Bluetooth® Low Energy Protocol Stack

Case studies for good connectivity with smartphones

R01AN4322EJ0100
Rev.1.00
Apr 27, 2018

Introduction

This document provides good connectivity with smartphones when using "Bluetooth Low Energy Protocol Stack" (referred to as "BLE Software") used for developing Bluetooth application products using the Renesas Bluetooth low energy microprocessor RL78/G1D the corresponding case for doing it is described.

Target Device

RL78/G1D

Android device

Related Documents

The documents referred in this document may be preliminary version but might not marked as such version.

Document	Document No.
Bluetooth Low Energy Protocol Stack	—
User's Manual	R01UW0095E
API Reference Manual Basic	R01UW0088E
rBLE Command Specification	R01AN1376E
Quick Start	R01AN2767E

Contents

1. Overview

1.1 Equipment used in this document

- Commercially available smartphones and tablets with Android OS

  (referred to as "Android device")

  - The android device will be our master device. It encrypts pairing and communication when making a connection request to the slave device.

- Equipment using RL78/G1D

  (referred to as “Terminal device”)

  - The terminal device is a slave device. The terminal device automatically starts advertising when turning on the power. When connecting with an Android device, it performs pairing and communication encryption.

1.2 Case list

1. Case that the connection cannot be established again by turning on, after turning off, the terminal device.
If you turn on the power immediately after turning off the terminal, and make a connection request from the Android device from the state where the connection is established between the Android device and the terminal, the connection may not be established.
2. The connection may not be established due to turning on the power of the terminal device (failure of the pairing sequence)
When turning on the terminal and making a connection request from the Android device, the pairing sequence fails, and the connection cannot be established in some cases.
3. Connection may not be established due to turning on the power of the terminal device (Feature exchange sequence failure)
When turning on the terminal and issuing a connection request from the Android device, the Feature exchange sequence may fail, and the connection cannot be established in some cases.

2. Case that the connection cannot be established again by turning on, after turning off, the terminal device.

2.1 Outline

- Phenomenon

  If you turn on the power immediately after turning off the terminal device, and then make a connection request from the Android device from the state where the connection is established between the Android device and the terminal device, the connection may not be established.

- Assumed cause

  Since a disconnection request is not issued from the terminal device when the terminal device is powered off, the Android device cannot communicate with the terminal device and waits for timeout (supervision timeout).

  When the terminal device is turned on again, advertising is started, and the Android device tries to establish a new connection. But a connection waiting for the supervision timeout before the power is turned off remains for the terminal device, it is presumed to be caused by the unexpected state of "Dual Connection".

- Measures

  Send disconnect command to Android device before turning off terminal device. Make sure that you cannot make a connection request to the same terminal device until disconnection is notified by the Android device application.

- Symptom confirmation device

  Some Android devices with Android 7.1.1

2.2 State explanation

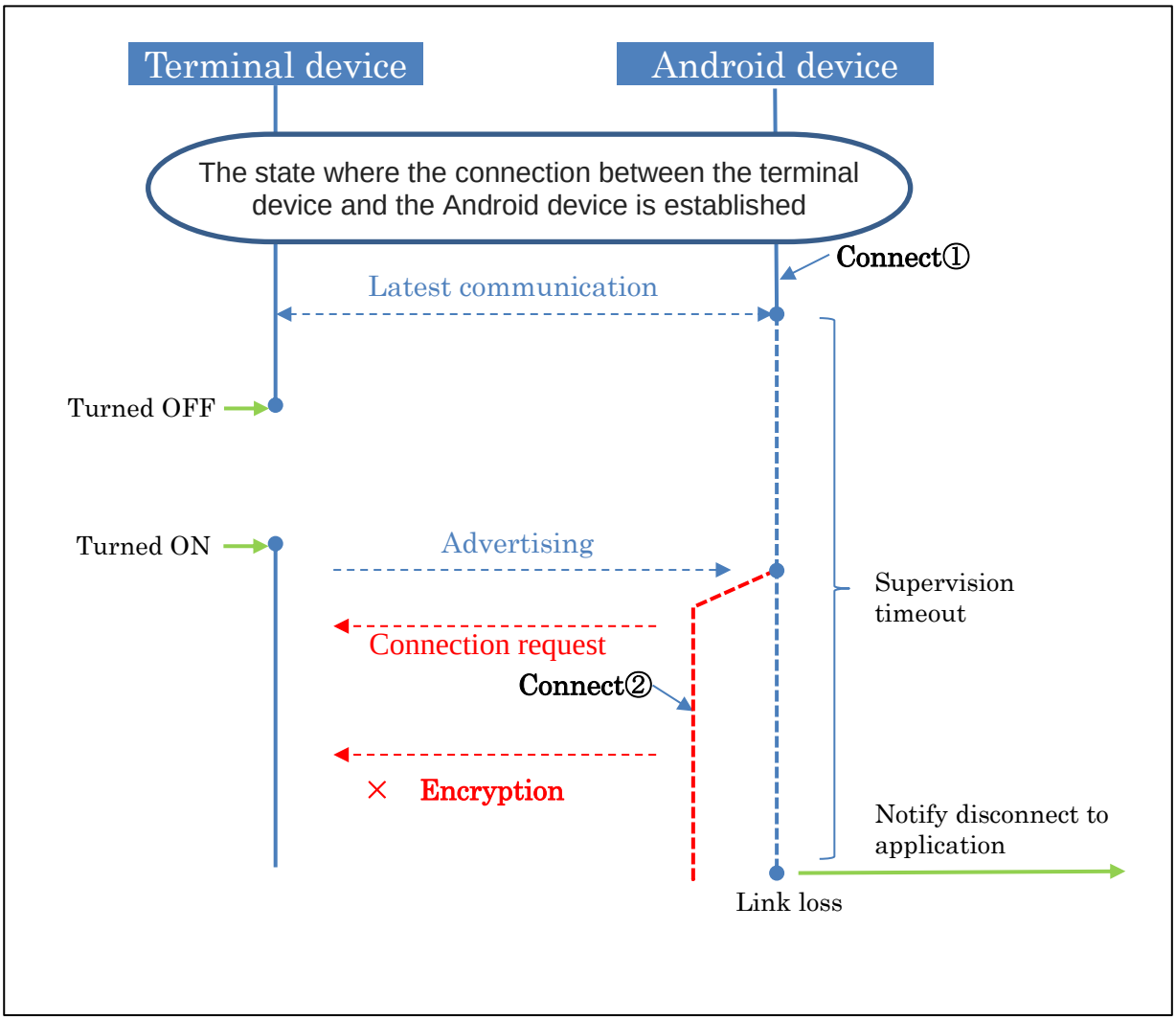


Figure 2-1 State when the terminal device cannot be reconnected from power OFF to ON

- When pairing is completed between the terminal device and the Android device, and the terminal device is turned off "Connection ①" of the Android device is supervision timeout (20 seconds for some Android devices with Android 7.1.1.).

- When the terminal device is powered on while in the above state, the Android device tries to establish a connection by issuing a connection request of "Connection ②" to the advertisement from the terminal device. Now the connection of the android device is doubly connected to the terminal device due to the presence, encryption is not started, and an abnormal connection state is established.

