PTM 535Z 2.4 GHz Pushbutton Transmitter

PTM 535Z 2.4 GHz Pushbutton Transmitter

31 May 2016

Observe precautions! Electrostatic sensitive devices!

Patent protected:
WO98/36395, DE 100 25 561, DE 101 50 128,
WO 2004/051591, DE 103 01 678 A1, DE 10309334,
WO 04/109236, WO 05/096482, WO 02/095707,
US 6,747,573, US 7,019,241

PTM 535Z 2.4 GHz Pushbutton Transmitter

REVISION HISTORY

The following major modifications and improvements have been made to this document:

Version	Author	Reviewer	Date	Major Changes
1.0	MKA	MH, MF	01.03.2016	Initial Release
1.1	MKA		02.05.2016	Minor corrections
1.2	MKA		31.05.2016	Added appendix on telegram analysis

Published by EnOcean GmbH, Kolpingring 18a, 82041 Oberhaching, Germany
www.enocean.com, info@enocean.com, phone +49 (89) 6734 6890

Important!
This information describes the type of component and shall not be considered as assured characteristics. No responsibility is assumed for possible omissions or inaccuracies. Circuitry and specifications are subject to change without notice. For the latest product specifications, refer to the EnOcean website: http://www.enocean.com.
As far as patents or other rights of third parties are concerned, liability is only assumed for modules, not for the described applications, processes and circuits.
EnOcean does not assume responsibility for use of modules described and limits its liability to the replacement of modules determined to be defective due to workmanship. Devices or systems containing RF components must meet the essential requirements of the local legal authorities.
The modules must not be used in any relation with equipment that supports, directly or indirectly, human health or life or with applications that can result in danger for people, animals or real value.
Components of the modules are considered and should be disposed of as hazardous waste. Local government regulations are to be observed.
Packing: Please use the recycling operators known to you.

PTM 535Z 2.4 GHz Pushbutton Transmitter

TABLE OF CONTENT

PTM 535Z 2.4 GHz Pushbutton Transmitter

PTM 535Z 2.4 GHz Pushbutton Transmitter

1 GENERAL DESCRIPTION

1.1 Basic functionality

PTM 535Z enables the realization of energy harvesting wireless switches for EnOcean systems communicating based on the 2.4 GHz IEEE 802.15.4 radio standard.

PTM 535Z is primarily intended for operation in conjunction with the EnOcean ECO 200 energy harvester. ECO 200 can be either mechanically connected using two contact pairs or connected to the electrical interface of PTM 535Z.

Upon detection of energy pulses from the ECO 200 harvester, PTM 535Z will read the status of additional input signals (on-board meander contact, external input signals) and report the result as IEEE 802.15.4 radio telegram. Both secure and normal transmission modes are supported.

PTM 535Z telegram format has been defined to maximize compatibility with a wide range of devices including such supporting the ZigBee Green Power standard. PTM 535Z radio telegrams are protected with AES-128 security based on a device-unique private key.

PTM 535Z contains a learn button (LRN) to send dedicated commissioning telegrams and to change the radio channel. Radio channel and security mode can also be selected using the hardware configuration interface consisting of six zero Ohm resistor pads (R1 … R6).

PTM 535Z provides a five pad external electrical interface with the following signals:

- External connection to ECO 200 (AC1 and AC2)
- Two external input signals (IN1 and IN2)
- Ground (GND)

PTM 535Z is mechanically compatible with the outline of existing PTM 33x modules. Figure 1 below shows PTM 535Z.

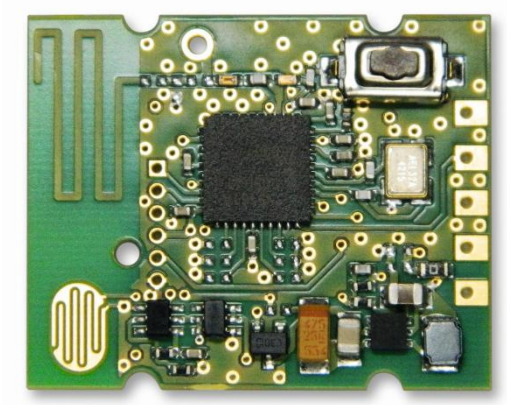


Figure 1 – PTM 535Z Product Outline

1.2 Technical data

Antenna	Integrated PCB antenna External 50 Ohm whip antenna (optional)
Radio Standard	IEEE 802.15.4 (2.4 GHz)
Supported Radio Frequency Range	IEEE 802.15.4 radio channel 11 … 26 (default: channel 11)
Radio Channel Selection	HW-configurable (0 Ohm resistor pads) User-selectable (Commissioning)
Commissioning	Learn Button (on-board)
Security	AES128 with Sequence Code (Can be disabled via HW configuration)
Transmit Power (typ, at 25°C)	+2 dBm
Power Supply	ECO 200 Kinetic Energy Harvester
Harvester Interface	2 pairs of contacts
On-board Button Interface	1 meander contact
External Interface	5 pins (solderable) 2 ECO 200 contacts, 2 button inputs, Ground
Certification	R&TTE (Europe)

1.3 Physical dimensions

Module Dimensions	26.2 x 21.15 x 3.5 mm
Module Weight	2g

1.4 Environmental conditions

Operating Temperature	-25°C ... 65°C
Storage Temperature	-25°C ... 65°C
Humidity	0% to 95% r.h. (non-condensing)

1.5 Packaging information

Packaging Unit	100 units
Packaging Method	Tray / Box (10 units per tray, 10 trays per box)

1.6 Ordering information

Type	Ordering Code	Frequency
PTM 535Z	S3071-A535	2.4 GHz (IEE 802.15.4)

2 FUNCTIONAL INFORMATION

2.1 PTM 535Z Device Overview

The radio transmitter device PTM 535Z from EnOcean enables the implementation of wireless remote controls without batteries. Power is provided by an external power generator (typically ECO 200).

PTM 535Z device transmits data based on the 2.4GHz IEEE 802.15.4 standard.
Key components of PTM 535Z are shown on the picture below.

Note that two contact pairs of AC1 and AC2 are located on the bottom side of the PCB and therefore not visible in the picture.

