FOSSASAT-1 Communication Protocol

# Changelog

|  |  |  |
| --- | --- | --- |
| Date | Author(s) | Description |
| 04/07/2019 | Jan Gromeš | Initial release |
| 06/07/2019 | Jan Gromeš | Added EEPROM wipe flag |
| 11/07/2019 | Jan Gromeš | Updated system info frame |
| 14/07/2019 | Jan Gromeš | Added RESP\_INCORRECT\_PASSWORD frame |
| 15/07/2019 | Jan Gromeš | Changed system info frame to use integers instead of floats |
| 20/07/2019 | Jan Gromeš | Added CMD\_TRANSMIT\_CALLSIGN\_LOW\_POWER and CMD\_GET\_LAST\_PACKET\_INFO frames |
| 22/07/2019 | Jan Gromeš | Clarified optData field usage in encrypted frames |
| 24/07/2019 | Jan Gromeš | Added CMD\_RETRANSMIT\_CUSTOM frame, removed CMD\_TRANSMIT\_CALLSIGN\_ALT\_SF and CMD\_TRANSMIT\_CALLSIGN\_LOW\_POWER frames |
| 26/07/2019 | Jan Gromeš | Added CMD\_RETRANSMIT\_CUSTOM frame example |
| 26/07/2019 | Jan Gromeš | Added note about callsign ITA-2 compatibility |
| 28/07/2019 | Jan Gromeš | Added maximum limit for bandwidth in CMD\_RETRANSMIT\_CUSTOM frame |
| 28/07/2019 | Jan Gromeš | Added MCU temperature field to RESP\_SYSTEM\_INFO frame |
| 06/08/2019 | Jan Gromeš | Removed CMD\_SET\_MPPT\_ENABLE |

# Introduction

The purpose of this document is to explain the communication protocol implemented on FOSSASAT-1.

# Terminology

* Packet = Physical layer minimum data unit, contains preamble, sync word, header, CRC and payload. See [1] for details.
* Frame = FOSSASAT Communication Protocol minimum data unit. Contains callsign, function ID and optional data. Payload of physical layer Packet.
* Field = Logical section of frame. For example, callsign and function ID are fields.
* Section = Collection of fields.
* Callsign = String of printable ASCII characters, sent as the first field of each frame. Due to integration with RTTY, callsign can only use ASCII characters that have equivalent in ITA-2 encoding, by default set to “FOSSASAT-1”.
* Password = String of printable ASCII characters, used to verify successful decryption of encrypted frames.
* FCP = FOSSASAT Communication Protocol.
* Command = uplink message (from ground station to satellite)
* Response = downlink message (from satellite to ground station)

# Physical Layer

The satellite is using two different modems as means of communication – LoRa and GFSK – which can be switched at any time. As such, the following protocol is designed to be independent of currently operating modem. Hence, description of physical packets is omitted and can be found in [1].

# Frame Structure

Each FCP frame consist of the following fields:

**<callsign><function ID>(optional data length)(optional data)**

Fields callsign and function ID are mandatory. Fields optional data length and optional data are not mandatory and may not be present in some frames. Due to the limitations of physical layer packets, total frame length shall be less than or equal to 255 bytes.

# Function IDs

Function ID is the single-byte field following callsign and determines the action satellite should take. In general, function IDs are separated into four types by communication direction (commands vs. responses) and access level (public vs. private). Function ID of every response has a value that is by 0x10 larger than that of associated command. Public function IDs start at value 0x00, while private function IDs at 0x20. Unless stated otherwise, response to any command is performed using the same modem that was used to receive the command frame. The response is sent immediately, where applicable.

