DRIP Implementation

Andrei Gurtov & students

Linköping University, Sweden

DRIP IETF 109th Online Meeting

November 18, 2020

Starting Points

- OpenHIP (v2 alpha branch) - 4 students
    - https://bitbucket.org/openhip/
    - draft-moskowitz-hip-new-crypto-06
- OpenDroneID - 5 students
    - https://www.opendroneid.org/code/
- TDDE21 Advanced Project: Secure Distributed and Embedded Systems (6 ECTS) Sep-Dec 2020
    - https://www.ida.liu.se/~TDDE21/

New Requirements for HIPv2

- New cryptographic algorithm (EdDSA)

- New ORCHIDs - include additional info in Host Identity Tag (HIT), needed for hierarchical HITs

- Hierarchical HITs - embed information about the issuing authority inside HIT

New ORCHID

- Overlay Routable Cryptographic Hash Identifiers
- Endpoint identifiers at applications
- Before => ORCHID := Prefix | OGA ID | Encode_96(Hash)
  - Prefix = 2001:20::/28 (IANA)
  - ODA ID = 4 bit hash identifier
  - Encode_96(Hash) = Middle 96 bits of the hash output
- Now => ORCHID := Prefix | OGA ID | Info (n) | Hash (m)
  - New prefix for HHITs
  - Hash(m) = Hash function which outputs m bits, use cSHAKE
  - Encode_96(Hash) split into Info(n) and Hash(m), Info(n) used in HHITs as a tag

New Crypto

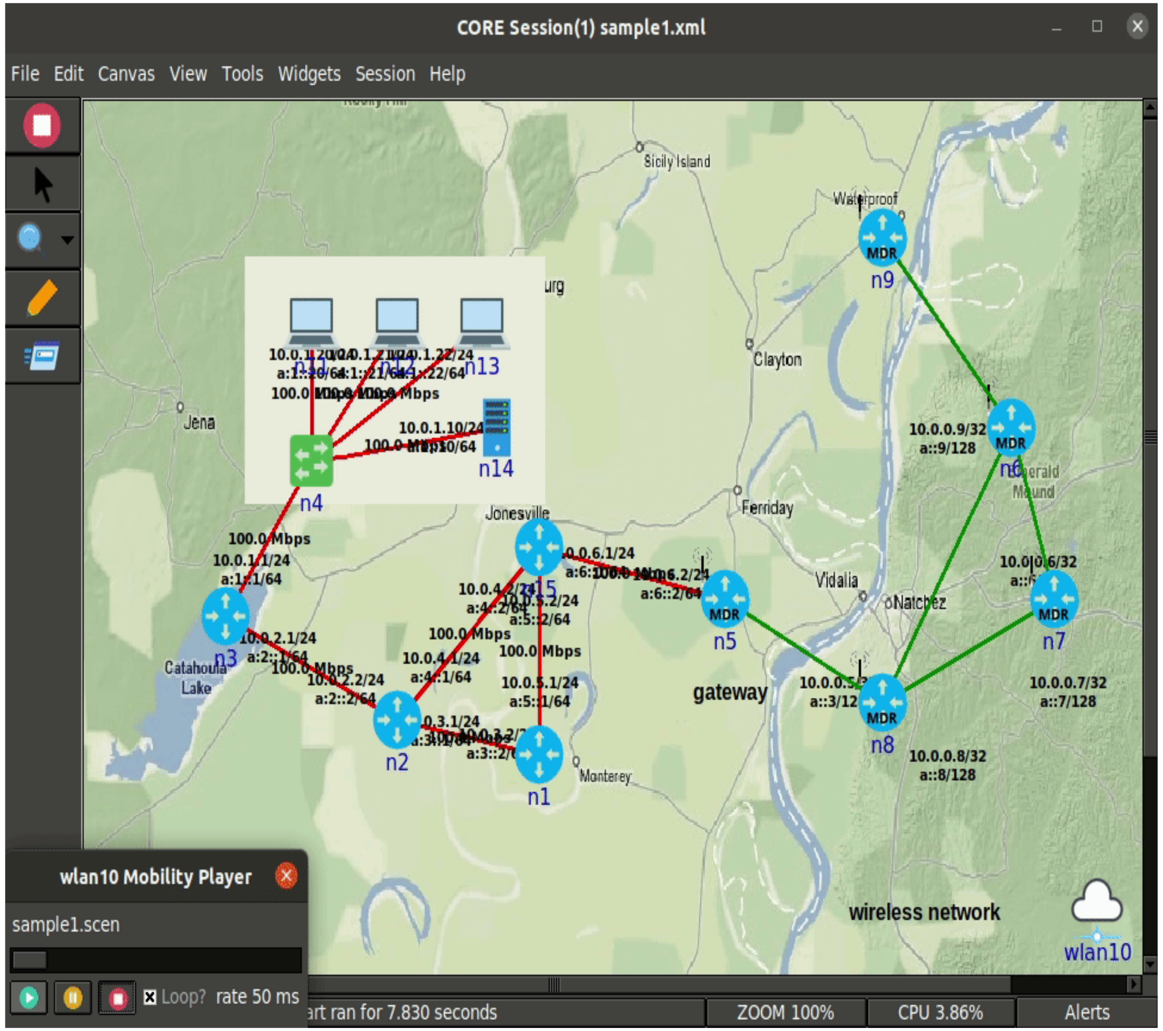
- EdDSA (Edwards-curve Digital Signature Algorithm) is a digital signature scheme that is based on elliptic-curve cryptography.
  - Designed to be a fast algorithm without sacrificing security
  - Less dependent on a good random number generator, compared to ECDSA

