Ceylan-Oceanic: Enocean facilities in Erlang

Organisation: Copyright (C) 2022-2022 Olivier Boudeville

Contact: about (dash) oceanic (at) esperide (dot) com

Creation date: Wednesday, September 7, 2022

Lastly updated: Sunday, December 18, 2022

Version: 0.0.2

Status: In development

Dedication: Users and maintainers of the `Ceylan-Oceanic` library.

Abstract: The role of the `Ceylan-Oceanic` library is to provide Erlang-based facilities for the support of the Enocean building automation system.

The latest version of this documentation is to be found at the official Ceylan-Oceanic website (`http://oceanic.esperide.org`).

This documentation is also mirrored here.

Table of Contents

Overview

The Ceylan-Oceanic library provides Erlang-based facilities for the support of the Enocean building automation system, whose devices are generally energy-harvesting / very low-consumption, and wireless (supported frequencies around 900 MHz, depending on countries; for a range of up to 300 meters in the open, and up to 30 meters inside buildings).

So Enocean, whose slogan could be "no wire, no battery", is rather unique. No Wifi (and very little radio frequency exposure: due to energy constraints, few short, terse telegrams are exchanged), no IP connectivity either, hence no real risk in terms of health or privacy/data leak[1] (Oceanic just receives / decodes / encodes / emits series of well-determined bytes, and remains in full control at all times). At least most of the Enocean specifications are freely available.

Besides Erlang, Ceylan-Oceanic relies only on Ceylan-Myriad and is a rather autonomous part of the Ceylan project. Ceylan-Oceanic can be readily built and run on most Unices, including of course GNU/Linux.

The project repository is located here.

At least a basic knowledge of Erlang is expected in order to use Ceylan-Oceanic.

Purpose

The main motivation of Oceanic is to provide some basic home automation features, especially here in terms of security, in order to be able to:

- **intercept and decode telegrams** emitted by sensors - notably single-input contacts (to detect the opening/closing of doors or windows), presence or temperature / humidity sensors or to detect electricity outages or jamming attempts, typically in order to implement one's own alarm center; should a security event happen, a network camera can be switched on, e-mails and/or SMS can be sent, etc.
- **generate and emit telegrams** to control any kind of electrical devices (driven by a smart plug or an in-wall module), typically to turn on an electric heater or to run one's own presence simulator (possibly with lamps and sound devices)

Progress & Enocean Coverage

The targeted basic Enocean support has been implemented, so EEP Enocean telegrams can be intercepted and, for the supported EEPs (other ones may be quite easily added), such telegrams can be properly decoded and notified as higher-level, incoming events to be managed by one's application.

[1] More recent technologies and open standards exist, including Matter. They are promoted by Amazon, Apple and Google, so that they integrate with their respective home assistants, and communicate over IP.

Everyone is entitled to their opinion; as for us, we prefer not having in our home "Big Five"-originating black boxes full of sensors, cameras and microphones able to communicate rather freely with any "cloud" on the Internet. We are puzzled that some people actually happily *purchase* such devices.

Reciprocally, telegrams for the supported EEPs can also be encoded and sent, and they are able to trigger appropriately-configured (Enocean) devices (actuators).

Oceanic can also execute a few common commands directly onto the local USB gateway chip.

Testing Ceylan-Oceanic in Two Steps

Now, let's discuss all these subjects a bit more in-depth.

Hardware Prerequisites

In terms of Enocean devices, one needs typically:

- any kind of emitter/sensor device, for example a single-input contact/rocker button like these ones; opening sensors are also convenient, as we can easily act on them directly
- a general-purpose emitter/receiver, typically a USB gateway, which includes a UART for asynchronous serial communication with an integrated RF module

For that popular USB dongles can be purchased, which often rely on the TCM 310 chip; this includes the USB300 one (around 37 Euros in France), or the USB310 one (around 50 Euros in France) that we prefer, as it features a SMA connector, which allows an external antenna to be connected in order to boost emission / reception ranges inexpensively.

We will rely here on such a configuration.

Operating System Support

Once the USB dongle is connected (here on an Arch Linux host), `lsusb` tells us that it is detected as:

```
Bus 003 Device 009: ID 0403:6001 Future Technology Devices International, Ltd FT232 Se
```

(which applies both to USB300 and USB310)

We will interact with this USB gateway as if it was a serial port.

