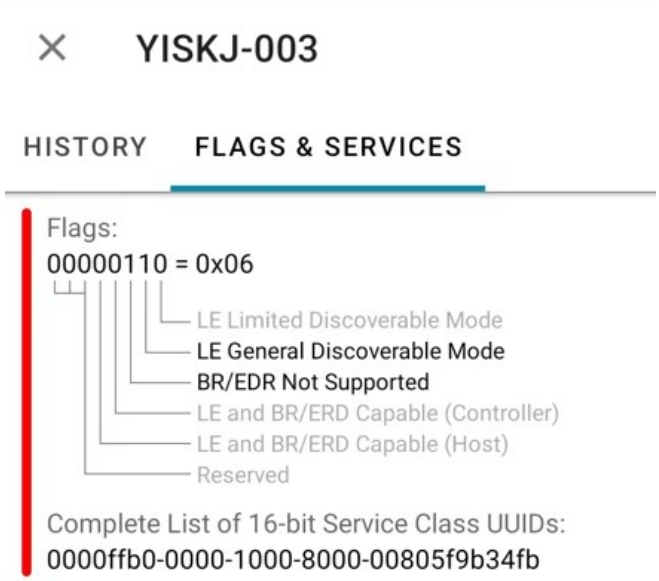
TDL_YISKJ-003_协议规范-V1.0

------2024.01.12

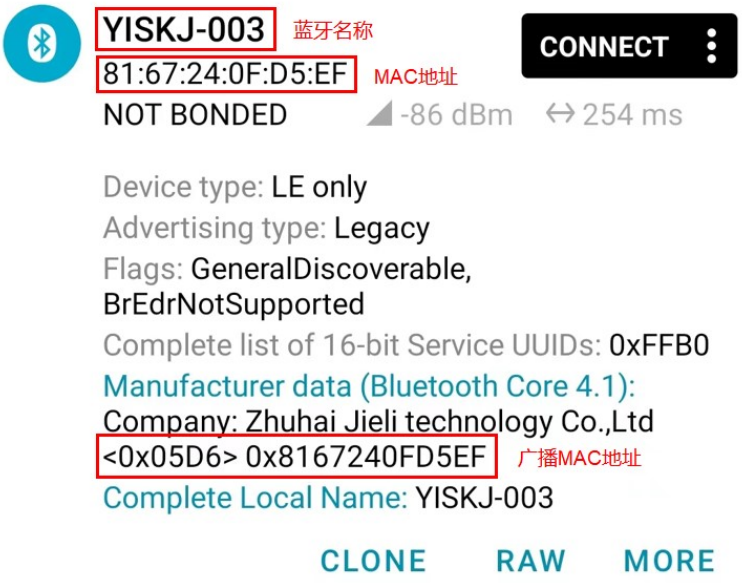
1.连接约定

APP 端扫描蓝牙设备时，仅 UUID 为 0000ffb0-0000-1000-8000-00805f9b34fb 的蓝牙设备 APP 端才会主动连接。

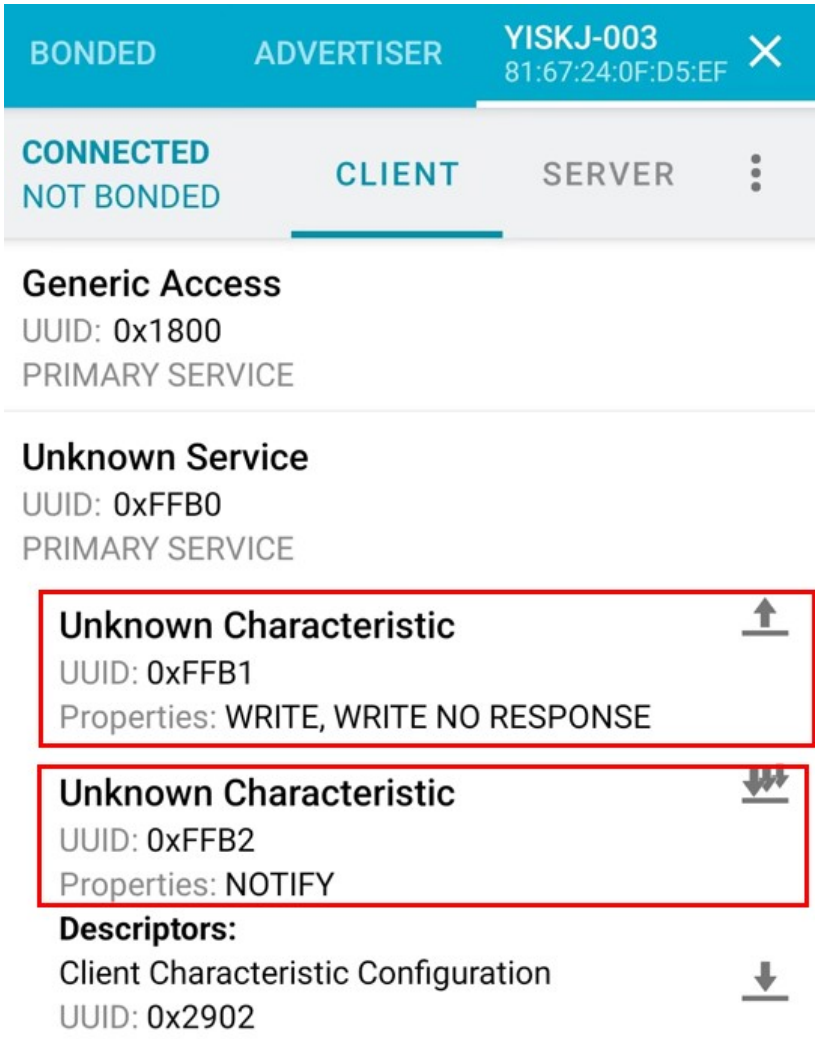
示例：



示例：



示例：



设备的 MAC 地址可作为每个设备的设备 ID。

APP 端所有数据下发通过 FFB1。

设备所有数据上报通过 FFB2。

2.通讯协议

2.1 通讯规则

1) 16 个字节为一条消息明文，不足长度的填充随机数。
2) 设备通过密钥对需要发送的明文指令进行加密，然后再通过蓝牙发送给 APP。
3) APP 端接收设备发来的消息密文，需要通过密钥进行解密后，才得到消息明文。
4) 将消息明文和协议文档对照，找到文档中对应的消息解读。
5) 加密算法约定为 AES-128_ECB。

2.2 加密协议

参考以下 AES-128 数据加密的 C 语言实现：

```c
bool tdl_ble_aes128_ecb_encrypt(uint8_t *key, uint8_t *input, uint16_t input_len, uint8_t *output)
{
    uint16_t length;
    mbedtls_aes_context aes_ctx;
    //
    if (input_len % 16) {
        return FALSE;
    }

    length = input_len;

    mbedtls_aes_init(&aes_ctx);

    mbedtls_aes_setkey_enc(&aes_ctx, key, 128);

    while (length > 0) {
        mbedtls_aes_crypt_ecb(&aes_ctx, MBEDTLS_AES_ENCRYPT, input, output);
        input  += 16;
        output += 16;
        length -= 16;
    }

    mbedtls_aes_free(&aes_ctx);

    return TRUE;
}
```

参考以下 AES-128 数据解密的 C 语言实现：

```c
bool tdl_ble_aes128_ecb_decrypt(uint8_t *key, uint8_t *input, uint16_t input_len, uint8_t *output)
{
    uint16_t length;
    mbedtls_aes_context aes_ctx;
    //
    if (input_len % 16) {
        return FALSE;
    }

    length = input_len;

    mbedtls_aes_init(&aes_ctx);

    mbedtls_aes_setkey_dec(&aes_ctx, key, 128);

    while (length > 0) {
        mbedtls_aes_crypt_ecb(&aes_ctx, MBEDTLS_AES_DECRYPT, input, output);
        input  += 16;
        output += 16;
        length -= 16;
    }

    mbedtls_aes_free(&aes_ctx);
    return TRUE;
}
```