- The Keyak cipher is used as a lightweight alternative to AES, and also supports authentication of the encrypted data
  - Move to Xoodyak, follow NIST

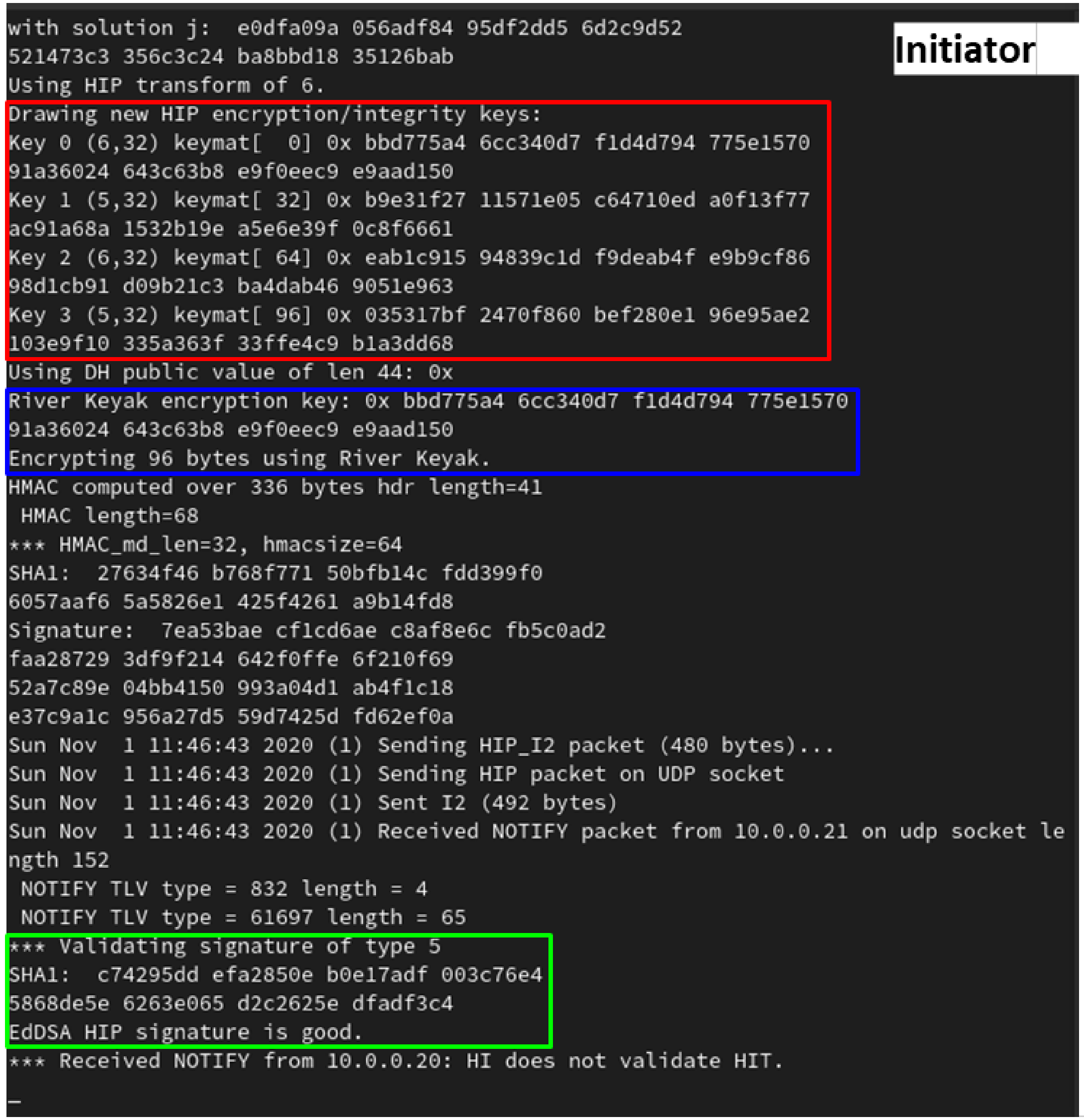
- The KKDF key derivation function (based on KMAC) is a more efficient alternative to the HMAC-based HKDF

