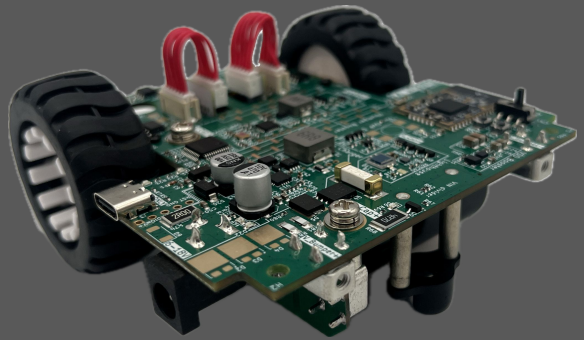
DotBots in the LAKE





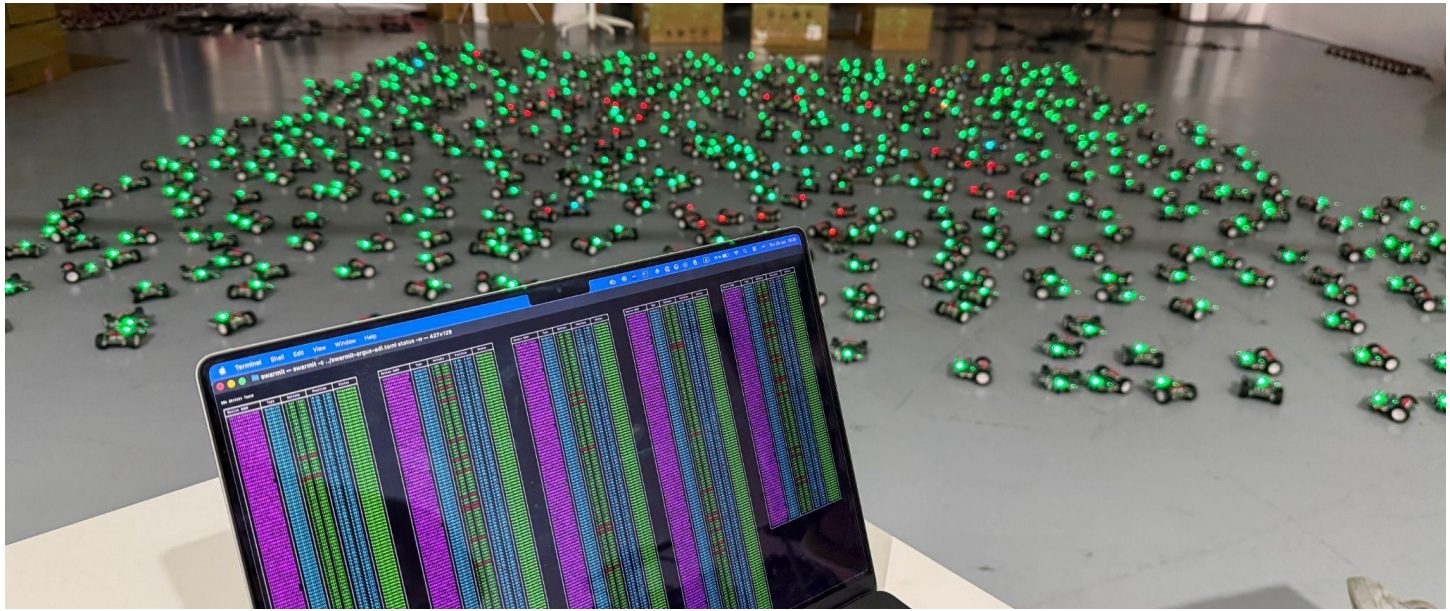
geovane.fedrecheski@inria.fr

IETF 126 | Vienna, Austria | July, 19, 2026

Problem

We want to deploy IETF protocols to a testbed of (up to) 1,000 robots!

The DotBot Testbed ➡️



https://pydotbot.readthedocs.io/en/latest

Context

1️⃣ **lakers** - formally-verified **Rust** implementation of **EDHOC (RFC 9528)**:

- lightweight authenticated key exchange for constrained IoT.

```
$ cargo add lakers
```

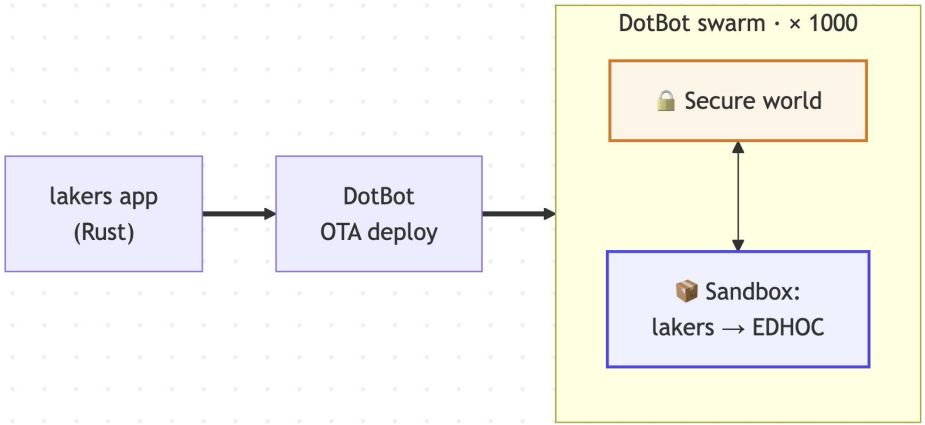
2️⃣ **DotBot testbed** - up to 1000 **nRF5340-based robots**.