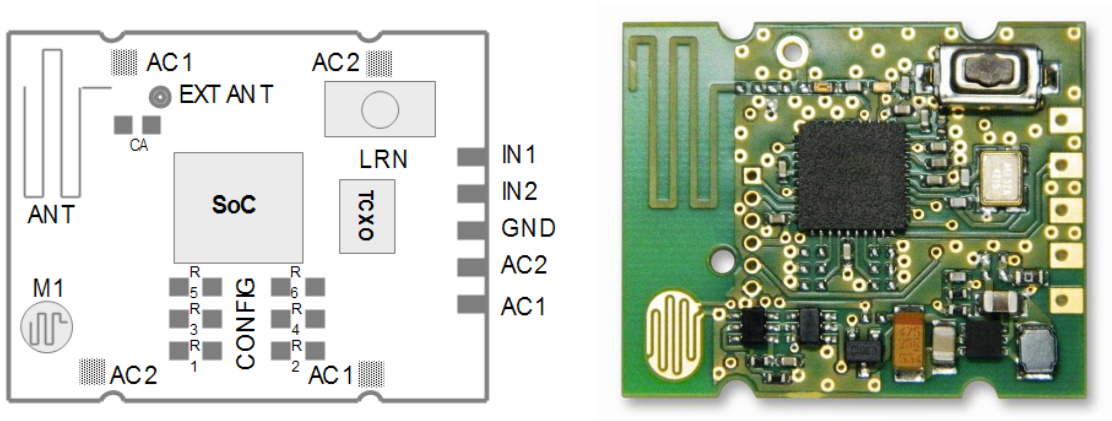


Figure 2 – Electro-dynamic powered radio transmitter device PTM 535Z

2.2 Basic Functionality

PTM 535Z devices contain an interface with two pair of signals (AC1 and AC2) used to connect an external energy generator (ECO 200). Having two contact pairs improves the mechanical design flexibility.

Upon detection of an energy pulse, PTM 535Z reports the status of the on-board meander contact (M1), the external input signals IN1 and IN2 and the polarity of ECO 200 action (press or release).

"Press" is defined within the scope of this document as a move of a mechanically connected ECO 200 away from the PTM 535Z PCB while "Release" is defined as a move towards the PTM 535Z PCB

Radio telegrams are transmitted using the on-board antenna (ANT). An external antenna (EXT_ANT) can optionally be used, capacitor CA needs to be removed in that case. Radio telegram format has been defined to maximize compatibility with a wide range of devices including such supporting the ZigBee Green Power standard.

2.3 Device interface signals

Table 1 below summarizes key elements and interface signals of PTM 535Z.

NAME	DESCRIPTION	NAME	DESCRIPTION
AC1	Input 1 from ECO 200	AC2	Input 2 from ECO 200
IN1	External input 1	IN2	External input 2
ANT	On-board PCB antenna	EXT_ANT	External antenna
M1	Meander contact	LRN	Learn button
R1 … R6	Configuration resistors	GND	Ground

Table 1: PTM 535Z key elements and interface signals

The PTM 535Z device interface is described in more detail below.

2.4 Power supply

PTM 535Z is intended to be supplied by a connected ECO 200 kinetic energy harvester. ECO 200 can be connected to PTM 535Z in the following ways:

- Mechanical connection to one of the two pairs of AC1 / AC2 pads
  Use of a suitable mechanical design is required to reliably fixate the ECO 200 contacts with the AC1 / AC2 connection pads
- Electrically connected using the AC1 / AC2 signals of the external interface

Figure 3 below illustrates the mechanical connection between an ECO 200 kinetic energy harvester and PTM 535Z.

Note that two pairs of contacts are provided by PTM 535Z to enable two orientations of ECO 200 (spring facing down = red lines / spring facing up = yellow lines) depending on the requirements of the customer mechanical design.

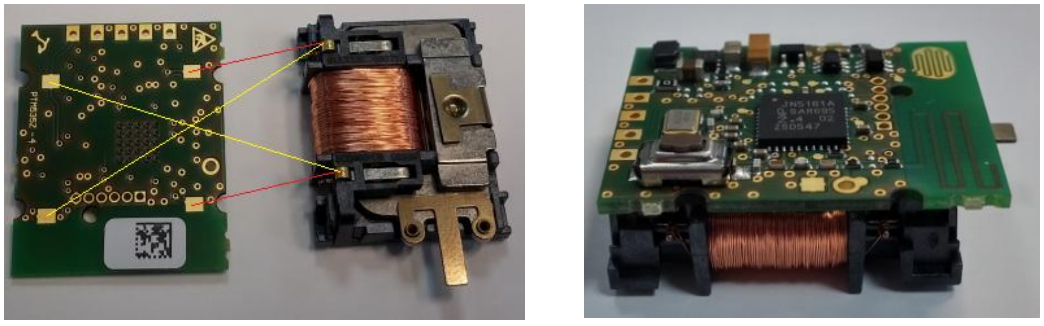


Figure 3: Mechanical connection between ECO 200 and PTM 535Z

2.5 Input signals

PTM 535Z data transmits telegrams indicating the status of the following input signals:

- ECO 200 action direction (press or release)
  Press indicates a move away from the PCB (and the ECO 200 contacts)
  Release indicates a move towards the PCB (and the ECO 200 contacts)

- On-board meander contact (M1)
  This meander contact is intended for use with a conductive rubber button and is considered to be active if it is closed.
  Contact EnOcean for reference on suitable rubber contact mats if required.

- External input signals (IN1 and IN2)
  PTM 535Z provides and internal pull-up resistor on these signals.
  These inputs are considered active if they are connected to Ground (GND).

2.5.1 PTM 535Z input status encoding

Table 2 below shows the encoding used by PTM 535Z.

Input 2 (IN2)	**Input 1 (IN1)**	**Meander (M1)**	**ECO 200**	**Command**
0 = Not Connected to GND 1 = Connected to GND		0 = Open 1 = Closed	Press= Move away from PCB Release = Move towards PCB	
0	0	0	Release	0x23
0	0	0	Press	0x22
0	0	1	Release	0x12
0	0	1	Press	0x13
0	1	0	Release	0x14
0	1	0	Press	0x15
0	1	1	Release	0x16
0	1	1	Press	0x17
1	0	0	Release	0x18
1	0	0	Press	0x19
1	0	1	Release	0x1A
1	0	1	Press	0x1B
1	1	0	Release	0x1C
1	1	0	Press	0x1D
1	1	1	Release	0x1E
1	1	1	Press	0x1F

Table 2: PTM 535Z input status encoding

2.6 Hardware configuration interface

PTM 535Z provides a hardware configuration interface based on six zero Ohm resistor footprints (R1 … R6).

Populating these resistors allows customer-specific adaption of the following parameters:

- Hardware-based security mode selection
- Hardware-based radio channel selection

2.6.1 Hardware-based security mode selection

By default, PTM 535Z transmits securely authenticated data telegrams based on AES128 encryption standard using a 16 byte device-unique secret key and a 4 byte sequence counter.

For certain applications it might be desirable to transmit data telegrams without sequence counter and device security key / telegram signature. PTM 535Z can be configured to do so by populating configuration resistor R2.