Testing

- Common Open Research Emulator (CORE)
  - Emulate real computer networks
- Current tests
  - ✓ Python 3.8
  - ✓ Core 7.2
  - ✓ Use of standard libraries
  - ✓ Separation of concerns

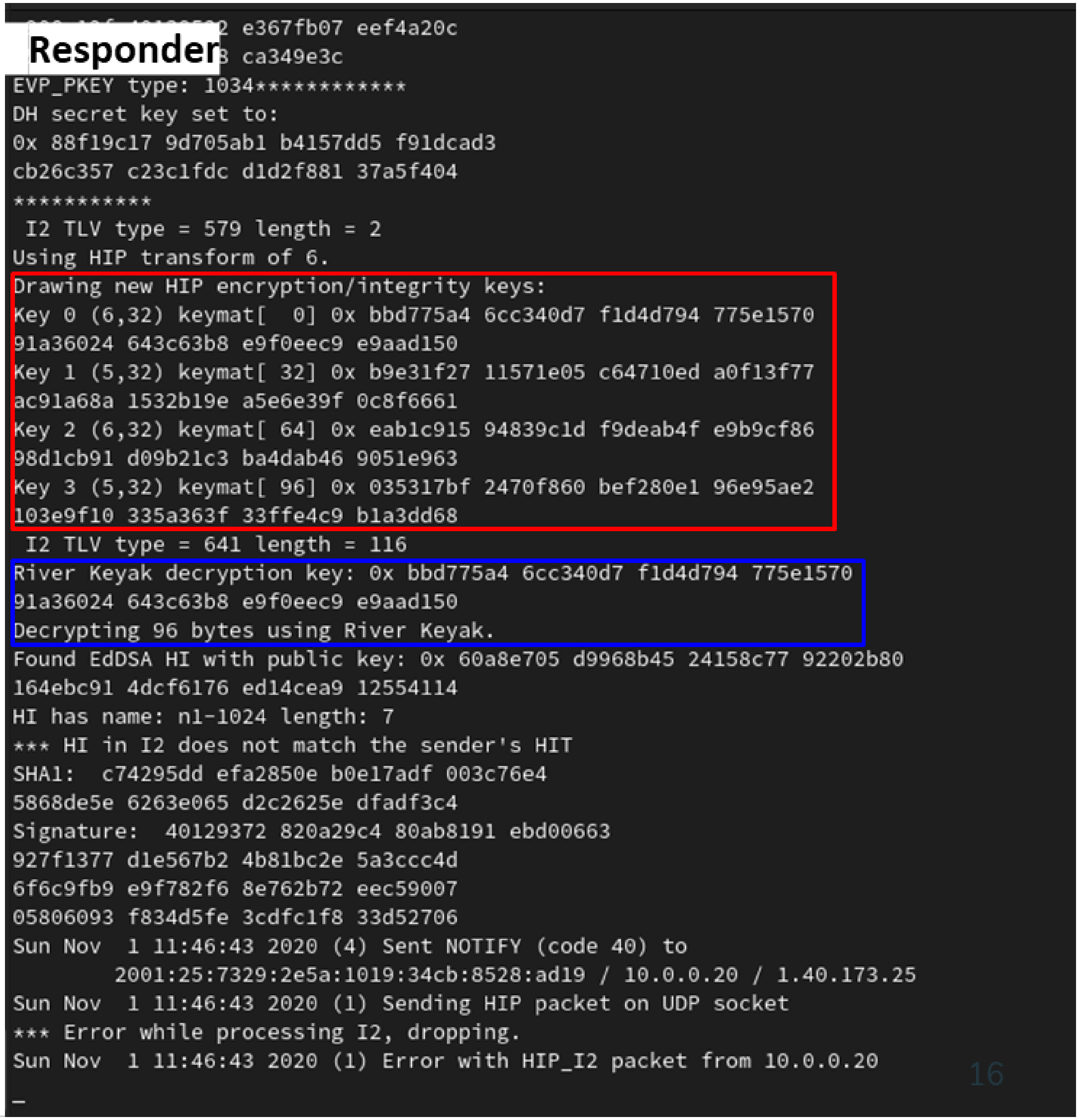


HIPv2 New Base Exchange Works



Initiator

```
with solution j:  e0dfa09a 056adf84 95df2dd5 6d2c9d52
521473c3 356c3c24 ba8bbd18 35126bab
Using HIP transform of 6.
Drawing new HIP encryption/integrity keys:
Key 0 (6,32) keymat[  0] 0x bbd775a4 6cc340d7 f1d4d794 775e1570
91a36024 643c63b8 e9f0eec9 e9aad150
Key 1 (5,32) keymat[ 32] 0x b9e31f27 11571e05 c64710ed a0f13f77
ac91a68a 1532b19e a5e6e39f 0c8f6661
Key 2 (6,32) keymat[ 64] 0x eab1c915 94839c1d f9deab4f e9b9cf86
98d1cb91 d09b21c3 ba4dab46 9051e963
Key 3 (5,32) keymat[ 96] 0x 035317bf 2470f860 bef280e1 96e95ae2
103e9f10 335a363f 33ffe4c9 b1a3dd68
Using DH public value of len 44: 0x
River Keyak encryption key: 0x bbd775a4 6cc340d7 f1d4d794 775e1570
91a36024 643c63b8 e9f0eec9 e9aad150
Encrypting 96 bytes using River Keyak.
HMAC computed over 336 bytes hdr length=41
 HMAC length=68
*** HMAC_md_len=32, hmacsize=64
SHA1:  27634f46 b768f771 50bfb14c fdd399f0
6057aaf6 5a5826e1 425f4261 a9b14fd8
Signature:  7ea53bae cf1cd6ae c8af8e6c fb5c0ad2
faa28729 3df9f214 642f0ffe 6f210f69
52a7c89e 04bb4150 993a04d1 ab4f1c18
e37c9a1c 956a27d5 59d7425d fd62ef0a
Sun Nov  1 11:46:43 2020 (1) Sending HIP_I2 packet (480 bytes)...
Sun Nov  1 11:46:43 2020 (1) Sending HIP packet on UDP socket
Sun Nov  1 11:46:43 2020 (1) Sent I2 (492 bytes)
Sun Nov  1 11:46:43 2020 (1) Received NOTIFY packet from 10.0.0.21 on udp socket le
ngth 152
 NOTIFY TLV type = 832 length = 4
 NOTIFY TLV type = 61697 length = 65
*** Validating signature of type 5
SHA1:  c74295dd efa2850e b0e17adf 003c76e4
5868de5e 6263e065 d2c2625e dfadf3c4
EdDSA HIP signature is good.
*** Received NOTIFY from 10.0.0.20: HI does not validate HIT.
_
```



