Hacking Ant+ with Python

Understanding the ANT+ power data broadcast

hackingantblog Uncategorized June 20, 2017June 20, 2017 3 Minutes

Calculator: http://www.scadacore.com/field-tools/programming-calculators/online-hex-converter/ (http://www.scadacore.com/field-tools/programming-calculators/online-hex-converter/)

Documents:

- ANT+ device profile – Bike Power (https://www.thisisant.com/resources/bicycle-power/)
- Common pages (https://www.thisisant.com/resources/common-data-pages/)

```
1593953 : Tx: [00][00][00][00][00][00][00][00]
```

First packet sent, and only one like this

```
1606437 : Tx: [10][18][FF][5A][88][1A][1B][01]
```

The power data packet: (page 29 Bike Power)

[10] Data page number: Standard – Power Only (page 24 Bike Power)
[18] Update event count
[FF] Pedal power (not used)
[5A] Instantaneous cadence (not used)
[88][1A] Accumulated power in watts, 1 watt increments. Total power measured so far
[1B][01] Instantaneous power. Use the calculator above to see this value calculates to 283W under Little Endian conversion

Default broadcast message

```
1606687 : Tx: [13][19][47][54][47][54][FF][FF]
```

Torque Effectiveness & Pedal Smoothness: (page 38 Bike Power)

[13] Data page number: Standard – Torque Effectiveness & Pedal Smoothness

[19] Update event count
[47] Left torque effectiveness
[54] Right torque effectiveness
[47] Left (or combined) Pedal Smoothness
[54] Right (or combined) Pedal Smoothness
[FF][FF] Reserved and set to 0xFF

Minimum: Interleave every 5 messages (1.25s)

```
1594203 : Tx: [50][FF][FF][01][0F][00][85][83]
```

Manufacturer's Information: (page 28 Common Pages)

[50] Data page number: Manufacturer's Information
[FF] Reserved
[FF] Reserved
[01] HW revision to be set by manufacturer
[0F] Manufacturer ID LSB
[00] Manufacturer ID MSB
[85] Model Number LSB
[82] Model Number MSB

Minimum: Interleave every 121 messages (30.25s)

```
1604203 : Tx: [51][FF][FF][01][01][00][00][00]
```

Product Information: (page 29 Common Pages)

[51] Data page number: Product Information
[FF] Reserved
[FF] SW Revision (Supplemental) – invalid: 0xFF
[01] SW Revision (Main) if byte 2 set to invalid
[01] Serial Number (Bits 0 – 7)
[00] Serial Number (Bits 8 – 15)
[00] Serial Number (Bits 16 – 23)
[00] Serial Number (Bits 24 – 31)
(The lowest 32 bits of the serial number. 4 Bytes Value 0xFFFFFFFF to be used for devices without serial numbers)

Minimum: Interleave every 121 messages (30.25s)

```
1609421 : Tx: [52][FF][FF][07][00][00][55][93]
```

Battery Voltage: (page 26 Common Pages)

[52] Data page number: Battery Status
[FF] Reserved
[FF] Battery identifier – 0xFF not used
[07] Cumulative Operating Time (Bits 0-7)
[00] Cumulative Operating Time (Bits 8-15)
[00] Cumulative Operating Time (Bits 16-23)
[55] Fractional Battery Voltage
[93] Descriptive bit field . In this case binary is 10010011. Bits 0-3 voltage i.e. 0011 = 3V, bits 4-6 battery status 001 = New, bit 7 resolution 1= 2 second resolution

Minimum: Interleave every 61 messages (15.25s)

Frequency

Over 83.7 seconds the USB port sent 344 ANT + data packets (usb.src == host)

The ANT+ dongle sent 335 packets – 4 per second

[00] 1 packet at start
[10] 257 packets – 3.07 per second
[13] 63 packets – 0.75 per second
[50] 3 packets – every 28 seconds
[51] 3 packets
[52] 5 packets – every 16.7 seconds

Interleaving

```
1676109 : Tx: [10][A4][FF][5A][77][EB][36][02]
1676359 : Tx: [10][A4][FF][5A][77][EB][36][02]
1676609 : Tx: [13][A5][47][54][47][54][FF][FF]
1676843 : Tx: [10][A5][FF][5A][AD][ED][36][02]
1677093 : Tx: [10][A6][FF][5A][E3][EF][36][02]
```

update event count can be same as following data packet

```
1669843 : Tx: [10][97][FF][5A][B9][CE][36][02]
1670109 : Tx: [10][98][FF][5A][EF][D0][36][02]
1670343 : Tx: [52][FF][FF][26][00][00][55][93]
1670609 : Tx: [10][99][FF][5A][25][D3][36][02]
1670859 : Tx: [10][99][FF][5A][25][D3][36][02]
```

Useful sections from the profile document:

The update event count field is incremented each time the information in the message is updated. There are no invalid
values for update event count. For Power-only sensors (refer to section 7.2) the time period of the update count depends
on the system but must be a regular interval for accurate averaging.
The update event count in this message refers to updates of the standard Power-Only main data page (0x10). This update
event count value is also used by the optional Torque Effectiveness and Pedal Smoothness data page (0x13). The values in
Data page 0x13 must correspond to those sent in a Power-only page, and shall [MD_PWR_003] include the update
event count value of the related Power-only page (See section 12). The update event count shall [MD_PWR_003] not be
incremented due to data page 0x13 updates. This update event count should never be used as the update event count of
any other data pages.
Note that it is not permissible to send two different Torque Effectiveness and Pedal Smoothness data pages using the same
update event counter value. Therefore the Power-only page must be calculated at least as often as the TE & PS page, and
care must be taken with interleaving. The Power-only page and /or the Torque Effectiveness and Pedal Smoothness page
must be sent each time the update event counter is incremented. This is to ensure that the display is able to identify missed
messages.

Published by hackingantblog

View all posts by hackingantblog