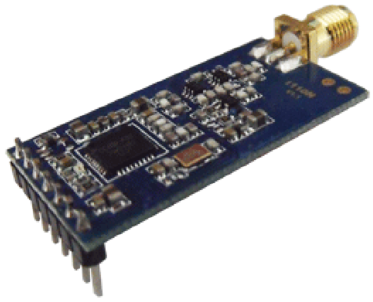
DRF1110N20

Advanced Wireless Mesh Network Modules V2.00

Features

- 433Mhz GFSK Transceiver
- 20dBm Max. output power
- Distributed mesh network
- 255 routing levels
- High data throughput
- Network notes plug and play
- Multiple Channels
- Adaptive data rate
- Six-byte MAC Address
- Configurable Network ID
- Versatile sleep mechanism
- Excellent anti-collision
- Multiple external devices
- Flexible configuration
- Supply voltage 2.1~3.6V



Applications

- Home automation
- Automatic meter reading
- Wireless data logger
- Wireless sensor network
- Intelligent agricultural
- Wireless industrial control

OVERVIEW

DRF1110N is a low-cost sub-1 GHz wireless distributed network module designed for operations in the MESH network applications such as AMR (Automatic Metering Reading), wireless sensor network,. The module has one main channel and 1~16 auxiliary channels which can be used for frequency hopping. The frequency and number of channels are all configurable. It communicates with external devices through standard UART interface with variable data format. Advanced Ad Hoc mesh network protocol is embedded into DRF1110N module

MNET III is the state-of-the-art distributed peer-to-peer mesh network protocol which takes full advantage of the network routing redundancy. The network features with self-healing ability, stability and high data throughput. It is a real drop-in network which no initialization is necessary and all network nodes are ready to work as soon as being powered-up. The network supports up to 255 routing levels and there is no limitation on the capacity of network which tens of thousands of nodes can be contained in large scale applications. The physical layer utilizes a lot of advanced wireless communication technologies such as frequency hopping, adaptive rate, secure and reliable wireless wake-up mechanism, interleaving error correction coding and so on. The intelligent collision avoidance algorithm used in the link layer has excellent anti-interference ability. The network provides three sleep modes: synchronous, asynchronous and hybrid modes, which provides high flexibility in battery-driven applications.

PIN FUNCTIONS

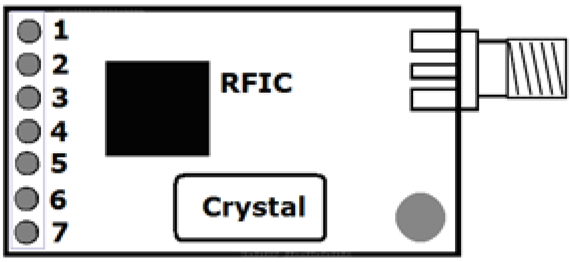


Figure 1: DRF1110N Pin Layout

PIN	Name	Function	Description
1	GND	Ground	Ground (0V)
2	VCC	Power	2.1~3.6V
3	Reset	Input	Low effective
4	RX	Input	UART input
5	TX	Output	UART output
6	ACT (1)	Output	External device evoking signal
7	SET (2)	In/Output	Mode selection/ data buffer free indication

Table 1: DRF1110N Pin Functions

Notes:

(1) The ACT pin can be used to wake up external devices. It can be enabled through configuration tool. In low power consumption applications, the external devices are usually in sleep status. When DRF1110N module needs to send data packet to external devices through UART interface, it will pull up the ACT pin first and then wait for the predefined time before sending data packet. After getting the correct response or timeout, the module will pull down ACT pin to inform external device that it can enter sleep mode again. If DRF1110N has more than one data package to send, the ACT pin will be kept in high till all data are sent. In this situation, the module will wait for the response from external device after each data packet is sent.

(2) The SET pin is acted as input pin while DRF1110N is powered on. If it is high, the module will work in normal mode; or else the module will be in configuration mode. After the module enters into normal mode, the SET pin will be used as output pin to indicate the status of UART receive buffer. The high level of it means the buffer is empty while low level means the buffer is full.

ELECTRICAL SPECIFICATIONS

Symbol	Parameter (condition)	Min.	Typ.	Max.	Units
VCC	Supply Voltage	2.1		3.6	V
Temp	Operating temperature range	-40	25	80	°C
RH	Operating relative humidity	10		90	%
Freq	Frequency range	430		436	MHz
Mod	Modulation type		GFSK		
RF_{IDD}	RF TX Peak current @20dBm, 3.6V @18dBm, 3V @15dBm, 2.1V		120 105 80		mA mA mA
SL_{IDD}	Sleep current		0.5		uA
Pout (1)	Output power @3.6V @3.3V @3.0V @2.5V @2.1V		20 19 18 17 15		dBm dBm dBm dBm dBm
Sen	Receiving sensitivity @1.2 kbps		-110		dBm
DR_{FSK} (2)	GFSK data rate	1.2		500	Kbps
DR_{IN} (3)	UART data rate	2.4		230.4	Kbps
CH_{BW}	Channel spacing		200		KHz
CH_M	Main channel number		1		
CH_A (4)	Auxiliary channel number	1		16	
T_{NET}	Networking time @ 200 nodes		20		Minutes
RL	Routing level			255	
N_{MAX}	Max. network nodes			1024	
Z_{ANT}	Antenna Impedance		50		

Table 2: DRF1110N Electrical Specifications

Notes:

(1) Configurable output power: 20dBm, 17dBm, 15dBm, 10dBm, 5dBm, 0dBm, -5dBm, -10dBm.

(2) GFSK data rate: 1.2k, 2.4k, 4.8k, 7.2k, 9.6k, 19.2k, 38.4k, 76.8k, 100k, 175k, 250k, 500kbps.

(3) UART data rate: 2.4k, 4.8k, 9.6k, 14.4k, 19.2k, 28.8k, 38.4k, 57.6k, 76.8k, 115.2k, 230.4kbps.

(4) Auxiliary channel number can be varied from 1 to 16, which is determined by applications.

ABSOLUTE MAXIMUM RATINGS

Symbol	Parameter	Min.	Max.	Units
Vcc	Supply voltage	-0.3	3.6	V
V_I	CMOS input voltage	-0.3	3.3	V

V_O	CMOS output voltage	-0.3	3.3	V
T_{ST}	Storage temperature	-55	125	°C

Table 3: DRF1110N Maximum Ratings

NETWORK FEATURES

MNET III is the state-of-the-art distributed peer-to-peer mobile Ad Hoc network protocol which is specially designed for low power and low cost wireless networking applications. There is no central node within the network and each node maintains its own routing information independently. It allows multiple concentrators or gateway equipments coexisting in one network. Comparing with centralized network, distributed network is more robust, more sensitive to the change of network topology, much faster network initialization, larger network capacity, higher data throughput and lower cost.

Num.	Feature	Description
1	Network topology	Point-to-point, point-to-multipoint, multipoint-to-multipoint, distributed peer-to-peer, Mobile Ad Hoc network
2	Initialization	0s, ready to work on power-up
3	Routing level	Up to 255 levels
4	Packet MTU	250 bytes (user packet payload)
5	Large network capacity	Supports more than tens of thousands of network nodes and supports up to 128-bit address length which is the same as IPV6. The address of external device can be directly used for routing which let users integrate the module into the existing equipment without any modification.
6	High throughput	Concurrent Mechanism in spatial domain, time domain and frequency domain
7	Drop-in network	All nodes are plug-and-play capable. New node can join the network immediately after being powered-up. No initializing is necessary for network when adding or deleting any node.
8	High reliability	Three-way handshake; intelligent collision avoidance; interleaving error correction coding, frequency hopping, adaptive RF baud rate; robust multi-path routing protocol
9	Self-healing	If any node is off network, the remaining nodes still work well. A private multi-path routing protocol is utilized to let nodes switch to new transmission path smoothly when necessary. Nodes are sensitive to the change of network topology and new path can be established before the current path fails so the network is very robust against the node failure, interference, topology change and so on.
10	Auto frequency offset correcting	Automatic frequency offset detection and correction
11	Wake-up mechanism	All sleeping node modules in network can be waken-up quickly and

		efficiently.
12	Data transmission	Two-way reliable transmission; supporting unicast, multicast and broadcast. To make sure all packets can reach its destination other mechanisms such as several attempts, collision avoiding and congestion control, etc. are used
13	Variable data packet	The data packet parameters such as sync word, frame length, address field offset and length, etc.
14	Adaptive rate	The best GFSK data rate can be achieved according to the link quality and times of delivery errors. With the adaptive GFSK data rate, the network can realize the best data throughput and longest transmission distance. Meanwhile the stability of network can also be improved.
15	Sleep mode	Synchronous, asynchronous and hybrid mode
16	Network ID	Three-byte length
17	MAC address	Six-byte length
18	External address	1~16 bytes (optional)
19	Variable external devices	0 (pure relay node), 1, multiple devices. A node module can be connected to 0 or multiple external devices through configuration tool. Without external device, the module works as a pure relay node in the network. When it connects one external device, the module will filter irrelated data according to MAC address or external device address. In the situation of connecting more than one external device, the module will forward all received data packet to external devices.

Table 4: DRF1110N Network Features

The MNET III network is an optimized solution for wireless meter reading, sensor network, intelligent agriculture, industrial controlling and so on. The main feature of these applications is that the network is composed by main node devices which are controlled by one or multiple root nodes (or concentrators). Bidirectional data exchanging between node modules or node module and concentrator module are required. Message can be relayed by node modules to expand the coverage area of network. The network topology is a multiple root tree with concentrators as roots. Data flow has two main directions: **uplink** and **downlink**. Downlink direction is from a concentrator to node modules and data transmission can be broadcasting, multicasting and unicasting. Uplink direction is from node modules to a concentrator and only unicasting is available.

A mobile ad hoc network (MNET III) is consisted of mobile node devices connected by wireless links. Each device in MNET network is free to move independently in any direction, and therefore links to other devices will be changed frequently. The main feature of MNET III is to let each node obtain the proper routing information continuously. Such a network can operate by itself independently or might be connected to the larger internet. The topology of network is keep refreshing and routing life circle is very short. Comparing to traditional networks, MNET III network has its unique features:

1. Distributed routing algorithm which is suitable for distributed Ad Hoc network
2. Higher adaptive ability which allows changing networking rapidly.
3. Loop-free routing is a basic requirement for any routing protocol which can avoid routing errors and bandwidth wasting.
4. The less cost of routing calculation and better maintenance.
5. Support very large scale network
6. Robust and easy expansion.

Single routing protocols such as AVOD is not suitable for MNET III because:

1. The topology of the MNET III changes very quickly and the wireless bandwidth is very limited. The life circle of a single routing path is short, which is likely to be broken frequently. The cost for recovering and maintaining a single routing path is very high and the speed of routing convergence is very slow.
2. Routing path is commonly established by flooding technique. The recovery of a broken routing path still needs to use flooding technique which occupies a lot of bandwidth. In a large scale network there are many routing paths needing to maintain which makes the network nearly impossible to work.
3. Single routing path algorithm does not consider fairness. It is inclined to assign all data messages to a single shortest routing path between the source and the destination node. The load of the nodes on the path is very heavy while other nodes off the path are idle.
4. It is difficult for routing path algorithm to obtain the topology information and trace the topology changing of the whole network. It can not change the path between two nodes smoothly till the path is broken and the delay of packet delivery might be very serious.
5. Data transfer in single path routing protocol only uses one path so it can not send data in parallel which results in low transmission speed, long delay, uneven network load and serious traffic jam.

Usually there are more than one path between source node and destination node in MNET III network. Using multi-path routing protocol can overcome the shortage of single path routing protocol and take full advantage of network resources, balance the network load, increase data throughput and avoid network instability. MNET III adopts requirement-on-demand lightweight dynamic multi-path routing protocol which is specially designed for mobile network with strict hardware resources and which is very sensitive to the change of network topology. It reduces the cost of establishing and maintaining of routing paths to the maximum extent. Data packets can be sent in parallel multiple paths and new paths can be established before current path fails. Data flow can switch seamlessly among different routes. The features of the routing protocol are listed as below:

1. Each node maintains its own routing information independently.
2. Routing is quick, stable and loop-free
3. Routing maintenance and updating take full use of the redundancy of wireless signal and there is no additional cost.

4. Many factors such as distance, signal energy, link quality and battery voltage, etc. are taken into consideration in selecting routing path.
5. Sensitive to the change of network topology structure and optimal routing paths can be updated dynamically.
6. High network throughput and data messages can be sent in different paths in parallel.