Responder

```
                    2 e367fb07 eef4a20c
                    3 ca349e3c
EVP_PKEY type: 1034*************
DH secret key set to:
0x 88f19c17 9d705ab1 b4157dd5 f91dcad3
cb26c357 c23c1fdc d1d2f881 37a5f404
***********
 I2 TLV type = 579 length = 2
Using HIP transform of 6.
Drawing new HIP encryption/integrity keys:
Key 0 (6,32) keymat[  0] 0x bbd775a4 6cc340d7 f1d4d794 775e1570
91a36024 643c63b8 e9f0eec9 e9aad150
Key 1 (5,32) keymat[ 32] 0x b9e31f27 11571e05 c64710ed a0f13f77
ac91a68a 1532b19e a5e6e39f 0c8f6661
Key 2 (6,32) keymat[ 64] 0x eab1c915 94839c1d f9deab4f e9b9cf86
98d1cb91 d09b21c3 ba4dab46 9051e963
Key 3 (5,32) keymat[ 96] 0x 035317bf 2470f860 bef280e1 96e95ae2
103e9f10 335a363f 33ffe4c9 b1a3dd68
 I2 TLV type = 641 length = 116
River Keyak decryption key: 0x bbd775a4 6cc340d7 f1d4d794 775e1570
91a36024 643c63b8 e9f0eec9 e9aad150
Decrypting 96 bytes using River Keyak.
Found EdDSA HI with public key: 0x 60a8e705 d9968b45 24158c77 92202b80
164ebc91 4dcf6176 ed14cea9 12554114
HI has name: n1-1024 length: 7
*** HI in I2 does not match the sender's HIT
SHA1:  c74295dd efa2850e b0e17adf 003c76e4
5868de5e 6263e065 d2c2625e dfadf3c4
Signature:  40129372 820a29c4 80ab8191 ebd00663
927f1377 d1e567b2 4b81bc2e 5a3ccc4d
6f6c9fb9 e9f782f6 8e762b72 eec59007
05806093 f834d5fe 3cdfc1f8 33d52706
Sun Nov  1 11:46:43 2020 (4) Sent NOTIFY (code 40) to
        2001:25:7329:2e5a:1019:34cb:8528:ad19 / 10.0.0.20 / 1.40.173.25
Sun Nov  1 11:46:43 2020 (1) Sending HIP packet on UDP socket
*** Error while processing I2, dropping.
Sun Nov  1 11:46:43 2020 (1) Error with HIP_I2 packet from 10.0.0.20
_
```

DRIP Implementation

Broadcast a Drone ID over Bluetooth or WiFi as a HIP Host identity tag

- Raspberry Pi + GPS receiver
- 20 Bytes
- Observer app in Android
- Specifications from DRIP IETF Working Group
    - UAS Remote ID: draft-ietf-drip-uas-rid-01

Android Application

Extending software

OpenDroneID

- Bluetooth only
- Includes parser for Bluetooth messages
- Functionality for Maps, points and information about the drone inside the GUI

WifiAnalyzer

- Analyzing Wifi-networks
- Bands, SSID, connectivity status, and more

Method to scan

- Connect to each individual drone (Since the raspberry Pi needs to be its own access point).
- Read and parse the messages the drone is sending.

Android Application for Observer

- New application to test the wifi in isolation
- Adding the wifi-module to the OpenDroneID Bluetooth receiver

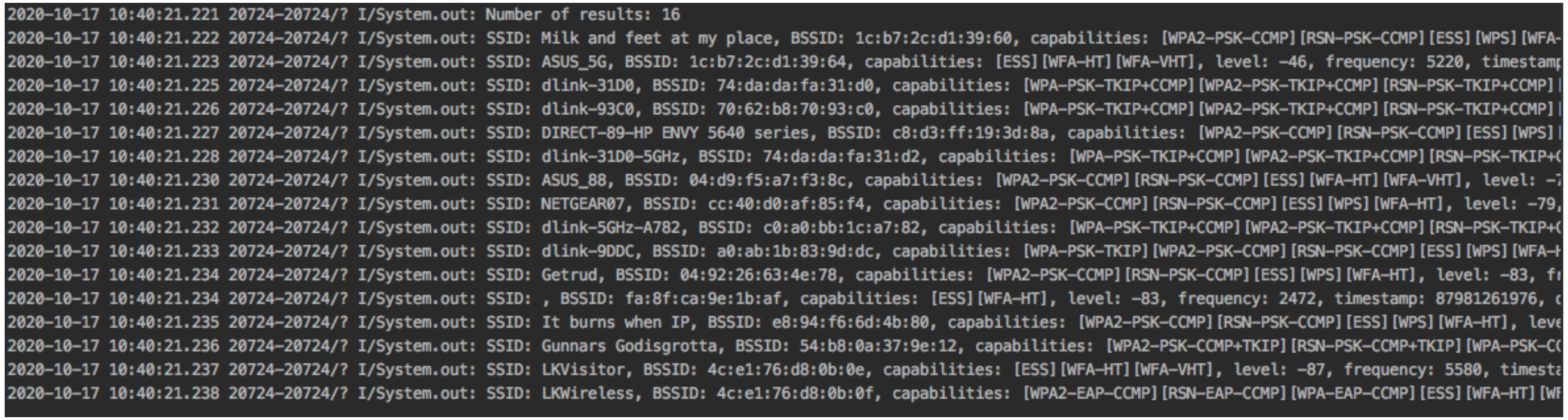
Currently:

- Reading WiFi-SSIDs. Next: WiFi NAN mode?
- No low-level broadcast reading
- Researching open source WiFi scanning applications for methods already in use

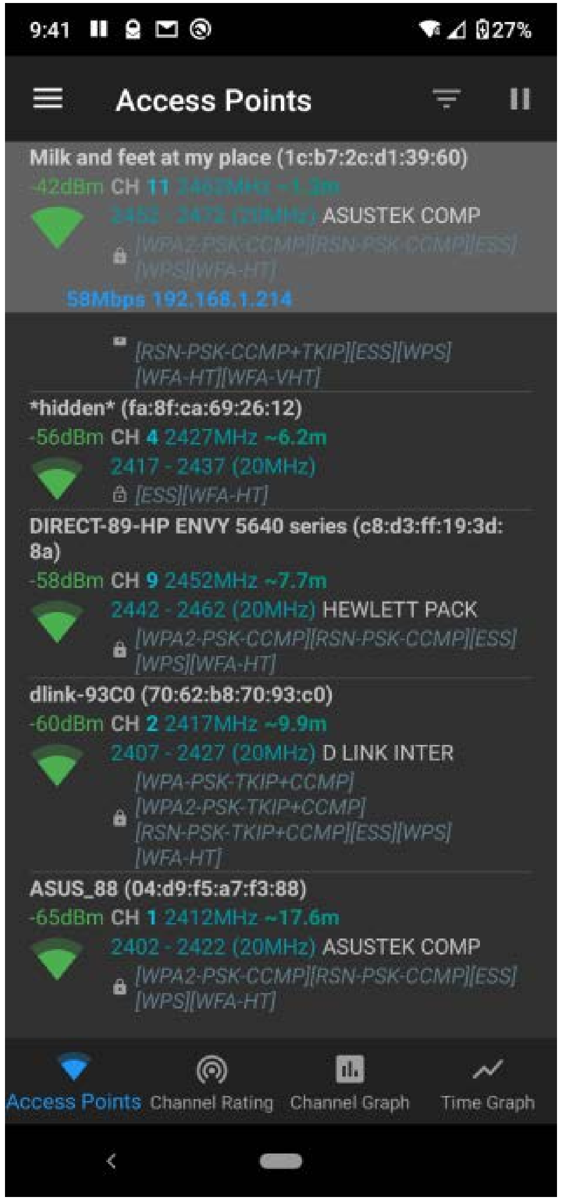
Possible switch to Linux application to get low-level access to broadcast messages since methods in Android might require rooting the Android device.

Android (images)

