

## Challenges in capturing and analyzing ZigBee RF4CE networks

November 26, 2009

ZigBee RF4CE (RF for Consumer Electronics) is a new standard for enhanced control of home entertainment devices. With RF technology, larger range, higher flexibility, and enhanced topologies are supported.

As with any new standard, especially such that involves multi-vendor large scale consumer products, being able to quickly identify interoperability problems and implementation issues is an important requirement.

Unlike infrared controls that are limited by line of sight, when RF is involved, interference as well as coexistence of several networks in the same proximity (e.g. neighboring apartments, different rooms) imposes additional implementation challenges.

When looking for professional RF4CE analysis tools, on top of regular analysis features that allow understanding network topology, transactions, look into message details, etc, the above issues must be well addressed.



**Figure 1 – Analyzing a simple RF4CE network**

### **Use of multiple RF channels**

The ZigBee RF4CE uses the unlicensed ISM (Industrial Scientific Measurement) 2.4 Ghz frequency band. This band defines 16 possible channels. However, keeping in mind that typical RF4CE equipment will work in consumer in-door environment, that is most likely to have WiFi equipment, the 3 channels that are less affected by WiFi were chosen as possible RF4CE channels – i.e. channels 15, 20 and 25:

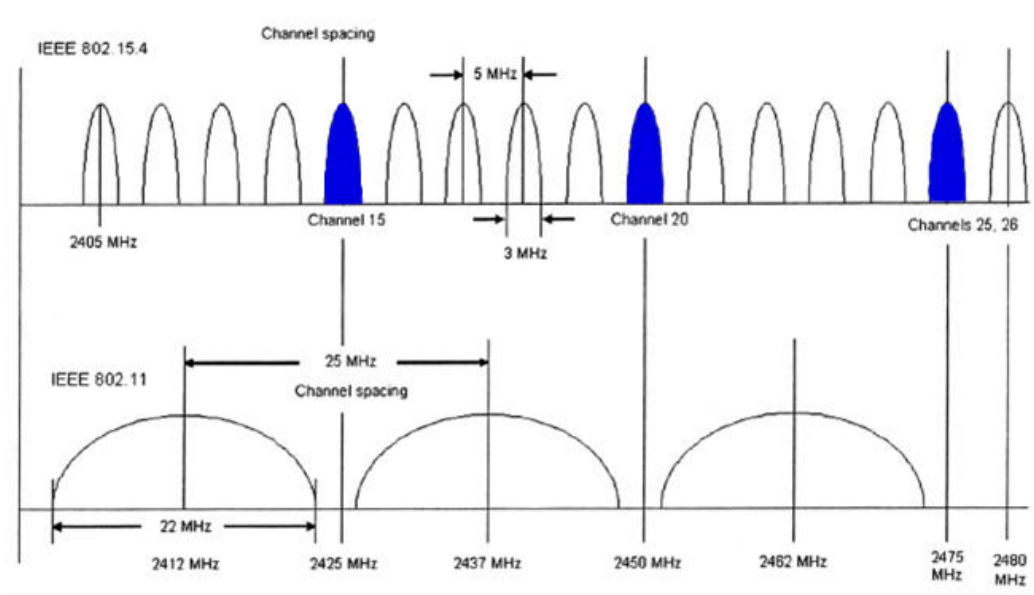


Figure 2 – RF4CE 2.4GHz band channel allocation

The selection of the RF4CE channel to be used can be done in one of the following methods:

- Hard coded, as preconfigured in the factory.  
This method is not good practice because it is not robust to interference that may cause problems on this specific channel. It also doesn't allow for interoperability between different vendor equipments that are not likely to have the same channel hard coded.
- Manual selection  
Let the user configure the right channel in all relevant equipment. This is unpractical
- Automatic selection  
Let the RF4CE units select the channel randomly, and change it from time to time to overcome potential interference. This is the most suitable method

In order to analyze the traffic in the network, the analyzer needs to 'listen' to the right channel. However if the network under test chose the channel randomly, the only way for a single channel analyzer to find this channel is by scanning the possible channels for traffic. Therefore the first messages transmitted in the network may not be received by the analyzer that is currently scanning other channels. Furthermore the analyzer has no way to indicate that the network has switched to a different channel.

