ZigBee®

Control your world™

July 2009

Understanding ZigBee RF4CE

Foreword

Since its inception, the ZigBee Alliance has worked with a singular focus: create a much needed global wireless language capable of giving "voices" to the myriad of everyday devices which surround us as we go about our daily lives. This focus has been aimed at the little devices, often overlooked in an IT centric world, such as light switches, thermostats, electricity meters, remote controls as well as more complex sensor devices found abundantly in the health care, commercial building and industrial automation sectors. As a result, ZigBee Alliance members have created a wireless standard offering extraordinary control, expandability, security, ease-of-use and the ability to use ZigBee technology in any country around the world.

Today, organizations use ZigBee to effectively deliver solutions for a variety of areas including consumer electronic device control, energy management and efficiency, home and commercial building automation as well as industrial plant management. With this comprehensive set of attributes, the nonprofit, open membership and volunteer driven Alliance has become a thriving ecosystem of more than 300 members. As an ecosystem, the Alliance offers everything prospective product and service companies need to develop ZigBee products and services and benefit from the Alliance's competitive and stable supply chain.

Executive Summary

Infrared (IR) remote controls have been around since the late 1970s and have simplified the control of many devices. While widely deployed, IR remotes have a number of limitations and can prove difficult to use with large screen high-definition televisions because of high intensity light emitted from the screen. Other issues with these remotes include field-of-vision limits, line-of-sight restrictions and one-way communications. With the growth and increasing sophistication of today's consumer electronics, new trends in electronics storage, IR remotes are losing their effectiveness and limiting innovation.

Replacing decades old IR technology with the ZigBee RF4CE radio frequency (RF) standard will improve product robustness and user experience. Devices using the standard will free consumers from pointing a remote at an exact target, allowing them to more easily control entertainment equipment accurately and easily. Devices will confirm to the remote control that a command was executed, no longer making the consumer repeatedly hit buttons to execute a command. This two-way communication provides the consumer electronics industry with a new platform and standard designed to accommodate growth beyond traditional device control. Ultimately, these new capabilities will spur innovation and integration with other automation devices using ZigBee technology.

Consumer electronics based on ZigBee RF4CE will be part of a growing ZigBee presence in homes. ZigBee has already emerged as the preferred solution in three major markets; energy, home automation and health care. The ZigBee Smart Energy, ZigBee Home Automation and ZigBee Health Care public application profiles address each of those verticals and are focused on improving consumer's lives by helping them save time, money, improve energy efficiency and live longer independent lives.

Table of Contents

List of Figures

High-level overview

- Based on the 2.4GHz PHY/MAC IEEE 802.15.4 standard.
- The networking layer is thin, flexible and future-proof.
- Co-existence with other 2.4 GHz technologies is built-in through techniques as defined in the IEEE 802.15.4 standard and ZigBee RF4CE's advanced channel agility mechanism.
- A simple and intuitive pairing mechanism defined for establishing communication links.
- Support for multiple communication types.
- Power management mechanism included in network layer for power efficient implementations.
- The standard ensures that ZigBee RF4CE implementations will co-exist.
- The ZigBee RF4CE specification allows for both public application profiles and manufacturer specific profiles or transactions.
- Support for different applications through application layer profiles ensuring device interoperability.

Technical Summary

1. Introduction

The ZigBee RF4CE specification defines a simple, robust and low-cost communication network that allows wireless connectivity in consumer electronics applications. The ZigBee RF4CE specification enhances the IEEE 802.15.4 standard by providing a simple networking layer and Alliance developed public application profiles that can be used to create multi-vendor interoperable solutions for use within the home.

Some of the characteristics of a ZigBee RF4CE network are as follows:

- Operation in the 2.4GHz frequency band according to IEEE 802.15.4.
- Channel agile solution operating over three channels.
- Incorporates power management mechanism for all device classes.
- Discovery mechanism with full application confirmation.
- Pairing mechanism with full application confirmation.
- Multiple star topology with inter-PAN communication.
- Various transmission options including unicast, broadcast, acknowledged, unacknowledged, secured and un-secured.
- Security key generation mechanism.
- Utilizes the industry standard AES-128 security scheme.
- First public application profile targeted towards remote control applications.
- Allows for manufacturer specific profiles to be added.

2. Network topology

A ZigBee RF4CE PAN is composed of two types of devices: a target device (or node) and a controller device (or node). A target device has full PAN coordinator capabilities and can start a network on its own right. A controller device can join networks started by target devices by pairing with the target. Multiple ZigBee RF4CE PANs form a ZigBee RF4CE network and devices in the network can communicate between ZigBee RF4CE PANs.