This is WiFi. Maybe a dead-end.
Now switched to Bluetooth 4&5 connectivity, less issues.



```
2020-10-17 10:40:21.221 20724-20724/? I/System.out: Number of results: 16
2020-10-17 10:40:21.222 20724-20724/? I/System.out: SSID: Milk and feet at my place, BSSID: 1c:b7:2c:d1:39:60, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-
2020-10-17 10:40:21.223 20724-20724/? I/System.out: SSID: ASUS_5G, BSSID: 1c:b7:2c:d1:39:64, capabilities: [ESS][WFA-HT][WFA-VHT], level: -46, frequency: 5220, timestamp
2020-10-17 10:40:21.225 20724-20724/? I/System.out: SSID: dlink-31D0, BSSID: 74:da:da:fa:31:d0, capabilities: [WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][RSN-PSK-TKIP+CCMP]
2020-10-17 10:40:21.226 20724-20724/? I/System.out: SSID: dlink-93C0, BSSID: 70:62:b8:70:93:c0, capabilities: [WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][RSN-PSK-TKIP+CCMP]
2020-10-17 10:40:21.227 20724-20724/? I/System.out: SSID: DIRECT-89-HP ENVY 5640 series, BSSID: c8:d3:ff:19:3d:8a, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS]
2020-10-17 10:40:21.228 20724-20724/? I/System.out: SSID: dlink-31D0-5GHz, BSSID: 74:da:da:fa:31:d2, capabilities: [WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][RSN-PSK-TKIP+
2020-10-17 10:40:21.230 20724-20724/? I/System.out: SSID: ASUS_88, BSSID: 04:d9:f5:a7:f3:8c, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WFA-HT][WFA-VHT], level: -
2020-10-17 10:40:21.231 20724-20724/? I/System.out: SSID: NETGEAR07, BSSID: cc:40:d0:af:85:f4, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT], level: -79,
2020-10-17 10:40:21.232 20724-20724/? I/System.out: SSID: dlink-5GHz-A782, BSSID: c0:a0:bb:1c:a7:82, capabilities: [WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][RSN-PSK-TKIP+
