Part V ECHONET Lite System Design Guidelines

Revision History

・Version 1.00 Draft	9 March 2011	Released / Open to the Consortium Members
・Version 1.00	30 June 2011	Open to the Consortium Members
	3 September 2012	Open to the public

Contents

Chapter 1 Guidelines on Handling ECHONET Property Values

This chapter provides guidelines on handling cases where a previously set property value is within the ECHONET property definition range but is outside the range in which the corresponding actual device can operate.

(1) In a case where the continuous value range in which the actual device represented by an ECHONET property can operate is narrower than the ECHONET property definition range and a value has been set in the ECHONET property that falls between the upper and lower limit values for the ECHONET property but not between the upper and lower limit values for the actual device, it is recommended that the application software program in the ECHONET Lite node use the following as the property value for the actual device and the ECHONET property value:

The upper limit value for the actual device when the previously set value in the ECHONET property falls between the upper limit value for the ECHONET property and the upper limit value for the actual device; and

The lower limit value for the actual device when the previously set value in the ECHONET property falls between the lower limit value for the ECHONET property and the lower limit value for the actual device.

For example, when the ECHONET property definition range is 0x00 to 0xFD (0°C to 253°C) and the operation range of the actual device represented by the ECHONET property is 0x0A to 0x32 (10°C to 50°C) and a value (e.g. 60°C) has been set in the ECHONET property that falls between the upper limit value for the actual device and the upper limit value for the ECHONET property, it is recommended that the upper limit value for the actual device (0x32 (50°C)) be used as the ECHONET property value. When a value (e.g. 5°C) has been set in the ECHONET property that falls between the lower limit value for the actual device and the lower limit value for the ECHONET property under the same range conditions, it is recommended that the lower limit value for the actual device (0x0A (10°C)) be used as the ECHONET property value.
Fig. 1.1 illustrates these examples.

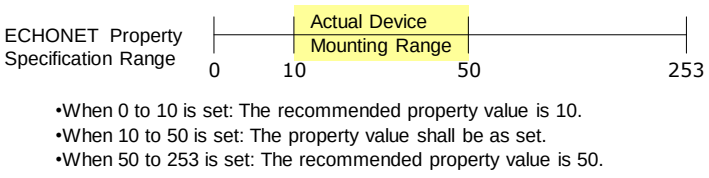

Fig. 1.1 Property Value Setting Example 1

(2) In a case where the number of step values that can be used for step adjustment of the operation of the actual device represented by an ECHONET property is smaller than the number of step values included in the ECHONET property definition range, and one of the values within the ECHONET property definition range that has been set in the ECHONET property is other than the step values for the actual device, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value that can be used for the actual device and is closest to the value previously set in the ECHONET property.

For example, when the ECHONET property definition range includes eight step values between 0x31 and 0x38 but only 0x31, 0x35 and 0x38 (three step values) can be used for step adjustment of the operation of the actual device represented by the ECHONET property, and one of the eight values within the ECHONET property definition range has been set in the ECHONET property, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value among the three values that is closest to the value previously set in the ECHONET property, based on mapping of the 8-value range onto the 3-value range, as shown in Fig. 1.2.

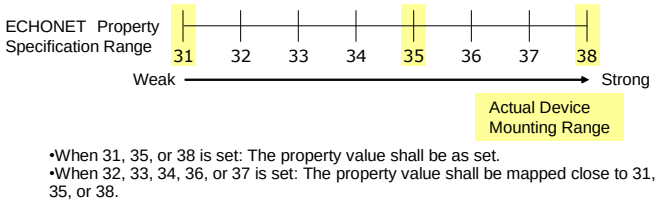

Fig. 1.2 Property Value Setting Example 2

(3) In a case where the previously set value in an ECHONET property specifies a function that is included in the ECHONET property definition range but is not implemented in the actual device represented by the ECHONET property, it is recommended that the application software program in the ECHONET Lite node ignore the setting and use, as the ECHONET property value, the current value specified for the actual device, as shown in Fig. 1.3.

