UG103.10: RF4CA Fundamentals

This document describes the ZigBee RF4CE specification, with notes about considerations when implementing an RF4CE solution. It includes a basic description of RF4CE device types, the network formation process, power saving, and security.

Silicon Labs' *Application Development Fundamentals* series covers topics that project managers, application designers, and developers should understand before beginning to work on an embedded networking solution using Silicon Labs chips, networking stacks such as EmberZNet PRO or Silicon Labs Bluetooth Smart, and associated development tools. The documents can be used a starting place for anyone needing an introduction to developing wireless networking applications, or who is new to the Silicon Labs development environment.

KEY POINTS

- RF4CE devices
- Network formation
- Topology
- Power saving
- Security
- Transmission modes
- Frequency agility
- Profiles

1. Introduction

The ZigBee RF4CE specification describes mechanisms for building remote control (RC) networks for simple, robust, low cost communication for consumer electronic (CE) devices. RF4CE provides simple networking and application layers on top of the IEEE 802.15.4 standard in the 2.4 GHz frequency band. A multiple star network topology is used in RF4CE with a variety of transmission options including both broadcast and unicast with optional MAC-level acknowledgement and optional network-level security. Frequency agility and standard power saving mechanisms help ensure that RF4CE products are able to meet consumer expectations for reliability and long life. These features together enable manufacturers to build a diverse range of remote control products, including home entertainment devices and keyless entry systems. At the discretion of the application, RF4CE networks are multi-vendor interoperable. A number of ZigBee-developed application profiles as well as manufacturer-specific profiles are already available.

2. Definitions

- Controller – a network participant that has ZigBee RF4CE functionality
- Originator – the device from which a transmission is sent
- Recipient – the device to which a transmission is sent
- Target – a network coordinator that has ZigBee RF4CE functionality

3. Devices

RF4CE networks consist of controller nodes and target nodes. The fundamental difference between these two device types is that targets may create their own networks while controllers are only capable of joining existing networks. In ZigBee PRO terms, controllers are roughly analogous to end devices while targets are more similar to coordinators.

3.1 Controllers

Controllers are network participants, which means they can join existing networks. An example of a controller device is a handheld remote control for a television or set-top box. Consumers will typically interact with a controller to operate a target some distance away. Before communicating with other nodes, controllers must first join to an existing network using a discovery and pairing process described in section 4. Network Formation.

Controllers are frequently battery operated and therefore usually operate in a low power mode in order to meet consumer expectations for battery longevity. The RF4CE specification offers a specific power saving mechanism to allow nodes to sleep for extended periods while still allowing other nodes to communicate with them. A node that wishes to conserve power will enable its receiver for some duration within a larger period. The duty cycle of sleepy nodes helps them save power while also facilitating communication to them by other nodes in the network. Power saving is described in more detail in section 6. Power Saving.

Because most actions begin with a user operating a controller, controllers often perform the originator role in RF4CE networks and the terms “controller” and “originator” are frequently synonymous. This is not always the case, however, so care must be taken not to conflate the two concepts.

3.2 Targets

Targets are network coordinators, which mean they can create new networks. In addition to being capable of forming networks, targets may also join networks created by other targets. The equivalent in ZigBee PRO is a coordinator that may choose to join an existing network as a router instead of forming its own network. The ability to form a network is the key distinction between a controller and a target, but it is important to remember that either device type can join a network.

Typical examples of a target device are televisions or set-top boxes. These types of products are often packaged with a dedicated remote control from the same manufacturer. The product itself plus its dedicated remote control comprise the most basic example of a complete RF4CE network. A television, for example, would create a network in which to operate and the included remote control would join to that network in order to interact with the television. The network parameters could be specified during production so the two products are already joined together before reaching the consumer or the network creation and the joining process could be completed during an initial setup procedure initiated by the consumer.

Targets frequently perform the recipient role in RF4CE networks. As before, it is important to remember that “target” and “recipient” are not always synonymous. It is possible for a target to have its own network and to be joined with another network created by a separate target. For example, a set-top box will typically have its own network with its own dedicated remote. It may also join to the network of the television to which it is physically connected. In a setup like this, the set-top box would be the recipient on its own network and an originator on the network belonging to the television.

4. Network Formation

RF4CE networks consist of one or more devices paired to a target. The network joining process is comprised of two distinct steps: discovery and pairing. The discovery procedure is used to identify targets within radio range. Once a potential target is identified, the pairing process is used to join with that device. Discovery usually precedes pairing, but a device is free to pair with other devices whose identities are made known to it through out-of-band means. For example, a bar code printed on a set-top box may provide the information to a remote control for pairing.

4.1 Discovery

Discovery is the process by which devices learn about other devices in the vicinity. Its primary purpose is to identify targets with which to pair. The device that initiates discovery is known as the originator while devices that are discovered are known as recipients. Typically, discovery is performed by controllers, but targets are permitted to act as originators as well.

During discovery, the originator periodically transmits discovery request messages on each of the RF4CE channels. These messages are typically directed to all nodes within range, but may also be transmitted to a specific node or to all nodes within an existing network. The discovery request includes information about the originator, including its capabilities and vendor information. Additionally, the originator specifies which application device types it is attempting to discover. A multi-function remote control, for example, may wish to discover only televisions.

Because ZigBee RF4CE does not have parent-child relationships like in ZigBee PRO, discovery can only identify other nodes that have their receiver enabled and are within immediate range of the originator. Originators are free to repeat discovery until an application- or profile-specific condition has been satisfied. For example, discovery may continue for a fixed duration or until some number of responses have been received. Repeating the discovery process increases the likelihood of locating devices within range.

When a target receives a discovery request, it examines the originator information and the requested application device type contained in the request in order to determine whether to respond. A set-top box, for example, should not to respond to a discovery request for a television. Similarly, a device may choose to respond only to requests from the same manufacturer. Ignoring discovery requests is one way that a target can exert control over the devices that join its network.

If a target decides to respond to a discovery request, it transmits a discovery response back to the originator. The response includes information about the recipient, including its capabilities and application device type.

Targets may also enable an automatic discovery mode. When activated, the stack will automatically determine whether to respond to discovery requests based on whether the capabilities advertised by the originator and the requested application device type are compatible with the local node. If so, the stack will automatically respond with the information for the local node. Otherwise, the stack will ignore the request. Automatic discovery mode ends after an application-specified duration or if a response is sent, whichever comes first.

As the originator receives discovery responses from recipients, it uses the recipient information to decide whether the recipient is an acceptable target. At the conclusion of the discovery process, the application will have collected a list of potential targets. Typically, the originator will attempt to pair with one or more of the targets in the list. The decisions about which targets are acceptable and whether to proceed to pairing are application and profile specific.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.