2.3 Improvement plan

2.3.1 Improvement plan on terminal device side

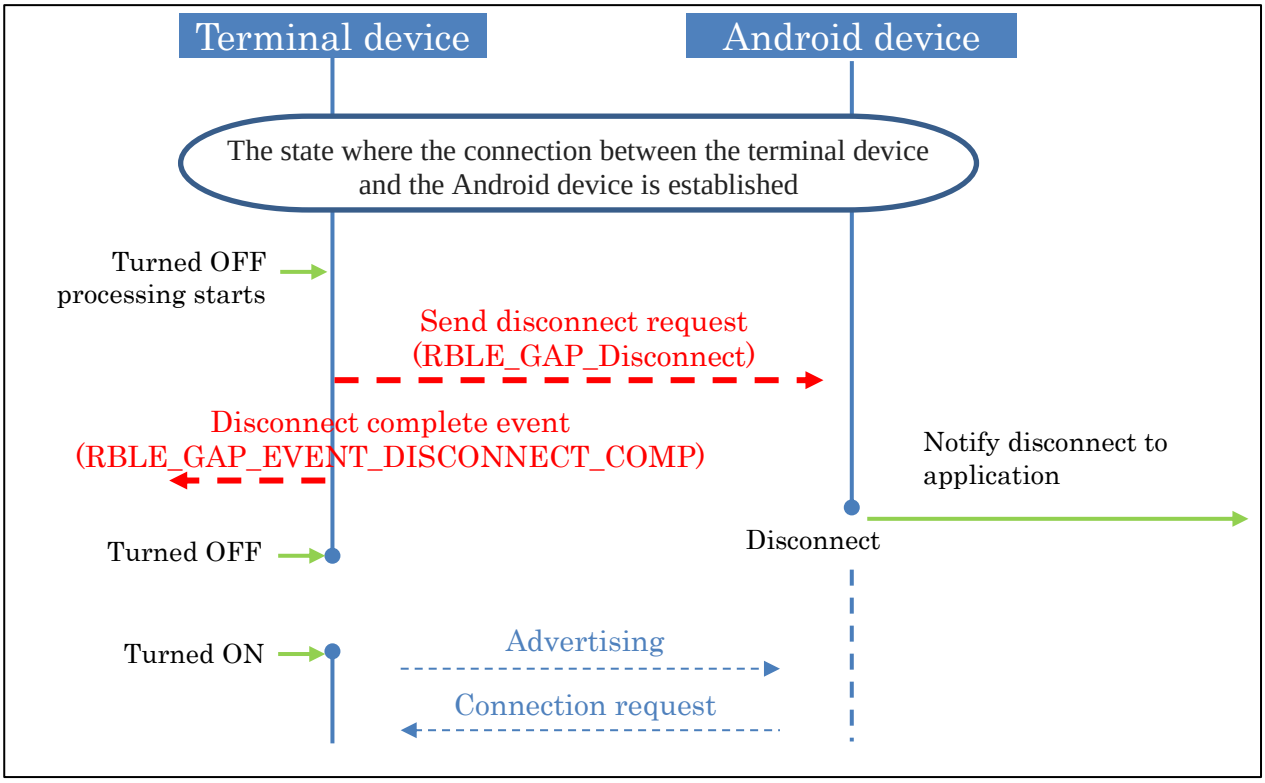


Figure 2-2 Improvement plan for the case where the terminal device cannot be reconnected from the power OFF to ON (Terminal device side: No.1)

- Before turning off the power of the terminal device, execute a disconnection command (RBLE_GAP_Disconnect) to send a disconnection to the Android device. The terminal device waits for a disconnection completion event (RBLE_GAP_EVENT_DISCONNECT_COMP) and turns off the power. By explicitly disconnecting the connection with the Android device, it is possible to normally connect to the advertising by turning on the power of the terminal device.

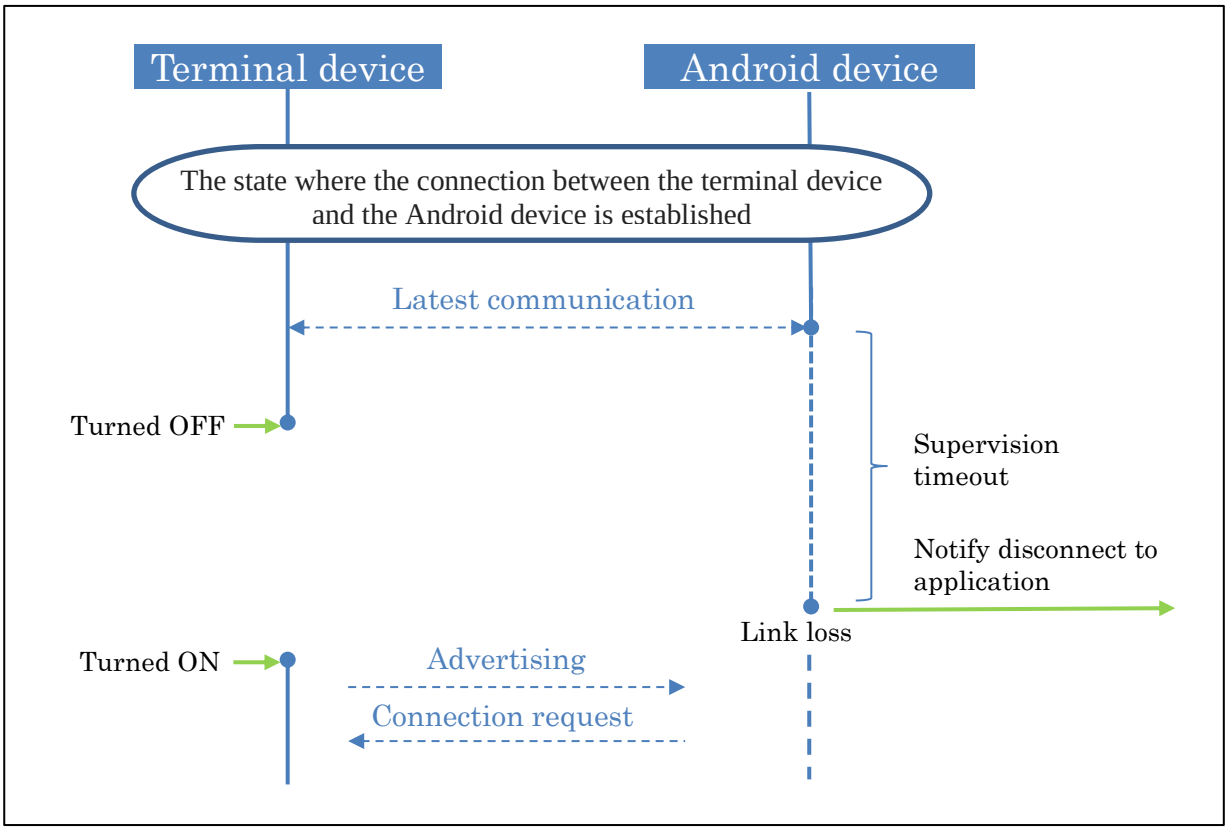


Figure 2-3 Improvement plan for the case where the terminal device cannot be reconnected from the power OFF to ON (Terminal device side: No.2)

- Turn on the power of the terminal device after the time of supervision timeout elapses. Since the connection between the Android device and the terminal device has been disconnected, the Android device issues a connection request to the advertisement from the terminal device, so that the connection is established normally.