Rather than having it designated by an obscure, potentially changing name (like `/dev/ttyUSB0`, `/dev/ttyUSB1`, etc.), we prefer assigning it a fixed, clearer, well-chosen path, like `/dev/ttyUSBEnOcean`.

For that, one may define a suitable udev rule, typically stored in `/etc/udev/rules.d/99-enocean.rules`, whose content can simply[2] be:

```
SUBSYSTEM=="tty", ATTRS{idVendor}=="0403", ATTRS{idProduct}=="6001", SYMLINK+="ttyUSBE
```

Following extra option could be added to the previous line, in order to set the group of this TTY: `GROUP="dialout"` or `GROUP="uucp"` (depending on the

[2] Note though the different roles played by == (for matching) and = (for assignment).

system's conventions), in which case your user shall be in that group (rather than executing `sudo chmod 777 /dev/ttyUSB0` each time the USB dongle is inserted for example).

So one may prefer:

```
SUBSYSTEM=="tty", ATTRS{idVendor}=="0403", ATTRS{idProduct}=="6001", SYMLINK+="ttyUSBE
```

and, to ensure that the user of interest for Oceanic (let's name it `stallone`) belongs to that group:

```
$ sudo usermod -a -G uucp stallone
```

One may then run `sudo udevadm control --reload-rules && sudo udevadm trigger` to ensure that these changes are taken into account from now on.

Then inserting said USB dongle should generate log entries that `journalctl -xe` can show, like (timestamps and hostname edited):

```
kernel: usb 3-11: new full-speed USB device number 9 using xhci_hcd
kernel: usb 3-11: New USB device found, idVendor=0403, idProduct=6001, bcdDevice= 6.00
kernel: usb 3-11: New USB device strings: Mfr=1, Product=2, SerialNumber=3
kernel: usb 3-11: Product: FT232R USB UART
kernel: usb 3-11: Manufacturer: FTDI
kernel: usb 3-11: SerialNumber: A600AVJD
mtp-probe[74533]: checking bus 3, device 9: "/sys/devices/pci0000:00/0000:00:14.0/usb3
kernel: ftdi_sio 3-11:1.0: FTDI USB Serial Device converter detected
kernel: usb 3-11: Detected FT232RL
kernel: usb 3-11: FTDI USB Serial Device converter now attached to ttyUSB0
mtp-probe[74533]: bus: 3, device: 9 was not an MTP device
mtp-probe[74548]: checking bus 3, device 9: "/sys/devices/pci0000:00/0000:00:14.0/usb3
mtp-probe[74548]: bus: 3, device: 9 was not an MTP device
```

On insertion we have then, with the former settings:

```
$ ls -l /dev/ttyUSBEnOcean /dev/ttyUSB0
 crw-rw---- 1 root uucp 188, 0 Nov 13 10:24 /dev/ttyUSB0
 lrwxrwxrwx 1 root root      7 Nov 13 10:24 /dev/ttyUSBEnOcean -> ttyUSB0
```

Software Prerequisites

Ceylan-Oceanic relies on general-purpose services offered by Ceylan-Myriad (implying of course Erlang itself), and on a suitable Erlang driver for serial communication.

Erlang

If needed, follow these Myriad guidelines for installing Erlang in order to obtain a proper, recent-enough version thereof.

Serial

We use our version[3] of erlang-serial for that, which we prefer installing in user space (rather than in the system tree) that way:

```
$ mkdir ~/Software && cd ~/Software
$ git clone https://github.com/Olivier-Boudeville/erlang-serial
$ cd erlang-serial
$ make && DESTDIR=. make install
```

Then using `erlang-serial` will be just a matter of adding it to one's code path[4].

To test this erlang-serial installation (whether or not any dongle is connected):

```
$ erl -pa $HOME/Software/erlang-serial/erlang/lib/serial-1.1/ebin
Erlang/OTP 25 [erts-13.0] [source] [64-bit] [smp:8:8] [ds:8:8:10] [async-threads:1] [j

Eshell V13.0  (abort with ^G)
1> serial:start().
<0.82.0>
```

Perfect!

