The HumPRO™ Series RF Transceiver Join Process

Reference Guide RG-00107

Introduction

The HumPRO™ Series transceiver module is designed for the reliable transfer of digital data. It has a very flexible addressing method that allows for the creation of many different types of networks. The addition of AES encryption makes the messages very secure.

The modules include a Join process that simplifies establishing and configuring a network. This includes generating and distributing a random network encryption key and creating and assigning network addresses to modules joining the network.

The basic operation uses push buttons to activate the process. Holding the button for 30 seconds sets the module to be the network administrator. A single push of less than 2 seconds triggers node modules and an administrator to join. This makes creating networks in the field as simple as pushing a button on each end and watching an LED flash.

The process offers several options to tailor the operation to a specific application. These include using fixed addresses, using a pre-defined network key, joining without encryption, and disabling the pushbutton operation. This gives the designer a great deal of freedom in establishing the system.

Pre-Join Configuration

The only configuration required prior to initiating the Join process is setting the modules to the same baud rate. The modules are set to 9,600bps by default. If a higher rate is desired, then all of the modules need to be set the same before triggering the Join process.

The Network Administrator

A network administrator is the module that is responsible for generating and distributing the network key and assigning addresses to each module that joins the network. A module is set to be an administrator by holding its PB line high for 30 seconds. When the 30 seconds expires the MODE_IND line flashes to indicate that the module will start to generate the network key and address when the PB line goes low.

The default Generate Key operation performs several functions:

- The module generates a random 128-bit AES encryption key based on ambient RF noise and scrambled by an encryption operation.
- The Address Mode (ADDMODE register) is set to Extended User Address with encryption (0x27).

- The User Address Mask (UMASK registers) is set to 0x000000FF, supporting up to 254 nodes in the network (256 total addresses minus the administrator's address and the network broadcast address; 2^8-2=254).

- A random 24-bit address is generated and assigned as the high order bytes of the User Source Address (USRCID registers). The low byte is 0, forming the network base address. Other nodes are assigned sequential addresses, starting with network base address +1.

- The Destination Address (UDESTID registers) is set to the bitwise OR of USRCID and UMASK, which is the network broadcast address.

It is possible to use pre-configured values for the key, address and mask. Those options are discussed later.

When all of these functions are complete the module flashes the MODE_IND line to provide visual indication that the network is defined and the module is ready to Join other modules.

Joining a node

The Join process adds new nodes to the network and is triggered by taking the PB line high on the administrator and the module that is to join the network at the same time. The lines should be held for between 0.1 and 2 seconds. The modules attempt to find each other for 30 seconds after the lines are released.

The modules automatically search for each other using a special protocol. When they find each other, the Administrator sends the node the network encryption key, UMASK value and its network address. The node UDESTID is set to the address of the administrator. The values are encrypted using a special key that is defined at the factory. Once the Join process is complete, the MODE_IND blinks on both units and they now operate together.

Figure 1 shows the default assignments after the join process is complete.

Device Assignments After Joining

Assignment	Administrator	Node
Source Address	Network Base Address	Join-Assigned Address
Destination Address	Network Broadcast Address	Network Base Address
Transmission Operation	Broadcasts to the entire network	Sends to the base address

Figure 1: HumPRO™ Series Transceiver Device Assignments After Joining

The Join process establishes a star network by default with the administrator as the hub or access point. However, this is simply for convenience. The destination address of any module can be changed at any time to communicate peer-to-peer with any other node in the network that is in range.

This allows the Join process to be used to establish the network, then code running on an external processor can be used to create any network topology that is desired.

The Administrator is primarily responsible for establishing the network key and addresses. Code on an external processor determines if it controls the network or simply operates as another node. This gives the system designer many options when implementing the HumPRO™ Series.

Figure 2 shows an example of the Join process.