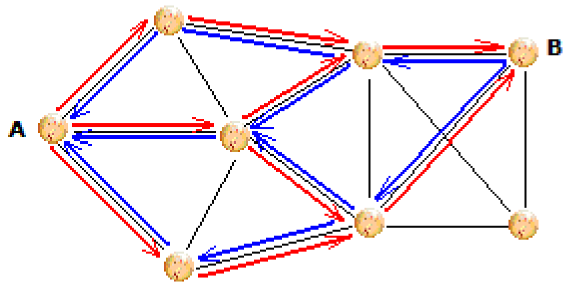


Figure 5: MNET III Multi-path Routing

The figure above shows the routing paths established between Node A and Node B. Red lines are the paths from A to B and blue lines are the reverse directions. Routing is established through flooding first on demand. There is no loop among multiple paths but crossing among paths is allowed. Every node chooses as many as possible nodes as its next hopping. Data packet can be dynamically switched to any possible path and can be sent through multiple paths in parallel. Routing information is exchanged within the handshaking messages between adjacent nodes. A node also can perceive the failed path, discover a potential new routing path and track the change of the network topology from these messages. There is no need to apply flooding mechanism to maintain routing tables. All nodes including the source node only need to find their next hopping/relaying node without confirming the whole path so it is suitable for rapidly changing topology of mobile network which can quickly find the best routing in real-time.

MNET III routing protocol adopt versatile routing algorithm to calculate the best routing path by analyzing distance vector, signal quality, link status and the remaining power of battery (which is similar to Min-Max Battery Cost Routing). Each node maintains a vector table listing the shortest way to the known target node. The nearest node will be selected as the next hopping/relaying. However, the shortest path does not mean the best route to the target node because the environment of network is very complicated.

Different from wired networks, wireless links in MNET are very easily affected by interferences from other nodes or external devices and the network topology is keeping changing so the survival cycle of a link is very short. Sometimes the optimal route is not the shortest way. The picture below shows the link-status routing algorithm used in MNET III. Node A can send messages to node C through node B. Anyway the path A-B-C is not stable because of interference. However, there is another path A-D-E-C which is stable; therefore this path will be chosen as the optimal link.

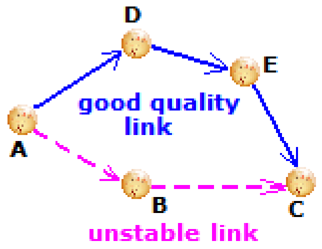


Figure 6: Stable Link in Optimizing Routing Path

The routing algorithm also takes battery voltage as reference to calculate the routing path. Nodes with higher battery voltage are more likely chosen as relay nodes by using some mechanisms similar to MMBCR algorithm (Min-Max Battery Cost Routing). The path A-D-E-C will be chosen as the best link between node A and node C because of higher battery voltage.

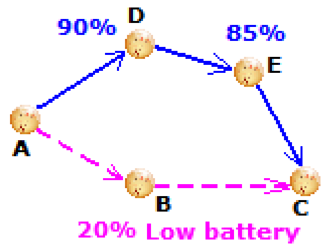


Figure 7: Battery Voltage in Optimizing Routing Path

CONNECTION DIAGRAM

The MNET 1110x network modules include: node module (DRF1110N20N) and root module or concentrator module (DRF1110N20C). Both node module and concentrator module use the same hardware and only are distinguished by software. Below is the connection diagram between DRF1110N module and external device.

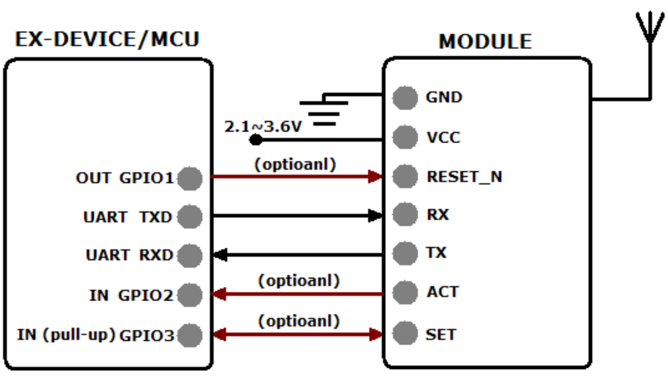


Figure 8: DRF1110N Connection Diagram

RX pin and TX pin must be connected. Other pins such as RESET_N, ACT, SET pin are all optional and can be left unconnected. The input pins RESET_N and RX only have weak pull-up inside the RFIC and there is no pull-up resistors outside in order to reduce power consumption. In sleep mode the output pins TX, ACT and SET are all pulled down.

RESET_N is the reset pin of DRF1110N module and is low effective. The reset pulse should be longer than 250ns (seeing the figure below).

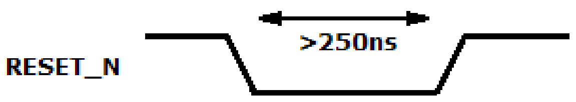


Figure 9: DRF1110N Reset Pulse

ACT is an optional pin which can be used to wake up external device and it is high effective. The sequence diagram of the ACT, TX and RX pins is showed as below. The "TX delay" and "response timeout" can be configured as necessary. The ACT pin is set to high before sending data to external device and set to low after receiving the response or timeout. External device can take use of the rising edge of ACT signal as wake-up signal and the falling edge as sleep signal.

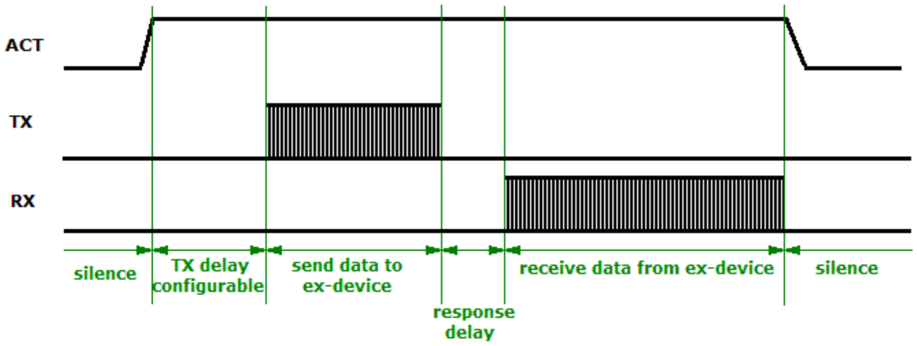


Figure 10: Two-way Communication of ACT, TX and RX Pins

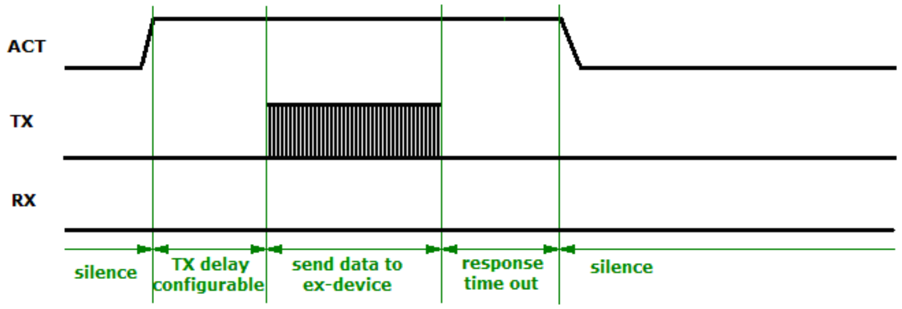


Figure 11: One-way Communication of ACT, TX and RX Pins

The SET pin has weak pull-up inside the RFIC and it is acted as input pin while module powering-on or resetting so DRF1110N module can use the feature to judge in which mode it will work. If level is high, the module will enter into normal working mode; otherwise sleep mode. In normal working mode, the SET pin is used as output pin to indicate the status of receive buffer of DRF1110N module. When the SET pin is high it means the buffer is empty, otherwise busy. The DRF1110N module will pull it up when it receives a full data packet from UART interface successfully. The external device can detect the status of SET pin to judge if the data packet is received correctly. Anyway it is used as auxiliary way to judge and more standard approach is to use the ACK packet as handshake to obtain more reliable communication. Please check related sections for details.

FUNCTION VERIFICATION

The network function of DRF1110N modules can be easily verified by shorting RX and TX pins or connecting them to computer. The verification can be done without changing default settings. The default application protocol is a half transparent transmission with MAC address for data forwarding. Any characters received by the UART port of node modules will be regarded as data payload. The boundary of data payload is determined by the interval between two continuous characters. If the interval is longer than 100ms, it is considered as the boundary of two payloads. One-byte start synchronization identification and six-byte source module MAC address are automatically added into the head of data payload to compose an integrate frame when sending data in uplink direction. When a node module receives data from the concentrator (or root module), it will remove the start synchronization byte and six-byte MAC address automatically and then transfer data to external device through UART interface. From the viewpoint of node module, the transmission is fully transparent.

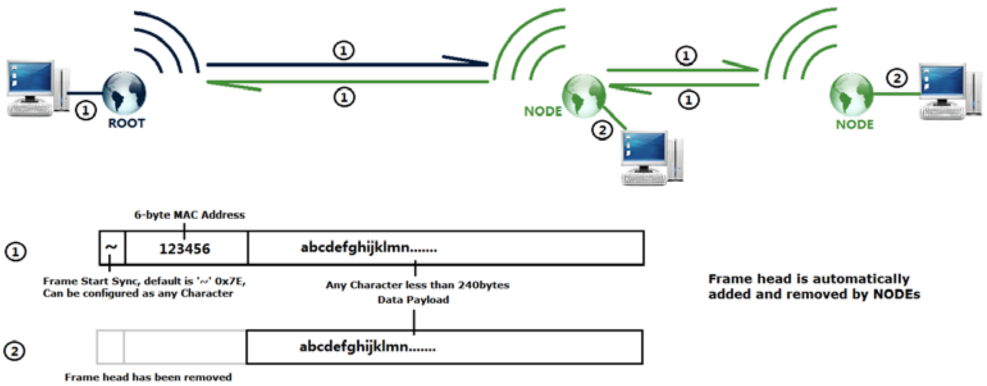


Figure 12: Frame Structure of Half Transparent Transmission

The default frame start synchronization byte is '~' which corresponding value in hexadecimal is 0x7e. 'F' and 'f' are wildcards of broadcasting or multicasting address. The interval time of any two continuous characters should be less than 100ms; otherwise it will be regarded as the end of a data payload. For example:

1. **Broadcast downlink**
   The external device sends "~FFFFFFabcdefg" to the root module. The destination MAC address is 'FFFFFF' which is the broadcasting address and 'abcdefg' is the data payload and '~' is the frame synchronization byte. All nodes will receive this packet. After removing the head "~FFFFFF" automatically, the node module then will transfer the data payload 'abcdefg' to external device through UART interface.
2. **Unicast downlink**
   The external device sends "~000001xyz" to the root module through UART interface. The destination MAC address is '000001' which is a specified address of a node module. 'xyz' is the data payload and '~' is the frame synchronization byte. Only the node module with MAC address '000001' will receive it and transfer the data payload 'xyz' to external device after removing the head '~000001'.
3. **Multicast downlink**
   The external device sends "~00000F12345" to the root module through UART interface. The destination MAC address is ‘00000F'which is a multicasting address. '12345'is the data payload and '~' is the frame synchronization byte. Nodes with MAC address '00000x' will receive it, which 'x' refers to any legal character.
4. **Unicast uplink**
   The external device sends "abcdefg" to the node module with MAC address '123456' through UART interface. The node module will combine '~123456' into data packet as frame head. The nearest root module is the default destination address of an uplink packet.

Because the MAC address is automatically added as the frame head, it is easy for a root module to distinguish the original node even if the data payload of different node modules is the same. The destination address of uplink packets is omitted since the nearest root module is the default destination and the source address of downlink is also omitted because the data packet is always sent from a root module. If there are more than one root modules coexisting in one network, the node modules will send the data packet to the nearest root module so data flow can be in parallel. Node modules send data synchronously without considering the collision of packets because collision avoidance algorithm ensures all packets can be sent to the root module accurately and reliably.

Loop-back Test: Data packet loop-back at the UART port of node modules can be used to verify the basic network function. The loop-back test does not need to connect node modules to any external device or computer. It is very easy to carry out and verify the functions below:

1. Zero network initialization, routing stability, self-healing, reliability of data transmission.
2. Broadcasting, multicasting and unicasting of downlink data.
3. Simulating the process of network data acquisition.
4. Data transmission on multi-path in parallel in a network with multiple root modules.

Operation steps:

1. Connect root module(s) to PC COM port with UART-to-USB converter board DAC04.

2. Open the COM port by using serial port tools such as 'SecureCRT' on computer with data format (baud rate: 115200 bps, 8-bit data, 1 stop bit, no parity bit and no flow control).
3. Short the RX and TX pins of node modules.
4. Power on node modules with batteries and put them in a reasonable range.