Ceylan-Myriad

Oceanic expects to find a fully-built Myriad source tree as a sibling of its own tree, named `myriad`, and possibly made available through a symbolic link.

As per these Myriad guidelines, this source tree can be obtained by changing to a directory of choice that will contain both Myriad and Oceanic, and issuing:

```
$ git clone https://github.com/Olivier-Boudeville/Ceylan-Myriad.git
$ ln -s Ceylan-Myriad myriad && cd myriad && make all && cd ..
```

Ceylan-Oceanic

From the same parent directory, very similarly:

```
$ git clone https://github.com/Olivier-Boudeville/Ceylan-Oceanic.git
# Symlink just for consistency:
$ ln -s Ceylan-Oceanic oceanic && cd oceanic && make all && cd ..
```

[3] This is a fork of the original erlang-serial, which had to be modified notably in terms of disabled RTS/CTS flow control, in order to be able to properly send data to the Enocean gateway.

[4] Later in the installation one may update the `Erlang-serial section` in Oceanic's GNU-makevars.inc in order to take into account any other path convention. One may then run, from the root of Oceanic, `make info-serial` to check that `ERLANG_SERIAL_BASE` points indeed to a directory containing erlang-serial's `ebin` directory. Otherwise runtime checks will detect and report any issue.

Testing Enocean

Ensure first that none of the next serial tools / terminals has been left running, otherwise exclusive access may block your ability to send telegrams thanks to Oceanic.

To check, one may rely on:

```
$ lsof /dev/ttyUSBEnOcean
COMMAND    PID      USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
serial  214977 your_user   3u   CHR  188,0      0t0 1066 /dev/ttyUSB0
```

Note also that, from that point EURIDs are altered/edited (fake ones used). Minor discrepancies may happen.

Basic, Direct Command-line Testing

It is as simple as executing from the command-line (thus without Oceanic, Serial or Erlang being involved):

```
$ od -x < /dev/ttyUSBEnOcean
0000000 0055 0707 7a01 10f6 2e00 96e1 0130 ffff
0000020 ffff 0039 554b 0700 0107 f67a 0000 e12e
```

(of course for such a binary content to be received, Enocean telegrams must be emitted; the simplest approach is to trigger any Enocean device able to send on demand such telegrams, like a button/rocker/switch)

`hexdump` can be also used to intercept telegrams. If needing to set the transmission speed beforehand, use `stty -F /dev/ttyUSBEnOcean 57600`.

Incoming data can also be recorded and "replayed" (yet this is not expected to activate an Enocean receiver, see Protocol Information):

```
$ cat < /dev/ttyUSBEnOcean > my_record.bin
$ cat my_record.bin > /dev/ttyUSBEnOcean
```

With a Graphical Serial Terminal

One may use cutecom to directly test input/output telegrams.

A priori neither RTS nor DTR shall be enabled (yet in our tests these had no impact with cutecom; however not disabling them with Oceanic was leading to emitting telegrams not understood by their target devices).

We recommend using the `Hex` input and output.

Oceanic Testing

First test: executing a few Common Commands

This consists in having Oceanic discuss with the local USB gateway dongle, regardless of any actual Enocean device.