Following is a list of function IDs currently implemented in FOSSASAT-1.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function ID type** | **Function ID value** | **Function ID alias** | **Description** |
| Public commands | 0x00 | CMD\_PING | PING command. Satellite shall respond with RESP\_PONG. |
| 0x01 | CMD\_RETRANSMIT | Repeater command. Satellite shall respond with RESP\_REPEATED\_MESSAGE containing the same data that was received as the optional data of the command frame (maximum length is 64 bytes). |
| 0x02 | CMD\_RETRANSMIT\_CUSTOM | Command to retransmit message with custom configuration (1). |
| 0x03 | CMD\_TRANSMIT\_SYSTEM\_INFO | Command to send system info. |
| 0x04 | CMD\_GET\_LAST\_PACKET\_INFO | Command to get information about last received packet. |
| Public responses | 0x10 | RESP\_PONG | Response to CMD\_PING. |
| 0x11 | RESP\_REPEATED\_MESSAGE | Response to CMD\_RETRANSMIT. |
| 0x12 | RESP\_REPEATED\_MESSAGE\_CUSTOM | Response to CMD\_RETRANSMIT\_CUSTOM. |
| 0x13 | RESP\_SYSTEM\_INFO | Response to CMD\_TRANSMIT\_SYSTEM\_INFO. (2) |
| 0x14 | RESP\_LAST\_PACKET\_INFO | Response to CMD\_GET\_LAST\_PACKET\_INFO. (3) |
| Private commands | 0x20 | CMD\_DEPLOY | Command to initiate deployment sequence. |
| 0x21 | CMD\_RESTART | Command to restart satellite. |
| 0x22 | CMD\_WIPE\_EEPROM | Command to wipe EEPROM. |
| 0x23 | CMD\_SET\_TRANSMIT\_ENABLE | Command to enable/disable all transmissions from satellite. (4) |
| 0x24 | CMD\_SET\_CALLSIGN | Command to set new satellite  callsign. (5) |
| 0x25 | CMD\_SET\_SF\_MODE | Command to set standard/alternative LoRa spreading factor. (6) |
| 0x26 | CMD\_SET\_MPPT\_MODE | Command to set MPPT mode. (8) |
| 0x27 | CMD\_SET\_LOW\_POWER\_ENABLE | Command to enable/disable low power mode. (9) |
| Private responses | 0x30 | RESP\_DEPLOYMENT\_STATE | Response to CMD\_DEPLOY, sent after deployment sequence has finished. (10) |
| 0x31 | RESP\_INCORRECT\_PASSWORD | Sent when received decrypted password is incorrect. (11) |

1. Spreading factor is sent in the optional data field:

optionalDataLen = 7 + N

optionalData[0] = bandwidth value (0x00 for 7.8 kHz, 0x07 for 125 kHz)

optionalData[1] = spreading factor value (0x00 for SF5, 0x07 for SF12)

optionalData[2] = coding rate (0x05 to 0x08, inclusive)

optionalData[3 - 4] = preamble length in symbols (0x0000 to 0xFFFF; LSB first)

optionalData[5] = CRC enabled (0x01) or disabled (0x00)

optionalData[6] = output power in dBm (signed 8-bit integer; -17 to 22)

optionalData[7 - N] = message to be repeated (64 bytes or less)

1. System info is sent in the optional data field. Variables larger than a single byte are sent LSB first:

optionalDataLen = 15

optionalData[0] = battery charging voltage \* 20 mV (unsigned 8-bit integer)

optionalData[1 - 2] = battery charging current \* 10 uA (signed 16-bit integer; LSB first)

optionalData[3] = battery voltage \* 20 mV (unsigned 8-bit integer)

optionalData[4] = solar cell A voltage \* 20 mV (unsigned 8-bit integer)

optionalData[5] = solar cell B voltage \* 20 mV (unsigned 8-bit integer)

optionalData[6] = solar cell C voltage \* 20 mV (unsigned 8-bit integer)

optionalData[7 – 8] = battery temperature \* 0.01 °C (signed 16-bit integer; LSB first)

optionalData[9 – 10] = board temperature \* 0.01 °C (signed 16-bit integer; LSB first)

optionalData[11] = MCU temperature \* 1 °C (signed 8-bit integer)

optionalData[12 – 13] = reset counter (unsigned 16-bit integer; LSB first)

optionalData[14] = power control configuration

1. Packet information is sent in the optional data field:

optionalDataLen = 2

optionalData[0] = SNR \* 4 dB

optionalData[1] = RSSI \* -2 dBm

1. Transmission enable/disable is sent in the optional data field:

optionalDataLen = 1

optionalData = 0x00 (transmission disable) or 0x01 (transmission enable)

1. New callsign is sent in the optional data field:

optionalDataLen = length of the new callsign in bytes

optionalData = new callsign

1. Spreading factor mode is sent in the optional data field:

optionalDataLen = 1

optionalData = 0x00 (standard spreading factor) or 0x01 (alternative spreading factor)

1. MPPT mode is sent in the optional data field:

optionalDataLen = 2

optionalData[0] = 0x00 (temperature switch disabled) or 0x01 (temperature switch enabled)

optionalData[1] = 0x00 (keep-alive disabled) or 0x01 (keep-alive enabled)

1. Low power mode enable/disable is sent in the optional data field:

optionalDataLen = 1

optionalData = 0x00 (low power mode disabled) or 0x01 (low power mode enabled)

