Bluetooth Low Energy Pairing

서동훈

What is BLE...?

Bluetooth Low Energy (BLE)

- 블루투스 저전력 프로토콜(Bluetooth Low Energy) 또는 줄여서 BLE은 블루투스 4.0스펙이 2010년 채택된 이후로 배포되는 저전력 블루투스이다.
- 저전력을 사용하며, BT Classic(기존 블루투스)와는 장단점이 존재한다.
- 주로 피트니스, 스포츠, 헬스케어와 같은 분야에서 많이 사용된다.

Advertising

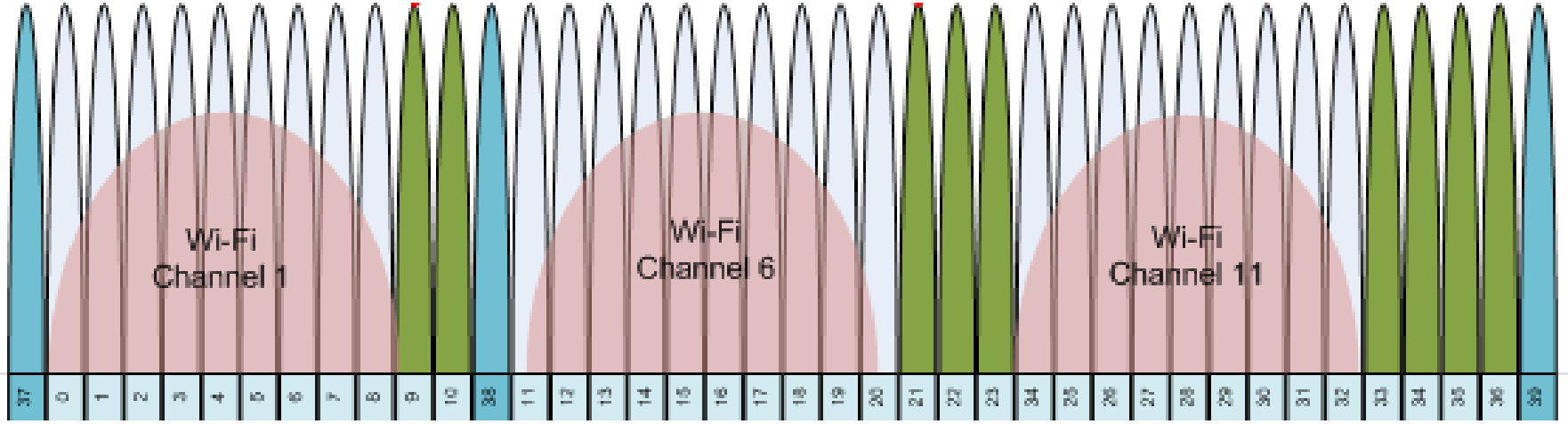
Advertising

- 페어링을 진행할 수 있도록 주변의 모든 기기에게 신호를 보내 자신을 알리는 행위
- Advertising 진행하는 두 기기는 다음과 같은 역할을 맡는다.
  - Advertiser : Advertising Packet을 주기적으로 송신하는 역할
  - Observer : Advertiser가 보내는 패킷을 주기적으로 수신하는 역할

Advertising

Advertising

- Hopping기법을 사용하여 다음 3개의 채널(2402MHz (Ch37), 2426MHz(Ch38), 2480MHz(Ch39))에서 Advertising을 진행한다.
- 각각 자신의 Time Interval을 가지고 Hopping을 진행한다.