The root module will automatically broadcast the data frame "~FFFFFFRDD\r" to the network and receive loop-back frames from node modules periodically with the interval of 2s. Node modules remove the frame head '~FFFFF' and transfer the data payload 'RDD\r' to UART interface. Because RX and TX pins are shorted, the payload 'RDD\r' from the UART port. Frame head '~xxxxxx' is added to the data payload by node modules automatically. Among which '~' is the frame start synchronization byte and 'xxxxxx' is the MAC address of node module. If there are five nodes in the network with MAC addresses '000001', '000002', '000003', '000004', '000006' respectively. The serial port tool on the computer connecting root module will periodically print out the data below:

"~000001RDD\r"
"~000002RDD\r"
"~000003RDD\r"
"~000004RDD\r"
"~000005RDD\r"

Notes:

1. The order of node data printed by serial port tool is not fixed.
2. The interval of data acquisition of root module can be changed through AT command.
3. The routing stability, self-healing and reliability of the network can be verified by changing the position of node modules.
4. Parallel data transmission can be tested by adding more root modules.

The content of data payload can be changed by sending a new frame to root module through computer or external device. If the new frame is recognized by root module correctly, an ACK packet '~OK\r" will be printed as confirmation. Please note that the interval between two continuous characters can not be longer than 100ms. For example:

Active Uplink Test: The loopback test can verify the typical functions of an AMR network. During the whole testing, data transmission is originated from the root module and note modules only respond to root module with loopback frames. The active uplink test will simulate the process which data transmission is issued by node modules.

1. Node modules trigger on data transmission in uplink actively.
2. The capability of two-way communication
3. The data throughput and transmission delay of the network.

Operation steps:

1. Connect node and root modules to PC serial port with UART-to-USB converter board

DAC04.

2. Open the serial port tool like "SecureCRT" on computer with data format (baud rate: 115200 bps, 8-bit data, 1 stop bit, no parity bit and no flow control).
3. Send AT command "ATCO\r" to root module to disable repeat packet sending.
4. Send data payload to node modules arbitrarily and monitor the output of root module.
5. Send data frame to root module to monitor the simultaneous data flow of uplink and downlink.

PARAMETERS CONFIGURATION

The DRF1110N module can be configured by several ways. The simplest way is to connect module to PC through UART-to-USB converter board DAC04. After installing USB driver of DAC04 board, the virtual COM device should appear when inserting the configuration board. Users can run the configuration tool as administrator in Windows Vista/7. If users don't know which port the USB board uses, users can choose the correct serial port which can be found in the device manager.

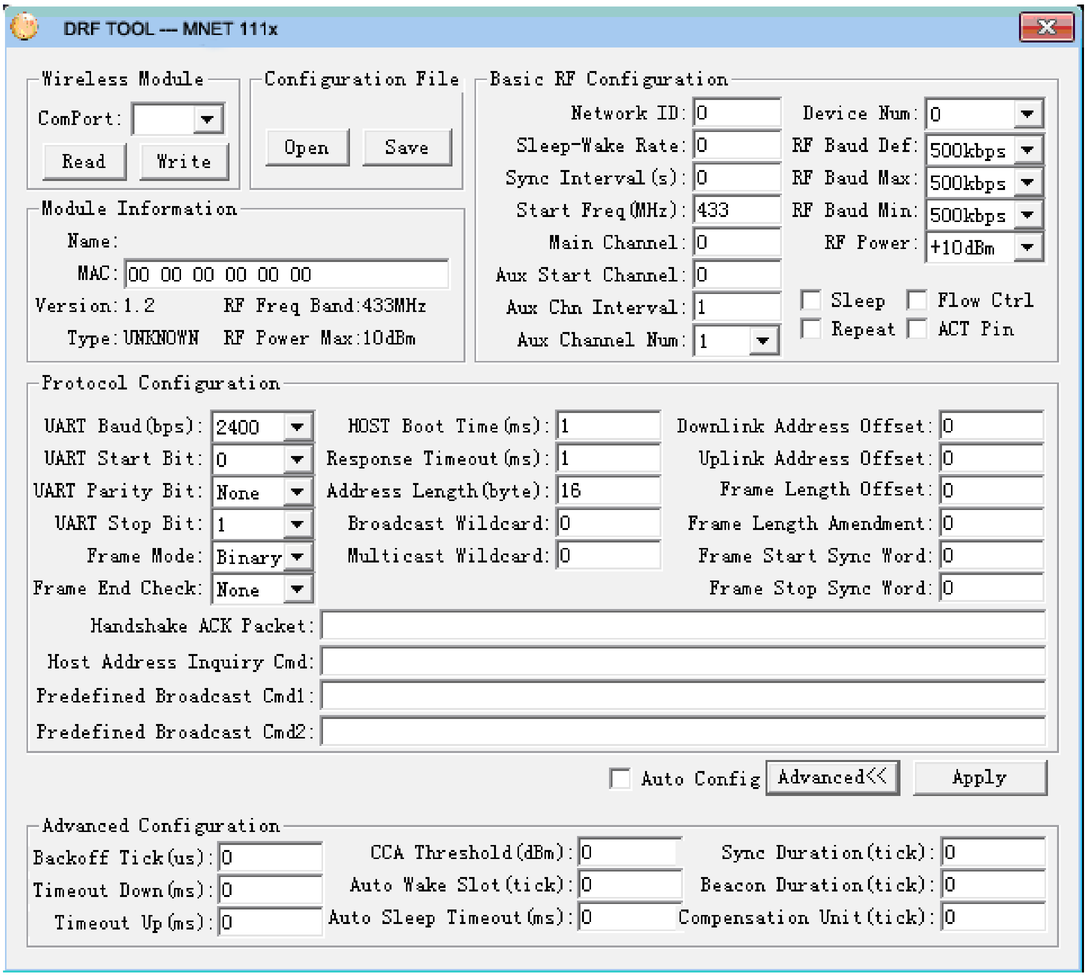
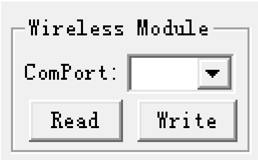


Figure 13: Configuration Tool Interface

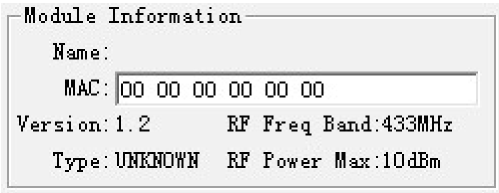
The configuration tool is consisted of several function blocks which are outlined with boarders. The following content will give detailed description on the functions of each block.

1. WIRELESS MODULE



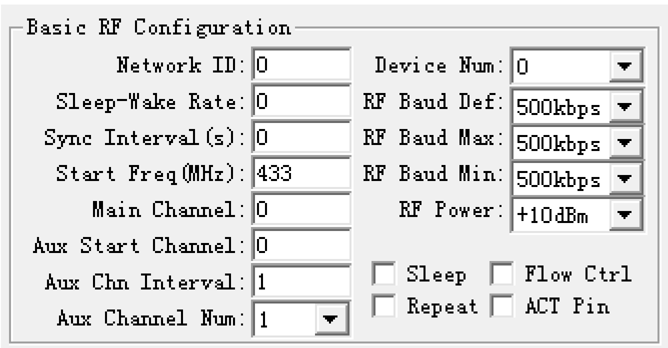
The first thing that users need to do is to choose the right COM port from the selection menu after running the configuration tool. The configuration tool can detect the insertion/removal of converter board from the USB port and gives corresponding messages. Users can use "Read" and "Write" button to read/write related parameters.

2. MODULE INFORMATION



The basic information of module will be displayed in this area after the module is detected by configuration tool successfully. Users can get data such as MAC address, RF frequency band, Output power and which type of module (root or node).

3. BASIC RF CONFIGURATION



Parameters related to RF and network parameters such as network ID, sleep mode, RF channels, RF frequency, external devices, flow control, etc. will be explained item by item.

Network ID: It is used to distinguish different networks. The three-byte ID can be set from 0 to 65535. It allows multiple networks coexisting in the same area and frequency with different network ID. The probability of network ID conflict is about 0.0015% without any plan and it even can be reduced by configuring networks working on different frequency channels.

Sleep-Wake Rate: When a DRF5150N is enabled asynchronous sleep function, it will wake up at preset intervals to monitor the wireless network signal. The module will enter into normal operation mode automatically as soon as it detects there is any data packet needing to be sent. This parameter refers to the ratio of "sleep time slice" and "listening time slice" which is depicted in the picture below:

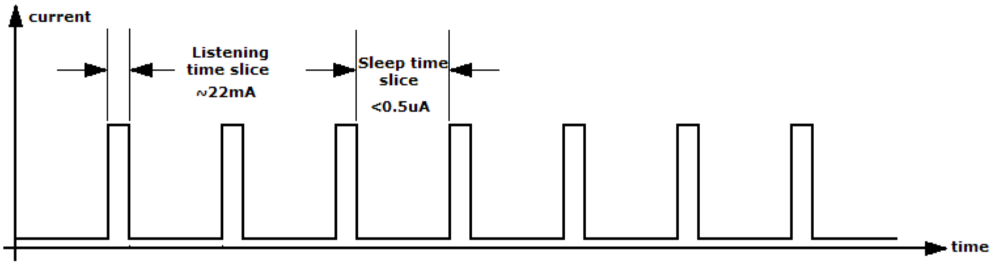


Figure 14: Sleep-Wake Ratio

This parameter ranges from 0 to 2500. The receive current of module is 22mA and sleep current is 0.5uA. The average usage current of module will vary between 9.3uA and 22mA. Usually the average current is more concerned than sleep current in actual applications. If this parameter is set too large, the smaller average current will be achieved but it will takes more time for modules to wake up and deliver data packets which also consumes more energy so this parameter needs to be considered carefully according to the actual network application in order to achieve the lowest power consumption.

Notes:

1. "Sleep-Wake Rate" is a parameter for asynchronous sleep mode and it has no relation with synchronous sleep mode.
2. Even if this parameter is set to a non-zero value, it still needs to activate the "**sleep**" option to enable the asynchronous sleep. In the application which non-sleep modules and sleep modules coexist in the same network this parameter for non-sleep modules still need to be set the same as sleep modules in order to ensure the stability of data delivery.

Sync Interval: It is the abbreviation of synchronous sleep interval time which refers to the "sleep time slice" of synchronous sleep mode. The parameter can be configured by AT command and the parameter set here is the initial value on powering-on. In synchronous sleep mode, the "sleep time slice" of adjacent nodes is strictly synchronized and the inaccuracy among them is less than 1ms. The "sleep time slice" is synchronized by broadcasting sleep packets at the end of each "work time slice" to the whole network. Synchronous sleep packets contain the length of the following "sleep time slice". These packets are sent by the root module automatically when the uplink is in silence for a threshold time. If there is no data transmission in a "work time slice", the synchronous sleep packets are also sent periodically.

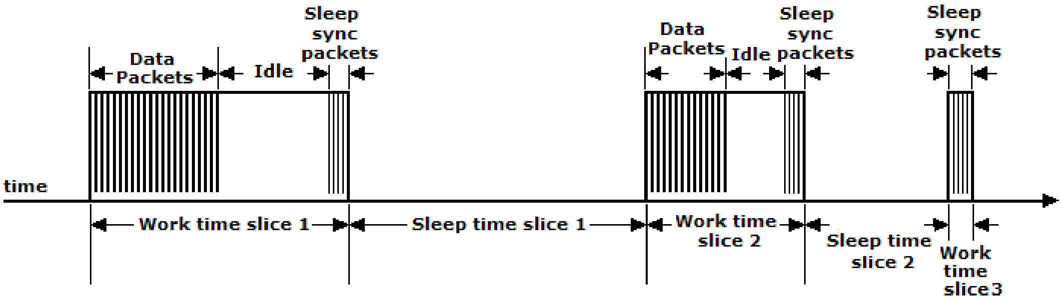


Figure 15: Synchronous Sleep Interval

Notes:

1. "Sync interval" is a parameter of synchronous sleep mode. If this parameter is not set to zero, the synchronous sleep mode is always enabled.
2. The synchronous and asynchronous sleep modes can be enabled simultaneously, which is the hybrid sleep mode.
3. The parameter is only effective for root modules and is ignored by node modules.
4. For node modules, sleep mode will still be activated when receiving synchronous sleep packets from root module even though the "**sleep**" checkbox is not selected.
5. For root module, the "**sleep**" checkbox should be selected to enable sleep during the "synchronous sleep time slice".
6. If there is more than one root module in a network, only one root module needs to be set with this parameter. If different parameters are set to root modules in the same network, the behavior of synchronous sleep is unpredictable.

Sleep: For asynchronous sleep mode, this checkbox must be selected even if the parameter "Sleep-Wake Rate" is non-zero. For synchronous sleep mode, it must be enabled for root modules but for node modules they are forced into sleep mode even if it is not checked.