2.6.2 Hardware-based radio channel selection

By default, the radio channel used by PTM 535Z can be changed by the user during commissioning as described in chapter 2.8.2.3.

For certain applications it is desirable to pre-configure the radio channel in a way that it cannot be modified by the user.

This can be achieved by populating configuration resistor R1. If this resistor is populated then the radio channel used by PTM 535Z will exclusively be determined by configuration resistors R3 … R6 as shown in Table 3 below.

Using the LRN button, the user will trigger the transmission of a commissioning telegram, but he cannot modify the radio channel.

R3	R4	R5	R6	Channel
Not populated	Not populated	Not populated	Not populated	11
Not populated	Not populated	Not populated	Populated	12
Not populated	Not populated	Populated	Not populated	13
Not populated	Not populated	Populated	Populated	14
Not populated	Populated	Not populated	Not populated	15
Not populated	Populated	Not populated	Populated	16
Not populated	Populated	Populated	Not populated	17
Not populated	Populated	Populated	Populated	18
Populated	Not populated	Not populated	Not populated	19
Populated	Not populated	Not populated	Populated	20
Populated	Not populated	Populated	Not populated	21
Populated	Not populated	Populated	Populated	22
Populated	Populated	Not populated	Not populated	23
Populated	Populated	Not populated	Populated	24
Populated	Populated	Populated	Not populated	25
Populated	Populated	Populated	Populated	26

Table 3: Resistor encoding for HW-based radio channel selection

2.7 Radio interface

2.7.1 Antenna

PTM 535Z transmits data based on an on-board PCB antenna (ANT). An external 50Ω whip antenna connected to the EXT_ANT pin can alternatively be used. Connection to the internal antenna has to be cut in this case by removing capacitor CA.

Please check with EnOcean if you intend to use an external antenna.

2.7.2 Supported Radio Channels

PTM 535Z supports all sixteen IEEE 802.15.4 radio channels in the 2.4 GHz band (channels 11 … 26 according to IEEE 802.15.4 notation).

Table 4 below shows the correspondence between channel number and channel frequency (in MHz).

Channel ID	Lower Frequency	Centre Frequency	Upper Frequency
11	2404	2405	2406
12	2409	2410	2411
13	2414	2415	2416
14	2419	2420	2421
15	2424	2425	2426
16	2429	2430	2431
17	2434	2435	2436
18	2439	2440	2441
19	2444	2445	2446
20	2449	2450	2451
21	2454	2455	2456
22	2459	2460	2461
23	2464	2465	2466
24	2469	2470	2471
25	2474	2475	2476
26	2479	2480	2481

Table 4: IEEE 802.15.4 Radio Channels and Frequencies (in MHz)

2.7.3 Radio channel selection

The radio channel used by PTM 535Z can be selected in two ways:

- User selection (using LRN button, default mode)
  If configuration resistor R1 is not populated (default) then the radio channel can be selected by the user as described in chapter 2.8.2.3
- HW selection (using configuration resistors, requires R1 to be populated)
  If configuration resistor R1 is populated then the radio channel used by PTM 535Z is fixed exclusively by the configuration resistors R3 … R6 as discussed in chapter 2.6.2.

2.8 Operation modes

PTM 535Z can operate in two modes:

- Data mode
  Data mode is used to transmit data telegrams reporting the status of PTM 535Z button inputs

- Commissioning mode
  Commissioning mode is used to commission (learn, teach-in) PTM 535Z into a specific receiver or network. To do so, PTM 535Z will identify its capabilities and its security parameters and – if required – change the radio channel it uses for telegram transmission.

2.8.1 Data mode

Data mode is the standard mode of operation. In this mode, PTM 535Z will transmit data telegrams identifying the status of its inputs.

PTM 535Z uses the following sequence to identify and transmit input status:

1. Determine polarity of ECO 200 pulse (to identify press or release direction)
2. Read input status of all signals
3. Calculate data part of IEEE 802.15.4 radio telegram
4. Calculate security part of IEEE 802.15.4 radio telegram (if security is enabled)
5. Transmit radio telegram

2.8.2 Commissioning mode

Commissioning mode provides two key functions:

- Transmission of a commissioning telegram in order to learn-in PTM 535Z into a network
- Radio channel selection in order to set the radio channel of PTM 535Z to that used by the network

Figure 4 below shows the commissioning state chart used by PTM 535Z.

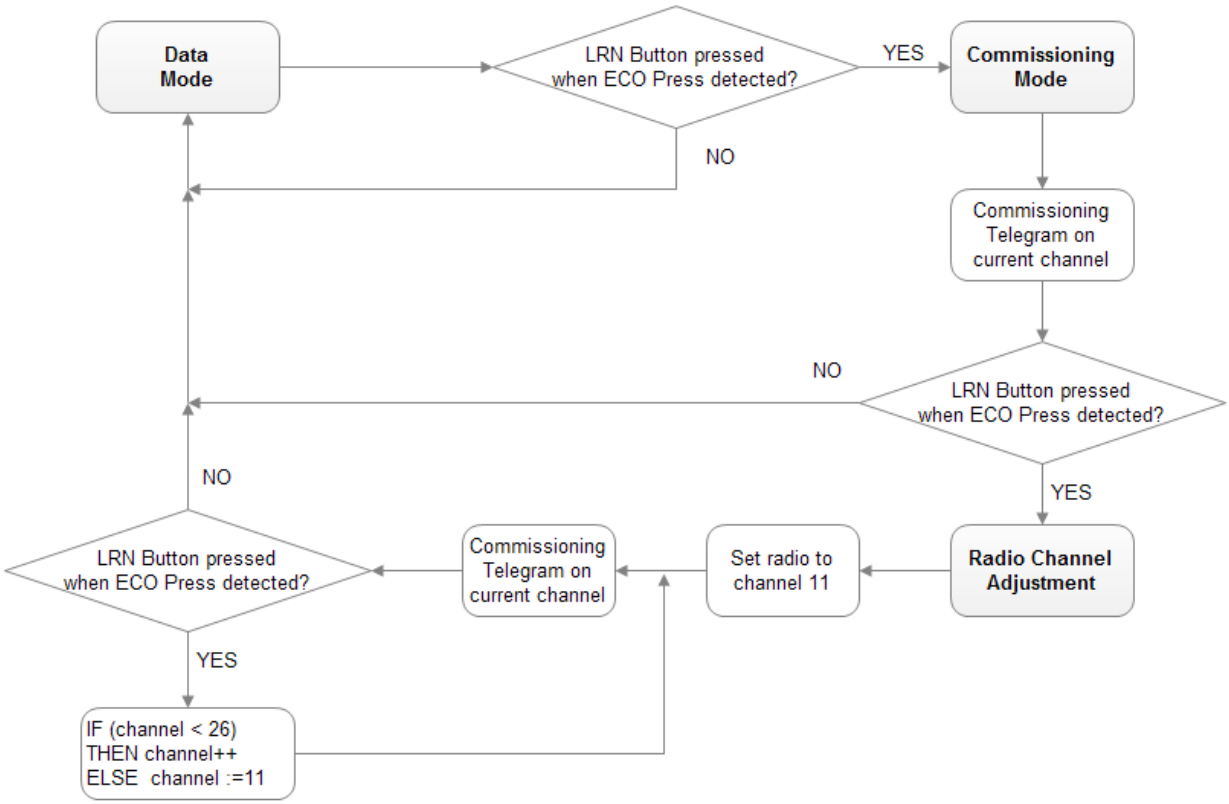


Figure 4: Commissioning state chart used by PTM 535Z

The different functions are described subsequently in more detail.