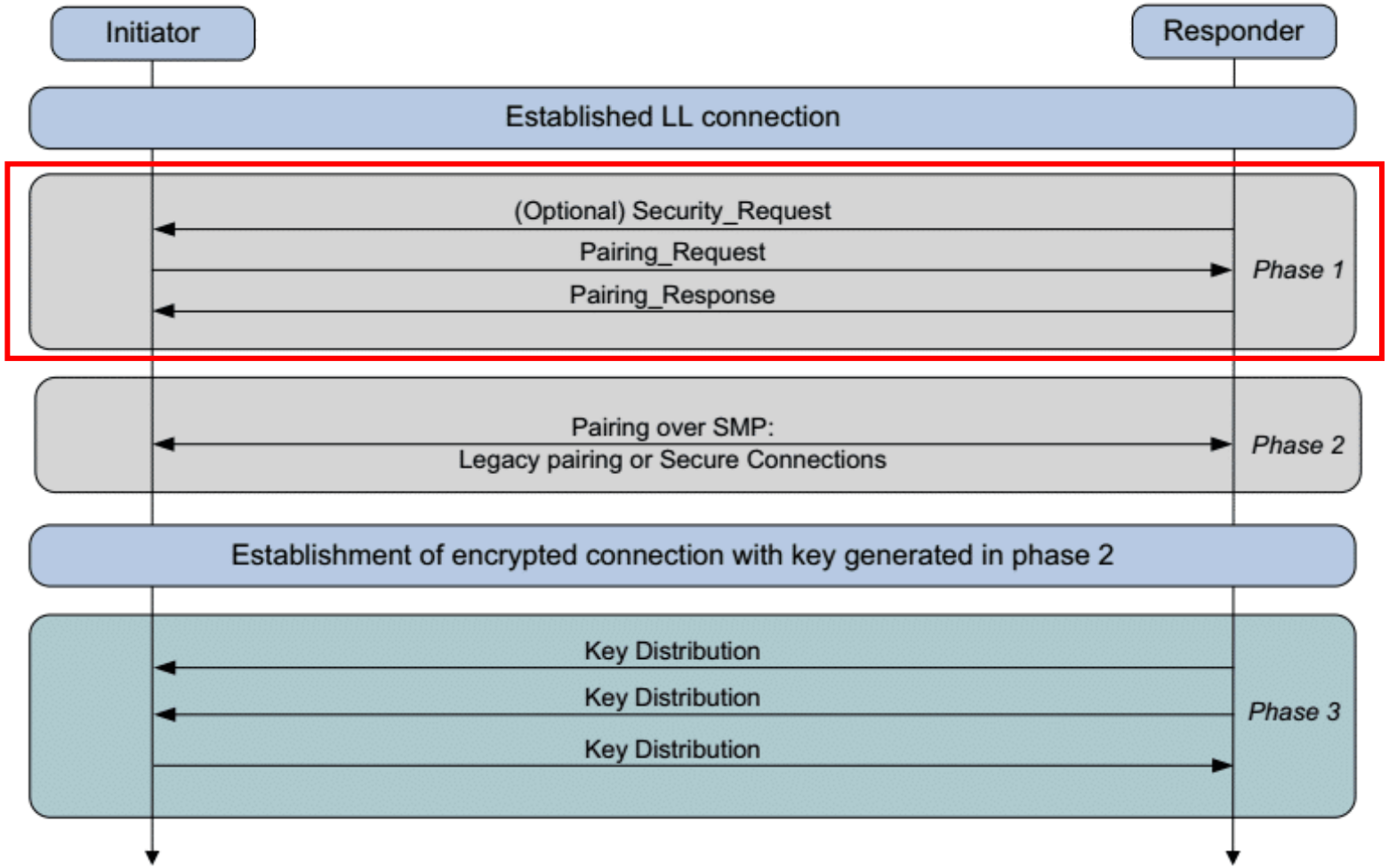


Pairing

Pairing Security

- Legacy Pairing과 SSP(Simple Secure Pairing)으로 나뉘던 BT Classic과 다르게 BLE는 Legacy Pairing과 Secure Connection 둘로 나뉜다.
- 페어링 진행 이전 서로의 정보를 교환한 후 다음 4가지 중 하나를 사용하여 진행한다.
  - Just Works - Legacy or Secure
  - Passkey Entry - Legacy or Secure
  - Out Of Band - Legacy or Secure
  - Numeric Comparison - Only Secure Connection

Pairing


Initiator
Responder
Established LL connection
(Optional) Security_Request
Pairing_Request
Pairing_Response
Phase 1
Pairing over SMP:
Legacy pairing or Secure Connections
Phase 2
Establishment of encrypted connection with key generated in phase 2
Key Distribution
Key Distribution
Key Distribution
Phase 3

Pairing

Security Request (Optional)

- Slave가 Master에게 보내는 보안 요청으로 Master는 해당 요청을 통해 링크를 암호화하거나 페어링을 시작하게 할 수 있다.