In order to overcome this problem, and to allow analysis of the channel selection process (e.g. device sending beacon request or discovery request channel by channel looking for a reply) a multi-channel analyzer should be used.

In the RF4CE case, a 3 channel analyzer will capture data from channels 15, 20, and 25 simultaneously. Such an analyzer not only is able to capture the channel selection process but also enables to easily examine and understand a system under test that is switching between different channels.

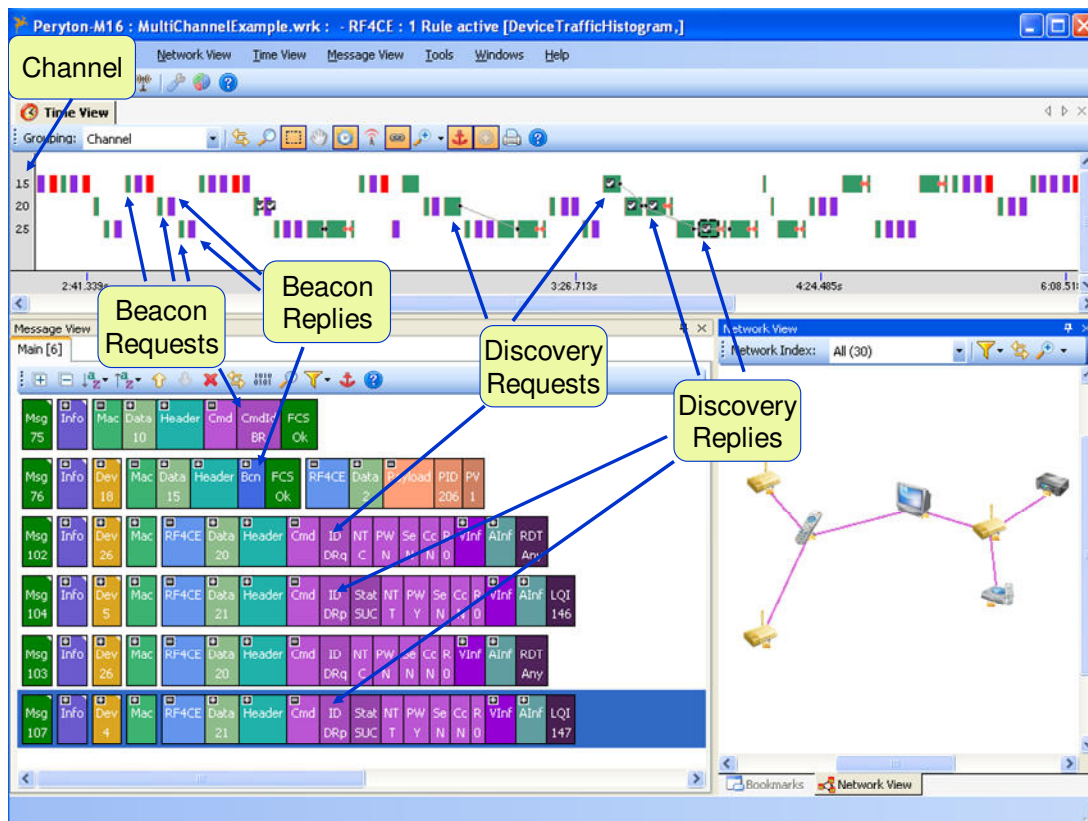


Figure 3 – RF4CE beacon and discovery requests over multiple channels

## Encryption

RF4CE uses AES-128 encryption and authentication to secure message content and guarantees that only the authorized device can control the appliance.

