# Radio Packets

# Types of Radio Packets

Radio Packets for SPRN have two main parts: A non-encrypted part, and a decrypted part. The first part includes a length byte, indicating the length of the payload, a 4-byte network key, and a 3-bit sequence number.

The encrypted part is a byte string of 16 bytes minimum and 240 bytes maximum, which contains data such as the packet type, device ID, etc. The structure of this part for each packet type is explained down below.

## MSG (TYPECODE 0X01)

A MSG packet is used by a device to send a string of data to the main node.

Type Code (1 byte): Always 0x01 for this type of packet.

Device ID (4 bytes): The device ID assigned to the device.

Origin Device (4 bytes): The origin device of the packet.

Payload Length (1 byte): Length of the payload part in bytes.

Payload (0-222): The payload containing the data which should be sent to the main node.

CRC-32 (4 bytes): The CRC digest of the Payload block.

Zero padding (varying): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

## CHECK (TYPECODE 0X02)

A CHECK packet is sent by a device to notify their parent node of their connectivity.

Type Code (1 byte): Always 0x02 for this type of packet.

Device ID (4 bytes): The device ID assigned to the device.

Zero padding (7 bytes): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

## ACK (TYPECODE 0X04)

An ACK packet is sent by a device which has successfully received a payload to indicate that the payload was successfully received, or a parent device which has received a check packet from its child node.

Type Code (1 byte): Always 0x04 for this type of packet.

Device ID (4 bytes): The device ID assigned to the device.

Sequence Number (3 bytes): The sequence number of the acknowledged packet.

Zero padding (4 bytes): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

## CMD (TYPECODE 0X08)

A CMD packet is a packet containing command data sent by the central node to another node in the network.

Type Code (1 byte): Always 0x08 for this type of packet.

Device ID (4 bytes): The device ID assigned to the device.

Target Device (4 bytes): The target device of the packet.

Payload Length (1 byte): Length of the payload part in bytes.

Payload (0-222): The payload containing the data which should be sent to the main node.

CRC-32 (4 bytes): The CRC digest of the Payload block.

Zero padding (varying): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

## SRCH (TYPECODE 0X10)

A SRCH packet is sent by a node which is trying to find a parent node in the network. Since a device which is searching for a parent does not have a device ID, an SRCH packet does not have the 4 device ID bytes, and instead has a 2-byte temporary ID, which is used by network devices to distinguish between devices that are trying to enter the network simultaneously.

Type Code (1 byte): Always 0x10 for this type of packet.

Temporary ID (2 bytes): The temporary ID chosen by the device.

Zero padding (9 bytes): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

## ADP (TYPECODE 0X20)

An ADP packet is sent by a node which has agreed to act as a parent device for a stray node.

Type Code (1 byte): Always 0x20 for this type of packet.

Device ID (4 bytes): The device ID assigned to the child device.

Temporary ID (2 bytes): The temporary ID indicated in the SRCH packet.

Zero padding (5 bytes): a sequence of zero bytes, so that the total length of the encrypted message is divisible by 16.

Timestamp (4 bytes): The value in the global timer of the device in seconds.

# Device IDs and packet routing

## Device ID structure

The device ID in this network consists of a series of n-bit words, which are put together to form a 32-bit address. For an address of the form:

$$Addr_{device} = a_1 a_2 ... a_d 0 ... 0$$

The addresses for the parent and direct children would be of the form:

$$Addr_{parent} = a_1 a_2 ... a_{d-1} 0 ... 0$$
$$Addr_{child} = a\,1\,a\,2 ... a_{d+1} 0 ... 0$$

Taking this into consideration, by choosing an n-bit address word for each device, the network would have a maximum depth of $\frac{32}{n}$ and each device would be able to have $2^n$ children. Considering that a low depth would cause problems in long range network propagation, and the fact that 3 evenly-spaced child nodes at maximum range from a parent node can connect to any node that is also at maximum range from the parent node, a word size of 2 bits would seem appropriate for this network.

Each of the class B devices are given a depth-one address by the server, which is used to avoid packet collisions between neighboring networks.

## Device ID allocation

A device which is trying to join a network would periodically send SRCH packets with a constant, randomly generated temporary ID. A device which receives these packets, and has enough ID space to accept more children, will then send an ADP packet and set the device ID in its children list with a short timeout. The child device will then listen for packets ADP packets, and chooses one of them. The priority can be set to low or high depth devices depending on the physical requirements of the network. The child device will then set its ID and timer value, and sends a CHECK packet to its parent device. Doing so would reset the timeout to a larger value, and allow the other ADP-sending devices to remove the unused IDs from their memory more quickly.

## Packet routing

The only packets that need routing in this network structure are MSG and CMD packets. The routing of MSG packets is done easily from the bottom up, since there is only one target for these packets, i.e. the parent node of the device.

Routing of CMD packets is more tricky. Each time that a device receives a CMD packet, it will check its target device, and chooses which child should receive the packet next, according to the target device. It will then modify the target to one of its children, and retransmit the packet.

# Payload Content

There are 3 types of payload packets in general, MSG payloads, CMD payloads, and ADP payloads. The last of these can be seen as an extension of the ADP packet, rather than an actual payload.

## MSG Payloads

A MSG payload is a payload carrying sensor data to the central server. Each of the sensors in a device is assigned a 1-byte sensor TYPE and a 1-byte sensor ID. The TYPE tells the server what kind of sensor is sending the data, while the ID is used to distinguish sensors of the same type. Also, each sensor reading might have a different byte length, therefore, the length of the reading is also appended to the reading. A block in the MSG payload has the following structure:

Sensor Type (1 byte): Type of the sensor.

Sensor ID (1 byte): The ID assigned to the sensor.

Message Length (1 byte): Length of the message sent by the sensor.

Message (varying length): The message sent by the sensor.

Several of these blocks can be concatenated to form the payload, which is then included in a MSG packet and transmitted.

## CMD Payloads

CMD payloads are payloads containing commands from the central server, controlling the actuators in the nodes. These packets have a structure similar to the MSG packets, with actuator data replacing the sensors. A block in these payloads has the following structure:

Actuator Type (1 byte): Type of the actuator.

Actuator ID (1 byte): The ID assigned to the actuator.

Message Length (1 byte): Length of the message sent to the actuator.

Message (varying length): The message sent by the actuator.