In order to communicate with a target device, a controller device first switches to the channel and assumes the PAN identifier of the destination

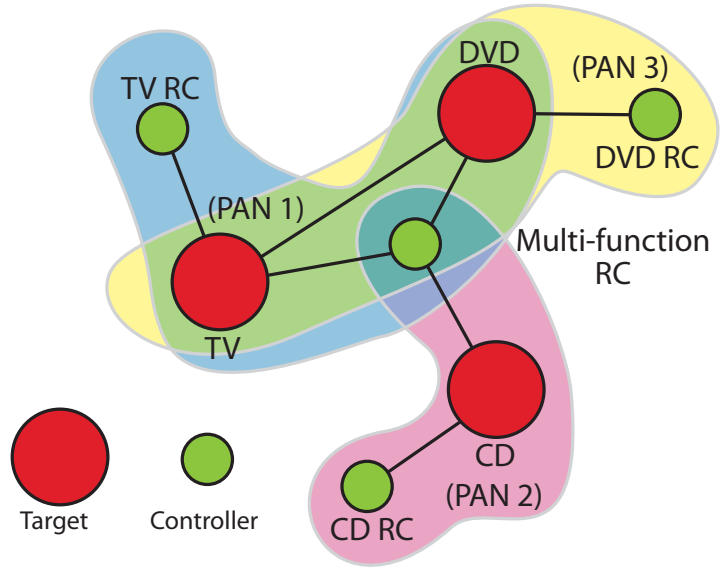

Figure 1 - Example ZigBee RF4CE network topology

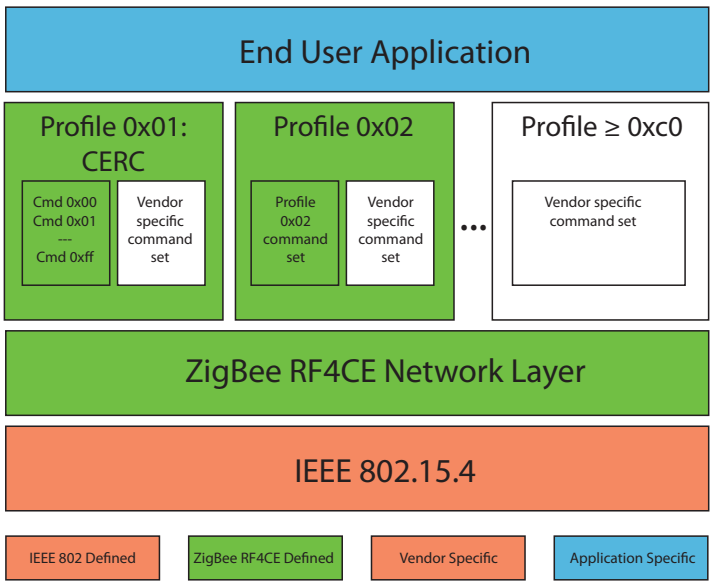

Figure 2 - The ZigBee RF4CE specification architecture

ZigBee RF4CE PAN. It then uses the network address, allocated through the pairing procedure, to identify itself on the ZigBee RF4CE PAN and thus communicate with the desired target device.

Figure 1 illustrates an example ZigBee RF4CE topology which includes three target devices: a TV, a DVD and a CD player and each target device creates its own ZigBee RF4CE PAN. The TV, DVD and CD player also have dedicated Remote Control's which are paired to each appropriate target device. A multi-function Remote Control, capable of controlling all three target devices itself, is added to the network by successively pairing to the desired target devices.

As a consequence, this ZigBee RF4CE network consists of three separate ZigBee RF4CE PANs: one managed by the TV (PAN 1), containing the TV Remote Control and the multi-function Remote Control; a second managed by the CD player (PAN 2), containing the CD Remote Control and the multi-function Remote Control and a third managed by the DVD (PAN3), containing the DVD Remote Control and the multi-function Remote Control.

3. Architecture

The ZigBee RF4CE architecture is defined in terms of a number of blocks or layers in order to simplify the specification. Each layer is responsible for one part of the specification and offers services to the next higher layer and utilizes services from the next lower layer. The interfaces between the layers serve to define the logical links that are described in this specification. The layout of the layers is based on the open systems interconnection (OSI) seven-layer model.