2.8.2.1 Entry into commissioning mode

Commissioning mode is entered as soon as PTM 535Z detects an energy pulse from ECO 200 in "Press" direction and the LRN button is pressed.

PTM 535Z will remain in commissioning mode as long as the LRN button is pressed whenever ECO 200 is actuated in the "Press" direction.

2.8.2.2 Commissioning telegram

PTM 535Z will transmit a commissioning telegram on the current radio channel upon entering commissioning mode. This enables PTM 535Z to be learned into additional devices without modifying the currently used radio channel.

The type of commissioning telegram depends on whether PTM 535Z operates in secure mode or standard mode, see chapter 2.9.1. The format of the commissioning telegram is described in chapter 3.4.

2.8.2.3 Radio channel adjustment

PTM 535Z will enter radio channel adjustment mode if it has entered commissioning mode and again the LRN button is pressed and ECO 200 is actuated in the "Press" direction.

PTM 535Z will then set the radio channel to channel 11 and transmit a commissioning telegram on this radio channel. Resetting the radio channel to channel 11 ensures that the number of required LRN events for selecting a radio new channel is independent of the currently used radio channel

Each subsequent press of the LRN button together with ECO 200 being actuated in the "Press" direction will then cause the radio channel to be incremented and a commissioning telegram to be transmitted on the channel. If channel 26 has been reached, then the sequence will start again with channel 11.

2.8.2.4 Determining the correct radio channel

The user requires system feedback to determine if the correct radio channel has been reached.

Several methods are possible for that, including:

- Feedback from the device into which PTM 535Z is learned in
  E.g. blinking a status light, toggling a connected load, moving a motor etc.
- Feedback from a dedicated user interface
  This could for instance instruct the user on the required key sequence and confirm correct execution

It is the responsibility of the system designer to define a suitable feedback mechanism.

2.8.2.5 Storing the new radio channel and return to data mode

If PTM 535Z has been successfully set to the desired radio channel then this radio channel has to be stored and operation should return to data mode.

This is achieved by releasing the LRN button and actuating ECO 200 in the “Press” direction.

2.9 Security modes

PTM 535Z can operate in two security modes:

- Secure mode (default, R2 not populated)
  PTM 535Z operates in secure mode by default using AES128 security for data telegrams. Security is based on a random, device-unique security key which is generated during the production of the device.

- Standard mode (if R2 is populated)
  PTM 535Z can operate in standard mode for applications requiring shorter payloads and without the need for an AES128 signature.

2.9.1 Selecting the security mode

The default operation mode is secure mode. Standard mode can be selected by populating configuration resistor R2.

2.9.2 Security parameters

PTM 535Z transmits data is secured based on a 4 byte sequence counter, an out of the box device-unique key and a 4 byte signature calculated based on the AES128 encryption using CBC mode.

The current status of the sequence counter together with the device-unique key are transmitted during commissioning and have to be stored by the device where PTM 535Z is learned in. These parameters are subsequently used to authenticate received telegrams.

EnOcean can provide references for the implementation of the required routines for key exchange and message validation upon request.

2.10 Number of redundant telegrams

For most telegram types, PTM 535Z will transmit the telegram more than once (redundant transmission) in order to increase transmission reliability. The timing of the individual telegram transmissions is random within a 5ms window.

The number of telegram transmissions is limited by the available energy and therefore dependent on the telegram length (number of bytes to be transmitted).

Typically, PTM 535Z will transmit the following number of telegrams in secure mode:

- 2 secure data telegrams
- 1 secure commissioning telegram

Standard mode telegrams are shorter because the sequence counter and the security key (commissioning telegram) / security signature (data telegram) do not need to be transmitted.

Typically, PTM 535Z will transmit the following number of telegrams in standard mode:

- 3 data telegrams
- 3 commissioning telegrams

3 IEEE 802.15.4 Frame Structure

PTM 535Z transmits radio telegrams in the 2.4 GHz band according to IEEE 802.15.4 frame structure. For detailed information about the IEEE 802.15.4 standard, please refer to the applicable specifications.

The following information about the IEEE 802.15.4 frame structure is given for reference only. Note that the data format used is little endian. This means that for multi-byte structures (such as 2 byte, 4 byte or 8 byte fields) the least significant byte (LSB) is transmitted first. The IEEE 802.15.4 frame structure used by PTM 535Z consists of the following four main parts:

- PHY Header
  The PHY header indicates to the receiver the start of a transmission and provides information about the length of the transmission.
  It contains the following fields:
  - Preamble
    Pre-defined sequence (4 byte, value 0x00000000) used to adjust the receiver to the transmission of the sender
  - Start of frame
    Pre-defined symbol (1 byte, value 0xA7) identifying the start of the actual data frame
  - Length
    1 byte indicating the combined length of all following fields

- MAC Header
  The MAC header provides detailed information about the frame.
  It contains the following fields:
  - Frame control field
    2 bytes to identify frame type, protocol version, addressing and security mode
  - Sequence number
    1 byte sequential number to identify the order of transmitted frames
  - Address
    PAN ID and address of source (if present) and destination of the telegram
    PTM 535Z does not use source address and source PAN ID

- MAC Payload
  The MAC Payload field contains telegram control, device ID, telegram data and telegram security (if present) fields.
  The MAC Payload field structure depends on telegram type (data or commissioning) and security mode (secure or non-secure transmission).

- MAC Trailer
  The MAC Trailer contains the Frame Check Sum (FCS) field used to verify the integrity of the telegram data.

Figure 5 below summarizes the IEEE 802.15.4 frame structure.

Figure 5: IEEE 802.15.4 Frame Structure

The content of these fields is described in more detail below.

