Relationship between the Wize Protocol and Wireless M-Bus

By P. M. Evjen

The Wize Protocol is a new wireless LPWAN network standard for Industrial IoT applications based on Wireless M-Bus at 169 MHz. This brief note will describe some of the commonalities and differences between the two.

Introduction

The Wize protocol is the result of the development of a new LPWAN (Low Power Wide Area Network) solution based on Wireless M-Bus at 169 MHz. The technology was first utilized and developed for gas and water metering in France. Now this technology is made available for a wider market, not only in France and not only within smart metering, but in Smart City and Industrial IoT applications in general.

The Wize protocol provides

- Robust communication and wide area coverage using VHF frequency
- Secure transfer of data in terms of privacy, data integrity and authentication
- A low power battery operated solution with lifetime > 15 years
- A proven solution based on the established Wireless M-Bus standard
- Firmware download over-the-air as an integral part of the protocol

In this short paper we will look at some of the commonalities and differences between Wize and Wireless M-Bus protocols. In summary, the main differences are

- Introduction of a priority bit in the C-field of the Link Layer
- The Link Layer Address always using the device address
- A new Wize Application Layer protocol with encryption and authentication
- A ping/pong mechanism for installation
- A new firmware download OTA protocol

Physical layer

The Wize protocol use the Wireless M-Bus mode N as physical layer. It is a narrowband radio (12.5 kHz channels) in the VHF frequency band at 169 MHz with up to 500 mW output power. This is a license free band in Europe. The data rates of 2.4, 4.8 and 6.4 kbps can be used in Wize.

The low data rates in a narrowband radio channel, together with the relative low operating frequency (169 MHz) and high transmission power, is the fundamental key to the long range that can be achieved with Wireless M-Bus mode N and Wize. Even kilometres in urban areas, with deep penetration into buildings and other “hard to reach” places.

Medium access and Link Layer

The medium access of Wize is the same as for Wireless M-Bus, which means to transmit at “any time”. Usually periodic transmissions of utility data are used, typically every few hours, but with a random factor to avoid successive collisions. Alarms may be transmitted immediately.

The link layer of Wize is the same as Wireless M-Bus with some exceptions. Wize redefines the C-field to signal priority frames, which the concentrator should process immediately.

As for two-way communication the (battery operated) device turn on the receiver 5 seconds after a transmission. This corresponds to the default response delay in the wireless M-Bus protocol. However, the frequent access protocol of Wireless M-Bus is not supported in Wize, only allowing one command/response sequence in each session.

The biggest difference between Wize and the standard Wireless M-Bus Link Layer is the use of the address field, whereas Wize relies on the same definition as in the 2005 (initial) revision of the standard. In this case the device address is used as the Link Layer Address in both directions. There is no real big impact of this change, other than that the frames from concentrator to device can be made shorter (no “source” address).

Application layers

As Wize was originally introduced and used for gas meters and water meters, two specific application protocols were invented for this purpose. The Wize protocol hooks into the M-Bus protocol by the Control Information field (CI-field), which is always set to 20h to signal the Wize protocol.

Inside the Wize protocol several “applications” are defined by the L6App field (00h is water, 01h is gas etc.). In addition to gas and water, new application layers are being defined, both generic and allowing manufacturer specific. One of the generic application frames are based on the M-Bus application layer using DIF and VIFs as descriptors.

For legacy systems using the M-Bus protocol, or even a manufacturer specific application layer, there is therefore a simple way to migrate these over to Wize.

Installation

The Wize protocol use the SND-IR (Installation Request) and CFR-IR (Confirm Installation) in a special Ping-Pong sequence. After the device has transmitted a Ping (SND-IR), all concentrators receiving this message can answer back with the Pong (CFR-IR) within a few seconds at a random time. The device will after that report the signal quality of each concentrator link, for the system to decide which concentrator to use for the best connection.

Security

Although Wireless M-Bus offers several security modes, the Wize protocol defines its own transport layer (sometimes referred to as the presentation layer) that provides the security services of privacy, integrity, authentication and protection against replay.

The security is based on AES-128 using the CTR mode for encryption and CMAC for authentication. Actually, there are two authentication hash tags appended to the message; one is used by the base station to authenticate and allow messages for further processing, and the other is an end-to-end authentication. Each message is using a unique message counter and a time stamp based on an EPOCH second counter.

Firmware download

Wize has introduced a new protocol for firmware download over the air (OTA). Only the original physical layer is used, but the rest of the protocol is optimised for the purpose of transferring large firmware images.

The firmware downloads over-the-air use a broadcast protocol to update multiple devices in parallel. First, all devices that are intended for the FW upgrade are notified on a one-to-one basis about the rendezvous time at which the broadcast transmission start. A large number of devices can therefore be upgraded in a short time, utilizing the somewhat narrow bandwidth

available. The same physical layer as Wireless M-Bus is used, but a new frame format has been defined for the download messages as indicated by the length field = FFh. The download then takes place in the “blackout period”, typically lasting 4 hours during the night, where no Wize devices are allowed to transmit in order not to interfere with the download.

The download frames include redundant data to provide Forward Error Correction. A Reed-Solomon block code is used for this purpose.

The Wize module solution

Radiocrafts is the first to offer a complete and compact Wize radio modem module, the RC1702HP-WIZE. It is based on the Wireless M-Bus 169 MHz product portfolio consisting of the RC1701HP-MBUS4 radio modem, RC1701HP-MPC1 pulse counter, and RC1701HP-MSM sensor interface module.

With the same UART communication interface as MBUS4, it offers an easy way to migrate products to the new Wize protocol.

Radiocrafts also offers customized solutions based on the Wize protocol including hardware and the firmware with a complete application for installation, meter/sensor data acquisition, command/response for reading/writing parameters, and firmware upgrade over-the-air.

Please visit Radiocrafts webpages for more information. www.radiocrafts.com

Document Revision History

Document Revision	Changes
0.1	Draft
1.0	First release

Disclaimer

Radiocrafts AS believes the information contained herein is correct and accurate at the time of this printing. However, Radiocrafts AS reserves the right to make changes to this product without notice. Radiocrafts AS does not assume any responsibility for the use of the described product; neither does it convey any license under its patent rights, or the rights of others. The latest updates are available at the Radiocrafts website or by contacting Radiocrafts directly.

As far as possible, major changes of product specifications and functionality, will be stated in product specific Errata Notes published at the Radiocrafts website. Customers are encouraged to check regularly for the most recent updates on products and support tools.

Trademarks

RC232™ is a trademark of Radiocrafts AS. The RC232™ Embedded RF Protocol is used in a range of products from Radiocrafts. The protocol handles host communication, data buffering, error check, addressing and broadcasting. It supports point-to-point, point-to-multipoint and peer-to-peer network topologies.

ZigBee® is a registered trademark of the ZigBee Alliance

All other trademarks, registered trademarks and product names are the sole property of their respective owners.

Life Support Policy

This Radiocrafts product is not designed for use in life support appliances, devices, or other systems where malfunction can reasonably be expected to result in significant personal injury to the user, or as a critical component in any life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness. Radiocrafts AS customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Radiocrafts AS for any damages resulting from any improper use or sale.

Contact Information

Web site: www.radiocrafts.com
Email: radiocrafts@radiocrafts.com

Address:
Radiocrafts AS
Sandakerveien 64
NO-0484 OSLO
NORWAY

Tel: +47 4000 5195
Fax: +47 22 71 29 15
E-mail: sales@radiocrafts.com