2.3.2 Improvement plan for Android device side

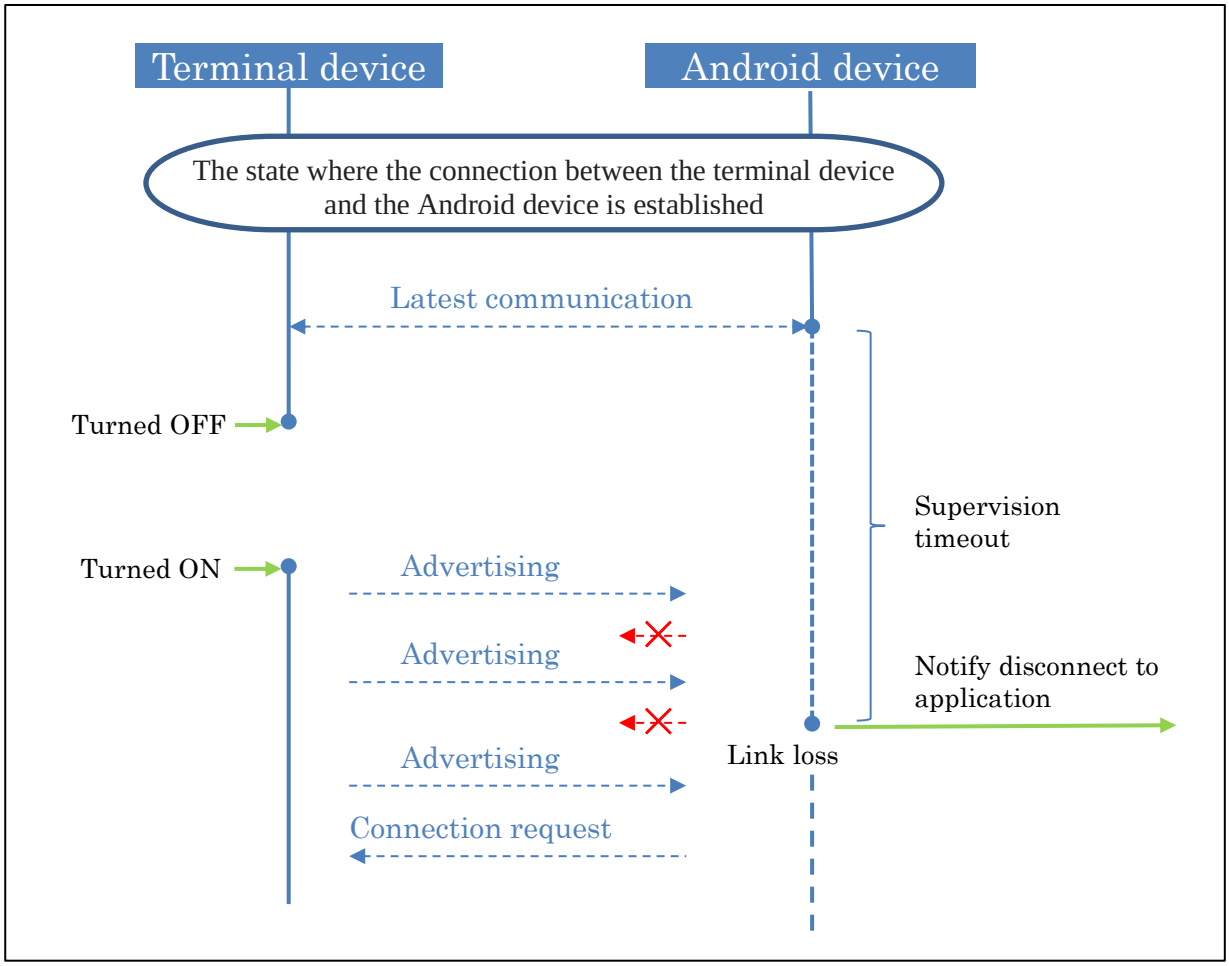


Figure 2-4 Improvement plan for the case where the terminal device cannot be reconnected from the power OFF to ON (Android device side)

- Avoid an abnormal connection state caused by the Android device not issuing a connection request for advertising from the terminal device received during the period of judging that the connection with the terminal device is continuing (until the supervision timeout expires).

Note: If possible, at the time of receiving advertisement from the connected terminal device, judge the link loss, issue a disconnection request from the application to the controller, shift to the disconnected state, and issue a connection request to the terminal device.

3. The connection may not be established due to turning on the power of the terminal device (failure of the pairing sequence)

3.1 Outline

- Phenomenon

When turning on the power of the terminal device and making a connection request from the Android device, the pairing sequence may fail, and connection may not be established in some cases.

- Assumed cause

In the pairing sequence of the Android device, the Encryption Information and Master Identification are notified from the controller layer of the Android device to the host layer prior to the Encryption Change event, whereby inconsistency occurs in the order of the pairing sequence and processing stops.

- Measures

Delay the execution of the function RBLE_SM_Ltk_Req_Resp responding to the LTK request with the RL78 / G1D program so that the Encryption Information and Master Identification will be notified after the Encryption Change event on the Android device.

Note: For delay time, "connection interval × 2" is recommended.

- Symptom confirmation device

Some Android devices with Android 7.0

3.2 State explanation

- Symptom occurrence status

A phenomenon in which connection cannot be established, and an error message with content saying "Cannot connect to Bluetooth" is displayed on the application of the smartphone.

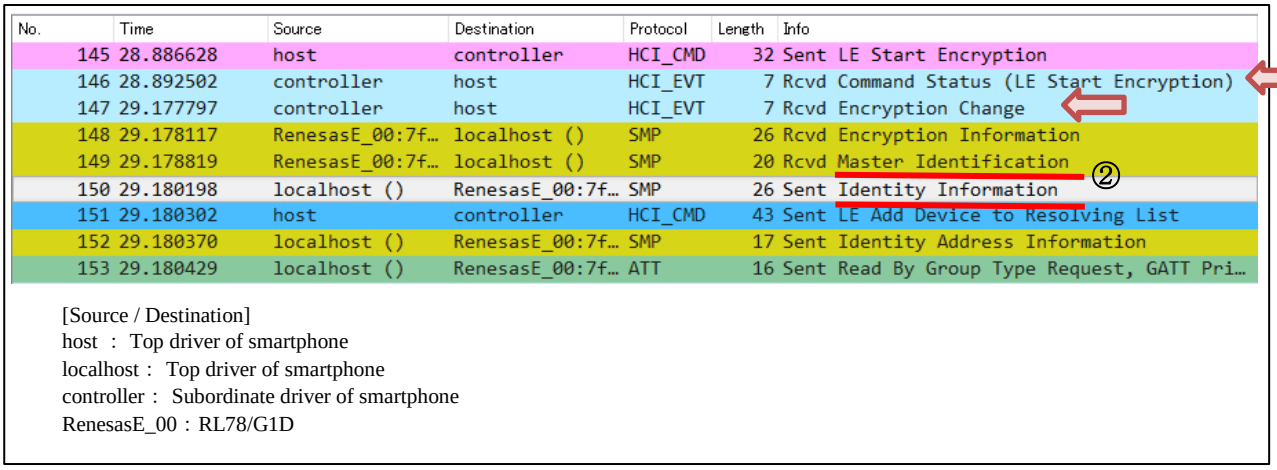
- Analysis method

Analyze the HCI snoop log, which is the communication log in the Android device, using the Android device and the terminal device where the symptoms occur.

- Analysis result

When an error message of symptom occurrence status is displayed on the Android device, the pairing sequence after the connection between the terminal and the Android device is stopped. After the terminal transmits Master Identification, since the Android device does not transmit Identify Information, the pairing sequence is not completed, and the terminal and the Android device remain in an incomplete connection state. This is because the controller layer of the Android device notifies the host layer of Encryption Information and Master Identification prior to the Encryption Change event, thereby causing a discrepancy in the order of the pairing sequence and halting the processing.