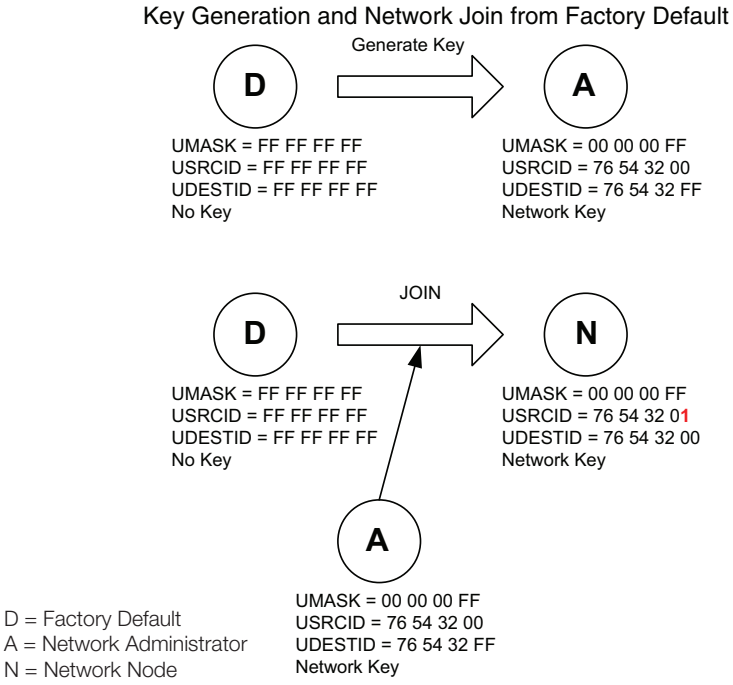

Figure 2: HumPRO™ Series Transceiver Join Process

Configuration Options

As mentioned earlier, there are some aspects of the Join process that can be set by the system before the Join process is triggered. This allows the system designer to tailor the process for specific applications or deployments.

Things To Remember

- Make sure SECOPT register bit 4 (KEYRCV) is set the proper way (0 for Administrator, 1 for Node) when you modify the register. If you are not careful, you can accidentally set the Administrator back into a Node, and the Join process will fail until the module is configured properly.
- When modifying the UMASK registers, make sure their bits are of the form [block of contiguous 0's][block of contiguous 1's]. This is the format the Generate and Join processes expect. Other configurations can cause unintended behavior.
- If not explicitly stated, SECOPT bits are set high (default).
- When changing register values, be sure to change both the Volatile and Non-Volatile registers at the same time. Setting only one or the other can cause unintended behavior.

Disable Push-Button Features

This provides some security in that it prevents an accidental factory reset from the button press. This can be beneficial in applications where the button may get hit by other objects (if in a pocket) or if unsophisticated users are setting up the network.

- Set the SECOPT register bit 0 to 0 to disable the factory reset from the button input

Serial Command control

The modules can be completely controlled using an external microcontroller instead of using the hardware pushbutton. This may be desired in applications that have their own user interface, such as an LCD screen. This interface can be used to set up the network instead of requiring another button for the user.

- Set the address and key if not using the default values
- Use the CMD register to trigger Join operations
  0x10 0x01 to generate a random network key and base address.
  0x10 0x02 to start the Join process
  0x10 0x00 to halt the Join process
- Read the Join Status register (JOINST) for the results of the Join process

Defining Larger Networks

By default, the HumPRO™ Series Join process defines a network that supports up to 254 nodes. This can be modified to allow for a larger (or smaller) number of nodes.

Configuration for Larger Networks

Administrator	Node
1. Set the UMASK to the desired network size. The total number of nodes is determined by the 1 bits in the low order positions (e.g., 0x0000FFFF for 2^{16}-2 possible node addresses). The default is 0x000000FF for 2^{8}-2 or 254 node addresses. 2. Set the ADDMODE register to the desired type. 3. Use the CMD.JOINCTL command with a Subcommand of 0x01 to set the module as the Administrator and generate a key and network address.	1. Set the ADDMODE register to the desired type.

Write both the volatile and non-volatile registers where applicable.

Figure 3: Configuration for Larger Networks

The ADDMODE registers must be set the same on all of the modules that are to be in the same network. When the Join process is triggered the administratior distributes the key and assigns addresses to all nodes.

Use Fixed Address Assignment

The HumPRO™ allows the use of a pre-configured address to be used with the Join process. This allows the system to use known addresses or allow more addresses within an existing network.

Configuration for Fixed Addresses

Administrator	Node
1. Set the ADDMODE register to the desired type. The default mode is Extended User with Encryption. 2. Set the UMASK registers (the default is 0x000000FF). 3. Set the USRCID registers to whatever address is desired. 4. Set the SECOPT register bit 3 (CHGADDR) to 0 (prevents changing the address). 5. Set the LASTNETAD registers to match the USRCID registers identically. 6. Use the CMD.JOINCTL command with a Subcommand of 0x01 to set the module as the Administrator and generate the network key.	1. Set the ADDMODE register to the desired type. The default mode is Extended User with Encryption. 2. Set the UMASK registers (the default is 0x000000FF). 3. Set the USRCID registers to whatever address is desired. 4. Set the SECOPT register bit 3 (CHGADDR) to 0 (prevents changing the address).

Write both the volatile and non-volatile registers where applicable.