From the root of the Ceylan-Oceanic clone, supposing that Myriad and erlang-serial are already available and built (whereas here debug flags have been activated, see Oceanic's `GNUmakevars.inc`):

```
# Ensure erlang-serial is available:
$ make info-serial
ERLANG_SERIAL_BASE = /home/stallone/Software/erlang-serial/erlang/lib/serial-1.1

# Ensure that Ceylan-Oceanic is built:
$ make all

$ cd test

# Triggering a Common Command does not need any target device:
$ make oceanic_common_command_run

       Running unitary test oceanic_common_command_run (third form) from oceanic_commo

--> Testing module oceanic_common_command_test.

Testing the management of Common Commands.
[debug] Using TTY '/dev/ttyUSBEnOcean' to connect to Enocean gateway, corresponding to
[debug] Discovering our base EURID.
[debug] Sending to serial server <0.86.0> actual telegram <<85,0,1,0,5,112,8,56>> (hex
[debug] Waiting initial base request (ToSkipLen=0, AccChunk=<<>>).
[debug] Read telegram <<85,0,5,1,2,219,0,255,162,223,0,10,180>> of size 13 bytes (corr
[debug] Trying to decode '<<85,0,5,1,2,219,0,255,162,223,0,10,180>>' (of size 13 bytes
[debug] Start byte found, retaining now following chunk (of size 12 bytes; after dropp
 <<0,5,1,2,219,0,255,162,223,0,10,180>>.
[debug] Examining now following chunk of 12 bytes:<<0,5,1,2,219,0,255,162,223,0,10,180
[debug] Packet type 2; expecting 5 bytes of data, then 1 of optional data; checking fi
[debug] Header CRC validated (219).
[debug] Detected packet type: response_type.
[debug] Full-data CRC validated (180).
[debug] Decoding a command response, whereas awaiting command of type co_rd_idbase, ba
(corresponding to hexadecimal '5500010005700838'), on behalf of requester internal.
[debug] Returning the following internal response: read gateway base ID ffa3df00, for
[debug] Successfully read gateway base ID ffa3df00, for 10 remaining write cycles.
[info] No preferences file ('/home/stallone/.ceylan-settings.etf') found.
[debug] Waiting for any message including a telegram chunk, whereas having 0 bytes to
[debug] Requested to execute common command 'co_rd_version', on behalf of requester <0
[...]
[debug] Sending back to requester <0.9.0> the following response: read application
version 2.11.1.0, API version 2.6.3.0, chip ID 19d46ce, chip version 1162805507 and ap
[debug] Waiting for any message including a telegram chunk, whereas having 0 bytes to
Read version: read application version 2.11.1.0, API version 2.6.3.0, chip ID 19d46bc
[debug] Requested to execute common command 'co_rd_sys_log', on behalf of requester <0
[...]
Read logs: read counters: 6 for application: [254,255,255,255,255,255], and 38 for API
255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,25
[debug] Stopping the Oceanic server <0.85.0>.
[debug] Stopping serial server <0.86.0>, while in following state: Oceanic server usin
not having any command pending, based on a time-out of 1 second, with no command queue
having <0.9.0> registered as listener of Enocean events, having sent 3 telegrams, not
```

```
[debug] Oceanic server <0.85.0> terminated.
Stopped.

--> Successful end of test.

(test finished, interpreter halted)
```

Second test: controlling an actual device

This more complete test will rely on experimental settings typically involving:

- a **controller device** (e.g. a double-rocker switch), which will be, once discovered, spoofed next by Oceanic
- a **target device** (e.g. a smart plug / socket switching actuator) that already learnt - according to its own procedure (typically pressing adequately buttons thereof) - the previous controller device; for example a lamp would be plugged on that actuator so that, when pressing and releasing a given button of the rocker switch, the lamp is toggled (on/off)

The objective is to control that lamp programmatically, through Oceanic (only).

First, the EURID of the controller device must be determined. Either it can be directly read from some actual label on the device, or it has to be obtained through passive listening.

In this last case, start by running the following test (still in `oceanic/test`):

```
$ make oceanic_integration_run

       Running unitary test oceanic_integration_run (third form) from oceanic_integrat

--> Testing module oceanic_integration_test.

(test waiting indefinitely for Enocean events; hit CTRL-C to stop)
[debug] Using TTY '/dev/ttyUSBEnOcean' to connect to Enocean gateway, corresponding to
[debug] Discovering our base EURID.
[...]
[debug] Waiting for any message including a telegram chunk, whereas having no byte to
```

Then act on the controller so that it emits a telegram (e.g. press a button of said rocker switch; it may be correspond for example to the bottom position of the first rocker, `A`).

If in range, the test should intercept it:

```
[debug] Received a telegram chunk of 21 bytes: <<85,0,7,7,1,122,246,48,0,46,225,150,48
hexadecimal 55000707017af630002ef1963001ffffffff4400fe (whereas there are 0 bytes to s
[debug] Decoding an ERP1 radio packet of R-ORG f6, hence rorg_rps, i.e. 'RPS (Repeated
[info] Discovering Enocean device 002ef196 through failure.

<----------------
[warning] Unable to decode a RPS (F6) packet for 002ef196: device not configured, no l
```

```
---------------->

[debug] Waiting for any message including a telegram chunk, whereas having no byte to
[...]
```

(hit CTRL-C to stop)

So we determined that this rocker switch has for EURID `002ef196`.

