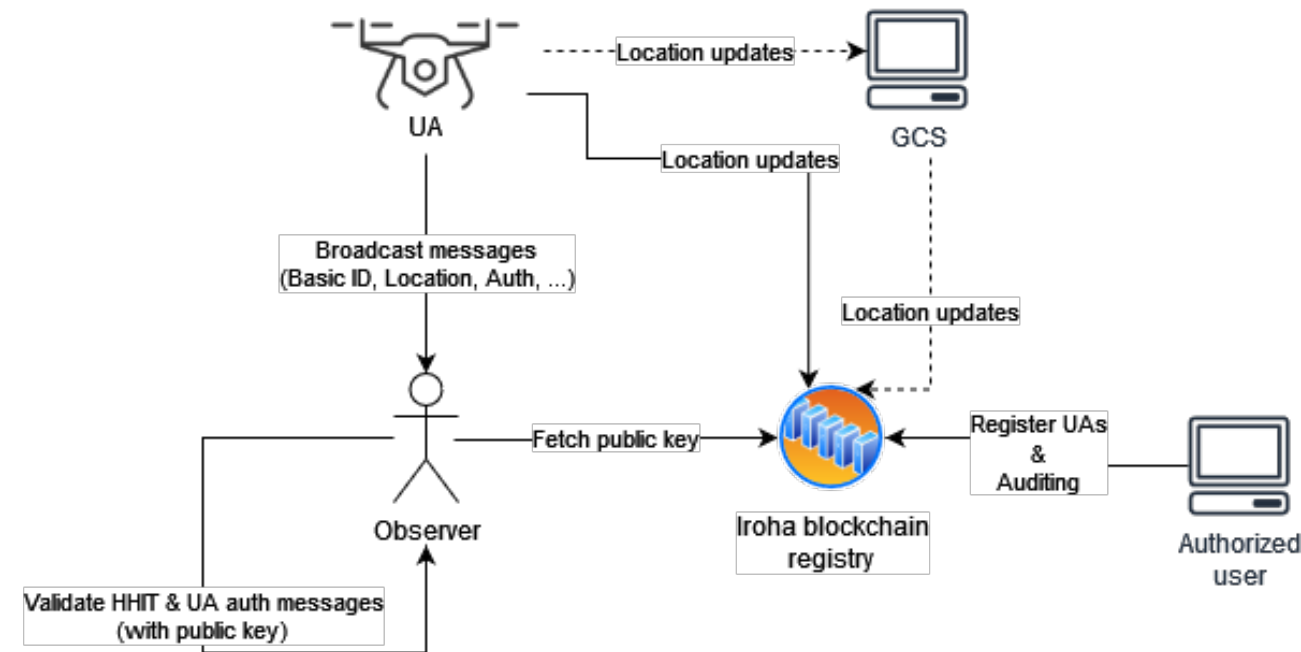


DRIP Experiments Update

IETF 115, 10th November 2022

Andrei Gurtov and students

DRIP Experimental Testbed



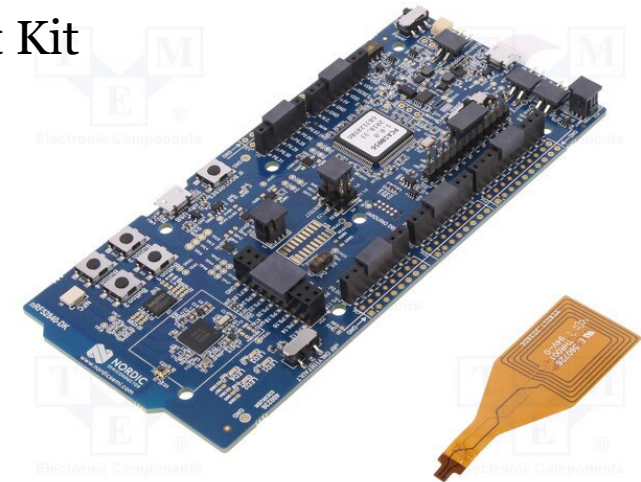
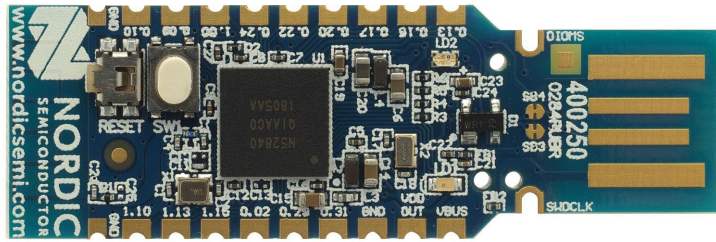
- Observers receive Direct RID messages, and perform lookups on registry
- UAs and GCSs send location updates to registry
- Admin registers new accounts (drone/operators)
- UAs do not participate in the blockchain