Flow Control: The baud rate of RF and UART might be mismatched. If the baud rate of RF is faster than double of UART baud rate, flow control checkbox needs to be selected in order to obtain the integrity of data packets because the RF FEC coding rate is 1/2. It is strongly recommended to disable this function if flow control is not necessary because the network throughput will be reduced.

Repeat: It is the abbreviation of repeat data acquisition. For sensor networks or other periodical data acquisition applications, it needs to broadcast data acquisition command repeatedly among the network. In such applications the "repeat" checkbox should be selected and the root module will do data acquisition repeatedly with intervals set in "**Sync interval**". It can be controlled through AT command.

ACT Pin: This option is used to enable/disable the ACT pin function. ACT pin can be used to wake up external devices.

Device Num: It refers to the number of external devices. A node module can be equipped with 0, 1 or more external devices. If a node module is used as a pure relay node, this parameter must be set to "0" and the node module will turn off the UART port. If a node module need to manage more than one external devices such as 465 or MBUS, this parameter can be set to ">=2" to disable address filtering function for data packets. If only one external device is needed, this parameter should be set to "1" to enable the address filtering function and receive the correct data packets.

RF Baud Rate: It is consisted of three drop-down selections: RF Baud Def, RF baud Max and RF baud Min which refer to the default and the adaptive range of RF baud rate. DRF1110N module supports 12 types of RF baud rate. "RF baud Def" refers to the default RF baud rate used by the handshake packets. "RF Baud Max" and "RF Baud Min define the range of adaptive RF baud rates used in data transmission. MNET III protocol can calculate the most suitable RF baud rate for current data transmission according to the quality of wireless link and packet error times. With the adaptive baud rate algorithm, the network can make the balance between stability and throughput.

The RF baud rate should be set according to the requirement of local wireless policy. In low-power applications, the “RF baud Def" is very critical to achieve low average current and short delay time of wake-up. It is recommended to set the "RF Baud Max" the same as the "RF Baud Def".

RF Power: Users can choose appropriate output power according to application. The default setting is the Max. output power +10dBm.

RF Channels: MNET III protocol supports one main channel and 1~16 auxiliary channels. It is recommended to set different main channel frequency for adjacent networks. The channel space is fixed to 200KHz. The "Start Freq" refers to the frequency of channel 0. "Main CH Start Num" means the frequency of main channel starts from this number of channel.
Main channel frequency= "Start Freq" + "Main CH Start Num" * 200 KHz

"Aux CH Start Num" means the first auxiliary channel should start from which number of channel. "Aux CH Interval" refers to the space between two adjacent auxiliary channels. " Aux CH Num" tells how many auxiliary channels will be use and it can be 1, 2, 4, 8 and 16. The frequency of auxiliary channel N can be calculated as below:
Freq="Start Freq" + ["Aux CH start num"+ (N * "Aux CH Interval")]

For example, if the "Start Freq" is 431.4MHz; "Main CH Start Num" is 0; "Aux CH Start Num" is 10; "Aux CH Interval" is 5 and "AUX CH Num" is 4. The frequencies of main channel and each auxiliary channel can be calculated as below:

The main channel: [431.4MHz+ (0 * 200KHz)] = 431.4MHz
The auxiliary channel 0: {431.4MHz+ [10 + (0*5)]* 200 KHz} = 433.4MHz
The auxiliary channel 1: {431.4MHz+ [10 + (1*5)]* 200 KHz} = 434.4MHz
The auxiliary channel 2: {431.4MHz+ [10 + (2*5)]* 200 KHz} = 435.4MHz
The auxiliary channel 3: {431.4MHz+ [10 + (3*5)]* 200 KHz} = 436.4MHz

Notes:

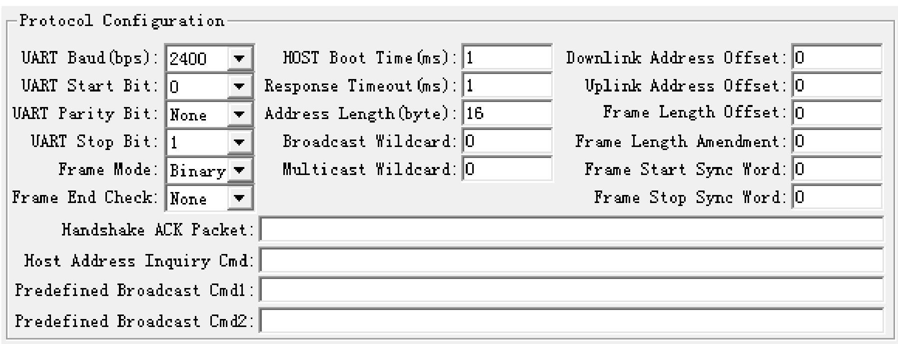
1. In order to avoid adjacent channel interference, the frequency space between any two channels should be wider than or equal to the Min. bandwidth listed in the table below:

RF Rate (bps)	Min.Bandwidth (Hz)	Channels
500K	2M	10
250K	1M	5
175K	600K	3
100K	400K	2
76.8K	400K	2
38.4K	200K	1
19.2K	200K	1
9.6K	200K	1
7.2K	200K	1
4.8K	200K	1
2.4K	200K	1
1.2K	200K	1

Table 5: RF Rate Vs Bandwidth

2. The channel number of the main channel can not be the same as any auxiliary channel.
3. The main channel can be non-zero and the channel number can not be larger than 255.

4. UPPER-LAYER PROTOCOL CONFIGURATION



This area includes the parameters related to UART data format, Frame format, Handshake protocol, predefined commands and so on.

UART Data Format: It includes four drop-down selections: "UART Baud (bps)", "UART Start Bit", "UART Parity Bit" and "UART Stop Bit". Users can use the default parameters or change them according to specific application. Please note that the UART does not support flow control.

HOST Boot Time: HOST here means the external device connected to the module. The "HOST Boot Time" is the initialization time of external device. The value range of this parameter is from 1 to 65535ms and this parameter has two usages:

1. The initialization time of external device from being powered-on to normal work
2. If the ACT pin function is enabled, this parameter can be used as the wake-up delay for modules before sending data packets to external device.

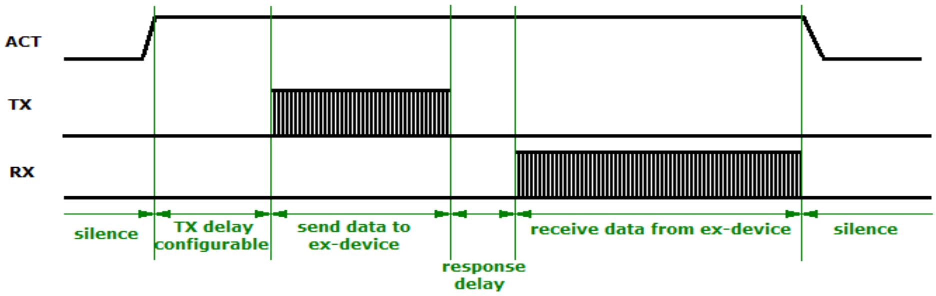


Figure 16: Time Sequence for TX Delay

Response Timeout: After sending a data packet to external device, the module will wait for the response from external device. It is used to define the waiting time for the module before it gives up. "Timeout" has two meanings:

1. The timeout of the response from external device
2. The maximum interval time between two successive characters of a data packet.

Please note that the parameter should be configured with the maximum timeout value of the twos above.

Address Offset: Modules need to analyze address information from upper-layer frame defined by customers for routing and data forwarding. For uplink the source address needs to be analyzed for routing; for downlink the destination address should be used for data forwarding. As to MNET III downlink refers the direction from root to node; vice versa is uplink direction. The "Downlink Address Offset" is the byte offset of the first character of destination address to the start of a downlink frame and the "Uplink Address Offset" is the byte offset of the first character of source address to the start of an uplink frame. Please note that the value range of the two parameters is 0 ~255, among which 255 indicates this parameter is not valid and the address field of a frame should not be analyzed.

Address Length: This parameter can be varied from 1 to 16 bytes and it specifies the actual address field length of the upper-layer frame.

Address Wildcard: Broadcast and multicast address wildcards can be used for broadcasting and multicasting. The wildcards of them can be configured respectively. When a node module receives a downlink packet, it will compare the address field with its own address. The wildcard bytes are omitted when address filtering is activated. Please note that the value of this parameter is decimal.

Frame Structure: Two frame parser modes are defined by MNET III protocol: ASCII mode and Binary Mode. The ASCII mode does not require all characters within the frame are ASCII codes. If the data packet doesn’t contain the character defined the same in the frame start and stop sync words, ASCII parser mode can be used. For Binary parser mode, the frame length field can be activated so the frame length can be known. The "Frame Start Sync Word" and "Frame Stop Sync Word" can be enabled separately to judge the frame boundary. If the frame sync word detection is disabled, interval time of two continuous characters will be used to judge the frame boundary.

Note:

1. The length of frame start and stop sync word is only one byte.
2. The value range of "Frame Length Offset" and "Frame Length Amendment" is 0 ~255, which 255 indicates this parameter is not valid and the frame length filed is not parsed.
3. If the frame sync word detection is disabled, the frame transmission mode is equivalent to transparent transmission.
4. The value configured here is decimal.

In "ASCII Frame Mode", frame boundaries are determined by the "Frame Start Sync Word" and "Frame Stop Sync Word". The frame length field is nor parsed so the parameters "Frame Length offset" and "Frame Length Amendment" are not used in this mode. "Frame Start Sync word" and "Frame Stop Sync Word" can be set to the same value. The frame start and stop sync word detection can be enabled or disabled separately. The frame boundary detection is depicted as below:

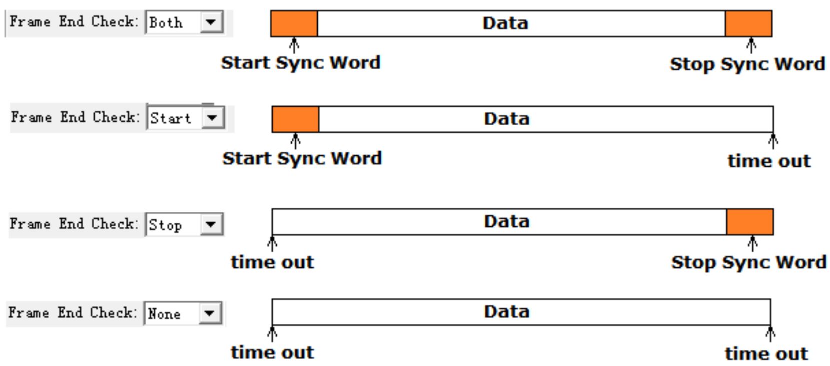


Figure 17: Synchronization Words in ASCII Frame Mode.

For example: A type of temperature and humidity sensor uses the "{" and "\r" characters as frame start and stop sync words correspondingly. The ASCII character '~' is the wildcard. The content of data payload never contains the two characters. The frame structure is showed in the table below:

Sensor Data Frame Structure		
Frame Start Sync Word	'{'	1 byte
Address Field	A0 ~ A5	6 bytes, '0' ~ '9'
Data Payload	DATA	Flexible length, ASCII Characters
Checksum	CS	1 byte
Frame Stop Sync Word	'\r'	1 byte

Table 6: Frame Structure of Sensor Data Packet

ASCII frame mode is very suitable for such a frame structure and the configuration of corresponding parameters is showed in the following table:

Parameter	Value	Comments
Frame Mode	ASCII	ASCII parser mode is used
Frame End Check	Both	Both start and stop sync word are checked
Frame Length Offset	N/A	This parameter is ignored at ASCII mode
Frame Length Amendment	N/A	This parameter is ignored at ASCII mode
Frame Start Sync Word	123	The start frame sign character - '{'
Frame Stop Sync Word	13	The stop frame sign character – '\r'
Address Length	6	The length of address field
Broadcast Wildcard	126	The address wildcard character '~'
Multicast Wildcard	126	The address wildcard character '~'
Downlink Address Offset	1	Bytes before " Address Field"
Uplink Address Offset	1	Bytes before " Address Field"

Table 7: Parameters Configuration in Sensor Data Packet

In "Binary Frame Mode" the frame length can be used to determine the boundary of a frame so the boundary checking is more flexible and rigorous than ASCII mode. According to the variation of frame length, the frame structures can be divided into: Fixed Frame Length, Variable Frame Length and Transparent Transmission in this mode.