We can notice that a failure is reported, as Oceanic cannot decode yet the telegrams from that emitter, short of knowing to which EEP it complies. As this EEP information is not carried by such packets, it cannot be determined automatically and has thus to be specified, here once for all through a proper Oceanic configuration file, typically to be found as `~/.ceylan-settings.etf`.

In this ETF file, among possibly other entries unrelated to Oceanic, we may have:

```
% Oceanic section:

% Information regarding the pseudo-device emitting any telegram to be sent by
% Oceanic:
%
% (if overriding the base ID of this chip, read as "ffa3df00")
%
%{ oceanic_emitter, "DEADBEEF" }.

% To spoof my green switch:
%{ oceanic_emitter, "002EF196" }.


% A list of device_config() entries, clearer with user-defined names than with
% only raw EURIDs:
%
{ oceanic_devices, [

   % Either {UserDefinedName :: ustring(), EURID :: ustring(), EEP ::
   % ustring()} or {UserDefinedName :: ustring(), EURID :: ustring(),
   %                EEP :: ustring(), Comment :: ustring()}:

   % For the local gateway (useful to decode/check self-encoded telegrams):
   { "my local USB gateway", "ffa3df00", "F6-02-01" },

   % Single-input contacts:
   { "my first opening sensor", "060533EC", "D5-00-01" },
   { "my second opening sensor", "02959F62", "D5-00-01" },

   % Temperature and humidity sensors:
   { "my only temperature and humidity sensor", "02A96926", "A5-04-01" },

   % Switches:
   { "my green switch", "002EF196", "F6-02-01",
     "This is actually a single-rocker switch" },
```

```
{ "my white switch", "012F50D6", "F6-02-01" },

% In-wall modules:
{ "my two-channel orange module", "06035E4A", "D2-01-12" }

% Socket switching actuators:
%{ "my smart plug", (unknown), (unknown) }

] }.
```

These entries are pretty self-explanatory:

- with `oceanic_emitter` we define the EURID that shall be used by Oceanic whenever emitting (the default being its in-chip first base ID, as automatically determined thanks to a Common Command)
- with `oceanic_devices` the EEP of the various devices that we want to be aware of are listed (naming them allows to have clearer Oceanic reports)

Now, as the test explicitly sets the EURID of the emitter, it is just a matter of updating, in `oceanic_static_sending_test.erl`, the `SourceEurid` variable in order that this test impersonates the controller of interest (here, said green switch):

```
SourceEurid = oceanic:string_to_eurid( "002EF196" ),
```

Running it[5] results in:

```
$ make oceanic_static_sending_run
       Running unitary test oceanic_static_sending_run (third form) from oceanic_stati

--> Testing module oceanic_static_sending_test.

Starting test; note that direct telegram sendings are made here, thus Oceanic will det
[debug] Using TTY '/dev/ttyUSBEnOcean' to connect to Enocean gateway, corresponding to
[debug] Discovering our base EURID.

[debug] Successfully read gateway base ID ffa3df00, for 10 remaining write cycles.
[debug] Initial state: Oceanic server using serial server <0.86.0>, using emitter EURI
on a time-out of 1 second, with no command queued whereas none has been issued; not ha
having sent a single telegram, not having discarded any telegram, and knowing 8 Enocea
+ device 'my first opening sensor' (EURID: 060533ec) applying EEP D5-00-01; it has bee
[...]
Decoding the 'pressed' one for the 'off' button results in following event: double-roc
pressed simultaneously at 2022/11/19 23:11:45, declared with a single subtelegram, tar
level: telegram not processed; its EEP is double_rocker_switch (F6-02-01)
[...]
All telegrams of interest encoded.
First we press (and then also release) the 'switch off' button, 'button_ao' (which mus
```

[5] The decoding printout corresponds to a check made by this test: prior to sending a telegram that it just generated, it ensures that it can decode it successfully.

```
Then, after a short waiting, we press (and then release) this 'switch off' button aga
[debug] Sending to serial server <0.86.0> actual telegram <<85,0,7,7,1,122,246,16,1,9
(hexadecimal form: '55000707017af6100109d9702001fffffffff00cc').
```

The lamp is expected first to turn on, then, and after one second, to turn off.