DRIP Interops & hackathon

- Some interop prior to IETF with Adam
 - HHIT format issues
 - Broadcast <-> app mutual compatibility
- IETF Hackathon
 - Mutual testing of Android app and DRIP implementations
 - Some success, issues identified

DRIP and Bluetooth 5

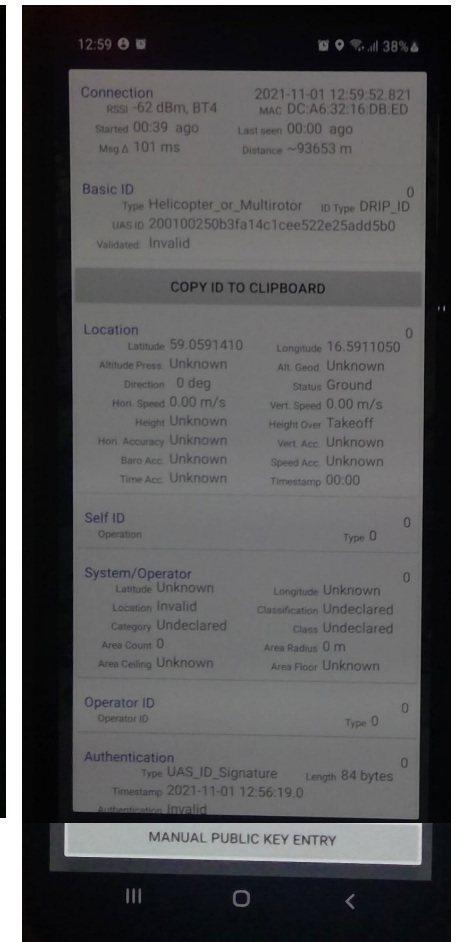
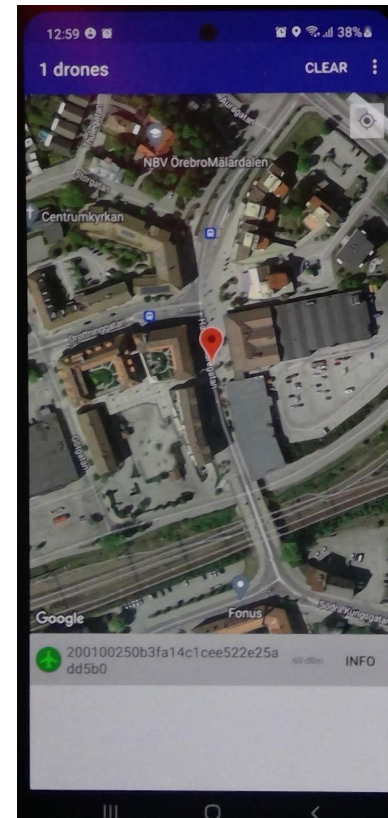
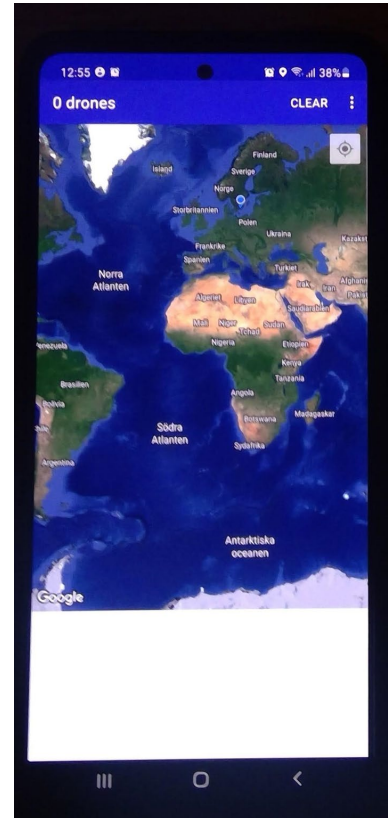
nRF52840 Dongle and Development Kit



Problem with Linux Drivers, also new external Bt5 dongle, now operational on RP4 after install of Ubuntu drivers. Need to add options to our script. BT5 works in NUC.