- **ARM TrustZone sandbox** + **OTAP** over a **TSCH** radio network

```
$ pip install pydotbot
```

🟣 **IDEA: deploy lakers onto DotBots!**

- Use the testbed as an instrument to **deploy and measure IETF protocol code on real hardware, at scale**
- Challenge: first time running Rust code on the DotBot sandbox (DotBots firmware is in C)



Plan

- 🟣 **Phase 1** - first embedded Rust on the nRF5340 app core (bare).
- 🟣 **Phase 2** - bare Rust inside the DotBot TrustZone sandbox
- 🟣 **Phase 3** - lakers EDHOC handshake bare (on-chip loopback): get real timing on the Cortex-M33.
- 🟣 **Phase 4** - lakers EDHOC running inside the sandbox.

What got done

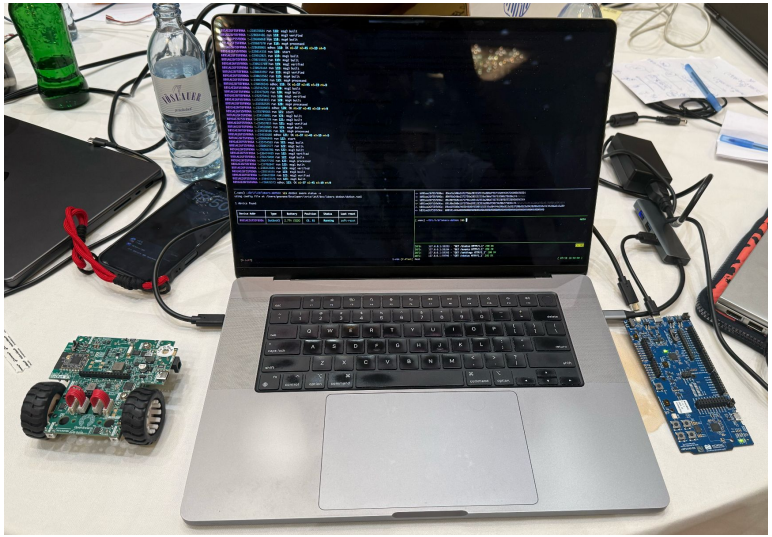
✅ **Phase 1** - first embedded Rust on the nRF5340 app core (bare).

✅ **Phase 2** - bare Rust inside the DotBot TrustZone sandbox

✅ **Phase 3** - lakers EDHOC handshake bare (on-chip loopback): get real timing on the Cortex-M33.

✅ **Phase 4** - lakers EDHOC running inside the sandbox.

- compile lakers EDHOC app, OTAP onto DotBots, full (local) handshake in **< 1 s**



```
B891AE26F55FB96A t=38959008 run 21: start
B891AE26F55FB96A t=39056724 run 21: msg1 built
B891AE26F55FB96A t=39359740 run 21: msg2 built
B891AE26F55FB96A t=39667363 run 21: msg2 verified
B891AE26F55FB96A t=39670868 run 21: msg3 built
B891AE26F55FB96A t=39776660 run 21: msg3 verified
B891AE26F55FB96A t=39778252 run 21: msg4 built
B891AE26F55FB96A t=39779752 run 21: msg4 processed
B891AE26F55FB96A t=39781248 edhoc 21: OK m1=37 m2=45 m3=19 m4=9
```

```
(.venv) ~/D/i/i/d/lakers-dotbot ❯❯❯ dotbot swarm status -w
using config file at /Users/geovane/Developer/inria/ietf/dev/lakers-dotbot/dotbot.toml

1 device found
```

Device Addr	Type	Battery	Position	Status	Last reset
B891AE26F55FB96A	DotBotV3	2.79V (93%)	(0, 0)	Running	soft-reset

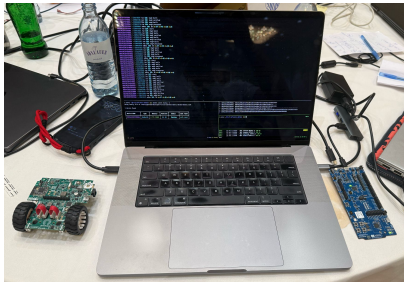
Final

✅ **Conclusion**:

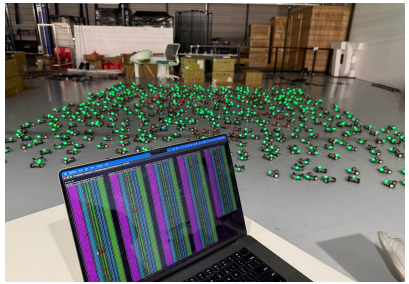
- The DotBots Testbed can be used to test IETF protocols
  - built-in mobility support, cryptographic accelerator, 2 Mbps radio
- Language is not a barrier (we just demonstrated Rust on it for the first time)

🟣 **Next steps**:

- message- and location-triggered handshakes
- DotBot <-> laptop via `lakers-python`
- scale to 10, 100, 1000 DotBots



➡️



➡️ We are looking for funding! geovane.fedrecheski@inria.fr