Fixed Frame Length:

The length of frames is fixed so the length information is not necessary to be contained in the frame payload. The frame sync word checking is optional but this function is highly recommended to be enabled in applications. The parameter configuration is described as below:

1. "Frame Mode": Binary
2. "Frame End Check": Select the appropriate mode according the requirement. Transparent transmission can be achieved by choosing 'None' of this parameter.
3. "Frame Length Offset": 255, this parameter is ignored.
4. "Frame Length Amendment": the fixed frame length setting.
5. "Frame Start Sync Word": the first character of a frame (optional)
6. "Frame Stop Sync Word": the last character of a frame (optional)

For fixed frame length in binary mode the frame boundary detection is showed as below:

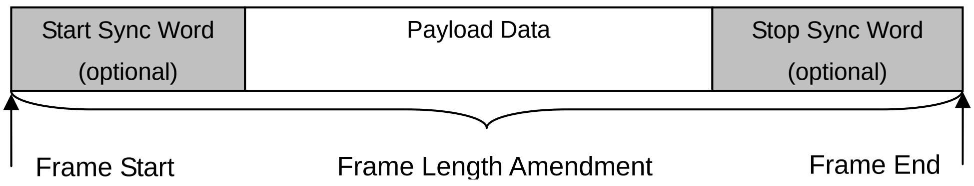


Figure 18: Fixed Frame Length in Binary Mode

For example: A mode of smart gas meter uses 44-byte fixed length packet and 0xEE as address wildcard. The frame structure of this application is showed in the table below:

Gas Meter Frame Structure		
Frame Start Sync Word	0x68	1 byte
Control Field	C	1 byte
Address Field	A0 ~ A4	5 bytes
Data Payload	DATA	35 bytes
Checksum	CS	1 byte
Frame Stop Sync Word	0x16	1 byte

Table 8: Fixed Frame Length in Gas Meter

Parameter	Value	Explanation
Frame Mode	Binary	Binary parser mode is used
Frame End Check	Both	Both start and stop sync word are checked
Frame Length Offset	255	Indicating this parameter is ignored
Frame Length Amendment	44	The fixed frame length
Frame Start Sync Word	104	The start frame sign character – 0x68
Frame Stop Sync Word	22	The stop frame sign character – 0x16
Address Length	5	The length of address field
Broadcast Wildcard	238	The address wildcard character - 0xEE
Multicast Wildcard	238	The address wildcard character - 0xEE
Downlink Address Offset	2	Bytes before " Address Field"

Uplink Address Offset	2	Bytes before " Address Field"

Table 9: Parameters Configuration in Gas Meter

Variable Frame Length:

The length of frames is not fixed but the length information can be obtained from frame payload. The frame sync word checking is optional but this function is highly recommended to be enabled in applications. The parameter configuration is described as below:

1. "Frame Mode": Binary.
2. "Frame End Check": Select the appropriate mode according the requirement. Transparent transmission can be selected by choosing "None" of this parameter
3. "Frame Length Offset": Offset from length byte to the first byte of frame.
4. "Frame Length Amendment": It is the value which the total length of the frame subtracts the value of length byte.
5. "Frame Start Sync Word": The first character of a frame (optional)
6. "Frame Stop Sync Word": The last character of a frame (optional)

For fixed frame length in binary mode the frame boundary detection is showed as below:

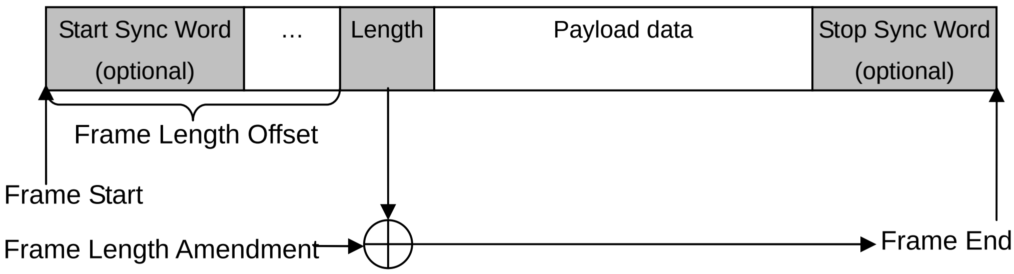


Figure 19: Variable Frame Length in Binary Mode

For example: The frame structure of smart electrometer DL/T645 protocol is showed in the table below.

The Frame Structure of DL/T645 Protocol		
Frame Start Sync Word	0x68	1 byte
Address Field	A0 ~ A5	6 bytes
Payload Start Sync Word	0x68	1 byte
Payload Control Field	C	1 byte
Payload Data Length	L	1 byte
Payload Data	DATA	L bytes
Payload Checksum	CS	1 byte
Frame Stop Sync Word	0x16	1 byte

Table 10: Variable Frame Length in DL/T645 Protocol

The 0x99 is the broadcast address wildcard and 0xAA is the multicast address wildcard. Parameters for this application can be configured as below:

Parameter	Value	Explanation
Frame Mode	Binary	Binary parser mode is used
Frame End Check	Both	Both start and stop sync word are checked
Frame Length Offset	9	Bytes before “Payload Data Length”
Frame Length Amendment	12	Bytes except “Payload Data”
Frame Start Sync Word	104	The start frame sign character – 0x68
Frame Stop Sync Word	22	The stop frame sign character – 0x16
Address Length	6	The length of address field
Broadcast Wildcard	153	The address wildcard character - 0x99
Multicast Wildcard	170	The address wildcard character - 0xAA
Downlink Address Offset	1	Bytes before “ Address Field”
Uplink Address Offset	1	Bytes before “ Address Field”

Table 11: Parameters Configuration in DL/T645 Application

Transparent Transmission:

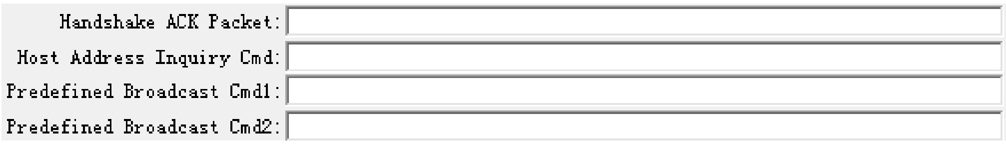
It takes upper-layer payload as opaque data and wraps it into packet directly without parsing any information. The transparent transmission can be used for carrying any upper-layer frame structure. However, it is no recommended if ASCII or Binary Mode can be used. The frame boundary is determined by the interval time between two continuous characters. It is recommended disabling the payload address field parser since the frame boundary is imprecise. If the address information can not be picked up from the frame, broadcasting is the only way for downlink in order to ensure each node can receive every downlink packet.

Parameter	Value	Comments
Frame Mode	Bin/ASCII	Either binary or ASCII parser mode is OK
Frame End Check	None	Both start and stop sync word are not checked
Frame Length Offset	255	Indicating this parameter is ignored
Frame Length Amendment	255	Indicating this parameter is ignored
Frame Start Sync Word	N/A	It is not used
Frame Stop Sync Word	N/A	It is not used
Address Length	N/A	It is not used if address field parser is disabled
Broadcast Wildcard	N/A	It is not used
Multicast Wildcard	N/A	It is not used

Downlink Address Offset	255	Recommended to disable it by setting it to 255
Uplink Address Offset	255	Recommended to disable it by setting it to 255

Table 12: Parameters Configuration in Transparent Transmission

Predefined Command Packets: Users can configure predefined command packets fro special purposes. Packet value should be configured in hexadecimal text format. Each original text byte should be converted to a two-byte hexadecimal ASCII characters. A space can be added into hexadecimal characters for separation. Parameters are described in details below:



"Handshake ACK Packet"

It is used as confirmation message to tell the external device that DRF1110N module has received a frame from UART. The maximum length of the "Handshake ACK Packet" is 48 bytes. There is no restriction on the content of this packet. It can be omitted by setting none to this parameter.

"Host Address Inquiry CMD"

DRF1110N module can use the address of external device or its own MAC address for routing and data forwarding. This parameter is used to let DRF1110N module get the external device address on power-up. When the module is powered up, it will wait for "HOST Boot Time" first, then send this predefined "Host Address Inquiry CMD" to external device and wait for the response from the external device within "Response Timeout". If response from the external device does not exceed "Response Timeout", DRF1110N module can pick up and record the address of external device. If DRF1110N module does not get the response from external device within "Response Timeout", it will send this command again. DRF1110N will give up this process if it still can not get response after five trials and it will act as a pure relay node. However, DRF1110N still can access the address of external device later when external device sends the first frame to the module.

Note:

1. The Maximum length of the "Host Address Inquiry CMD" is 48 bytes.
2. The "Host Address Inquiry CMD" can be used as probe for external device.
3. MNET III uses the external device address directly for routing and data forwarding. There is no special device which can convert the external device address to MAC address in the network.
4. The structure of response frame should follow the frame parser configuration. It is not necessary to define a special command for "Host Address Inquiry CMD" so any command can be used if external device can give response to it. For example the broadcasting data acquisition command can be used s the "Host Address Inquiry CMD".

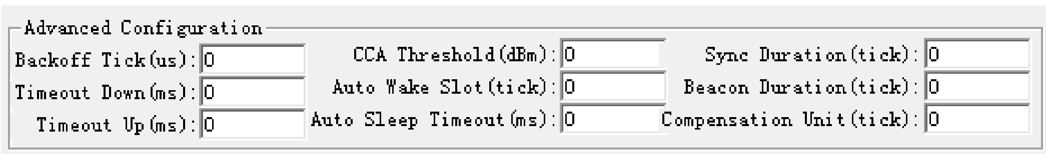
5. "Host Address Inquiry CMD" must be set if external address has to be used for data forwarding. Otherwise, the module MAC address will be used instead.

"Predefined Broadcast CMD1" and "Predefined Broadcast CMD2"

Two most commonly used broadcast commands such as broadcasting data acquisition command can be set and saved in this block. Root module can use very short message to replace original data packet if the content of command packets it receives these "Predefined Broadcast CMD". With the help of predefined commands, it can shorten the process of downlink data delivery, reduce response time and save power consumption. The maximum length of these two predefined broadcast commands is 48 bytes. The predefined broadcast commands also can be used for other purposes:

1. Packet conversion. Suppose there are different types of devices in the network and the data acquisition commands for different devices are different. These predefined broadcast commands can be used to unify the differences by setting interrelated predefined broadcast commands for different type of devices.
2. Force to use broadcasting for some special usage. For example there is no wildcard in broadcast address or the broadcast address is omitted by some kind of contracted protocols.

5. ADVANCED CONFIGURATION



After pressing the button "Advanced>>", the configuration tool will be expanded from the bottom and the advanced configuration block will be displayed. Users can configure special parameters to optimize the network according to actual applications. The configuration tool will not validate any parameter changed in this block. We don't recommend users to change related parameters unless they are acquainted with the basic parameters and have verified the function of networking.

Backoff Tick: This parameter is the time unit for collision avoidance and is related to RF data rate. It is recommended using the default parameter in the configuration tool.

CCA Threshold: CCA (Clear Channel Assessment) Threshold is used to judge whether the wireless channel is ideal or not. Larger value will increase the likelihood of packet collision. In contrast smaller value will increase the false alarming and wasting of channel resources. For channels with interference, an appropriate increment on the threshold will improve the competition of network to access the physical channels. For the situation which distance between nodes is long and wireless channel is clean, the threshold value can be decreased in order to reduce packet collision.

Auto Wake Slot: It appoints the length of "Listening time slice" in asynchronous sleep mode. The unit of this parameter is Backoff tick. It is recommended to use default parameter in configuration tool.

Auto Sleep Timeout: Or Auto sleep idle timeout. When asynchronous sleep mode is enabled, the module will automatically enter into sleep if it has been idle in "Auto Sleep Idle Timeout". This parameter is used as the timeout threshold. For modules with asynchronous mode disabled, it will be used as the cycle for calibrating radio frequency. This parameter is set according to the actual application and network topology. The value ranges in 1~5 seconds.

Compensation Unit: Or Auto sleep compensation unit. This parameter is designed to increase the speed for asynchronous wakeup process. If a node module is N hopping distance from the root module, it will take total ["Auto Sleep Timeout" + (N * "Compensation Unit")] as idle timeout. The appropriate value of this parameter is 1~3 packet forwarding time.

Downstream and Upstream Timeout: A node module could become isolated because of unpredictable accidents such as nodes powering-down, radio interference, etc. Users can set the downstream/upstream timeout in order to avoid long time attempts. The recommended timeout is 4s for non-sleep network. If asynchronous sleep mode is enabled, these parameters should be set at least twice of the "Sleep time slice".

Sync Duration: In synchronous sleep mode, sync sleep packets are broadcasted at the beginning of the coming "sleep time slice" to ensure the sleep boundary of all nodes are aligned. Sync sleep packets should be sent in a very short time slot. However it should be long enough to make sure all nodes can receive the sync sleep packets. The parameter "Sync duration" is used to set the duration time of sending sync sleep packets. Generally speaking, the time in sending a sync sleep packet needs 5 ticks. It is recommended to set this parameter as 20 ~30 ticks to ensure the sync sleep packet can be repeated about 4 times by each node.