3.1 PHY Header

The IEEE 802.15.4 PHY header consists of the following fields:

- Preamble
- Start of Frame
- Length of Frame fields

The content of the Preamble and Start of Frame fields is fixed for all telegram types supported by PTM 535Z as follows:

- Preamble = 0x00000000
- Start of Frame = 0xA7

The content of the Length field differs depending on the telegram type as follows:

- Secure commissioning telegram
  Length= 42 bytes (0x2A)
- Secure data telegram
  Length = 24 bytes (0x18)
- Standard commissioning telegram
  Length = 17 bytes (0x11)
- Standard data telegram
  Length = 15 bytes (0x0F)

3.2 MAC Header

The IEEE 802.15.4 MAC Header contains the following fields:

- Frame Control Field (2 byte)
  The Frame Control Field is set to 0x0801 in all PTM 535Z telegrams in order to identify them as data telegrams with short addresses based on version IEEE 802.15.4-2003
- Sequence Number (1 byte)
  The Sequence Number is an incremental number used to identify the order of telegrams
- Address Field (4 byte in PTM 535Z implementation)
  PTM 535Z uses short Destination Address (16 Bit) together with the Destination PAN ID (16 Bit). Both are set to 0xFFFF to identify the telegrams as broadcast.
  Source address and Source PAN ID are not present in PTM 535Z telegrams.

3.3 MAC Trailer

The MAC Trailer only contains the Frame Check Sum (FCS) field.

Its length is 2 byte and it is calculated as Cyclic Redundancy Check (CRC16) over the entire MAC payload including the "Length" field of the PHY Header using the following polynomial: $x^{16} + x^{12} + x^5 + 1$

3.4 MAC Payload

The MAC Payload depends on the telegram type:

- Telegram type
  - Data Telegram
  - Commissioning Telegram
- Security mode
  - Secure communication
  - Standard communication

MAC payloads for the different telegram types are described in the following chapters.

3.4.1 MAC payload structure for secure data telegrams

Figure 6 below shows the MAC Payload structure of a secure data telegram.

Telegram Control	Source ID	Sequence Counter	Command	Telegram Signature
2 Byte	4 Byte	4 Byte	1 Byte	4 Byte

Figure 6: MAC Payload structure for secure data telegrams

The following fields are used for secure data telegrams:

- Telegram Control (2 bytes)
  The *Telegram Control* field is set to 0x308C indicating that PTM 535Z uses 4 byte payload signature based on a device-unique key and a 4 byte sequence counter
- Source ID (4 bytes)
  The *Source ID* field contains a 4 byte ID uniquely identifying each PTM 535Z device
- Sequence Counter (4 bytes)
  The *Sequence Counter* field contains an always incrementing counter.
  Security processing is based on the combination of the Command and Sequence Counter in order to prevent replay attacks (sending the same telegram again)
- Command (1 byte)
  The *Command* field is a one byte field which identifies the state of the different inputs of PTM 535Z. For the encoding please seeTable 2.
- Telegram Signature (4 byte)
  The *Telegram Signature* field is used to validate the telegram authenticity. The telegram signature is calculated based on the telegram payload using AES128 (CBC mode).
  EnOcean can provide upon request additional information on how to implement telegram validation for PTM 535Z data telegrams.

3.4.2 MAC payload structure for secure commissioning telegrams

Figure 7 below shows the MAC payload structure of a secure commissioning telegram.

Telegram Control	Source ID	Commissioning Command	Device Type	Device Options	Device-unique Security Key	Security Key Validation	Sequence Counter
1 Byte	4 Byte	1 Byte	1 Byte	2 Byte	16 Byte	4 Byte	4 Byte

Figure 7: MAC Payload structure for secure commissioning telegrams

The following fields are used for secure commissioning telegrams:

- Telegram Control (1 byte)
  The *Telegram Control* field is set to 0x0C to identify a standard telegram (secure communication will be established based on the commissioning telegram)
- Source ID (4 bytes)
  The *Source ID* field contains a 4 byte ID uniquely identifying each PTM 535Z device
- Commissioning Command (1 byte)
  The *Command* field is set to 0xE0 by PTM 535Z
- Device Type (1 byte)
  The *Device Type* field is set to 0x02 by PTM 535Z
- Device Options (2 bytes)
  The *Device Options* field is set to 0xF281 by PTM 535Z when operating in AES128 secure mode with authentication.
- Device-unique Security Key (16 bytes)
  PTM 535Z implement a random, device-specific security key which is generated as part of the production flow. During commissioning, this key is transmitted in encrypted format. Contact EnOcean for details.
- Security Key Validation (4 bytes)
  In order to ensure correct reception, an additional 4 byte validation value is provided. Contact EnOcean for details.
- Sequence Counter (4 bytes)
  The *Sequence Counter* is an always incrementing counter which is used as part of the security processing to avoid replay attacks (sending the same telegram again).
  Receiving devices shall only accept data telegrams with sequence counter values higher than that of the last received telegram; therefore the current value needs to be communicated during commissioning.

3.4.3 MAC payload structure for standard data telegrams

PTM 535Z will operate in standard mode if configuration resistor R2 is populated. Figure 8 below shows the MAC payload structure of a standard data telegram.

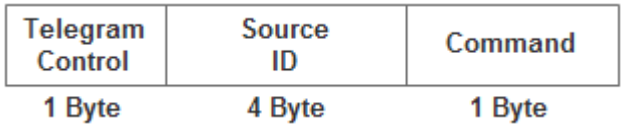


Figure 8: MAC Payload structure for Standard Data Telegrams

The following fields are used for Standard Data Telegrams:

- Telegram Control (1 byte, 0x0C)
  This field is set to 0x0C to identify a standard data telegram
- Source ID (4 bytes)
  4 byte ID uniquely identifying each PTM 535Z device
- Command (1 byte)
  This is a one byte field which identifies the state of the different input of PTM 535Z.
  For the encoding please see Table 2.

3.4.4 MAC payload for standard commissioning telegrams

Figure 9 below shows the MAC payload structure of a standard commissioning telegram.

Telegram Control	Source ID	Commissioning Command	Device Type	Device Options
1 Byte	4 Byte	1 Byte	1 Byte	1 Byte

Figure 9: MAC Payload structure for standard commissioning telegrams

The following fields are used for standard commissioning telegrams:

- Telegram Control (1 byte)
  The *Telegram Control* field is set to 0x0C to identify a standard telegram (secure communication will be established based on the commissioning telegram)
- Source ID (4 bytes)
  The *Source ID* field contains a 4 byte ID uniquely identifying each PTM 535Z device
- Commissioning Command (1 byte)
  The *Commissioning Command* field is set to 0xE0 by PTM 535Z
- Device Type (1 byte)
  The *Device Type* field is set to 0x02 by PTM 535Z
- Device Options (1 byte)
  The *Device Options* field is set to 0x01 by PTM 535Z

4 Device Integration

PTM 535Z is designed for integration with ECO 200 kinetic energy harvesters. EnOcean can provide mechanical reference designs upon request.

