

RedLINK CC1101 RF transceiver configuration

reg addr	name	value in hex	interpretation
00	GDO 2	06	output is "sync word sent/rcvd"
01	GDO 1	0D	output is "serial data out"
02	GDO 0	2F. 38	output is sometimes "hardwired to 0" and sometimes "CLK_XOSC/16"
03	FIFO threshold	47	ADC retention, threshold is 32 bytes TX, 32 bytes RX (of 64-byte FIFOs)
04/05	sync word	63xx,	where xx=90, 65, 75, 8E, 7A, 93, 7B, 94, 83, 9C, 87, 6E, 84, 6B, 91, 78, 86, 6D, 99, 80
06	packet length	63	99 bytes (but not used in variable-packet mode)
07	packet control 1	44	preamble quality threshold 2 no autoflush of RX FIFO on bad CRC append 2 status bytes to packet RSSI (dBm signal power), CRC OK, LQI) no address check
08	packet control 0	45	data whitening on normal FIFO mode CRC enabled variable packet length, set by first byte after sync word
09	device address	0, or 06	(for packet filtering)
0A	channel number	varies	00 1C 18 55 22 5F 2C 61 3C 79 46 0A 3E 04 5B 1E 44 08 73 36; 0C 1A 57 4F 72 14 51 4D 10 5D 20 32 6F 71 24 75 38 16 53 77 3A 59 1C 18 55 22 5F 2C 61 3C 79 46 0A 3E 04 5B 1E
0B	frequency control 1	06	IF frequency: 152 Khz
0C	frequency control 0	00	frequency offset for base, in units of 1587 Hz (none)
0D/0E /0F	frequency control word (H/M/L, 24 bits)	22BB33	2,274,099 * 396.7 = 902.1350 Mhz (only at init) 2,274,096 * 396.7 = 902.1338 Mhz (all other times)
10	modem config 4	CA	$BW = 26MHz / (8 * (4+00) * 2^{**3}) = 26MHz / (32 * 8) = 101.5 \text{ Khz}$
11	modem config 3	83	$symbol \text{ rate} = 26 \text{ Mhz} * (256+131) * 2^{**10} / 2^{**28} = 38.383 \text{ Kb}$
12	modem config 2	12	enable DC blocking, GFSK modulation, disable Manchester, 16/16 sync word bits
13	modem config 1	62	disable forward error correction, 16 preamble bytes, chan spacing exponent = 2
14	modem config 0	F8	chan spacing mantissa = 248. default spacing = 199.951 Khz
15	deviation	34	exp=3, man=4; deviation = 19.0 Khz
16	state machine 2	07	default (end-of-packet timeout for sync)

17	state machine 1	00	CCA always, idle after packet sent or received
18	state machine 0	18	calibrate when going to RX or TX from idle; expire count 64 (150 usec)
19	freq offset config	16	gain 3K, K/2, sat BWchan/4
1A	bit sync config	6C	defaults
1B	AGC control 2	43	
1C	AGC control 1	40	
1D	AGC control 0	91	
1E/1F	event timeout (H/L)	876B	default = 34,667, or 1 second
20	wake on radio control	F8	default
21	RX config	56	default
22	TX config	10	default (select PATABLE entry 0)
23	freq cal 3	E9	
24	freq cal 2	2A	
25	freq cal 1	00	
26	freq cal 0	1F	
27	RC osc config 1	41	
28	RC osc config 0	00	
29	freq calib ctl	59	default
2A	prod test	7F	default
2B	AGC test	3F	default
2C	test2	81	
2D	test1	35	
2E	test0	09	
...			
3E	PATABLE (power amp)	C0	default, always

Other notes

JimmySwimmy says RedLINK uses "50 channels, 903 to 926.4 Mhz, 69 Khz each channel, 400 Khz spacing".

Based on the CC1101 configuration, I see 101.5 Khz bandwidth channels with spacing of 199.9 Khz.

With a base frequency of 902.13 Mhz and a maximum observed channel number of $0x79 = 121$, that implies that the highest frequency is $902.13 + 121 * .1999 = 926.31$, which fits into the allowed band.

In the US the FCC requires a minimum of 50 channels in this band; see <http://www.ti.com.cn/cn/lit/an/swra077/swra077.pdf>.

The observed frequency-hopping sequence of 50 channel numbers that Honeywell uses is this:

44	08	73	36	2E	63	0E	4B	06	42	6D	30	49	0C	1A	57	4F	12
14	51	4D	10	5D	20	32	6F	71	34	75	38	16	53	77	3A	59	1C
18	55	22	5F	2C	61	3C	79	46	0A	3E	04	5B	1E				

I'm guessing this is just stored in a table, not generated by an algorithm in the microprocessor.