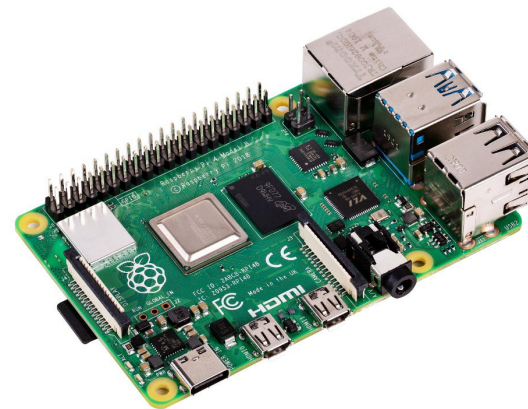
Observer application

- OpendroneID as a base
- Google API with maps required separate developer key
 - Hard to provide .apk packages
- Now in the progress to publish as Google Play App with OpenstreetMaps
 - Much bureaucracy



Hardware Kit for RP4

- Integrate with GPS and Battery Hat for on-the-drone mounting
- Antenna magnets disturbs drone compass -> remove!



DRIP on RP4 (ARM) and Phantom pro



19:31

67%

Connection

2022-07-08 19:31:20.381

RSI -32 dBm, BT4

MAC DC:A6:32:16:DC:95

Started 00:26 ago

Last seen 00:00 ago

Msg Δ 101 ms

Distance ~3 m

Basic ID

Type Helicopter_or_Multirotor

ID Type DRIP_ID

UAS ID 200100250b3fa14c1cee522e25add5b0

Unknown due to server issues or failed manua

Validated: entry

COPY ID TO CLIPBOARD

Location

Latitude 58.3654117

Longitude 15.7051900

Altitude Press. Unknown

Alt. Geod. 72.0 m

Direction 256 deg

Status Ground

Hori. Speed 0.00 m/s

Vert. Speed 0.00 m/s

Height Unknown

Height Over Takeoff

Hori. Accuracy Unknown

Vert. Acc. Unknown

Baro Acc. Unknown

Speed Acc. Unknown

Time Acc. Unknown

Timestamp 31:21

Self ID

Operation

Type 0

System/Operator

Latitude Unknown

Longitude Unknown

Location Invalid

Classification Undeclared

Category Undeclared

Class Undeclared

Area Count 0

Area Radius 0 m

Area Ceiling Unknown

Area Floor Unknown

Operator ID

Operator ID

Type 0

Authentication

UAS ID Signature

84 bytes

19:32

66%

2 drones

CLEAR

200100250b3fa14c1cee522e25add5b0

-32 dBm

INFO

46443334353442373738453536354332

-58 dBm

INFO

zebraland.ida.liu.se:8080/

https://zebraland.ida.liu.se:8080/

Luncha | Mjärdevi | Va... Webreg

Other Bookmarks

Register Drone

Enter Name:

Enter ID:

Enter Model:

Enter Public Key:

Submit

New Unit of Computing on DJI Matrics 300



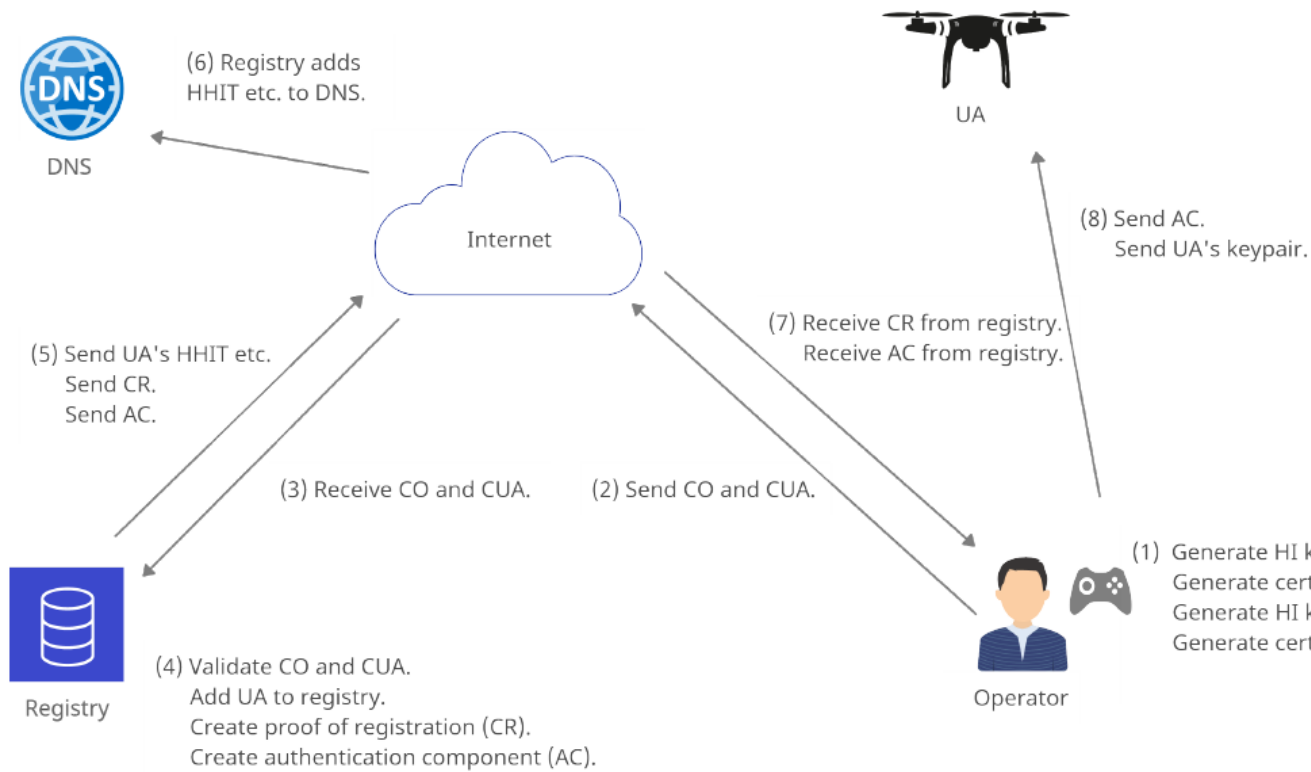
- New Unit of Computing (NUC)
Intel running DRIP remote ID over BT4 via API to a drone hardware (power, GPS)
- x86 architecture, Ubuntu Linux
- 5G modem
- Built-in BT4, BT5, WiFi

Wallenberg AI, Autonomous Systems and Software Program



- Public Safety Arena (sea rescue)
- Demo at [WASP-PS Arena](#) (Thanks Tommy and AIICS group)
- Pick up BT4 signal at 160m using Galaxy 10 phone.
- Also test OpenDroneID on NUC
 - Developed GPS patch
 - App backward compatible

Formal Analysis of DRIP with Tamarin



Lemma	Scope	Result
Executable	Exists-trace	Verified
Session_key_secrecy	All-traces	Verified
Aliveness	HIP BEX Session Key	Verified
Weak agreement	HIP BEX Session Key	Verified
Non-injective agreement	HIP BEX Session Key	Verified
Injective agreement	HIP BEX Session Key	Falsified

OpenHIP Updates

<https://bitbucket.org/openhip/openhip/src/master/>

HHIT support, new crypto, HIPv2 branches

Added Docker container for easier cross-platform installation and testing

OpenSSL 3.0

Current Status

- OpenHIP used OpenSSL 1.0.x
 - Support for OpenSSL 1.1.0 in Fall 2020
 - OpenSSL 3.0.0 was released in September 2021
 - 1.1.1 support ends in a year
-
- Current OpenSSL implementation lacks forward compatibility
 - High cohesion in the code that uses OpenSSL
 - Large amount of deprecated methods
 - Not all deprecated methods have one-to-one equivalents in 3.0.0
 - Code compiles, but needs testing