. "Technical Advisory – ExpressLRS vulnerabilities allow for hijack of control link". https://www.nccgroup.com/research/technical-advisory-expresslrs-vulnerabilities-allow-for-hijack-of-control-link/

(Github dji_droneid, 2022) proto17, 2022. https://github.com/proto17/dji_droneid.

(Militarnyi, 2024) Militarnyi, 2024. "Perspective Market of Ukrainian Short-Range EW Systems". https://militarnyi.com/en/articles/perspective-market-of-ukrainian-short-range-ew-systems/

(Vogt et al., 2026) Vogt et al., 2026, "From Passive Capture to Control: Recovering ExpressLRS Link State for Commercial-off-the-Shelf Drone Hijacking". Submission in preparation.