Beacon Duration: Beacon packets are mainly used to wake up sleeping modes in asynchronous sleep mode. It also can be used to eliminate the deviation of sync alignment in synchronous sleep mode. This parameter is the duration time used to send beacon packets. Longer time will increase the transmit times of beacon packets so it needs to be calculated based on parameters "Sleep Wake Rate" and "Auto Wake Slot". The recommended range of this parameter is ("Sleep Wake Rate" * "Auto Wake Slot" /2) ~ ("Sleep Wake Rate" * "Auto Wake Slot").

Auto Configure: If this option is activated, the configuration tool will lock the current parameters and automatically detects the insert and plug of USB board. The tool will increase the MAC address when it detects each insert/plug of USB board and write the current parameters to module.

ADDRESS MODES

Either the MAC address of DRF1110N module or the address of external device can be used for routing. DRF1110N module will detects whether the "Host Address Inquiry CMD'" exists or not. If this parameter is none, the MAC address will be chosen; otherwise, the external device address mode will be used.

1. External Address Mode

If the parameter "Host Address Inquiry CMD" is set, DRF1110N module will send this packet to external device to inquiry the external address when being powered-up. If external device responds without timeout, the module will pick up the address from the responded package and record it into its own RAM. DRF1110N will give up inquiring if five trials are all failed. The length of external device address can be 1~16 bytes by setting the parameter "Address Length". Once the module obtains the external device address, it will not change it any more except by resetting the module and let it inquiry the new address.

2. MAC Address Mode

If the address of external device can not be used for routing or data forwarding, the MAC address of module will be used instead. According to the philosophy of MNET III, the upper-layer payload should be left intact. An external frame head is added to users' upper-layer payload. The external frame head includes a sync word and the MAC address. Even though the length of actual MAC address is 6 bytes, the MAC address within the external frame head can be configured with length ranging from 1 to 16 bytes.

The external frame head is automatically added by node module so the external device connecting to the node module knows nothing about it. Therefore, no modification is required for users' upper-layer protocol. The external frame head is showed as below:

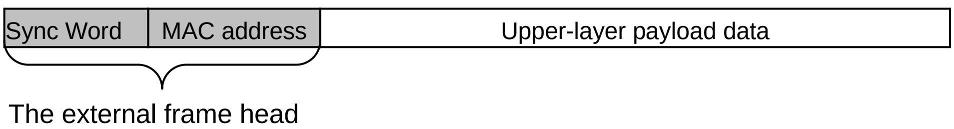


Figure 20: External Frame Head Structure

The sync word of the external frame head is parsed from the first character of "Predefined Broadcast CMD1" packet. The configuration for MAC address is described in details as below:

1. "Host Address Inquiry CMD": Null
2. "Predefined Broadcast CMD1": It must be configured with the external frame head and the first character should be the external sync word.
3. "Frame Start Sync Word": The start sync word of the original payload
4. "Frame Stop Sync Word": The stop sync word of the original payload

5. "Address length": The length of MAC address, which can be set to 1~16 bytes.
6. "Broadcast Wildcard" and "Multicast Wildcard": The wildcard of MAC address which can be defined as any value when necessary.
7. "Downlink Address Offset" and "Uplink Address Offset": 1; because there is only one byte ahead of the MAC address.

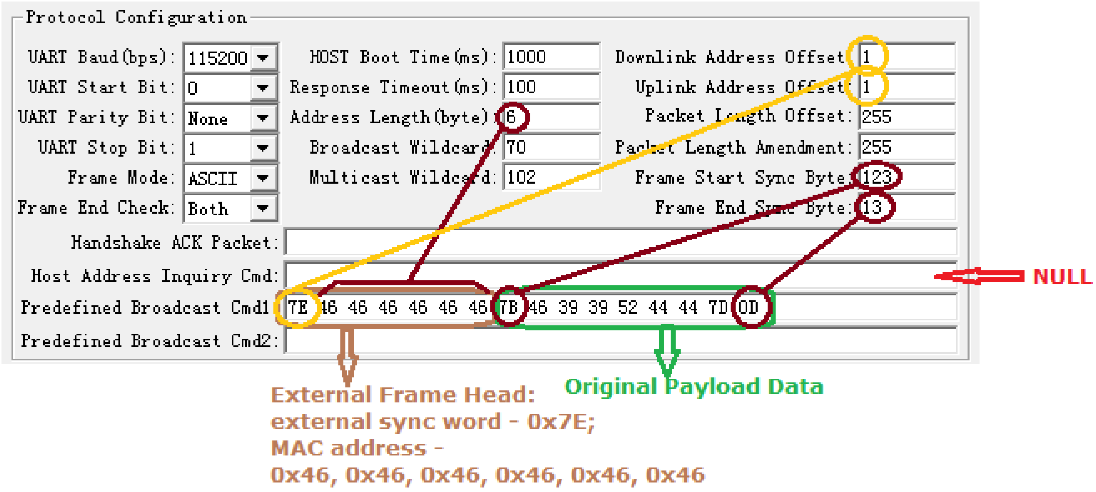


Figure 21: Predefined Broadcast CMD1 & MAC Address

Please note that if both "Host Address Inquiry CMD" and "Predefined are set to NULL, the external address mode is chosen. In this case the DRF1110N module can not take initiative to get the external device address since 'Host Address Inquiry CMD" is NULL at power-on. However, external device can send message to DRF1110N module to let it get the external address. If the module can not get message from external device, the module will act as a pure relay node in network and will not deliver any message at downlink to external device.

SLEEP MODES

In parameter configuration section different sleep modes are described. In this section more details about sleep modes will be explained. All nodes including gateway and concentrator nodes all can sleep. Sleep-enabled nodes and non-sleep nodes can coexist in the same network.

1. Asynchronous Sleep Mode

Nodes can enter sleep mode periodically and wake up automatically according to the 'Sleep-Wake Ratio" in asynchronous sleep mode. The node will turn on radio part to monitor the potential incoming data packets in the network in a short period called "listening time slice". If any data packet is detected in a "listening time slice", the module will enter normal work mode or else it will enter into short-time sleep called "sleeping time slice". The length of "listening time slice" and "sleeping time slice" can be configured flexibly according to the actual application. In asynchronous mode the boundary of time slices of different nodes are not synchronized.

The module consumes 0.5uA current in sleep mode and 22mA in normal receive mode. The power consumption of asynchronous mode is easy to calculate with the parameter "Sleep -Wake Ratio". For example, if the "Sleep-Wake Ratio" is set to 1000, the average current consumption is (0.5uA*1000+22Ma*1)/1001=22.5uA.

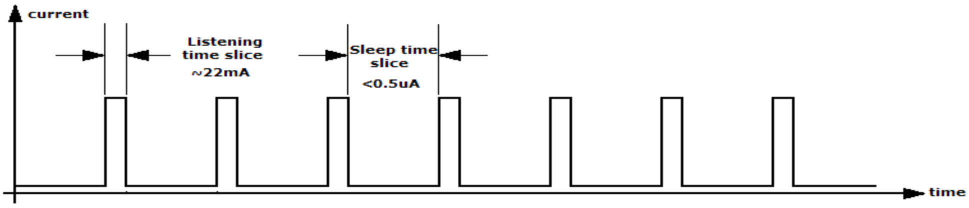


Figure 22: Power Consumption in Asynchronous Sleep Mode

There are two ways to wake up a sleeping node in asynchronous sleep mode. The first one is to prolong the preamble of a wireless packet. Users can make the preamble longer than the "sleeping time slice" of the receive nodes. Another way is resend short wake-up packets repeatedly. However this method is harder to realize due to the data packet collision in a mesh network. However the later method is more reliable and quicker to awake a sleeping node. Also external information such as routing table can be carried within wake-up packets to do data exchange. Though the second method is more complicated to realize in order to reduce collision, MNET III uses advanced anti-collision technique and overcomes the disadvantage of data collision so the delay of waking up the whole network is very short and the delay time is almost predictable no matter how large scale of the network is. The more dense the network is, the faster the wake-up time.

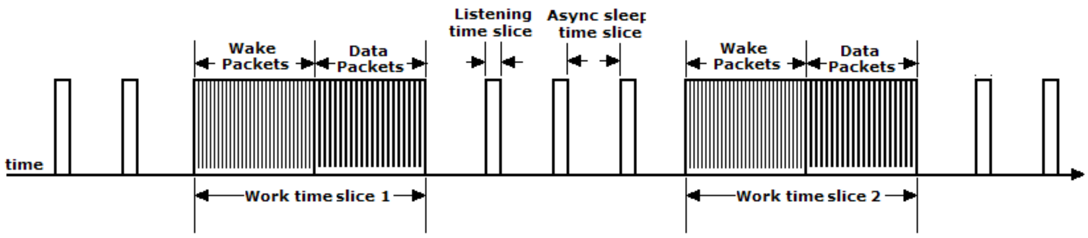


Figure 23: Wake-up Packets in Asynchronous Sleep Mode

In asynchronous sleep mode, all nodes keep will keep in silence in sleep status so there is no interference to external wireless network. It supports very large scale network and data packets can be sent at any time if necessary so it is very suitable for low power applications such as wireless meter reading, alarm system, industrial control, etc.

2. Synchronous Sleep Mode

The "sleeping time slice" of nodes is strictly synchronized in synchronous mode. The alignment error of time slice between adjacent nodes is less than 1ms. The time slice synchronization is realized through broadcasting the synchronous sleep message triggered by gateway or concentrator (or root node) when the network is idle. The sleep message contains the length of the next "sleeping time slice". MNET protocol does not assume or forecast the current payload of the whole network. If there is no data transmission in a "working time slice", all nodes can enter into sleep mode immediately without needing to wait for the end of a predetermined time slice. There is also no restriction that the data transmission must be finished at the end of a predetermined time slice. In synchronous sleep mode the wake-up process is not required in a "working time slice" since the synchronous time error between adjacent nodes is very small.

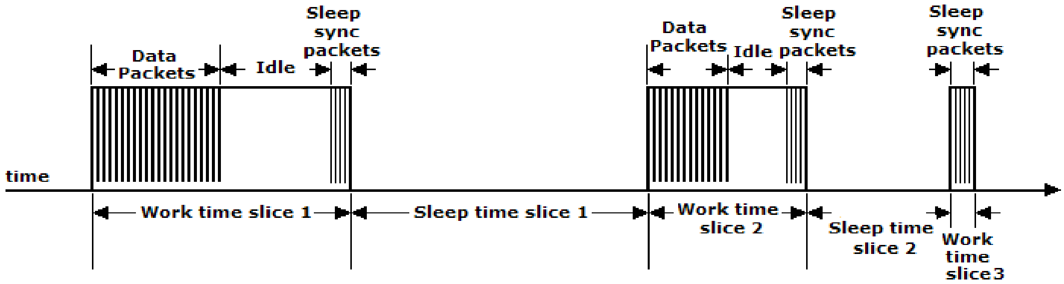


Figure 24: Wake-up Packets in Synchronous Sleep Mode

The "work time slice" and "sleep time slice" can be dynamically changed by gateway or concentrator. Data packets transmit in each "work time slice". The synchronous sleep packet indicates the end of 'work time slice" and determines the length of the following "sleep time slice". In the diagram above the synchronous sleep packets are broadcasted in the "work time slice 3", which means synchronous sleep packets are always broadcasted to synchronize the time slice of all nodes even if there is no data transmission in the network.

3. Hybrid Sleep Mode

Hybrid sleep mode refers to the situation which synchronous and asynchronous sleep modes are both used in the same network. The sleep mode is identified by the flag bit in the data packet head. Each "sleep time slice" and "work time slice" can be set for different sleep modes. The typical hybrid sleep mode is showed as below:

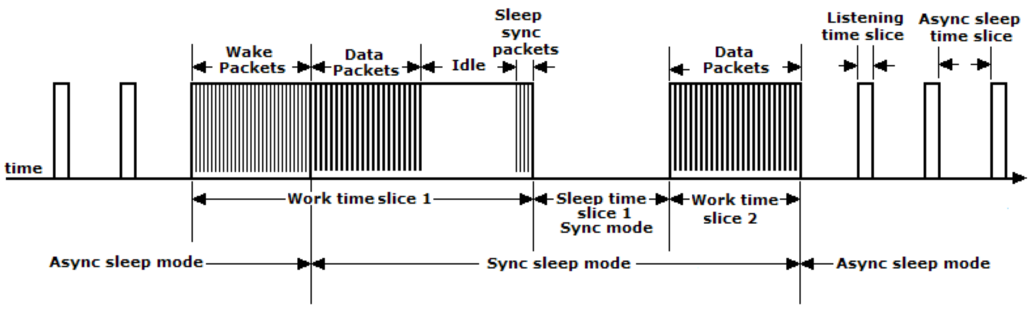


Figure 25: Wake-up Packets in Hybrid Sleep Mode

In the diagram the default sleep mode is asynchronous sleep mode. If a node misses the synchronous sleep broadcasting packets, it will enter asynchronous sleep mode automatically. In "work time slice 1" wake-up packets are sent repeatedly and the packet contains the message that the following work slice will be synchronous mode by setting the flag bit at the wake-up packet head. Synchronous sleep packets are sent at the end of "work time slice 1" and they also indicate the length of incoming "sleep time slice1". Because the starting time of the "work time slice 2" is synchronized, data packets can be directly sent without sending wake-up packets at the beginning of this work time slice. The node modules will enter asynchronous sleep mode after "work time slice 2" finishes by setting the sleep mode flag bit of the data packet sent in "work time slice 2".