Figure 2 illustrates the ZigBee RF4CE Stack architecture. The ZigBee RF4CE specification is designed to be built onto the IEEE 802.15.4 standard MAC and PHY layers and provides networking functionality and public application profiles which can interface to the end user application. Manufacturer specific extensions to public application profiles can be defined by sending vendor specific data frames within the profile. In addition, manufacturer specific profiles can also be defined.

4. The ZigBee RF4CE NWK layer

The NWK layer provides two services: the NWK layer data service, interfacing to the NWK layer data entity (NLDE) and the NWK layer management service, interfacing to the NWK layer management entity (NLME). These services are accessed through the NWK layer data entity SAP (NLDE-SAP) and the NWK layer management entity SAP (NLME-SAP).

The NWK layer data service enables the transmission

and reception of NWK protocol data units (NPDUs) across the MAC data service. The NWK layer management service permits service discovery, pairing, unpairing, receiver control, device initialization and NIB attribute manipulation.

2.4 GHz band frequencies

A ZigBee RF4CE device operates in the 2.4GHz frequency band, as specified by IEEE 802.15.4. However, to provide robust service against other common sources of interference in this band, only a small subset of channels is used - channels 15, 20 and 25. A target device can choose to start its network on the best available channel at startup time and so a ZigBee RF4CE network may operate over one or more of the available three channels.

Channel agility

All ZigBee RF4CE devices support channel agility across all three permitted channels. As described above, a target device selects its own initial channel, based on the channel conditions during startup. During the course of the life of the target device; however, the channel conditions may vary and the target device can elect to switch to another channel to maintain a high quality of service.

Each device paired to the target records the channel on which communication is expected. However, in the event that the target switches to another channel, the device can attempt transmission on the other channels until communication with the target is reacquired. The device can then record the new channel accordingly for the next time communication is attempted.

Node initialization

A ZigBee RF4CE device initializes itself according to whether it is a target or a controller. Controller devices simply configure the stack according to this standard and start operating normally. Target devices configure the stack and then attempt to start a network.

To do this, the target device first performs an energy detection scan that allows it to obtain information on the usage of each available channel, thereby allowing it to select a suitable channel on which to operate. The target device then performs an active scan allowing it to determine the identifiers of any other IEEE 802.15.4 PANs (ZigBee RF4CE or other ZigBee networks) operating on the selected channel, thus allowing a unique PAN identifier to be selected for its network. The target device then begins operating normally.

Power saving

Power saving is an important consideration for a ZigBee RF4CE device. As a consequence, the specification defines a power save mechanism that allows both controller devices as well as target devices to manage their power consumption by entering a power saving mode. The power saving mechanism is under the control of each public application profile.

A device can manipulate its receiver in a number of ways:

- The receiver can be enabled until further notice (e.g. when a TV comes out of standby).
- The receiver can be enabled for a finite period (e.g. when a TV enters standby mode and wants to engage the power saving mode).
- The receiver can be disabled until further notice (e.g. when a remote control enters a dormant state due to none of its buttons being pressed) When the power saving mode is engaged, the receiver is enabled for an application defined duration (known as the active period) and then disabled. This mechanism is then repeated at an application defined interval (known as the duty cycle). Other devices can still communicate with a device in power saving mode by targeting the transmission during the active period. The result is a device that periodically enables its receiver for only a short time, allowing it to conserve power while remaining active on the network.

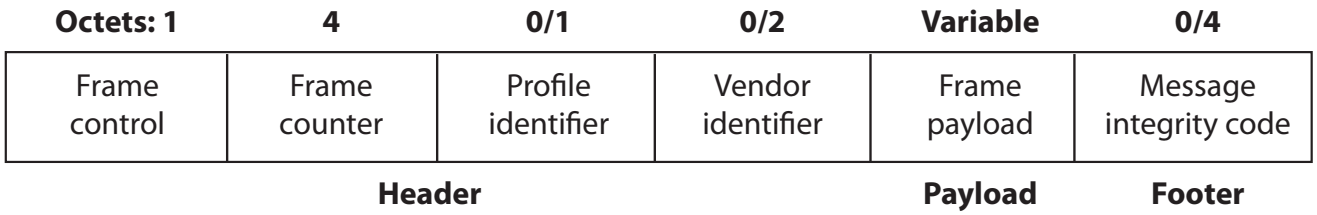

Figure 3 - General schematic view of a NWK frame

NWK frames

The ZigBee RF4CE NWK layer defines three frame types: standard data, network command and vendor specific data. Standard data frames transport application data from public application profiles. Network command frames transport frames that allow the network layer to accomplish certain tasks such as discovery or pairing. Vendor specific data frames transport vendor specific application data. The general NWK frame format is illustrated in Figure 3.