Congratulations, your Oceanic program can control electrical appliances!
If this test does not work as intended:

- did the right position of the right button was learnt?
- depending on the switch, apparently:
  - either each of the individual buttons will act as a rocker by itself (e.g. to switch on then off the lamp, a learnt button - top or bottom - of a given rocker will have to be pressed and released twice[6])
  - or the whole rocker (that is the pair made of its top and bottom buttons) will work as intended as a rocker (e.g. to switch on the lamp, the top button will have to be pressed and released, then, to switch off the lamp, the bottom button will have to be pressed and released[7])

[6] This is the case for my white switch, an O2 Line Comfort double-rocker; the top and bottom buttons can then be used indifferently.

[7] This is the case for my green switch, a VIMAR Vita (single) rocker, for which each button has a role. For example, pressing a given button more than once will have no effect (as it corresponds to a state already reached), only using the other will trigger a new transition.

Enocean Documentation

- [ETS]: Enocean Technical Specifications, notably for:
  - [EEP-gen]: EnOcean Equipment Profiles (e.g. version 3.1.4, 36 pages), a short, general view onto the structure of the various telegram types that are available (e.g. the RPS one)
  - [EEP-spec]: EEP Specification (e.g. version 2.6.7, 270 pages), for a detailed specification of the various equipment profiles (e.g. `F6-01-*` being for *Switch Buttons*)
- [ESP3]: Enocean Serial Protocol (ESP3) - SPECIFICATION (e.g. version 1.51, 116 pages), a point-to-point packet-based protocol that is lower-level in the network stack; of lesser interest here)

Note also that, despite the availability of ERP2 specifications, at least most devices we are aware of rely on ERP1 ones.

Protocol Information

Guarding Against Spoofing: Lying about One's Source EURID will Not Suffice

Provided that the serial link is properly configured (in terms of speed, parity, start/stop bits, RTS/CTS flow control, etc.), apparently even with the default, usual level of security (that is: none) implemented by the devices that we tested, Enocean telegrams could *not* be replayed[8]: just intercepting a raw telegram and re-emitting was not acknowledged by the target device and did not trigger its intended effect on at least our main test actuator (e.g. the smart plug did not switch on/off).

One explanation could have been that we were re-emitting from Oceanic "receive" telegrams (as opposed to "send" ones), as we actually always receive information different from what was sent (e.g. the dbM measure, the repeating count, etc. are visibly set between the emission and the receiving; and of course the checksums are modified accordingly) - so replaying a received telegram *could* be rejected on these bases.

Nevertheless, forging from scratch proper "send telegrams" (yet carrying the same functional information) and sending them by ourselves still did not trigger the actuator (we did multiple tests on multiple devices of different manufacturers).

So we believe that extra information is available to actuators through the Enocean network stack, that may/will be used by them in order to discriminate between actual emitters.

This was further confirmed by testing the same telegram exchanges after having learnt a device, either the real one, or one impersonated by Oceanic: apparently, only the ones that have been explicitly learnt previously will be accepted afterwards.

[8] See the `replay_telegrams/1` function in the `oceanic_just_send_to_device_test` module for an example.

By forging telegrams bearing a source EURID different from the base one, we came to the conclusion that:

- most if not all telegrams carry a source EURID that can be freely set (typically through Oceanic calls)
- yet in parallel each emitter (be them an USB dongle controlled by Oceanic or a "real" device) has its own internal, "base" ID (or a base ID range, for such dongles); these IDs have the same type as EURIDs, and we suppose that they can be considered as actual EURIDs - yet they *could* be handled specifically only in low-level ESP3-like protocols (invisibly from the "applicative layer" seen when exchanging with the dongle); by default, unless specified (see the `oceanic_emitter` configuration entry), the source EURID used by telegrams generated by Oceanic match the ID obtained (through a Common Command) from the USB dongle[9]
- learning a device relies at least on these internal IDs, sometimes also on the specified in-telegram source one
- a telegram will be considered by an actuator iff the internal ID of the emitter carried by this telegram matches with one that has been learnt by the actuator (hence no easy spoofing with rogue, undeclared emitters)
- the source EURID included in a telegram will designate a device but may not match the internal ID of the emitter; so for example we could forge, from Oceanic, telegrams whose source EURID matches the one of an actual device (a rocker switch) - and therefore did not match the internal ID of the dongle - while nevertheless, *provided that the dongle had already been learnt by the actuator, typically thanks to a previous Oceanic sending*, we could operate the actuator programmatically (despite these telegrams having inconsistent IDs)
- yet, do these Oceanic telegrams have to specify the same EURID as used for their registering, or any already-registered EURID - or would any EURID would do the trick?
- for the repeating mechanisms to have an interest, their re-emitted telegrams must be taken into account by the target actuators; so accepting already-sent telegrams emanating from different emitters than the one specified in the telegrams is needed; repeating is most probably handled transparently by lower-level protocols as well