2020-10-17 10:40:21.233 20724-20724/? I/System.out: SSID: dlink-9DDC, BSSID: a0:ab:1b:83:9d:dc, capabilities: [WPA-PSK-TKIP][WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-
2020-10-17 10:40:21.234 20724-20724/? I/System.out: SSID: Getrud, BSSID: 04:92:26:63:4e:78, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT], level: -83, f
2020-10-17 10:40:21.234 20724-20724/? I/System.out: SSID: , BSSID: fa:8f:ca:9e:1b:af, capabilities: [ESS][WFA-HT], level: -83, frequency: 2472, timestamp: 87981261976,
2020-10-17 10:40:21.235 20724-20724/? I/System.out: SSID: It burns when IP, BSSID: e8:94:f6:6d:4b:80, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT], leve
2020-10-17 10:40:21.236 20724-20724/? I/System.out: SSID: Gunnars Godisgrotta, BSSID: 54:b8:0a:37:9e:12, capabilities: [WPA2-PSK-CCMP+TKIP][RSN-PSK-CCMP+TKIP][WPA-PSK-C
2020-10-17 10:40:21.237 20724-20724/? I/System.out: SSID: LKVisitor, BSSID: 4c:e1:76:d8:0b:0e, capabilities: [ESS][WFA-HT][WFA-VHT], level: -87, frequency: 5580, timesta
2020-10-17 10:40:21.238 20724-20724/? I/System.out: SSID: LKWireless, BSSID: 4c:e1:76:d8:0b:0f, capabilities: [WPA2-EAP-CCMP][RSN-EAP-CCMP][WPA-EAP-CCMP][ESS][WFA-HT][W
```



Milk and feet at my place (1c:b7:2c:d1:39:60)
-42dBm CH 11 2462MHz ~1.2m
2452 - 2472 (20MHz) ASUSTEK COMP
[WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT]
58Mbps 192.168.1.214

[RSN-PSK-CCMP+TKIP][ESS][WPS][WFA-HT][WFA-VHT]

hidden (fa:8f:ca:69:26:12)
-56dBm CH 4 2427MHz ~6.2m
2417 - 2437 (20MHz)
[ESS][WFA-HT]

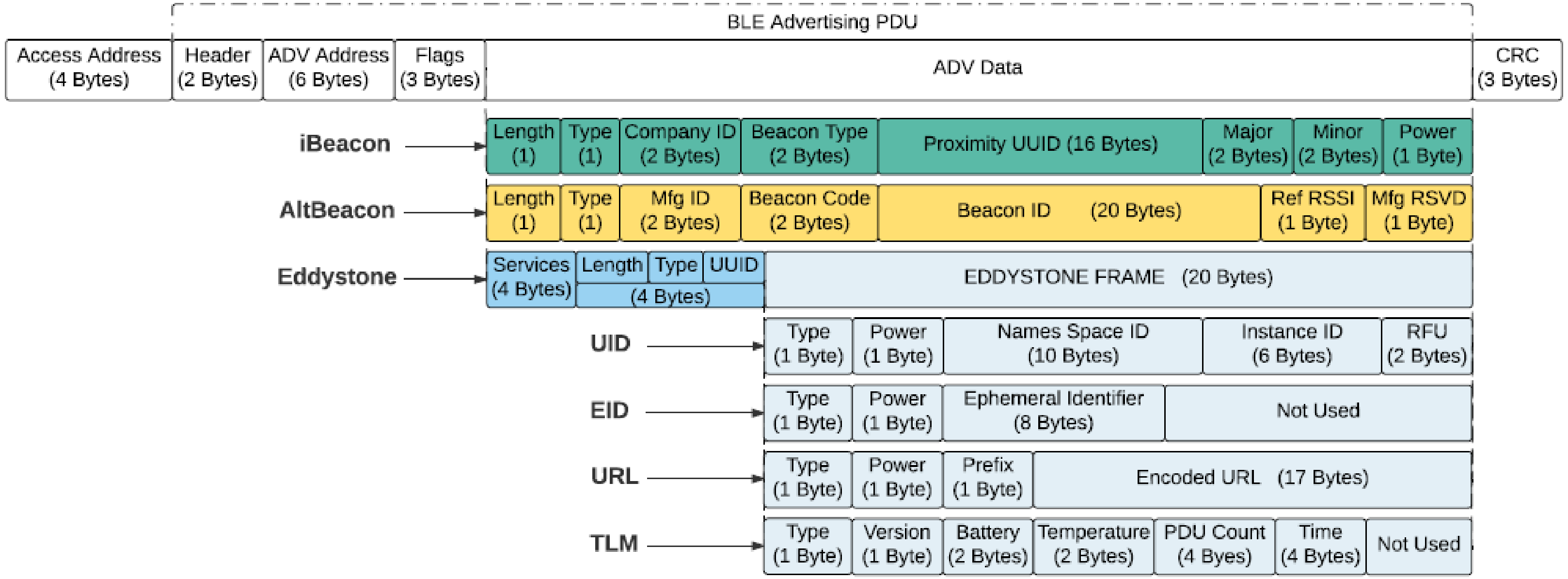
DIRECT-89-HP ENVY 5640 series (c8:d3:ff:19:3d:8a)
-58dBm CH 9 2452MHz ~7.7m
2442 - 2462 (20MHz) HEWLETT PACK
[WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT]