3.2.1 HCI snoop log (Normal)



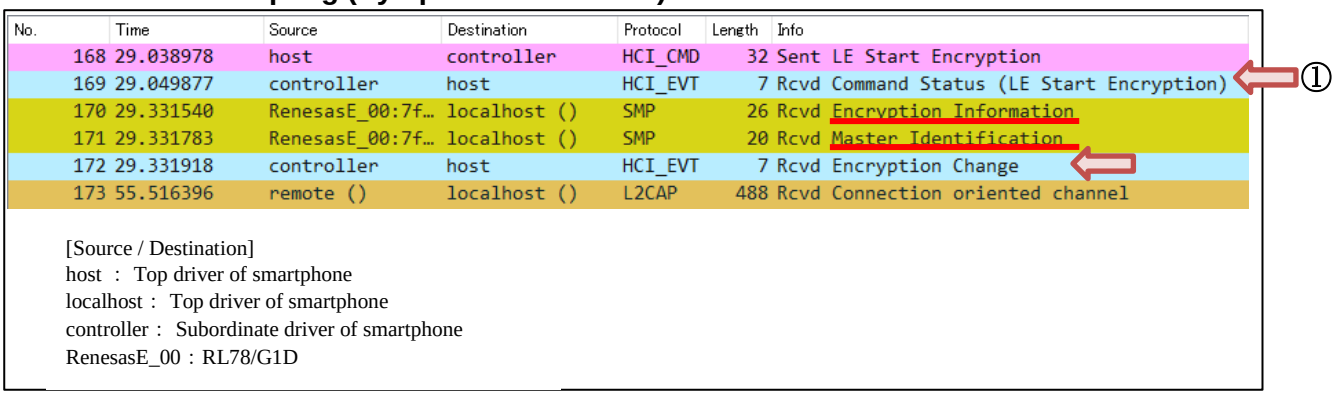
No.	Time	Source	Destination	Protocol	Length	Info
145	28.886628	host	controller	HCI_CMD	32	Sent LE Start Encryption
146	28.892502	controller	host	HCI_EVT	7	Rcvd Command Status (LE Start Encryption)
147	29.177797	controller	host	HCI_EVT	7	Rcvd Encryption Change
148	29.178117	RenesasE_00:7f…	localhost ()	SMP	26	Rcvd Encryption Information
149	29.178819	RenesasE_00:7f…	localhost ()	SMP	20	Rcvd Master Identification
150	29.180198	localhost ()	RenesasE_00:7f…	SMP	26	Sent Identity Information
151	29.180302	host	controller	HCI_CMD	43	Sent LE Add Device to Resolving List
152	29.180370	localhost ()	RenesasE_00:7f…	SMP	17	Sent Identity Address Information
153	29.180429	localhost ()	RenesasE_00:7f…	ATT	16	Sent Read By Group Type Request, GATT Pri…

Figure 3-1 HCI snoop log (Normal)

① When an Encryption Change event occurs immediately after the LE Start Encryption event from the controller layer in the Android device, Identity Information is transmitted from the host layer.

② Encryption information and Master Identification transmitted from the terminal device are notified from the controller layer in the Android device. Identity Information is transmitted from the host layer, after that, the pairing sequence is completed.

3.2.2 HCI snoop log (Symptom occurrence)



No.	Time	Source	Destination	Protocol	Length	Info
168	29.038978	host	controller	HCI_CMD	32	Sent LE Start Encryption
169	29.049877	controller	host	HCI_EVT	7	Rcvd Command Status (LE Start Encryption)
170	29.331540	RenesasE_00:7f…	localhost ()	SMP	26	Rcvd Encryption Information
171	29.331783	RenesasE_00:7f…	localhost ()	SMP	20	Rcvd Master Identification
172	29.331918	controller	host	HCI_EVT	7	Rcvd Encryption Change
173	55.516396	remote ()	localhost ()	L2CAP	488	Rcvd Connection oriented channel

Figure 3-2 HCI snoop log (Symptom occurrence)

① The Encryption Information and Master Identification transmitted from the terminal device are notified from the controller layer of the Android device before the Encryption Change event. When this state occurs, since the host layer of the Android device does not transmit the Identify Information, the pairing sequence is not completed, and the incomplete connection is maintained.

Note: When the occurrence of the Encryption Change event is delayed after the LE Start Encryption event from the controller layer in the Android device, the Identify Information is not transmitted from the host layer.

3.3 Improvement plan

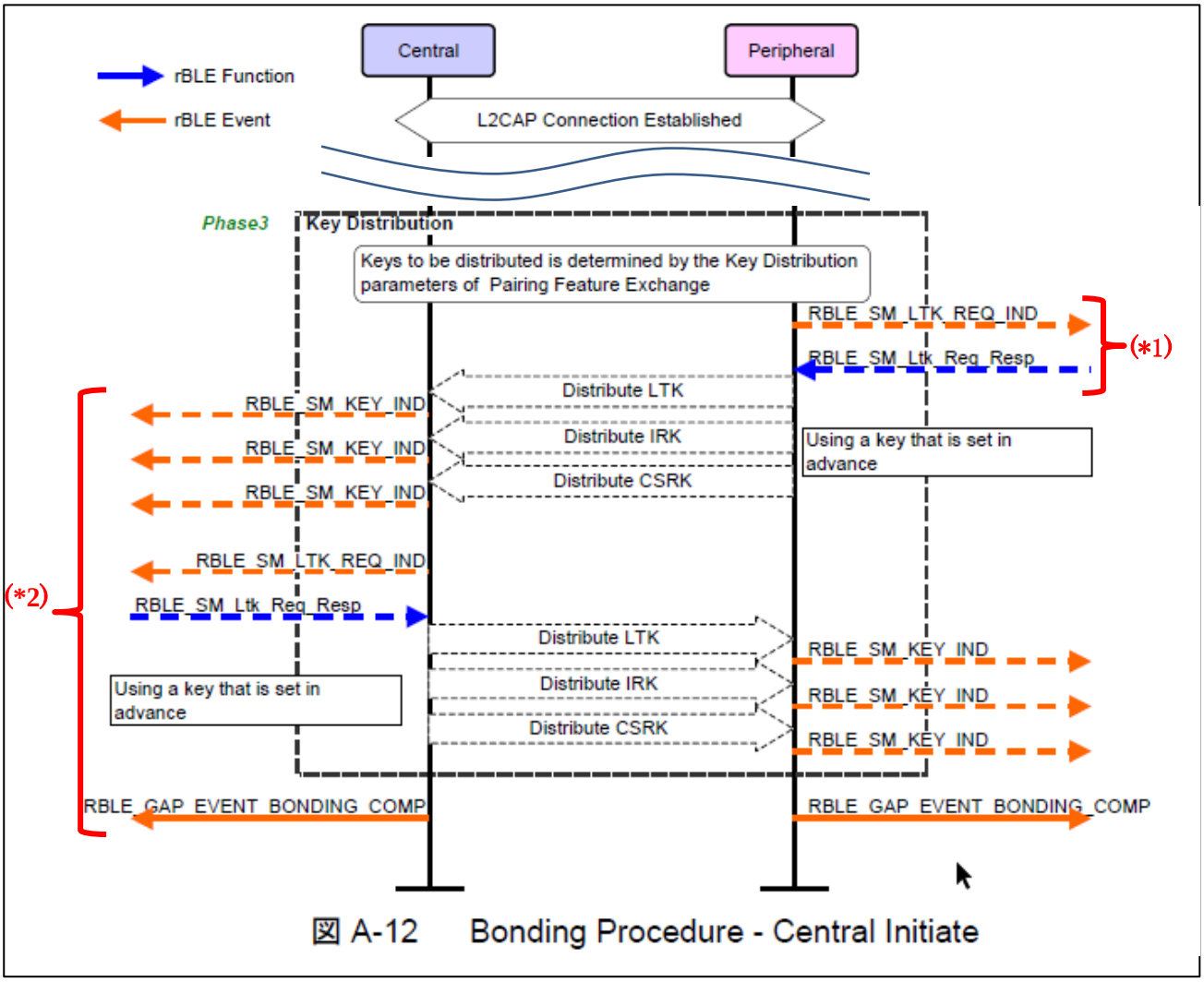


Figure 3-3 Improvement plan for cases where connection cannot be established by turning on terminal device (Pairing sequence failure)

- In pairing sequence processing of the terminal device program, wait insertion ((*1) in Figure 3-3) is performed while calling the RBLE_SM_Ltk_Req_Resp function since the occurrence of the RBLE_SM_LTK_REQ_IND event, thereby intentionally sending Encryption Information and Master Identification It can be delayed.

