Named Data Networking of Things: NDN-RIOT Progress Update

March 30, 2017
ICNMRG Meeting, Chicago, IL, US
NDN-RIOT Overall Goals

- Enable flexible experimentation with NDN IoT apps on RIOT-OS
  - Capture the “edge” of edge-in effort
- Support for NDN packet format for limited MTU links
- Support of data-centric security, including ECDSA and HMAC signatures, AES encryption
- Support replaceable forwarding strategies
- Support of transmission (+fragmentation) over IEEE 802.15.4 and Ethernet
- Become the networking stack in RIOT-OS 😊

https://github.com/named-data-iot/ndn-riot
Recent progress

- Added basic forwarding strategy framework
  - Define callback functions (hooks) at three critical points in the forwarding pipeline
    - After Interest is received
    - Before Interest is satisfied by Data
    - Before Interest expires in PIT
  - Callback functions have full access to forwarder’s internal data structures
    - FIB, PIT, CS, …
  - Applications can set forwarding strategy choice through API
Recent progress

- **AES-CCM signature type**
  - AES-CCM is an authenticated encryption scheme:
    - (additional data, plaintext, nonce, key) \(\rightarrow\) (additional data, ciphertext, auth_tag)
    - Authentication tag covers both “additional data” and plaintext
  - Define a new content type for CCM-encrypted Data packet
    - Data packet format:
      - Name | Metadata | Nonce | Ciphertext | AuthTag
      - Content:
        - ContentType = CCM
        - 8 bytes
        - 12 bytes

- Additional data = \{Name, Metadata, Nonce\}
- CCM algorithm takes “additional data” in continuous block and outputs \{ciphertext, auth_tag\} in continuous block
**NDN-RIOT and RIOT Integration**

Currently, a fork of official RIOT-OS repo

- **8c1b977f4** tests/unit_tests/test_tests-ndn_encoding: add unit tests for ndn_encoding module
- **6d3d446a1** net/gnrc/auto_init: Add prerequisites for NDN-RIOT module
- **0afa547a5** crypto: fix bugs in ccm mode (under review)
- **ba7f1af7a** pkg/micro-ecc: support boards without hwrng feature (merged)
- **600c8f626** hashes/sha256: support unaligned memory access in be32enc_vect (merged)
Getting Started

- First, set up dev environment
  - https://github.com/RIOT-OS/RIOT/wiki/Family:-native#dependencies

Then type the following commands:

```
mkdir my_riot_dir
cd my_riot_dir
git clone https://github.com/named-data-iot/RIOT
git clone https://github.com/named-data-iot/ndn-riot
git clone https://github.com/named-data-iot/ndn-riot-examples
cd ndn-riot-examples/ndn-ping
make
```

Follow https://github.com/RIOT-OS/RIOT/wiki/Virtual-riot-network to set up virtual network with 2 tap devices, then launch a RIOT instance on each tap device
Running Basic Examples (In Emulation Mode)

On tap0 device:

```bash
ndnping server /prefix repo1
```

This will set tap0 device to listen on /prefix and generate data under /prefix/repo1

On tap1 device:

```bash
ndnping client /prefix 20
```

This will set tap1 device to ping /prefix for 20 times
Running Basic Examples (For Real)

- Flash devices
  - One with ping client
  - One with ping server

- Ping should be running after that