dlink-93C0 (70:62:b8:70:93:c0)
-60dBm CH 2 2417MHz ~9.9m
2407 - 2427 (20MHz) D LINK INTER
[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][RSN-PSK-TKIP+CCMP][ESS][WPS][WFA-HT]

ASUS_88 (04:d9:f5:a7:f3:88)
-65dBm CH 1 2412MHz ~17.6m
2402 - 2422 (20MHz) ASUSTEK COMP
[WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS][WFA-HT]

Broadcasting over bluetooth

Multiple Beacon standards



BLE Advertising PDU

Access Address (4 Bytes) | Header (2 Bytes) | ADV Address (6 Bytes) | Flags (3 Bytes) | ADV Data | CRC (3 Bytes)

iBeacon → Length (1) | Type (1) | Company ID (2 Bytes) | Beacon Type (2 Bytes) | Proximity UUID (16 Bytes) | Major (2 Bytes) | Minor (2 Bytes) | Power (1 Byte)

AltBeacon → Length (1) | Type (1) | Mfg ID (2 Bytes) | Beacon Code (2 Bytes) | Beacon ID (20 Bytes) | Ref RSSI (1 Byte) | Mfg RSVD (1 Byte)

Eddystone → Services (4 Bytes) | Length | Type | UUID (4 Bytes) | EDDYSTONE FRAME (20 Bytes)

UID → Type (1 Byte) | Power (1 Byte) | Names Space ID (10 Bytes) | Instance ID (6 Bytes) | RFU (2 Bytes)

EID → Type (1 Byte) | Power (1 Byte) | Ephemeral Identifier (8 Bytes) | Not Used

URL → Type (1 Byte) | Power (1 Byte) | Prefix (1 Byte) | Encoded URL (17 Bytes)

TLM → Type (1 Byte) | Version (1 Byte) | Battery (2 Bytes) | Temperature (2 Bytes) | PDU Count (4 Byes) | Time (4 Bytes) | Not Used

Figure 1. Hernández-Rojas DL, Fernández-Caramés TM, Fraga-Lamas P, Escudero CJ. Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications. *Sensors*. 2018; 18(1):57.

Broadcasting over bluetooth

- Easy to switch between standards, they have very similar structure
- Easy to send out beacons using hcitool on the RPi, only requires a few lines of code
- Much easier to scan, there is already widespread support for scanning beacons on both Android and IOS devices
- Max range for BLE with Bluetooth 4 is around 50m

TODO

- Complete a working prototype by end of 2020
  - About 60% progress so far
  - Broadcast RID HIT with Bluetooth and WiFi
  - Observer Android App
  - With HIPv2 features, ORCHID2.5, Xoodyak, draft-ietf-drip-rid-04
- Test on a flying drone DJI Phantom 4 Pro+ V2.0
  - RPI+GPS+Battery+BT Dongle as a payload
- Future: draft-moskowitz-drip-secure-nrid-c2-01