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 an encryption scheme, the details of which are separately explained.

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 0X01)

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.

Note: The IV for encryption and decryption is set to the packet where the source device (Bytes 5 to 8) is 0x00.

CHECK (TYPECODE 0X02)

A CHECK packet is sent by a device to check for the availability of their 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.

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. 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 0X08)

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 0X10)

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 (10-13): The end device which is meant to receive the command.

Bytes (14-15): A random string of bytes. This is used to randomize the values of the final packet header, which is then used as an IV for the AES encryption and decryption.

Note: The IV for encryption and decryption is set to the packet where the source device (Bytes 5 to 8) is 0x00.

SRCH (TYPECODE 0X20)

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.

Bytes (5-6): The temporary ID used by the device.

ADP (TYPECODE 0X40)

An ADP packet is sent by a node which has agreed to act as a parent device for a stray node. It contains 15 bytes in total.

Bytes (5-8): The device ID assigned to the child device.

Bytes (9-13): The global timer value of the parent device in seconds.

Bytes (14-15): The temporary ID of the device.

An ADP packet is followed by a payload, which is the encrypted network key. This is used by the child to ensure that the node claiming to be a parent is in fact an authorized device on the network.

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 7.

Then the following bytes are added to the final 16-byte chunk of the packet:

Byte (7): A byte indicating the length of the raw data in bytes.

Bytes (8-11): A 4-byte timestamp, indicating the time in which the packet was created. This timestamp is used to prevent replay attacks and omit replicated packets.

Bytes (12-15): CRC-32 checksum of the raw message.

This sequence is then sent either in 16-byte chunks, or all at once.

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:

Byte (0): Sensor TYPE.

Byte (1): Sensor ID.

Byte (2): Length of the sensor's reading in bytes, a.k.a LEN.

Bytes (3 – LEN+2): The reading of the sensor.

Several of these blocks can be concatenated to form the payload, which is then padded, encrypted, 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:

Byte (0): Actuator TYPE.

Byte (1): Actuator ID.

Byte (2): Length of the command in bytes, a.k.a LEN.

Bytes (3 – LEN+2): The command that is sent to the actuator.

ADP Payloads

ADP payloads are the payloads sent after ADP packets. Each ADP packet has a 4-byte payload, which is simply the network ID. This payload is then padded with its CRC-32 and timestamp, and encrypted. The child device that receives this packet will then decrypt this payload and check if the network ID is correct, and if the timestamp in the payload matches with the timestamp in the packet header. If these parameters are correct, the child device can be sure that the ADP packet has come from a valid network node, and not from an adversary.