In order to allow this level of encryption, both parties participating in the connection should have the same, 128 bit long, encryption key.

Being impractical for the user to enter such a long key, the RF4CE uses automatic key generation. I.e. one of the parties randomly selects a key, and sends it to the other party as part of the pairing process.

Since sending a key over the air is a major weakness of the encryption process, the key is hidden in a list of long random key-seed numbers exchanged between the parties. Each key-seed is 80 bytes long, and the number of such key-seeds is set by the implementation. Typical numbers are 4, 16 or 64 key-seeds.

The devices exchanging the key uses the 802.15.4 MAC acknowledge service to make sure all key-seeds messages well received by the other party. A message that was not received is retransmitted (with a new random number).

When looking to analyze secure RF4CE communications, the analyzer must have the encryption key. Therefore it must intercept all key-seed messages. If even one key-seed message is missed by the analyzer it will not be able to decode the communication between the devices.

However, in an RF environment, and especially in in-door environment with multi-path and other interference sources, this is not a simple task. A typical link is expected to have between 1% to 10% packet loss ratio or even higher given the length of each key seed message (~1000bits).

The following table summarizes the analyzer chances to receive all key-seed messages for 4, 16, 32 and 64 seeds cases, given 1% or 10% packet loss:

# of key seed messages	1% packet loss	10% packet loss
4	96%	66%
16	85%	19%
32	72%	3%
64	53%	0.1%

**Table 1 – a single receiver analyzer key interception probability**

We see that if 64 key-seeds are chosen by the system, the analyzer has less than a 50% chance to intercept the key.

In smaller seed numbers, in hard RF environment, only one of 5 or more key exchanges will be well intercepted by an analyzer.

These results make it barely unpractical to analyze secure RF4CE networks.

**The solution** for that is using an analyzer with multiple receivers implementing **diversity algorithms**. In an 2.4 Ghz indoor environment, the use of 2 receivers rather than one, positioned in a distance of 6.5cm or more from each other, is expected to **reduce the packet loss by a factor of 10**.

The following table summarizes a diversity enabled analyzer chances to receive all key-seed messages for 4, 16, 32 and 64 seeds cases, given 0.1% or 1% packet loss:

# of key seed messages	0.1% packet loss	1% packet loss
4	99.6%	96%
16	98%	85%
32	97%	72%
64	94%	53%

**Table 2 – a diversity enabled analyzer key interception probability**

We can see that in a normal indoor environment, with 0.1% packet loss probability (using diversity), the worth case is not intercepting one out of 20 key exchange sessions.

Comparing this with a single antenna analyzer we can see that diversity is an essential analyzer feature when looking to analyze secured RF4CE traffic.

### **Coexistence**

Given the nature of the RF communication, and its use in consumer electronics, multiple networks are likely to operate in a close proximity – neighboring apartments, different rooms in the same house etc.

When looking to analyze RF4CE networks, the user has two conflicting needs. The first is to be able to see only the relevant network and to filter all non relevant traffic. The second is to be able to see if other network traffic is the cause for problems detected in the system under test.

In order to achieve these two conflicting goals, the RF4CE analyzer needs to capture all messages regardless of their source and save them into a data file. Yet when displaying the messages to the user it should enable smart filtering driven by the

specific scenario. Such filtering may be done according to network ID, manufacturer ID, reception level, and more. The filtering mechanism should allow maximal flexibility and refrain from limiting the user to a single specific field. For example the user may want to see all messages with RSSI (Received Signal Strength Indicator) above some threshold, plus all messages in a specific network ID plus all messages with unknown network ID.

### **Summary**

Analyzing RF4CE networks brings some unique challenges on top of 'regular' analysis issues.

A good RF4CE analyzer must include, on top of the regular analysis features, the ability to simultaneously capture data from 3 channels, the use of diversity for decreased packet loss, and enhanced filtering.