1. Deployment state is sent in the optional data field:

optionalDataLen = 1

optionalData = number of times deployment sequence has run

1. The optional data field contains additional information about the frame which caused this response:

optionalDataLen = N + 2

optionalData[0] = function ID of the failed frame

optionalData[1] = optionalDataLen of the failed frame

optionalData[2 – N] = optionalData of the failed frame

# Encryption

Due to the nature of some of the above commands, it is undesirable to expose them to general public. Such sensitive function IDs are protected using additional encryption. All frames in the private function ID space are protected using encryption. The structure of encrypted frame is as follows:

**<callsign><function ID>[<optionalDataLength><password>(optionalData)(padding)]**

The encrypted part of frame above is marked using square brackets. FOSSASAT-1 implements AES-128 as the encryption algorithm. Since this algorithm is a block cipher, padding bytes may be added to fill the encrypted part of frame up to full block size. Pseudo-random bytes are used to fill this padding. To decide which part of decrypted frame contains valid data, and which part is the random padding, the optionalDataLength field is the sum of password length, and the length of optionalData in bytes. For this reason, optionalDataLength field is mandatory when using encryption – optionalData may not be present in some frames.

# Frame Validation

Upon receiving any new packet, the following steps SHALL be taken in order to validate frame integrity and access level:

1. **Physical packet CRC check.** This step is done by the communication library, and can be fulfilled by checking the return value of reception methods receive() or readData(). Frames that do not pass this step SHALL be quietly discarded.
2. **Callsign check**. Received frame callsign field SHALL be checked against the value stored on satellite for exact match. Frames that do not pass this step SHALL be quietly discarded.
3. **Function ID check**. Received function ID SHALL be checked to decide whether decryption should follow this step. Frames with function IDs in the public ID space MAY be executed at this point. Frames with function IDs in the private ID space SHALL continue to the next step.
4. **Decryption and password check.** The optional data of encrypted packets SHALL be decrypted at this point. After decryption, optional data SHALL be checked for password. Frames that do not contain correct password SHALL be reported to ground station for further evaluation.

# Examples

Following are examples of valid exchanges between ground station and satellite, assuming callsign “FOSSASAT-1” and password “password”. Quote marks not a part of the frame. Byte values representing unprintable ASCII characters are represented by their hexadecimal value in angle brackets. Sections protected by encryption are marked by square brackets - these sections may contain additional padding bytes. Variables are shown in curly brackets, with the respective size in bytes. Note that this list is by no means exhaustive and only serves to illustrate all sections above.

1. **Ping-Pong exchange:**

From ground station: “FOSSASAT-1<0x00>”

From satellite: “FOSSASAT-1<0x10>”

1. **Repeater exchange:**

From ground station: “FOSSASAT-1<0x01><0x0C>Hello World!”

From satellite: “FOSSASAT-1<0x11><0x0C>Hello World!”

1. **Repeater exchange with custom configuration:**

From ground station:   
“FOSSASAT-1<0x02><0x15><0x07><0x0C><0x06><0x20><0x00><0x01><0x0A>I’m a message!”

From satellite: “FOSSASAT-1<0x0E>I’m a message!” (transmitted with bandwidth 62.5 kHz, spreading factor 12, coding rate 4/7, preamble length 32 and with CRC)

1. **System info exchange:**

From ground station: “FOSSASAT-1<0x03>”

From satellite:

“FOSSASAT-1<0x13><0x0E>{batteryChargingVoltage, 1B}{batteryChargingCurrent, 2B} {batteryVoltage, 1B}{solarCellAVoltage, 1B}{solarCellBVoltage, 1B}{solarCellCVoltage, 1B} {batteryTemperature, 2B}{boardTemperature, 2B}{mcuTemperature, 1B}{resetCounter, 2B}  
{powerConfig, 1B}”

1. **Deployment command:**

From ground station: “FOSSASAT-1<0x20>[<0x08><0x08>password]”

From satellite: no response

1. **Spreading factor mode configuration:**

From ground station: “FOSSASAT-1<0x25>[<0x09><0x08>password<0x00>]”

From satellite: no response

1. **MPPT mode configuration:**

From ground station:

“FOSSASAT-1<0x28>[<0x0B><0x08>password{tempSwitchEnabled, 1B}{keepAliveEnabled, 1B}]”

From satellite: no response

# References

[1] SX1268 datasheet. *Semtech*. Rev. 1.0 March 2018, online. Available from <https://www.semtech.com/uploads/documents/DS_SX1268_V1.0.pdf>