  Thus, after an Encryption Change of the HCI event occurs, in the Android device, Encryption Information and Master Identification from the terminal device can be received, and a normal pairing sequence can be executed.

- On the smartphone side which is the Central side, in the case of Android, the OS automatically performs the processing of (*2) in Figure 3-3, so there is no processing done on the application side.

3.4 Example of terminal device program implementation

An implementation example for delaying the invocation of the RBLE_SM_Ltk_Req_Resp function using the kernel timer is shown below.

3.4.1 Add message ID for delay

Adds the delay message ID to the enum enumeration of the message ID of the kernel used in the terminal device program.

Note: In our sample program, there is a definition in “r_ble_sample_app_peripheral.h”.

```
typedef enum {
    APP_MSG_BOOTUP = KE_FIRST_MSG(APP_TASK_ID) + 1,
    APP_MSG_RESET_COMP,
    APP_MSG_SECLIB_SET_PARAM_COMP,
    APP_MSG_CONNECTED,
    APP_MSG_SECLIB_CHK_ADDR_COMP,
    APP_MSG_SECLIB_PASSKEY_IND,
    APP_MSG_SECLIB_ENC_COMP,
    APP_MSG_DISCONNECTED,
    APP_MSG_PROFILE_ENABLED,
    APP_MSG_PROFILE_DISABLED,
    APP_MSG_TIMER_EXPIRED,
    APP_MSG_LTK_REQ_DELAY,  // ①Message ID for delay
} APP_MSG_ID;
```

Figure 3-4 Add message ID for delay

3.4.2 Added message processing for LTK response

When the RBLE_SM_LTK_REQ_IND event occurs, add a message function process to set the kernel timer and set the wait time and perform the LTK response.

Note: In our sample program, add message function processing to “r_ble_sample_app_peripheral.c”.

```
// ②Added Prototype Declaration of Message Function for LTK Response
static int_t app_ltk_req_delay(ke_msg_id_t const msgid, void const *param,
                               ke_task_id_t const dest_id, ke_task_id_t const
src_id);
```

Figure 3-5 Added Prototype Declaration of Message Function for LTK Response

```
const struct ke_msg_handler app_connect_handler[] = {
    { APP_MSG_CONNECTED,       (ke_msg_func_t)app_profile_enable },
    /* { APP_MSG_PROFILE_ENABLED, (ke_msg_func_t)NULL }, */
    { APP_MSG_TIMER_EXPIRED,   (ke_msg_func_t)app_timer_expired },
    // ③Register message function after elapse of timer time
    { APP_MSG_LTK_REQ_DELAY,   (ke_msg_func_t)app_ltk_req_delay },
};
```

Figure 3-6 Add message function after connection of timer time to connected message handler

```
/* ##### SM Event Handler ##### */
void app_sm_callback(RBLE_SM_EVENT *event)
{
    switch (event->type) {
    case RBLE_SM_LTK_REQ_IND:
        req_result = event->param.ltk_req;

        // ④Set the kernel timer for the delay time wait(unit time is 10 msec)
        //   -> Delay the response of LTK (Long Term Key)
        ke_timer_set(APP_MSG_LTK_REQ_DELAY, APP_TASK_ID, 50);//Wait 500 msec
        break;

    default:
        break;
    }
}
```

Figure 3-7 Added kernel timer setting process when RBLE_SM_LTK_REQ_IND event occurs

```
// ⑤Additional message function for LTK response → Execute after delay time
static int_t app_ltk_req_delay(ke_msg_id_t const msgid, void const *param,
                               ke_task_id_t const dest_id, ke_task_id_t const
src_id)
{
    /* Generate LTK/EDIV/NB. */
    seclib_generate_key(&ld_ltk.val);
    seclib_generate_nb(&ld_ltk.nb);
    ld_ltk.ediv  = SecLib_Rand();
    ld_ltk.valid = SECDB_VALID_KEY;

    /* LE Long Term Key Request Reply */
    RBLE_SM_Ltk_Req_Resp(req_result.idx, RBLE_OK,
                         RBLE_SMP_KSEC_NONE,
                         ld_ltk.ediv,
                         &ld_ltk.nb,
                         &ld_ltk.val);

    return KE_MSG_CONSUMED;
}
```

Figure 3-8 Added message function for LTK response

4. Connection may not be established due to turning on the power of the terminal device (Feature exchange sequence failure)

4.1 Outline

- Phenomenon

When turning on the power of the terminal device and making a connection request from the Android device, the Feature exchange sequence may fail, and the connection cannot be established in some cases.

- Assumed cause

When another command or event is executed between the connection request command HCI_LE_Create_Connection executed from the host layer of the Android device and the connection completion event LE Connection Complete, the command after the command HCI_LE_Read_Remote_Used_Features after the command which reads the function supported by the remote device The sequence for establishing the connection is not executed.

- Measures

After executing the connection request in the Android device application, do not enter any other processing until receiving the connection completion event LE Connection Complete.

