Radio Packets

Types of Radio Packets

Radio Packets for SPRN have two main types: header and payload. The header packets, each have a typecode byte in the beginning, which indicates the type of header, its structure, and length. Payload packets, are 16-byte packets, each encrypted using the AES-128 cipher.

Header Packets

Header packets can be 9 to 16 bytes long. The data in the first 9 mandatory bytes are as follows:

Byte (0): A number indicating the type of packet.

Bytes (1-4) : A 4-byte network ID. This can be used to exclude messages from neighboring networks which operate in the same area.

Bytes (5-8): A 4-byte device ID. This works similarly to the IP address in a network, and is given to each device by its parent node.

Each packet type might have a number of additional bytes, which is known by the receiver after receiving the first byte.

MSG (TYPECODE 1)

A MSG packet is used by a device to announce that it is about to send a message to its parent device. It has 16 bytes total.

Byte (9): A number indicating the length of the incoming message payload in bytes, which should be a multiple of 16, and no more than 256.

Bytes (10-15): A random string of bytes. This is used to randomize the values of the packet header, which is then used as an IV for the AES encryption and decryption.

CHECK (TYPECODE 2)

A CHECK packet is sent by a device to check for the availability of their parent node, or acquiring a new parent node. The network ID in this case should be the same as the network which the device is connected to, or is trying to connect to. The device ID should be equal to the value given by the parent node, or in the case of a device which is trying to find a node, equal to zero.

ACK (TYPECODE 3)

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. It has 5 additional bytes, which contain the message length and the CRC-32 checksum of the payload.

Byte (9): A number indicating the length of the received package, minus the padding, length, and checksum.

Bytes (10-13): The CRC-32 checksum of the received payload.

NACK (TYPECODE 4)

A NACK packet is sent by a device which has either failed to receive a payload, or has received corrupted data. It does not contain any additional bytes.

CMD (TYPECODE 5)

A CMD packet is a command packet sent by the central device to a node. It has 16 bytes in total, similar to an MSG packet, and is followed by a payload.

Byte (9): A number indicating the length of the incoming message payload in bytes, which should be a multiple of 16, and no more than 256.

Bytes (10-15): A random string of bytes. This is used to randomize the values of the packet header, which is then used as an IV for the AES encryption and decryption.

ADP (TYPECODE 6)

An ADP packet is sent by a node which has agreed to act as a parent device for a stray node. It contains 13 bytes in total.

Bytes (9-12): The device ID assigned to the child device.

Payload Packets

Payload packets are packets which contain data that is to be transferred to a node. These packets are made by taking raw data, padding them with zero until the length of the packet modulo 16 is equal to 9. Then one byte indicating the original length of the packet is added to the sequence. Finally, CRC-32 checksum of the raw data is added to the sequence. Finally, the packet is encrypted using AES-128 in CFB-128 mode. This sequence is then sent either in 16-byte chunks, or all at once.

Payload Content

TODO