2.3 通讯指令

AES-128 密钥固定为：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F6	38	BC	9C	FA	47	74	80	AB	32	42	F6	B0	45	57	A1

下文将结合实例来描述加密解密的过程：

2.3-1 控制蠕动泵

APP 控制蠕动泵工作的明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	A0	01	01	00	3C	5A	15	D8	1E	C2	D3	72	4A	63

绿色填充部分为控制蠕动泵的指令。
蓝色填充部分为蠕动泵的工作状态，00：停止；01：正转；02：反转。
黄色填充部分为蠕动泵的工作时间，范围为：0x0000-0xFFFF，单位：秒。
橙色填充部分为随机填充字节。

用 AES-128 加密后，得到的密文如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1A	46	4D	2F	C2	99	C5	56	14	0A	CE	01	50	84	75	1D

2.3-2 控制抽水泵

APP 控制抽水泵工作的明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	A0	02	01	00	3C	4E	59	DF	2B	42	48	F3	A8	B1

绿色填充部分为控制抽水泵的指令。
蓝色填充部分为抽水泵的工作状态，00：停止；01：正转。
黄色填充部分为抽水泵的工作时间，范围为：0x0000-0xFFFF，单位：秒。
橙色填充部分为随机填充字节。

2.3-3 暂停工作

明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	A0	03	9B	2F	53	C0	15	74	5D	E1	A6	39	B4	78

绿色填充部分为暂停工作的指令。
橙色填充部分为随机填充字节。

设备收到 APP 下发的暂停工作的指令后，蠕动泵和抽水泵都将停止工作。

2.3-4 查询工作状态

明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	A0	04	9B	2F	53	C0	15	74	5D	E1	A6	39	B4	78

绿色填充部分为查询工作状态的指令。
橙色填充部分为随机填充字节。

设备收到 APP 端查询工作状态的指令后，将上报蠕动泵和抽水泵的工作状态，明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	B0	01	01	00	14	0A	CE	01	53	C0	15	74	46	4D

绿色填充部分为上报工作状态的指令。
蓝色填充部分为蠕动泵的工作状态，00：停止；01：正转；02：反转。
黄色填充部分为抽水泵的工作状态，00：停止；01：正转。
橙色填充部分为随机填充字节。

用 AES-128 加密后，得到的密文如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
8B	3D	70	15	08	C0	5F	FE	F9	0B	C3	58	76	35	F8	C4

2.3-5 上报压力值

每 0.2 秒设备将上报一次压力值给 APP，设备上报的明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	B0	02	01	03	02	10	CE	01	53	C0	15	74	46	4D

绿色填充部分为上报压力值的指令。
蓝色填充部分为压力传感器 A 的数值，范围为：0x0000-0xFFFF。
黄色填充部分为压力传感器 B 的数值，范围为：0x0000-0xFFFF。
橙色填充部分为随机填充字节。

2.3-6 获取电量

APP 下发的获取电量的明文如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	A0	05	9B	2F	53	C0	15	74	5D	E1	A6	39	B4	78

绿色填充部分为获取电量的指令。
橙色填充部分为随机填充字节。

设备收到 APP 端获取电量的指令后，将上报电量给 APP，明文指令如下：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BF	0F	B0	03	10	74	5D	E1	CE	01	74	46	4D	53	C0	15

绿色填充部分为上报电量的指令。
蓝色填充部分为上报的电量，范围为：0x00-0x64。
橙色填充部分为随机填充字节。

3.修订记录

2024.01.12------初次编写，版号 V1.0。