The fields of the general NWK frame are described below:

- Frame control: control information for the frame
- Frame counter: incrementing counter to detect duplicates and prevent replay attacks (security)
- Profile identifier: the application frame format being transported
- Vendor identifier: to allow vendor extensions
- Frame payload: contains the application frame
- Message integrity code: to provide authentication (security)

Transmission options

The ZigBee RF4CE specification defines a number of transmission options that can be used by an application and combined as appropriate. Each transmission can be sent secured or un-secured.

- Acknowledged: Originator data is confirmed by the recipient
- Unacknowledged: Originator data is not confirmed by the recipient
- Unicast: Originator data is sent to a specific recipient
- Broadcast: Originator data is sent to all recipients
- Multiple channel: Originator attempts transmission using frequency re-acquisition mechanism
- Single channel: Originator attempts transmission on the expected channel

Discovery

A ZigBee RF4CE device can perform discovery in an attempt to find other suitable devices that can be paired to. Discovery can be attempted repeatedly on all three channels for a fixed duration or until a sufficient number of responses have been received. Service discovery is only available to devices that are not currently in power saving mode. During discovery, a number of pieces of information are exchanged between both devices. This information is passed to the application which can then make a decision whether it should respond. The information exchanged is as follows:

- Device capabilities: The type of the device (i.e. target or controller), whether the device is mains or battery powered and level of security.
- Vendor information: The ZigBee RF4CE allocated vendor identifier and a freeform vendor string

specifying vendor specific identification (e.g. a serial number).

- Application information: A short user defined string which describes the application functionality of the device (e.g. "lounge TV"), a device type list specifying which types of device are supported (e.g. a combo device may support both "TV" and "DVD" functionality) and a profile identifier list specifying which public application profiles are supported by the device (e.g. an public application profile or a manufacturer specific profile).
- Requested device type: The type of device being requested through the discovery (e.g. a multifunction remote control may be searching for "TV" functionality).

Pairing

Once a device has determined, through discovery, that there is another device within communication range offering compatible services, it can set up a pairing link in order to begin communication. Nodes within a ZigBee RF4CE network may only communicate directly with other devices on the network if a pairing link exists between the originator and the target devices.

A pairing link can be established on request from the application by exchanging a similar set of information as was exchanged during discovery. The application on the target device can choose whether to accept the pair (e.g. only if it has capacity to store the pairing link) and confirms the pairing request back to the originator device.

If the pairing request was successful, both devices store a pairing link in their respective pairing tables. This allows an originator to communicate with a target and the target to communicate back to the originator. Each entry in the pairing table contains all the information necessary for the network layer to transmit a frame to the target device. This removes the burden of addressing, etc. from the application layer which can simply supply an index into the pairing table in order to communicate with another device.

Each entry in the pairing table contains the following information:

- Pairing reference
- Source network address
- Destination logical channel
- Destination IEEE address
- Destination PAN identifier
- Destination network address
- Recipient device capabilities
- Recipient frame counter
- Security link key

Security

The ZigBee RF4CE specification provides a cryptographic mechanism to protect the transmissions. This mechanism provides the following security services:

- Data confidentiality: To ensure that the data contained in a ZigBee RF4CE transmission can only be disclosed to the intended recipient.
- Data authenticity: To ensure that the intended recipient of a ZigBee RF4CE transmission knows that the data was sent from a trusted source and not modified during transmission.
- Replay protection: To ensure that a secure transmission cannot simply be repeated by an attacking device if overheard.

128-bit cryptographic keys are generated by each end of a pairing link and stored in the pairing table for future use.

5. The ZigBee RF4CE application layer

The application layer of a ZigBee RF4CE device is composed of a profile component and an application specific component. The profile component can be thought of as a common language that devices implementing the profile exchange to accomplish certain tasks, e.g. switching the channel on a TV, and allows for interoperability between devices. The application component is provided by the end manufacturer in order to add specific functionality to the commands request through the profile.

The ZigBee RF4CE specification defines Alliance developed public application profiles, but also permits vendors to either extend public application profiles or to define completely proprietary profiles. This first defined public application profile defines commands and procedures to enable consumer electronic devices (e.g. a TV, DVD or CD player) to be controlled by remote control devices.