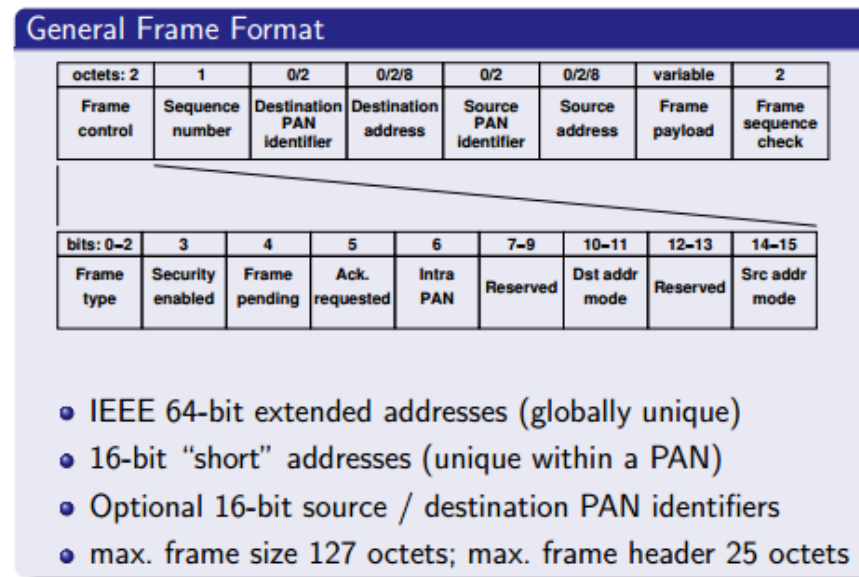
Example transmitted data packets from the Honeywell C7189R1004 indoor temperature sensor when not linked to any receiver:

12 23 30 0B FF FE E8 1F F0 00 00 87 82 12 00 E8 1F FF 81
12 23 F4 3F FF FE E8 1F F0 00 00 87 82 12 00 E8 1F FF 81

15 03 31 E4 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 07 ED 7F FF 06
15 03 9F 3D E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 BC 7F FF 06 (chan 63, 2E, 73)
15 03 56 65 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 BC 7F FF 00 (chan 0E)
15 03 02 F5 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 C4 7F FF 00 (chan 4B)
15 03 51 61 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 C7 7F FF 00 (chan 06)
15 03 16 A9 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 C7 7F FF 00 (chan 42)
15 03 31 24 E8 1F E8 1F F0 01 00 0A 12 80 00 46 34 08 CC 7F FF 00 (chan 6D)
15 03 98 73 E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 D2 7F FF 00 (chan 30)
15 03 E9 7A E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 D7 7F FF 00 (chan 49)
15 03 35 9A E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 DC 7F FF 00 (chan 0C)
15 03 01 53 E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 DA 7F FF 00 (chan 1A)
15 03 A3 EE E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 E2 7F FF 00 (chan 57)
15 03 79 FB E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 E4 7F FF 00 (chan 4F)
15 03 03 E5 E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 EA 7F FF 00 (chan 12)
15 03 FB AF E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 E7 7F FF 00 (chan 14)
15 03 2A E2 E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 EA 7F FF 00 (chan 51)
15 03 F2 4F E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 EC 7F FF 00 (chan 4D)
15 03 61 EF E8 1F E8 1F F0 01 00 0A 12 80 00 46 33 08 EF 7F FF 00 (chan 10)
15 03 FD BD E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 5D)
15 03 EA DC E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 20)
15 03 59 65 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 32)
15 03 B5 4F E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 EF 7F FF 00 (chan 6F)
15 03 09 05 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 71)
15 03 67 2D E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 34)
15 03 C8 E9 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F5 7F FF 00 (chan 75)
15 03 A5 50 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F2 7F FF 00 (chan 38)
15 03 7D 6B E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 FA 7F FF 00 (chan 16)
15 03 83 21 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 F7 7F FF 00 (chan 53)
15 03 D5 21 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 FD 7F FF 00 (chan 77)
15 03 5A 5B E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 FD 7F FF 00 (chan 59)
15 03 E2 97 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 08 FA 7F FF 00 (chan 1C)
15 03 CB 4C E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 09 05 7F FF 00 (chan 18)
15 03 60 4D E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 09 07 7F FF 00 (chan 55)
15 03 B5 D1 E8 1F E8 1F F0 01 00 0A 12 80 00 46 32 09 02 7F FF 00 (chan 22)

Does RedLINK use the IEEE 802.15.4 standard, like ZigBee?

If so, then the packet format after the length byte would need to be like this:



"All frame formats in this subclause are depicted in the order in which they are transmitted by the PHY, from left to right, where the leftmost bit is transmitted first in time. Bits within each field are numbered from 0 (leftmost and least significant) to $k - 1$ (rightmost and most significant), where the length of the field is k bits. Fields that are longer than a single octet are sent to the PHY in the order from the octet containing the lowest numbered bits to the octet containing the highest numbered bits."

I'm not sure how to interpret that because I don't know which way the TI CC1101 chip sends. But of the four interpretations of the 0x2330 frame control we see (23 30, 30 23, bits reversed or not), the only one that has no bits in reserved fields on is 001 1 0 0 0 000 10 00 11, which means "data packet, security enabled, 16-bit dst addr, 64-bit src addr". It seems unlikely that the address sizes would be different. And that only leaves 5 bytes of payload.

So I don't think RedLINK is using 802.15.4.