We can also verify that devices like rocker switches are apparently stateless, in the sense that they seem to send the same information regardless of their history when one of their buttons is pressed (they have no memory).

So from our experiments we believe that, in terms of identification, the devices rely on a lower-level protocol (possibly ESP3) than the one that can be

[9]This is merely a convention though, as apparently any another EURID could be used instead at this level. We used to add "*provided it is consistently used from then on*" (that is: when learning and also when sending telegram afterwards), yet we could see that even forging a telegram with a random source EURID but sending it from a right, already learnt device (hence using another EURID then) is sufficient to have the corresponding request accepted and processed - at least by some actuators.

handled programmatically (e.g. ERP1 and siblings); as these operations seem to be done through the firmware of the USB gateway, spoofing Enocean traffic may be out of the reach of programs relying on "standard" USB gateways (therefore Oceanic having to be involved also in the learn process, not only in the emitting one).

And forging custom source EURIDs may have an interest, yet the spoofer must have been previously learnt - otherwise this would be a bit like if one was spoofing IP addresses in forged packets, whereas the target device would first compare MAC addresses.

Other Network-Related Risks

The spoofing risk being mostly alleviated, the only extra risks that we could foresee are:

- possibly **brute-force attempts** to match already-learnt base identifiers, from a debug gateway allowing to act on ESP3 packets (a threat that does not seem likely for common burglaries)
- the **jamming of an actuator** by saturating it with telegrams (be them well-formed and sensible, or not[10]), so that any actual telegram of interest (e.g. regarding a door opening) may not reach the receiver
- sensors devices being **incapacitated before they are able to raise an alarm** (for example destroyed, or possibly flashed by an electromagnetic impulse)

Oceanic provides basic yet possibly sufficient mechanisms guarding against these three threats.

For the first two risks: in a wireless context, nothing can be done against emission, but a configurable threshold in terms of incoming traffic volume can be monitored (with proper back-off), so that, if the application registered as a listener, Oceanic notifies it whenever detecting such an attempt of denial of service - which can be considered by itself as a cause of alarm as serious as the other ones.

This threshold is expressed in bytes per second (knowing that telegrams are often fragmented), and its default value (see the `oceanic_jamming_threshold` configuration entry) is `250`. As the size of many Enocean legit telegrams is 21 bytes, an `onEnoceanJamming` event will be sent to the Oceanic-using application should a dozen of them be received during the same second, or a bit more in (a bit) longer time window (e.g. 20 in two seconds).

For the last risk, sensors (typically opening detectors) report instantly state transitions but also send periodic state notifications (even if no change happened). So a listener can monitor the duration elapsed since such a sensor was last seen, and if it exceeds a threshold (for example 30 minutes[11]), this may considered as a reason to raise an alarm.

[10] A battery-operated, generic-purpose jammer operating on the usual frequencies, like 868 MHz in Europe, may be able to affect most of the (now wireless) protocols for house-automation just by emitting powerfully-enough random noise on these bandwidths.

[11] So the event will be detected, albeit with a latency that, depending on the use case, may or may not be acceptable / useful.

Studying Actual Protocols

To experiment and troubleshoot communication issues (this may be especially of use should different devices/actuators interpret differently the Enocean specifications / develop their own behaviour), one may also use tests that perform direct listening / emitting (possibly bypassing partly the logic of the Oceanic server):

- use `make oceanic_just_record_device_run` to display and record in file (`enocean-test-recording.etf`) all raw, timestamped telegrams that can be intercepted
- use `make oceanic_just_send_to_device_run` to emit raw telegrams, typically recorded as explained above or forged (encoded) by Oceanic

Corresponding very handy scripts are available as well, `decode-telegram.sh` and `send-telegram.sh`, to which a raw telegram can be given (as an hexadecimal string).