- Symptom confirmation device

Some Android devices with Android 5.0.1

4.2 State explanation

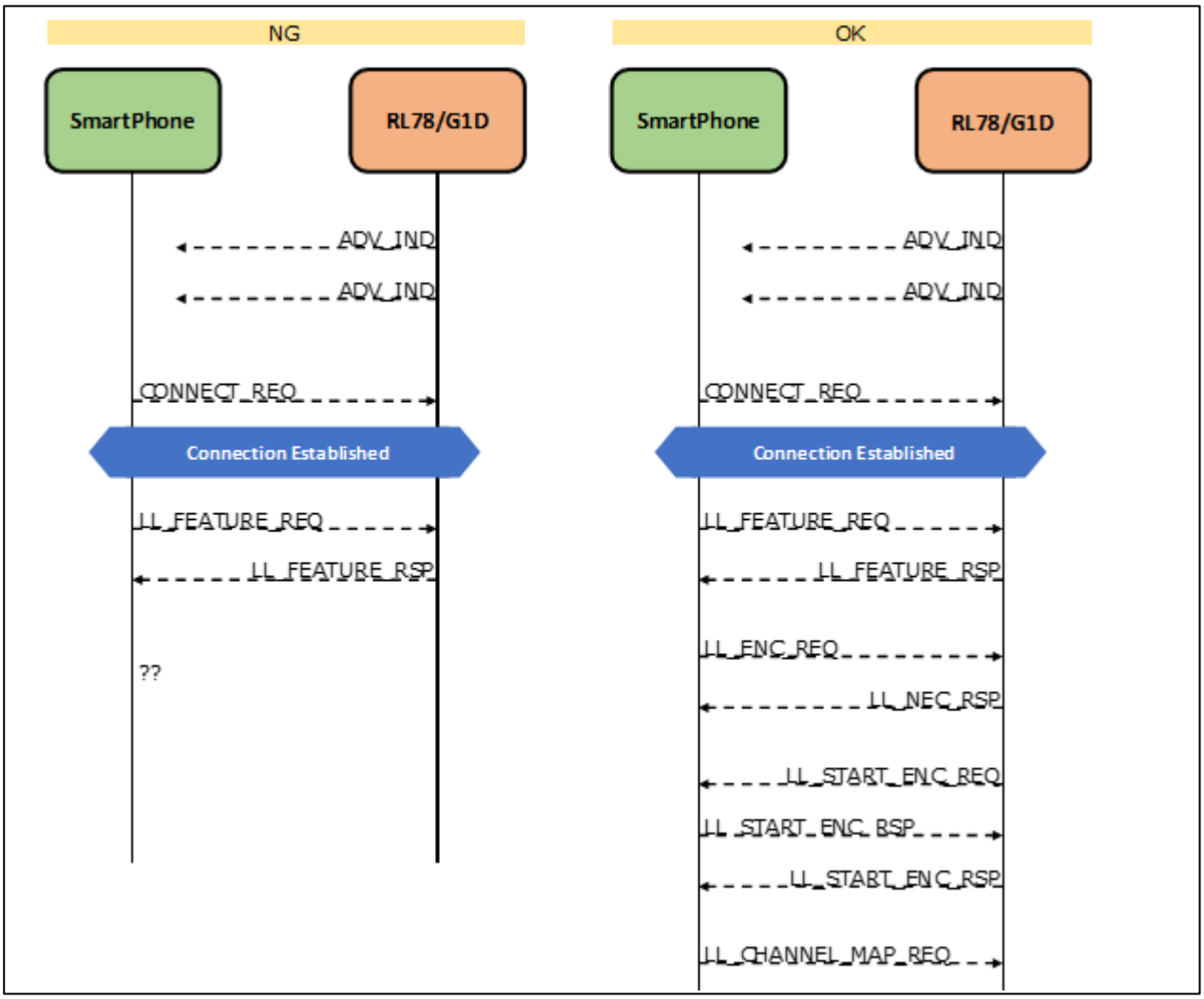
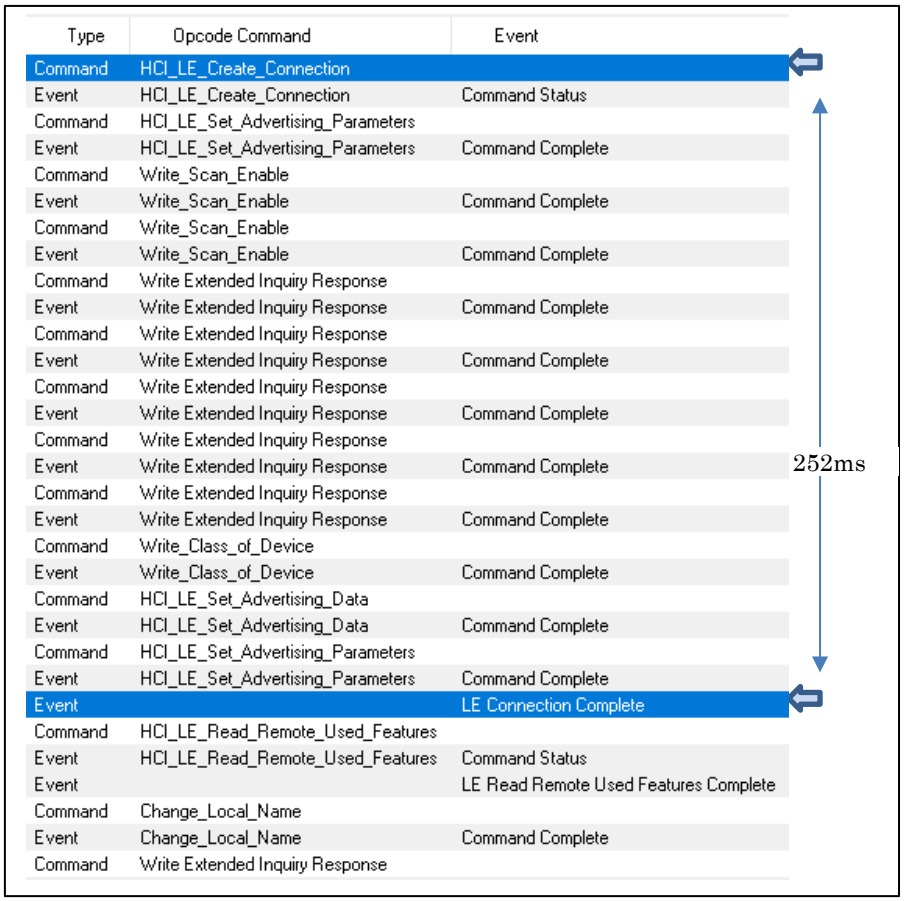


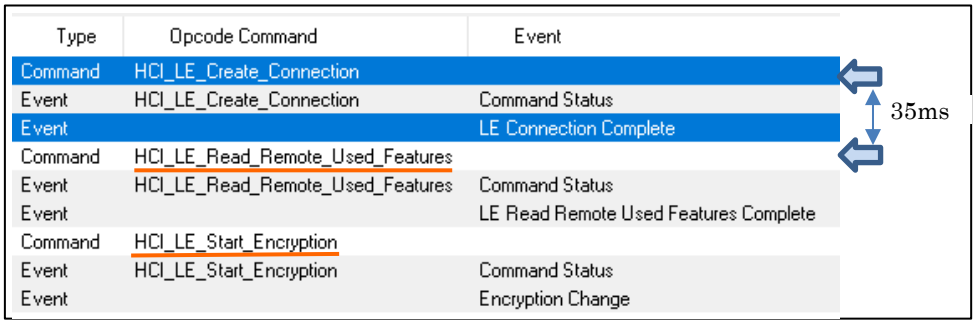
Figure 4-1 State when the terminal device cannot be connected due to power ON (Feature exchange sequence failure)

- Bluetooth Packet Sniffer log analysis result
  - In the case of NG, the Android device sends LL_FEATURE_REQ, and after the terminal device transmits LL_FEATURE_RSP, the Android device stops responding. Even in the case of NG, the Android device and the terminal device are connected. While maintaining the connection it will not proceed from the sequence of LL_FEATURE.
  - In case of OK, the Android device transmits LL_FEATURE_REQ, the sequence device is processed normally after the terminal device transmits LL_FEATURE_RSP.



Type	Opcode Command	Event
Command	HCI_LE_Create_Connection	
Event	HCI_LE_Create_Connection	Command Status
Command	HCI_LE_Set_Advertising_Parameters	
Event	HCI_LE_Set_Advertising_Parameters	Command Complete
Command	Write_Scan_Enable	
Event	Write_Scan_Enable	Command Complete
Command	Write_Scan_Enable	
Event	Write_Scan_Enable	Command Complete
Command	Write Extended Inquiry Response	
Event	Write Extended Inquiry Response	Command Complete
Command	Write Extended Inquiry Response	
Event	Write Extended Inquiry Response	Command Complete
Command	Write Extended Inquiry Response	
Event	Write Extended Inquiry Response	Command Complete
Command	Write Extended Inquiry Response	
Event	Write Extended Inquiry Response	Command Complete
Command	Write_Class_of_Device	
Event	Write_Class_of_Device	Command Complete
Command	HCI_LE_Set_Advertising_Data	
Event	HCI_LE_Set_Advertising_Data	Command Complete
Command	HCI_LE_Set_Advertising_Parameters	
Event	HCI_LE_Set_Advertising_Parameters	Command Complete
Event		LE Connection Complete
Command	HCI_LE_Read_Remote_Used_Features	
Event	HCI_LE_Read_Remote_Used_Features	Command Status
Event		LE Read Remote Used Features Complete
Command	Change_Local_Name	
Event	Change_Local_Name	Command Complete
Command	Write Extended Inquiry Response	

Figure 4-2 HCI snoop log (Symptom occurrence)



Type	Opcode Command	Event
Command	HCI_LE_Create_Connection	
Event	HCI_LE_Create_Connection	Command Status
Event		LE Connection Complete
Command	HCI_LE_Read_Remote_Used_Features	
Event	HCI_LE_Read_Remote_Used_Features	Command Status
Event		LE Read Remote Used Features Complete
Command	HCI_LE_Start_Encryption	
Event	HCI_LE_Start_Encryption	Command Status
Event		Encryption Change

Figure 4-3 HCI snoop log (Normal)

- Analysis result of HCI snoop log
  - In the normal case, it is executed continuously from HCI_LE_Create_Connection to LE Connection Complete. Thereafter, commands of HCI_LE_Read_Remote_Used_Features and HCI_LE_Start_Encryption are executed.
  - When a symptom occurs, another command or event is executed during HCI_LE_Create_Connection ~ LE Connection Complete. After LE Connection Complete, the HCI_LE_Read_Remote_Used_Features command is executed, but the HCI_LE_Start_Encryption command is not executed.