Hybrid sleep mode absorbs the advantages of synchronous and asynchronous sleep modes and can obtain the lowest power consumption but it is very complicated to switch between different sleep modes. This type of sleep mode is suitable for complicated applications.

APPLICATIONS

1. Wireless Sensor Network

Wireless sensor network refers to the application which data of all nodes need to be collected in real-time. The features of this kind of application are:

- Data acquisition time interval is short and periodic, usually the period is from a few seconds to a few minutes. Data collection of the whole network should be completed in a very short time
- Sensor nodes are often powered by battery so low-power consumption is required.

For such applications low-power consumption can be achieved by using synchronous or hybrid sleep mode. All node and root modules can enter into sleep mode. The time interval of data acquisition here is controlled by the 'sleep time slice' which can be flexibly set through AT command each time. Data acquisition could be processed by broadcasting at downlink and it only takes several seconds to collect all data of the whole network with hundreds of nodes. Wake-up process is not needed in synchronous sleep mode so it can minimize power consumption. However, the hybrid sleep mode can improve the robustness of the network since it can prevent unexpected power consumption if a node misses sleep messages.

In addition multiple root modules also can be employed in a sensor network. The network bandwidth will be increased effectively so the data transmission time and energy consumption can be reduced due to the higher throughput so sensor network based on MNET III protocol can greatly reduce the costs of equipment development, deployment and system maintenance.

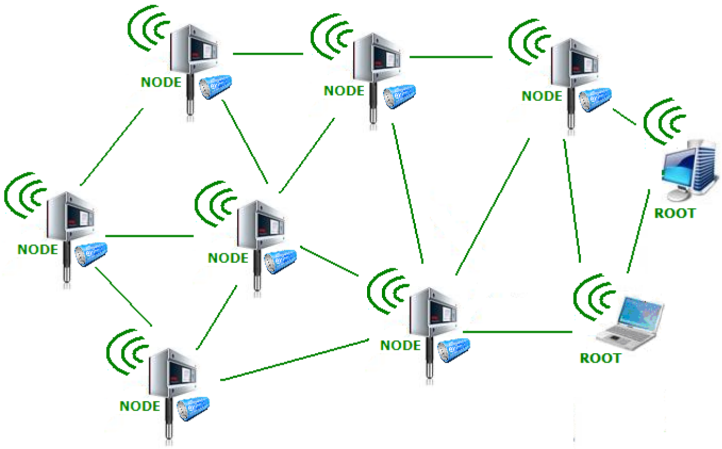


Figure 26: Wireless Sensor Network

2. Wireless Automatic Meter Reading

Power consumption is critical for Auto Meter Reading (AMR) applications such as gas, water and heat since these kinds of meters are usually powered by batteries. According to China national standard "Residential remote meter reading system", these low-power meters should be able to work normally at least 6 years without changing batteries. It makes very a stringent requirement on the power consumption. Considering the capacity and price of batteries available on the markets, the average current of a low-power meter should be less than 30uA. Characteristics of such applications are listed as below:

- The time interval of meter reading is long, which is generally 1-2 times one month.
- Need to control a single meter or multiple meters at the same time for recharge, shutting down, etc. The meters also can send alarm messages back to control center in emergency.
- Power consumption is very critical.

The diagram of the popular solutions for low-power meter reading (e.g. ZigBee) is shown below. Three kinds of devices required in such solutions are wireless meters, collectors and concentrator. Wireless meters only can exchange data with collectors or concentrators. However, data transmission can not be directly done between wireless meters. Wireless meters have no or only very simple routing functions. Only wireless meters can be low-power but collectors and concentrator should be powered by AC power supply. Wireless meters basically communicate with collectors by ways of active reporting or querying. Collectors are responsible for collecting and recording the data of wireless meters and they also delay data transmission originated from concentrators to meters. Collectors are connected to concentrators through wired cable (e.g. RS-485) or wireless (e.g. ZigBee). Concentrators communicate with the backbone database of the operating enterprises through private networks or wireless public network such as GPRS. Concentrators and collectors cannot enter into sleep mode and they must be always powered. The implementation for such solutions is simple but there are many drawbacks:

- A number of collectors are needed to buffer data messages sent from or to wireless meters. Collectors also need to maintain the routing information of the whole network and do packet forwarding. Because collectors need much more hardware resources than wireless meters, the cost for collector equipments is very high.

- Collectors need to be always powered, which usually are difficult for installation so the cost for maintenance is also very high.
- There are many different types equipment in a network. Wired bus is easy to break and the cost of system maintenance is high.
- As the backbone of the network, a collector usually manages a lot of wireless meters. If a collector is broken, all meters under its management are unavailable. The robustness of the system is not favorable.

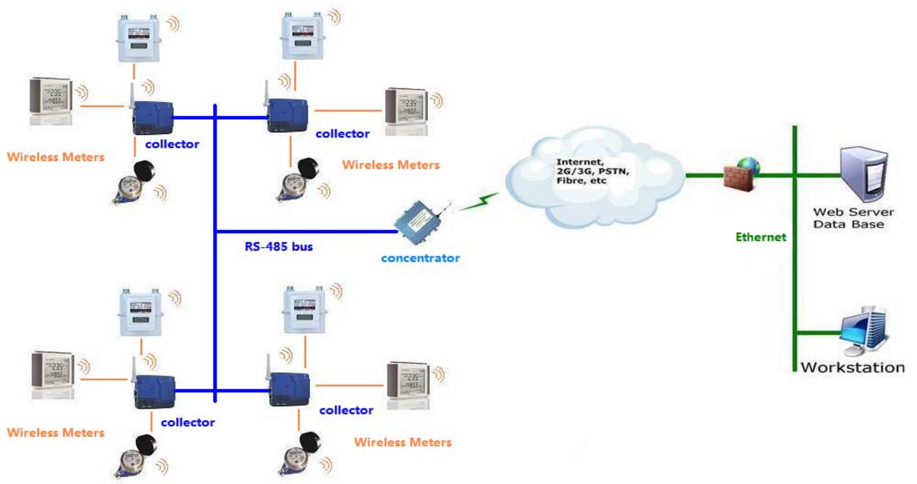


Figure 27: Typical Wireless AMR Network

There are only two types of equipments used in AMR solution based on MNET III: wireless meters (node) and concentrator (root). DRF1110N node modules can be employed for wireless meters and root modules can be used as concentrators. All of the wireless meters and concentrators can enter into sleep mode and be powered by battery. The installation of wireless meters and concentrators does not need any manual configuration. The configuration process is the same as traditional instruments. The diagram of AMR network based on MNET is show as below:

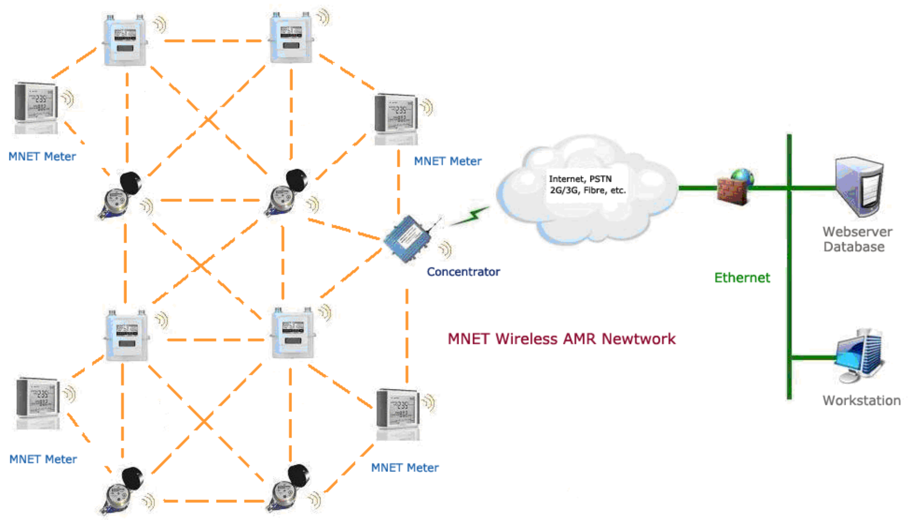


Figure 28: Wireless AMR Network Based on MNET III

For such applications asynchronous sleep mode can be used to save power consumption. The average standby current is about 20uA by using DRF1110N module. All devices are in silence at standby status. The network has good security and the anti-interference ability. All devices can work as soon as being powered-on so the whole network does not need initialization procedure. Meters can be read or controlled at any time. MNET protocol employs a unique wake-up algorithm which can wake up the whole network within a short time. The wake-up delay is almost fixed and is independent from the network scale. All meters can be read simultaneously through broadcasting so it saves a lot of time and energy consumption, compared with the way to read one by one. MNET AMR network can optimize routing table according to the remaining battery power and can automatically balance the data transmission through multiple paths.

3. Warehousing, Logistics, Alarm and Location

The applications of warehouse logistics and alarm positioning need to manage tens of thousands of mobile or fixed nodes in a larger scope. Nodes report to background servers their information such as position, status, etc. at any time if necessary. Background servers can also actively inquiry the current information of each node. The characteristics of this kind of application are:

- Very large number of nodes. Usually there are more than tens of thousands of commodities in a storage;
- The network coverage range is very wide, which the coverage radius of the logistics is up to a few kilometers or even more;
- Power-saving is required. Wireless modules need to work for more than 1 year without replacing coin batteries;
- Real-time is required for alarm and location applications. The background server should receive the alarm messages within a few seconds.

These kinds of applications can be achieved by adopting DRF1110N modules with MNET protocol. The network diagram is showed as below. Root modules can be used as the gateway to connect the network to background servers. Non-sleep node modules are adopted as the network backbone and cover the whole network. Sleep enabled node modules can be used as low-power wireless mobile tags. Multiple root modules can be dispersedly deployed to increase the connection bandwidth to background servers and reduce the transmission delay. Only the backbone nodes (non-sleep node modules) of the network take care of routing and the data forwarding. Mobile nodes do not participate in data forwarding; they just send burst data to the backbone nodes so the power consumption of mobile nodes could be ultra-low. Mobile nodes can roam within the coverage range of network and data transmission can be seamlessly switched to backbone nodes. The location of mobile nodes can be calculated by the signal strength RSSI detected by fixed nodes. If there are more than 3 fixed nodes within the wireless signal radiating area of a mobile node, the location of the mobile node can be accurately calculated.

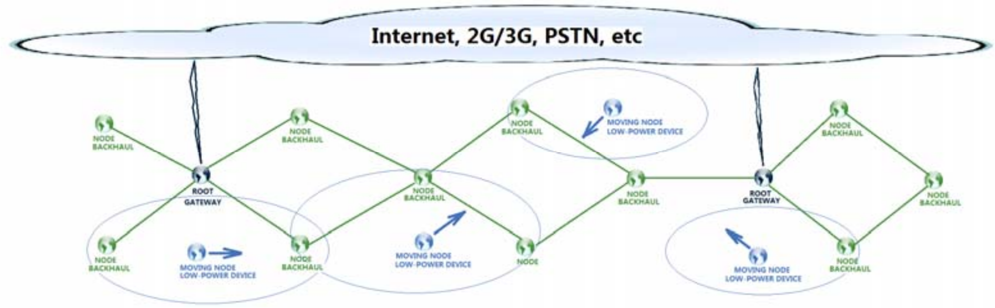


Figure 29: Warehouse Logistics, Alarm and Locating Application

4. Mobile Ad-Hoc Network

In a mobile Ad-Hoc Networks all nodes can move freely in any directions. Such applications include field teamwork, wartime network, emergency network, disaster network, etc. These applications have high requirement on the self-healing ability and routing robustness of network. In addition a big coverage is usually needed, which means the maximum routing hops should be large enough.