5 APPLICATION INFORMATION

5.1 Transmission range

The main factors that influence the system transmission range are:
- Type and location of the antennas of receiver and transmitter
- Type of terrain and degree of obstruction of the link path
- Sources of interference affecting the receiver
- "Dead spots" caused by signal reflections from nearby conductive objects.

Since the expected transmission range strongly depends on this system conditions, range tests should always be performed to determine the reliably achievable range under the given conditions.

The following figures should be treated as a rough guide only:

- Line-of-sight connections
  Typically 15 m range in corridors, up to 50 m in halls

- Plasterboard walls / dry wood
  Typically 15 m range, through max. 2 walls

- Ferro concrete walls / ceilings
  Maximum 1 wall or ceiling, depending on thickness and material

- Fire-safety walls, elevator shafts, staircases and similar areas should be considered as shielded

The angle at which the transmitted signal hits the wall is very important. The effective wall thickness – and with it the signal attenuation – varies according to this angle. Signals should be transmitted as directly as possible through the wall. Wall niches should be avoided.

Other factors restricting transmission range include:
- Switch mounting on metal surfaces (up to 30% loss of transmission range)
- Hollow lightweight walls filled with insulating wool on metal foil
- False ceilings with panels of metal or carbon fibre
- Lead glass or glass with metal coating, steel furniture

The distance between the receiver and other transmitting devices such as computers, audio and video equipment that also emit high-frequency signals should be at least 0.5 m.

5.2 Duty Cycle

PTM 535Z is designed for manually activated systems. In order to comply with duty cycle limitations, it shall not be used to transmit telegrams more often than 10.000 times per hour.

6 REGULATORY INFORMATION

PTM 535Z has been certified according to applicable regulations.

Changes or modifications not expressly approved by EnOcean could void the user's authority to operate the equipment.

6.1 FCC (United States) Certification

PTM 535Z has been certified according to FCC rules.

6.1.1 FCC (United States) Labeling Requirements

The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the final product. Attaching a label to a removable portion of the final product, such as a battery cover, is not permitted.

The label must include the following text:

> PTM 535Z Contains FCC ID: SZV-PTM535Z
> The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (i.) this device may not cause harmful interference and (ii.) this device must accept any interference received, including interference that may cause undesired operation.

When the device is so small or for such use that it is not practicable to place the statement above on it, the information required by this paragraph shall be placed in a prominent location in the instruction manual or pamphlet supplied to the user or, alternatively, shall be placed on the container in which the device is marketed.

However, the FCC identifier or the unique identifier, as appropriate, must be displayed on the device.

6.1.2 FCC (United States) Certificate

<TOB BE INSERTED>

6.1.3 FCC (United States) Regulatory Statement

This device complies with part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

6.2 IC (Industry Canada) Certification

PTM 535Z has been certified according to IC rules.

6.2.1 IC (Industry Canada) Labeling Requirements

OEM wishing to use PTM 535Z under limited modular approval conditions must sign the OEM Limited Modular Approval Agreement with EnOcean

The Original Equipment Manufacturer (OEM) must ensure that IC labeling requirements are met. Labelling requirements for Industry Canada are similar to those required by the FCC.

This includes a clearly visible label on the outside of the final product. Attaching a label to a removable portion of the final product, such as a battery cover, is not permitted. The label must include the following text:

Contains IC: *5713A-PTM535Z*

Pour utiliser le numéro IC EnOcean, le fabricant d'équipement d'origine (OEM) doit signer l'accord OEM limitée Approbation modulaire avec EnOcean et doit s'assurer que les exigences en matière d'étiquetage IC sont réunies.

Une étiquette clairement visible à l'extérieur d'une partie non amovible du produit final doit contenir le texte suivant:

Contient le module d'émission IC: 5713A-PTM535Z

6.2.2 IC (Industry Canada) Certificate

<TO BE INSERTED>

6.2.3 IC (Industry Canada) Regulatory Statement

This device complies with Industry Canada licence-exempt RSS standard(s).

The end product into which PTM 535Z is assembled must provide a clearly readable label with the following text: „Contains IC ID: SZV-PTM535Z"

Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement."

A Understanding PTM 535Z telegram structure

This appendix describes – purely for reference purposes – how to analyse the PTM 535Z radio telegram structure using the TI CC2531EMK packet sniffer (USB dongle) on a Windows 7 based system.

A.1 Installation instructions for TI CC2531 packet sniffer

The following description assumes the use of the TI CC2531EMK described here:

http://www.ti.com/tool/cc2531emk

CC2531EMK can be used in conjunction with the "TI SmartRF Protocol Packet Sniffer" to capture and visualize IEEE 802.15.4 data telegrams.

To use TI SmartRF Protocol Packet Sniffer, please download the SW package from the TI website. At the time of writing, the SW could be obtained using this link:

http://www.ti.com/tool/packet-sniffer

Please download and install this SW before proceeding with the instructions given in the next chapter.

A.1.1 CC2531EMK setup

After setting up the TI SmartRF Protocol Packet Sniffer please insert the CC2531EMK USB dongle into a USB port of the PC and make sure that the green LED of the dongle is active.

Please make sure that the required device driver for the CC2531EMK has been correctly installed. To do so, please check the Device Manager where you should see an entry named "CC2531 USB Dongle" under the group label "CEBAL Controlled Devices".

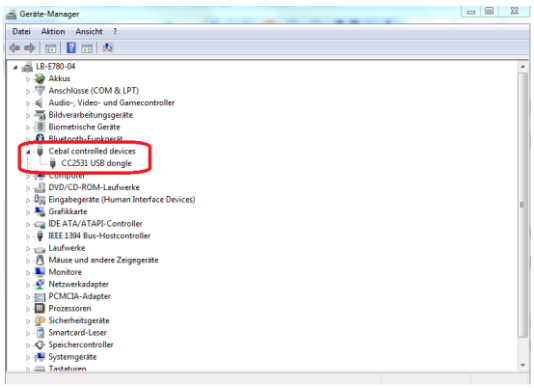


Figure 10 – Correctly installed CC2531EMK

A.2 Configuration

After the installation of the CC2531EMK driver, please start the TI SmartRF Packet Sniffer program. The protocol selection dialog program window which appears after the start of is shown in Figure 11 below.