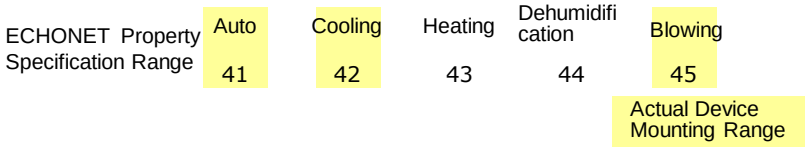

Fig. 1.3 Property Value Setting Example 3

Chapter 2 Guidelines for Secure Communications in ECHONET Lite

2.1 Overview

For secure communications in ECHONET Lite, tampering with communications is prevented: illegal access is prevented by authentication, and tapping is prevented by encryption. The ECHONET Lite Communication Middleware ensures security transmissively from ECHONET Lite by applying the existing standard technologies for secure communications to its lower layers. This chapter gives examples of mechanisms for secure communications in lower layers and describes their guidelines.

2.2 Secure Communications in Lower Layers

This section gives examples of mechanisms for secure communications in lower layers that are provided by the ECHONET Lite Communication Middleware. Security may also be ensured by using not the following mechanisms but the unique mechanism of each company. Negotiation by encryption algorithms, the encryption of communications between ECHONET Lite nodes, and authentication between ECHONET Lite nodes shall follow the specifications of each secure communications mechanism.

Table 2.1 Mechanisms for Secure Communications in Lower Layers

Lower Layer	Mechanism for Secure Communications
Transport	DTLS (Datagram Transport Layer Security)
Network	IPsec (Security Architecture for Internet Protocol) RFC5191
Data Link	WEP (Wired Equivalent Privacy) WPA (Wi-Fi Protected Access) WPA2 (Wi-Fi Protected Access2) AES-CCM (Advanced Encryption Standard Counter with CBC-MAC) IEEE802.1X

2.2.1 DTLS

DTLS is a protocol to provide secure communication functions for datagram. The functions are almost the same as those of TLS (Transport Layer Security). The use of DTLS on a UDP is specified in RFC4347. This protocol is applicable when using UDF in the transport layer or when encrypting ECHONET Lite transmission frames and

preventing tampering in the transport layer.

2.2.2 IPsec

IPsec is a protocol to provide functions for keeping data confidential and preventing tampering in units of an IP packet. This protocol is an option for IPv4 but is implemented in IPv6 as a standard feature. This protocol is applicable when using IP in the network layer or when encrypting ECHONET Lite transmission frames and preventing tampering in the network layer.

2.2.3 RFC5191

RFC5191 is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available in an arbitrary data link layer. A recommended configuration is where an ECHONET Lite node serves as a client issuing an authentication request and a device capable of communicating with an ECHONET Lite node serves as an authentication agent or server receiving an authentication request. A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

2.2.4 AES-CCM

The next-generation encryption system of the U.S. Government established by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. Counter Mode is used for encryption, Message Integrity Code (MIC) for detecting and preventing tampering, and CBC-MAC for MIC generation.

2.2.5 WEP

An encryption technology for wireless communications. This secret key encryption system, based on the RC4 algorithm, is standardized by IEEE and adopted as a security system of IEEE 802.11b.

2.2.6 WPA

A standard of encryption system for wireless LAN announced by the Wi-Fi Alliance, which is an organization in the wireless LAN industry. The security strength of WEP was improved by compensating for its vulnerable points. For encryption, WPA has a user authentication function, as well as SSID and WEP key, and uses the Temporal Key Integrity Protocol (TTKIP)), which updates the encryption key automatically at fixed time intervals.

2.2.7 WPA2

A new version of WPA. This system uses the encryption standard AES specified by the U.S. National Institute of Information and Communications Technology (NICT) for

powerful encryption using keys of variable length from 128 to 256 bits.

2.2.8 IEEE802.1X

IEEE802.1X is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available both for cable and wireless communications. A recommended configuration is where an ECHONET Lite node serves as a supplicant (authentication client) and a device capable of communicating with an ECHONET Lite node serves as an authenticator (authentication device) or authentication server (server which judges whether to allow a supplicant to participate). A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

Chapter 3 Guidelines on Handling Transmission-only Devices in ECHONET Lite

ECHONET Lite defines transmission-only devices to make not only always-live communication devices but also battery-driven devices of low power consumption compatible with ECHONET Lite. Guidelines are available on the handling of these special devices.

・When a transmission-only device joins a network, other devices that are not transmission-only in the system shall be set manually to recognize the transmission-only device.

・When a controller joins a system that has a transmission-only device, information of the transmission-only device shall be set manually in the controller.

・It is recommended that a transmission-only device periodically broadcast the instance list notification described in Section 4.3.1, Part 2.