Figure 4: Configuration for Fixed Addresses

When the Join process is triggered the administratior only distributes the key and does not change any of the addresses.

The UDEST registers can be preconfigured or they can be set by an external microcontroller during use. The ADDMODE and UMASK registers must be set the same in all modules.

Use Preassigned Encryption Key

There are two ways of using a preassigned encryption key. The key can be set in the administrator and then the normal Join process used to distribute the key to the nodes. Alternatively, the key can be written into all of the modules and the join process used to only set the addresses.

Configuration for Preassigned Encryption Key - Assiging to the Administrator Only	
Administrator	**Node**
1. Use the CMD.JOINCTL command with a Subcommand of 0x01 to set the module as the Administrator. 2. Set the ADDMODE register to an encrypted addressing mode. 3. Write the key into the module using the CMD. WRKEY command (the key cannot be read out of the module).	No additional setup is needed if starting from factory default.
Write both the volatile and non-volatile registers where applicable.	

Figure 5: Configuration for Preassigned Encryption Key - Assiging to the Administrator Only

When the Join process is triggered the administratior distributes the key and assigns an address to the joining node.

Configuration for Preassigned Encryption Key - Assiging to All Modules	
Pre-determined Administrator	
Administrator	**Node**
1. Use the CMD.JOINCTL command with a Subcommand of 0x01 to set the module as the Administrator. 2. Write the key into the module using the CMD. WRKEY command (the key cannot be read out of the module). 3. Set the SECOPT register bit 1 (PSHARE) to 0 (disables sharing a key).	1. Write the key into the module using the CMD. WRKEY command (the key cannot be read out of the module). 2. Set the SECOPT register bit 2 (PGKEY) to 0 (disables getting a key).
Field-determined Administrator	
1. Write the key into the module using the CMD.WRKEY command (the key cannot be read out of the module). 2. Set the SECOPT register bit 1 (PSHARE), bit 2 (PGKEY) and bit 7 (EN_CHANGE) to 0 (disables sharing and getting a key and disables making changes to the SECOPT settings). 3. Assign one module to be the administrator by holding the PB line high for 30 seconds. 4. Join other nodes by briefly holding the PB line high on both modules.	
Write both the volatile and non-volatile registers where applicable.	

Figure 6: Configuration for Preassigned Encryption Key - Assiging to All Modules

When the Join process is triggered the administratior assigns addresses to all nodes.

The key must be the same in all of the modules for them to communicate.

Disable Encryption

Encryption can be disabled and the Join process used to set the network addresses.

Configuration for Disabling Encryption	
Administrator	**Node**
1. Set the SECOPT register bit 1 (PSHARE) and bit 2 (PGKEY) to 0 (disables sharing a key and generating a key); and bit 5 (EN_UNENC) to 1 (enables receiving unencrypted packets). 2. Set the UMASK registers to a non-factory-default value. Normally this should be set to 0xFF to support up to 254 nodes. 3. Set the ADDMODE register to one of the modes with encryption disabled. 4. Use the CMD.JOINCTL command with a Subcommand of 0x01 to set the module as the Administrator.	No additional setup is needed if starting from factory default.
Write both the volatile and non-volatile registers where applicable.	

Figure 7: Configuration for Disabling Encryption

When the Join process is triggered the administratior distributes addresses to all nodes.

Common Troubleshooting Steps

If these steps don't seem to work for some reason, here are some common troubleshooting tips for debugging the configurations.

- Verify that ADDMODE has been modified properly by the Join processes. If the UMASK registers are a non-default value, ADDMODE does not update. This can be remedied either by setting the UMASK registers to their defaults and triggering the Join process again or by manually setting the ADDMODE register to the intended mode.
- Verify ADDMODE is compatible with the values in USRCID and UDESTID. If a destination address is a value greater than 0x0000FFFF, then User addressing mode does not work and Extended User mode is required.
- Verify the bits in the SECOPT register are set properly.

Network Topologies

The Join process is designed to simplify creating and distributing an encryption key and node addresses. By default it forms a star network with the administrator as the hub. However, each node can talk directly to every other node in the network in a peer-to-peer fashion. It simply need to have the address of a remote node written into it.

This allows a system to use the Join process for key and address management, but the actual network topology can be determined by code on an external microcontroller. The HumPRO™ establishes a low cost and low power data link that is equivalent to the MAC and PHY layers in protocol stacks. The higher layers reside in an external microcontroller. This allows the system designer to tailor the protocol to the system.

159 Ort Lane, Merlin, OR 97532
Phone: +1 541 471 6256
Fax: +1 541 471 6251
www.linxtechnologies.com