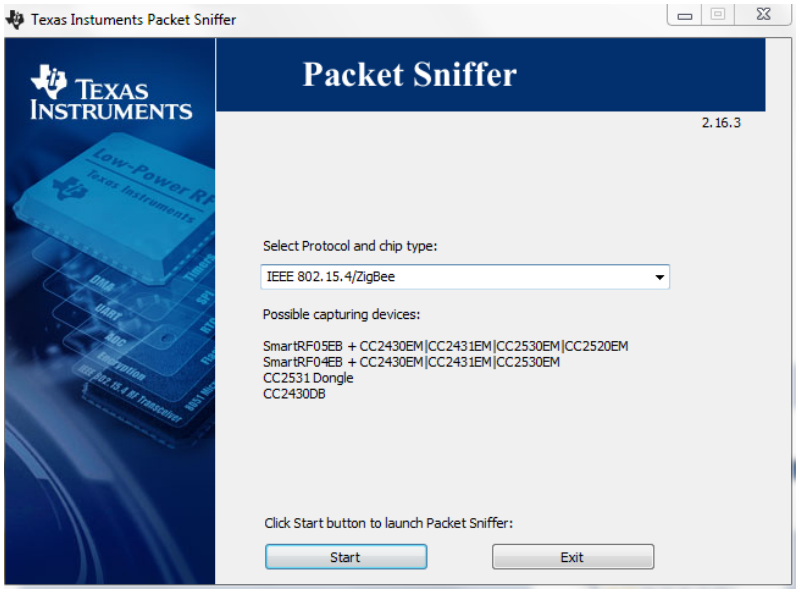


Figure 11 – Protocol selection dialog of TI SmartRF Packet Sniffer

In this dialog, please select "IEEE 802.15.4/ZigBee" as shown above and press the "Start" button. Once the main window comes up, please make sure that "CC2531" is shown in the "Capturing device" tab and in the "RF device:" footer line as shown in Figure 12 below.

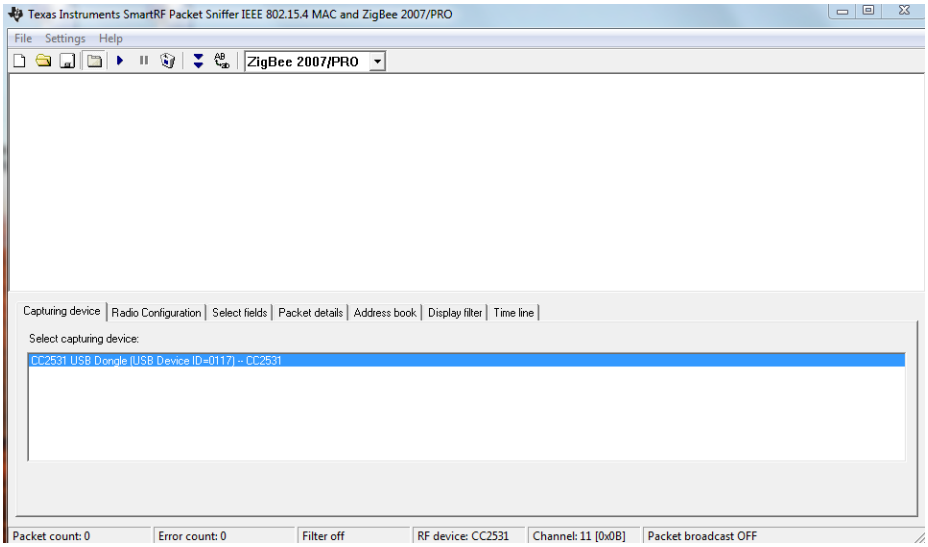


Figure 12 – Main window TI SmartRF Packet Sniffer

Out of the box, PTM 535Zis configured for using IEEE 802.15.4 radio channel 11. Make sure that this radio channel (0x0B) is selected in the "Radio Configuration" tab and shown in the "Channel:" footer line.

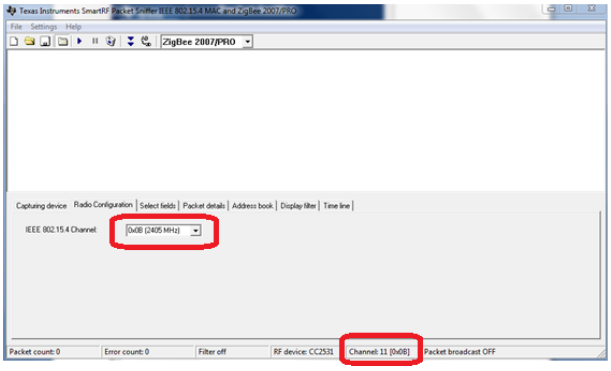


Figure 13 – Radio channel selection

The data fields that will be displayed can be selected in the "Select fields" tab. Make sure that all "MAC Header", "Data" and "Footer" fields are selected and that the "LQI/RSSI" drop-down list is set to "RSSI".

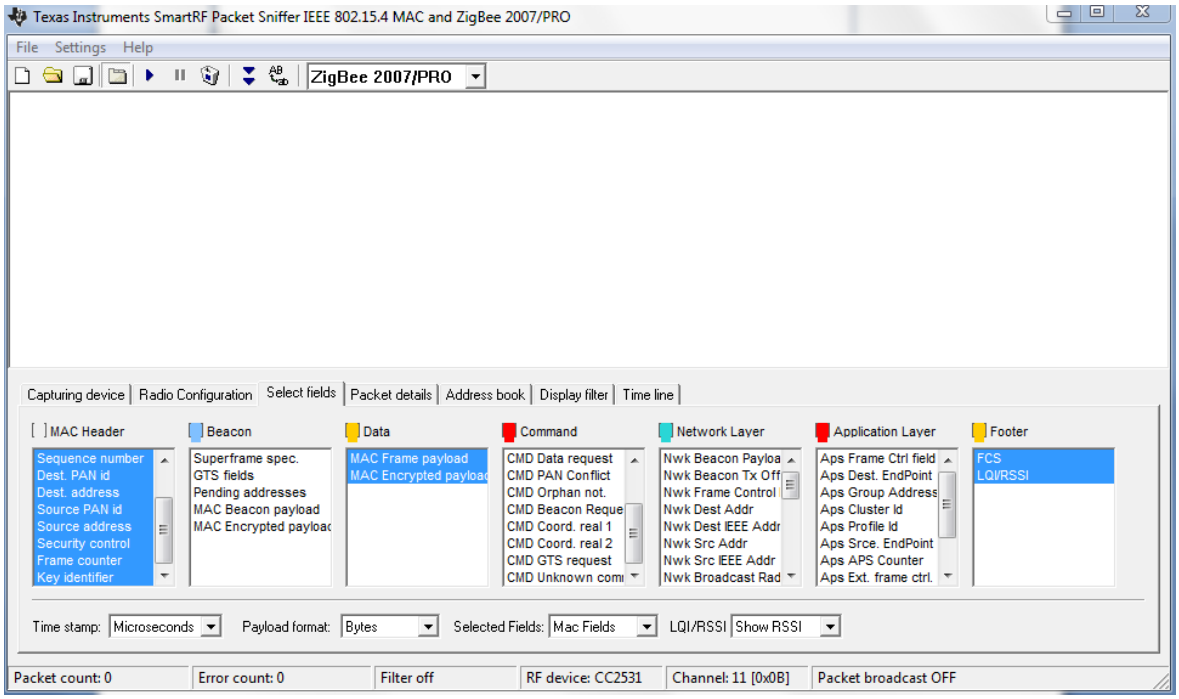


Figure 14 – Payload selection

The TI SmartRF Packet Sniffer is now ready.