Usage Hints

Good Practices

Before any new test, one should properly fully reset one's actuator, otherwise weird / wild / overly complex interpretations may happen.

Pairing

As mentioned, when using Oceanic as an emitter, it *must* have been paired to the target actuator.

Pairing can be done through teach-in (through an exchange of specific telegrams) or through learning (putting the actuator is a specific mode, and forcing the emitter to emit a telegram). Some actuators support both procedures.

As detailed in the next section, some actuators are able to learn a device according to various device types/EEPs (e.g. a rocker as a rocker, or as two push-buttons).

This choice matters: although this may not impact the telegrams to be sent by the device, it is bound to impact the behaviour of the actuator when receiving these telegrams.

Buttons vs Rocker: Transition vs State

Depending on the choice made by the user (typically as selected by pressing different buttons on the actuator, to enter a given learning mode), an actuator (e.g. a smart plug controlling a basic lamp) may learn a device (e.g. a rocker) differently (according to different EEPs).

For example a (single) rocker may be seen:

- case A: either as two independent push-buttons (a top button and an unrelated bottom one)
- case B: or as a whole rocker (hence two associated buttons together with the memory of the current state on the actuator)

A key difference is that, in case A (two push-buttons), each button taken individually may toggle the smart plug, while, in case B (rocker), pressing the top button whereas the smart plug is already passing (i.e. in the "triggered" state) will have no effect (e.g. the lamp remains on).

Said differently, case A is about toggling (forcing state transitions) while case B is about setting (forcing state values).

In the general case, setting (hence the rocker behaviour) may be seen as more reliable than toggling (the push-button behaviour): a given setting order may be sent multiple times to a rocker to ensure a given state is reached despite a possible message loss, whereas any loss of a toggling message will result in being consistently from then on in the opposite state of the intended one.

Another approach is to enable and manage state feedback / status return through confirmation telegrams about the current state of the actuator.

Eltako Socket switching actuator FSSA

In practice, in addition to the documentation, we found clearer to respect the following procedures:

- to reset: press left-button for about 3 "large" seconds, then the LED blinks continuously, then press the right-button for about 5 seconds, until the LED turns off
- to learn a device as:
  - a push-button : press left-button for about 1 "large" second, then the LED is on continuously, then press the right-button shortly *once*; the LED will blink once and stay fixed until a telegram is received and learnt: if for example we pressed the top bottom to generate such telegram, this button will act as a on/off toggle, whereas its associated bottom button will have no effect
  - a "direction push-button" (maybe a synonymous of rocker): press left-button for about 1 "large" second, then the LED is on continuously, then press the right-button shortly *twice*; the LED will blink twice and stay fixed until a telegram is received and learnt; in that case, even if we pressed only for example the top button (which from now on corresponds to "set on"), the bottom one will also be taken into account (even if it was involved in the learning stage) and will correspond to "set off"

Afterwards, the LED will blink once a telegram of a learnt device is received (whether or not this specified action has been learnt).

As mentioned in the previous section, we prefer the "direction push-button" mode, i.e. the rocker-based, "state setting" mode.

Support

Bugs, questions, remarks, patches, requests for enhancements, etc. are to be reported to the project interface (typically issues) or directly at the email address mentioned at the beginning of this document.

Additional Information

- use `make sync-sources-to-server` if needing to update directly Oceanic' sources on a remote server that hosts an appropriate USB dongle
- refer to EnOcean in Practice (very clear information, in French)

Related Projects

They may be used as sources of inspiration:

- [PY-EN] the rather complete Python EnOcean library, including for its EEP (XML) information
- a Java implementation: enocean4j
- the (Java) OpenEnocean openHAB binding
- a first Rust implementation

Please React!

If you have information more detailed or more recent than those presented in this document, if you noticed errors, neglects or points insufficiently discussed, drop us a line! (for that, follow the Support guidelines).

Ending Word

Have fun with Ceylan-Oceanic!