4.3 Improvement plan

After executing the connection request in the Android device application, do not enter any other processing until receiving the connection completion event LE Connection Complete.

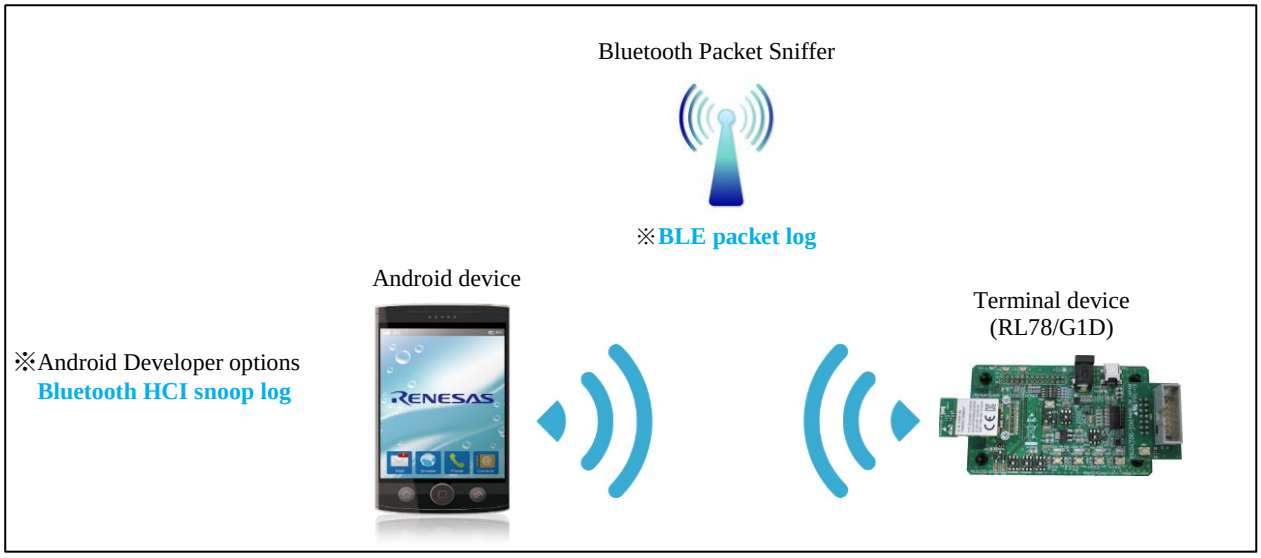
5. Appendix

The environment that can be used for analysis is shown below.

5.1 Analysis environment

There are two kinds of analysis environments as follows.

- Capture the communication between the terminal device (RL78/G1D) and Android device with Bluetooth Packet Sniffer and analyze with packet log
- Analyze BLE operation status of Android device with Bluetooth HCI snoop log



- **Figure 5-1 Analysis environment**

5.1.1 Packet Sniffer log

Capture communication on Air between devices and analyze logs.

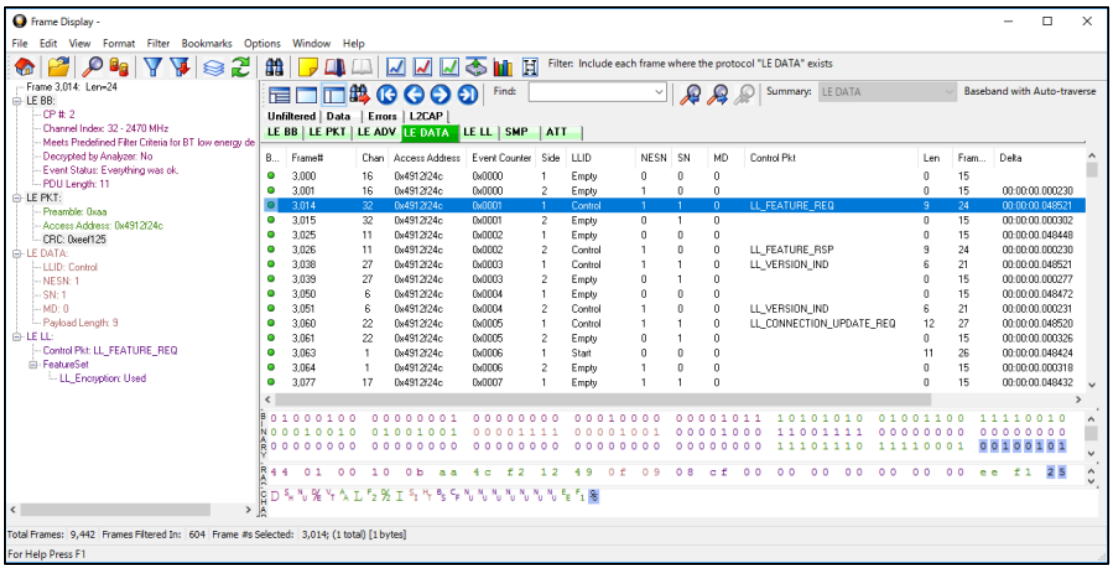


Figure 5-2 Packet Sniffer log

5.1.2 Bluetooth HCI snoop log

Record BLE HCI communication in Android smartphone and analyze log.

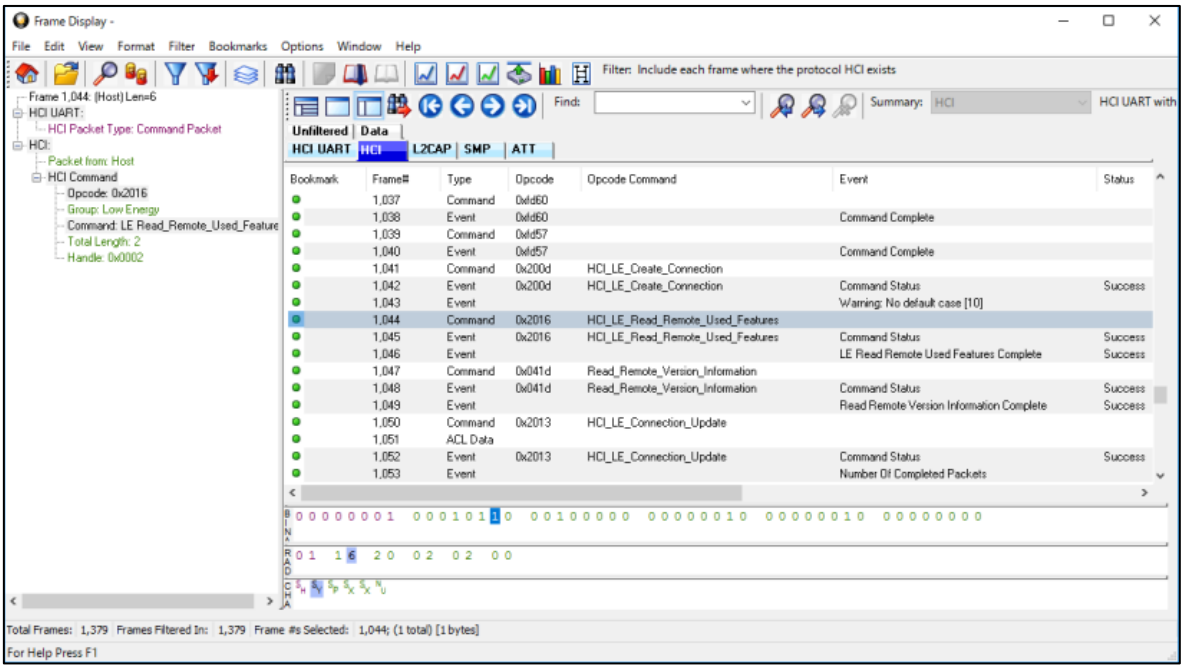


Figure 5-3 Bluetooth HCI snoop log

The recording method of Android's Bluetooth HCI snoop log is as follows.