The routing protocol of MNET is optimized for mobile Ad-Hoc network. It is an entirely distributed peer-to-peer, multi-path and on-demand routing protocol. The cost of routing establishment and maintenance is extremely reduced since it is sensitive to the network topology changing and can seamlessly switch the route among multiple paths. No flooding is needed to discover new routing paths while current routing paths are still working. Data transmission can be processed through multi-path in parallel. The routing protocol of MNET protocol supports up to 255 routing hops which guarantees that the network can be very large. The MNET mobile Ad-Hoc network diagram is showed as below:

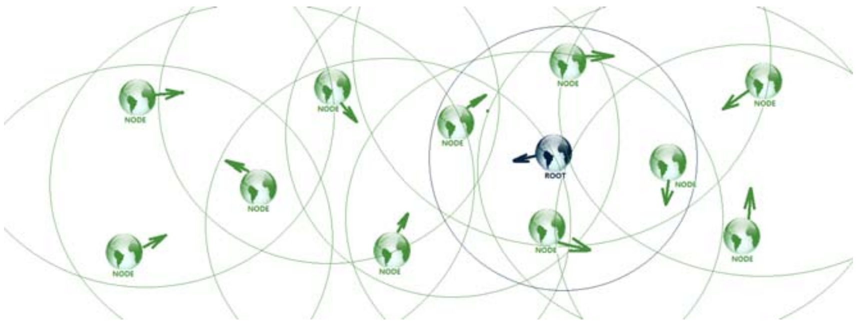


Figure 30: Mobile Ad-Hoc Network

5. Zigbee Replacement

The typical ZigBee network is consisted of three types of devices: coordinator, router and end devices. A ZigBee network needs a coordinator to do initialization. After network initialization, the Coordinator becomes a router. Routers are the network backbone which is responsible for data forwarding and routing maintenance. The routing protocols build on AODV to automatically construct a low-speed ad-hoc network of nodes. The network will be a cluster of many clusters in most large network applications. It can also form a mesh or a single cluster. The current ZigBee protocols support beacon and non-beacon enabled networks.

In non-beacon-enabled networks, a CSMA/CA channel access mechanism is used. ZigBee routers typically need their receivers continuously active in this type of network, which requires a more robust power supply. However, this allows for heterogeneous networks in which some devices receive continuously while others only transmit when an external stimulus is detected. In beacon-enabled networks, the special network nodes called ZigBee routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, which lowers their duty cycle and extends their battery life. The interval of beacons depends on data rate. However, low duty cycle operation with long beacon intervals requires precise timing, which can conflict with the need for low product cost.

In general the ZigBee protocols minimize the time of turning on the radio so as to reduce power consumption. In beaconing networks, nodes only need to be active while a beacon is being transmitted. In non-beacon-enabled networks, power consumption is decidedly asymmetrical because some devices are always active while others spend most of their time on sleeping. The replacement of the ZigBee network with MNET III modules is showed in the diagram below:

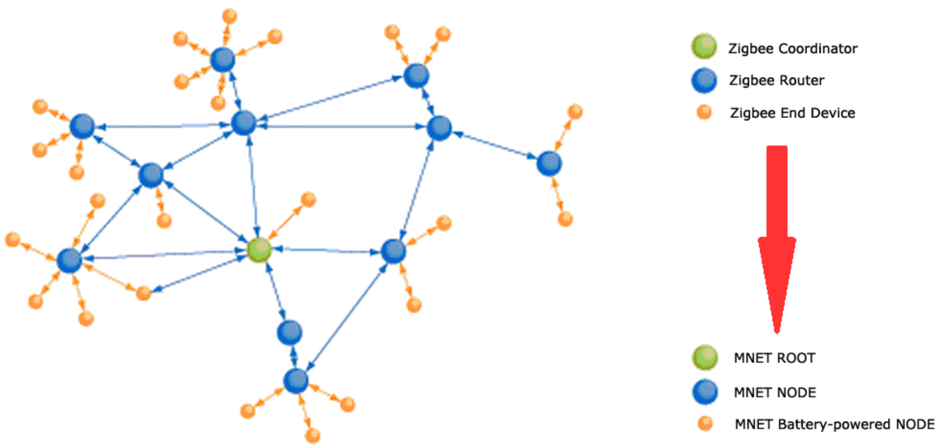


Figure 31: Replace Zigbee with MNET III Network

The philosophy of MNET III and ZigBee in networking are quite different. MNET III is a distributed peer-to-peer network while ZigBee is a hierarchical clustering asymmetrical network. However it is still possible to replace ZigBee modules with MNET III modules in most use cases:

- Replace ZigBee coordinator with MNET III root module.
- Replace ZigBee router with MNET III non-sleep node module.
- Replace ZigBee end device with MNET III sleep enabled node module.

The core idea of the replacement is that using non-sleep node and root modules to replace ZigBee routers and coordinator as the network backbone and use low-power sleeping node to replace ZigBee end device. Data transmission can be launched by sleeping node or root module. Sleeping nodes can initiatively send inquiry messages to a root module to ask if it has cached their messages in time when it wakes up. After the simple replacement of modules, it still needs to pay attention to the followings:

- ZigBee routers caches data messages sent to ZigBee end devices but MNET III non-sleep node modules do not need to cache messages sent to sleep nodes, which is relevant to the difference between MNET network and Zigbee network. Instead the root module should buffer packets of all nodes. A wake-up node from sleep mode can initiatively send inquiry messages to backbone nodes to ask for if the root module has cached messages. The root will respond to the inquiry and deliver data or inform nodes to sleep if necessary. Backbone nodes automatically forward massages between a sleep node and the root.

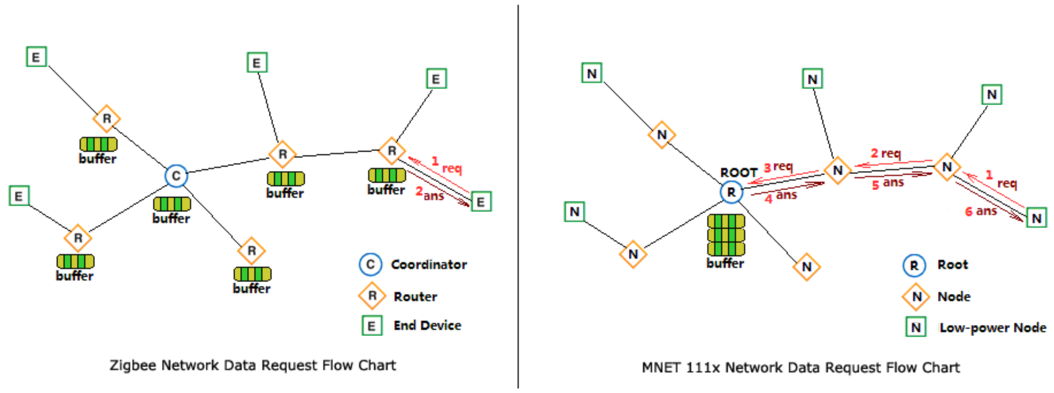


Figure 32: Zigbee Vs MNET III in Data Flow

- MNET synchronous sleep mode can be used to replace the beaconing mode ZigBee and MNET asynchronous sleep mode can be used to replace the non-beacon-enabled mode ZigBee.
- The backbone nodes of MNET do not buffer data messages belonging to sleep nodes under its administration. Whenever a backbone node has a data message need to send to a sleep node, it will wake up the sleep node and then send data message instead of buffering the data message.

6. Long Distance Remote Control

In some applications the network topology likes a very long flat line such as street lamp, railway, electronic billboards beside the street, etc. The end node is very far from the gateway or concentrator. Data messages need many times of relay to reach the destination. Broadcasting downlink and unicasting uplink is a common way of data transmission. MNET protocol can support up to 255 routing hops so MNET network can cover more than tens of kilometers. The network diagram is showed as below:

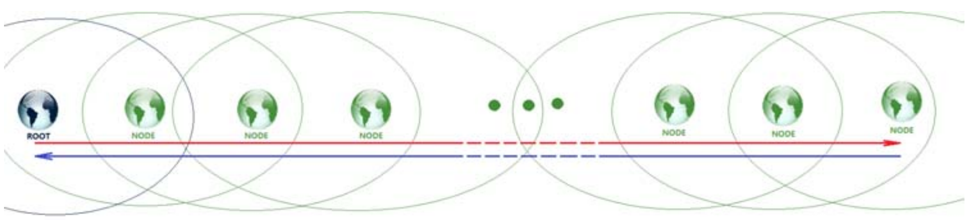


Figure 33: MNET III Network in Long Distance Remote Control

7. Building & Home Automation

MNET Building Automation offers a solution for secure and reliable monitoring and control of commercial building systems. Owners, operators and tenants can benefit from improved energy savings and ensure the lowest costs with this green and easy-to-install robust wireless network. By using MNET Building Automation products in your building, you can contribute with satisfying credits in the categories of Sustainable Sites, Energy and Atmosphere, Indoor Environmental Quality. MNET supports up to 255 routing hops so one network can cover any known buildings.

COMMANDS SET

MNET III protocol provides several commands to root module in order to dynamically change some parameters such as sync interval time, etc. The node module does not support these commands. The syntax of command is showed as below:

AT		**ASCII**		**Space**		**Parameter**		**<CR>**
Prefix	+	Command	+	(Optional)	+	(Optional, HEX)	+	Carriage Return

For example: ATCR 1F<CR>. Among which "CR" is the command and "1F" is the parameter.
Command Response: ATOK<CR>: succeeded; ATER<CR>: failed.

1. ATCR

Format: ATCR [0 ~FFFF]<CR>

This command activates the "Repeat" option and sets the "Sync interval" time. The unit of this parameter is second. If the parameter is not zero, synchronous sleep mode will be triggered with the "Sync interval" time, otherwise synchronous sleep mode will be disabled but the "Repeat" option is still activated. The "Repeat" option can be disabled by "ATCO" command. The range of this parameter is hexadecimal 0~0xFFFF. It is optional and the default value is 0 if omitted.

2. ATCO

Format: ATCO [0 ~ FFFF]<CR>

It disables the "Repeat" option and sets the "Sync interval" time. If the parameter is not zero, synchronous sleep mode will be triggered with the "Sync interval" time, otherwise synchronous sleep mode will be disabled. The range of this parameter is hexadecimal 0~0xFFFF. It is optional and the default value is 0 if omitted.

3. ATCS

Format: ATCS [0 ~ FFFF]<CR>

The command forces all node modules to enter into sync mode immediately. The parameter specifies the length of the incoming "sleep time slice". The unit of it is second. This command returns error when the network is already in sleep status. It does not change the parameter "Sync interval" which is configured by "ATCR" and "ATCO". Users can flexibly control the network sleep time with it. The range of this parameter is hexadecimal 0~0xFFFF. It is optional and the default value is 0 if omitted.

MECHANICAL DATA

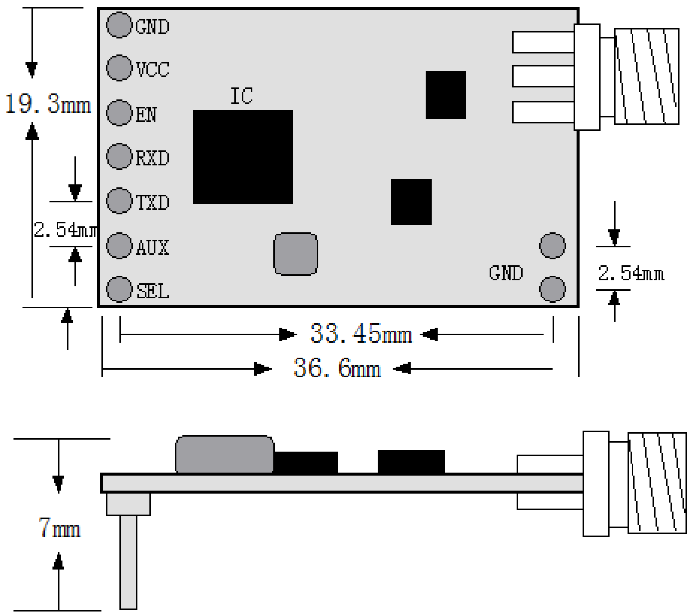


Figure 34: Mechanical Dimensions

ORDERING INFORMATION

<u>DRF</u> <u>1110</u> <u>N</u> <u>20C</u>— <u>043</u> <u>A</u>
① ② ③④⑤ ⑥ ⑦

Num	Symbol	Meaning
①	Category	RF GFSK module
②	IC Type	CC1110
③	Module Type	Network module
④	Power	20dBm output power
⑤	Module Function	C: concentrator module; N: node module
⑥	Freq. Band	043: 433MHz
⑦	ANT Interface	DIP package with SMA connector

Table 13: Ordering information

Dorji Applied Technologies A division of ***Dorji Industrial Group Co., Ltd*** Add.: Xinchenhuayuan 2, Dalangnanlu, Longhua, Baoan district, Shenzhen, China 518109 Tel: 0086-755-28156122 Fax.: 0086-755-28156133 Email: sales@dorji.com Web: http://www.dorji.com	Dorji Industrial Group Co., Ltd reserves the right to make corrections, modifications, improvements and other changes to its products and services at any time and to discontinue any product or service without notice. Customers are expected to visit websites for getting newest product information before placing orders. These products are not designed for use in life support appliances, devices or other products where malfunction of these products might result in personal injury. Customers using these products in such applications do so at their own risk and agree to fully indemnify Dorji Industrial Group for any damages resulting from improper use.

"