A.3 Data capture

Press the triangular button ( ) to start the radio capture and press the auto-scroll button ( ) to automatically select the most recent data telegram. Then press a button of PTM 535Z.

You should now see the captured radio telegrams (PTM 535Z sends several redundant radio telegrams per user action).

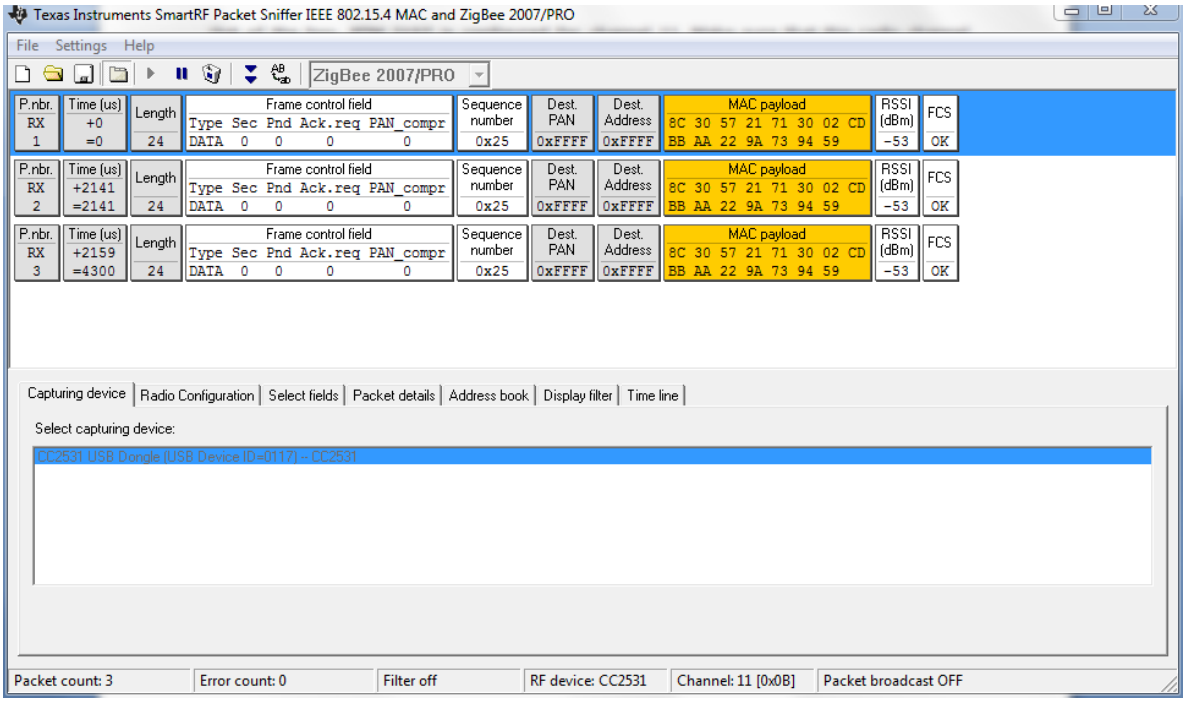


Figure 15 – Captured telegram data

A.4 Interpretation of the telegram data

The following parameters within captured radio telegrams are typically of interest:

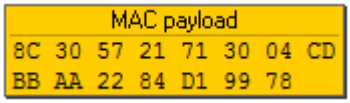
1. MAC Payload
   This will contain the ID of the sender, various control and security data fields as well as the actual command data (1 byte)
   The structure of this field is outlined subsequently in more detail.

2. RSSI
   This will show the received signal strength

3. FCS
   This will show the frame integrity (OK / not OK) and should normally show "OK".

A.4.1 MAC Payload

Below is an example of a captured MAC payload for a secure data telegram (see chapter 3.4.1):



The hexadecimal representation of this specific payload is:

8C 30 57 21 71 30 04 CD BB AA 22 84 D1 99 78

The location and interpretation of key parameters is described in the following chapters.

A.4.2 Device ID

The 4 byte device ID is used to uniquely identify each device in the network. In the case of secure data telegrams it is located at byte 2…5 of the MAC payload as highlighted below:

8C 30 **57 21 71 30** 04 CD BB AA 22 84 D1 99 78

Keep in mind that the byte order is little endian, therefore the ID of this specific device is 0x30712157.

A.4.3 Sequence Counter

The sequence counter is used to uniquely identify each telegram in order to avoid telegram replay. The sequence counter is 4 byte long and only present if PTM 535Z operates in secure mode.

In the case of a secure data telegram, the sequence counter is located at byte 6…9 of the MAC payload as highlighted below:

8C 30 57 21 71 30 **04 CD BB AA** 22 84 D1 99 78

Keep in mind that the byte order is little endian, therefore the current sequence counter value of this specific device is 0xAABBCD04.

A.4.4 Command payload

The command payload identifies the action performed on the switch (i.e. which buttons have been pressed). In the case of a secure data telegram, the command is located at byte 10 of the MAC payload as highlighted below:

8C 30 57 21 71 30 04 CD BB AA **22** 84 D1 99 78

In this case it is 0x22 meaning that button A0 has been pressed. Refer to chapter **Fehler! erweisquelle konnte nicht gefunden werden.** for the description of commands supported by PTM 535Z.

A.4.5 Telegram Signature

PTM 535Z secure data telegrams can be authenticated via a signature.

This signature is 4 byte long and only present if PTM 535Z operates in secure mode. It is calculated based on the private key (unique for each device), the data payload and a 4 byte sequence counter (which is incremented for each transmitted radio telegram).

This approach prevents unauthorized senders from sending commands. Note that the content of the telegram itself is not encrypted, i.e. the switch command is sent as plain text.

In the case of a secure data telegram, the telegram signature is located at the last 4 bytes of the telegram payload:

8C 30 57 21 71 30 04 CD BB AA 22 **84 D1 99 78**

Note that the signature changes with each transmission even if the remainder of the MAC payload remains the same.

This is due to the inclusion of the rolling code into the MIC calculation which prevents message replay attacks (capture and reuse of a previous message).