1. Activate "Developer options" from "Settings" of Android smartphone and turn on "Enable Bluetooth HCI snoop log" setting.
2. When Bluetooth of Android smartphone is enabled, log recording is started.

   The log file name is "btsnoop_hci.log".

   Note: The save destination of the file depends on the model. For details, refer to the smartphone manual.

3. If you continue to record logs and the file size becomes large and it is difficult to see it, disable Bluetooth on smartphone once, disable "Developer options" and "Enable Bluetooth HCI snoop log" before starting recording, then again It is possible to reset and reset the log recording.

After acquiring the Bluetooth HCI snoop log, it can be viewed in the viewer.

- Reference viewer

- BPA software

  http://fte.com/support/CPAS-download.aspx?demo=BPA%20500&iid=1U

  After installation, use Capture File Viewer.

- Wireshark

  https://www.wireshark.org/

Once opened in the viewer, you can do the analysis in the following procedure.

1. Search by keywords such as "disconnection" or "response timeout". If found, the cause of the error is analyzed from the error occurrence point backward.
2. If an error occurrence location cannot be found by keyword, search for the point where connection was established with the keyword "create_connection". Check Command and Event one by one and analyze error occurrence points and cause.

53	Command	HCI_LE_Create_Connection			00:00:00.024035	2017/09/26 9:26:58.951985
54	Event	HCI_LE_Create_Connection	Command Status	Success	00:00:00.005141	2017/09/26 9:26:58.957126
55	Event		Warning: No default case [10]		00:00:00.550315	2017/09/26 9:26:59.507441
56	Command	HCI_LE_Read_Remote_Used_Features			00:00:00.000640	2017/09/26 9:26:59.508081
57	Event	HCI_LE_Read_Remote_Used_Features	Command Status	Success	00:00:00.002543	2017/09/26 9:26:59.510624
58	Event		LE Read Remote Used Features Complete	Success	00:00:00.109168	2017/09/26 9:26:59.619792
59	Command	Read_Remote_Version_Information			00:00:00.000234	2017/09/26 9:26:59.620026
60	Event	Read_Remote_Version_Information	Command Status	Success	00:00:00.004088	2017/09/26 9:26:59.624114
61	Event		Read Remote Version Information Complete	Success	00:00:00.093136	2017/09/26 9:26:59.717250
:	:	:	:	:	:	:
173	ACL Data				00:00:00.009306	2017/09/26 9:27:07.672764
174	Command	HCI_LE_Connection_Update			00:00:00.006043	2017/09/26 9:27:07.678807
175	Event	HCI_LE_Connection_Update	Command Status	Success	00:00:00.006914	2017/09/26 9:27:07.685721
176	Event		LE Connection Update Complete	LMP Response Timeout	00:00:00.550251	2017/09/26 9:27:08.235972
177	Event		Disconnection Complete	Success	00:00:00.000642	2017/09/26 9:27:08.236614
178	Command				00:02:00.298772	2017/09/26 9:29:08.535386

Figure 5-4 **Viewer display example**

Website and Support

Renesas Electronics Website
http://www.renesas.com/

Inquiries
http://www.renesas.com/contact/

Revision History

		Description	
Rev.	**Date**	**Page**	**Summary**
1.00	Apr 27, 2018	-	First edition issued

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Handling of Unused Pins

   Handle unused pins in accordance with the directions given under Handling of Unused Pins in the manual.

   ¾ The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible. Unused pins should be handled as described under Handling of Unused Pins in the manual.

2. Processing at Power-on

   The state of the product is undefined at the moment when power is supplied.

   ¾ The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the moment when power is supplied.
   In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the moment when power is supplied until the reset process is completed.
   In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the moment when power is supplied until the power reaches the level at which resetting has been specified.

3. Prohibition of Access to Reserved Addresses

   Access to reserved addresses is prohibited.

   ¾ The reserved addresses are provided for the possible future expansion of functions. Do not access these addresses; the correct operation of LSI is not guaranteed if they are accessed.

4. Clock Signals

   After applying a reset, only release the reset line after the operating clock signal has become stable. When switching the clock signal during program execution, wait until the target clock signal has stabilized.

   ¾ When the clock signal is generated with an external resonator (or from an external oscillator) during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Moreover, when switching to a clock signal produced with an external resonator (or by an external oscillator) while program execution is in progress, wait until the target clock signal is stable.

5. Differences between Products

   Before changing from one product to another, i.e. to a product with a different part number, confirm that the change will not lead to problems.

   ¾ The characteristics of Microprocessing unit or Microcontroller unit products in the same group but having a different part number may differ in terms of the internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
5. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.

   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.

   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
6. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
7. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
8. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
9. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
10. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
11. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note 1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note 2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.4.0-1 November 2017)

RENESAS

SALES OFFICES

Renesas Electronics Corporation

http://www.renesas.com

Refer to "http://www.renesas.com/" for the latest and detailed information.

Renesas Electronics America Inc.
1001 Murphy Ranch Road, Milpitas, CA 95035, U.S.A.
Tel: +1-408-432-8888, Fax: +1-408-434-5351

Renesas Electronics Canada Limited
9251 Yonge Street, Suite 8309 Richmond Hill, Ontario Canada L4C 9T3
Tel: +1-905-237-2004

Renesas Electronics Europe Limited
Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K
Tel: +44-1628-651-700, Fax: +44-1628-651-804

Renesas Electronics Europe GmbH
Arcadiastrasse 10, 40472 Düsseldorf, Germany
Tel: +49-211-6503-0, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.
Room 1709 Quantum Plaza, No.27 ZhichunLu, Haidian District, Beijing, 100191 P. R. China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.
Unit 301, Tower A, Central Towers, 555 Langao Road, Putuo District, Shanghai, 200333 P. R. China
Tel: +86-21-2226-0888, Fax: +86-21-2226-0999

Renesas Electronics Hong Kong Limited
Unit 1601-1611, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2265-6688, Fax: +852 2886-9022

Renesas Electronics Taiwan Co., Ltd.
13F, No. 363, Fu Shing North Road, Taipei 10543, Taiwan
Tel: +886-2-8175-9600, Fax: +886 2-8175-9670

Renesas Electronics Singapore Pte. Ltd.
80 Bendemeer Road, Unit #06-02 Hyflux Innovation Centre, Singapore 339949
Tel: +65-6213-0200, Fax: +65-6213-0300

Renesas Electronics Malaysia Sdn.Bhd.
Unit 1207, Block B, Menara Amcorp, Amcorp Trade Centre, No. 18, Jln Persiaran Barat, 46050 Petaling Jaya, Selangor Darul Ehsan, Malaysia
Tel: +60-3-7955-9390, Fax: +60-3-7955-9510

Renesas Electronics India Pvt. Ltd.
No.777C, 100 Feet Road, HAL 2nd Stage, Indiranagar, Bangalore 560 038, India
Tel: +91-80-67208700, Fax: +91-80-67208777

Renesas Electronics Korea Co., Ltd.
17F, KAMCO Yangjae Tower, 262, Gangnam-daero, Gangnam-gu, Seoul, 06265 Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5338

Colophon 7.0