- 만약 Master가 Slave의 요청을 들어주지 못하는 환경일 때 Pairing Not Supported 명령을 보내는 것으로 연결을 해제한다.

Field	Opcode (1 Byte)	AuthReq (1 Byte)				
Sub-define		Bonding Flags	MITM	Secure Connection	Keypress Flag	Reserved
Bits	8	2	1	1	1	3

Pairing

AuthReq

- Bonding Flags(BF) : 페어링 이후 장기키(long-term)를 교환하여 저장할 것인지를 나타내는 값
- MITM : MITM 보호를 사용할 것인지를 나타내는 값
- Secure Connection(SC) : LE Secure Connection을 사용할 것인지를 나타내는 값
  - 두 기기 모두가 1일때 Secure Connection을 진행한다.
- Keypress Flag(KF) : Passkey Entry Protocol에서 사용되는 특수 값
- Reserved : 의미 없으며 무시되는 값

Field		AuthReq (1 Byte)				
Sub-define	Opcode (1 Byte)	Bonding Flags (2 Bits)	MITM (1 Bit)	Secure Connection (1 Bit)	Keypress Flag (1 Bit)	Reserved (3 Bits)

Pairing

Source	Destination	Protocol	Length	Info
SamsungE_23:8f:b7 (Galaxy Fit2 (8FB7))	localhost (��������� A80)	SMP	11	Rcvd Security Request

```
▼ Bluetooth Security Manager Protocol
    Opcode: Security Request (0x0b)
  ▼ AuthReq: 0x0c, Secure Connection Flag, MITM Flag, Bonding Flags: No Bonding
        000. .... = Reserved: 0x0
        ...0 .... = Keypress Flag: False
        .... 1... = Secure Connection Flag: True
        .... .1.. = MITM Flag: True
        .... ..00 = Bonding Flags: No Bonding (0x0)
```

Pairing

Pairing (Request & Response)

- 연결하려는 기기가 이후 서로의 IO(Input/Output), MITM, 보호 연결 요구와 같은 보안 기능을 교환하는 명령
- 해당 값들을 서로 교환하는 것으로 이후 페어링을 어떠한 방법으로 진행할지 결정된다.
- Request(Master to Slave), Response(Slave to Master)

Field	Opcode (1 Byte)	IO Capa (1 Byte)	OOB DF (1 Byte)	AuthReq (1 Byte)					Maximum Encryption Key Size (1 Byte)	Initiator Key Distribution (1 Byte)	Responder Key Distribution (1 Byte)
Sub-define				BF	MITM	SC	KF	Reserved			
Bits	8	8	8	2	1	1	1	3	8	8	8

Pairing

Pairing (Request & Response)

- IO Capability : 현재 기기가 사용할 수 있는 IO(Input/Output)을 나타내는 값
- OOB Data Flags(OOB DF) : OOB(Out-Of-Band) 즉, 블루투스가 아닌 다른 통신 수단(NFC, QR, ...)을 사용하여 페어링을 진행할 것인지를 나타내는 값
- AuthReq : 이전 장표와 동일
- Maximum Encryption Key Size : 암호화 키 크기를 나타내는 값 (7 ~ 16 octets 사이)
- (Initiator or Responder) Key Distribution : 배포/생성 또는 사용을 요청하는 키를 나타내는 값.

Opcode (1 Byte)	IO Capa (1 Byte)	OOB DF (1 Byte)	AuthReq (1 Byte)					Maximum Encryption Key Size (1 Byte)	Initiator Key Distribution (1 Byte)	Responder Key Distribution (1 Byte)
			BF	MITM	SC	KF	Reserved			

Pairing

Source	Destination	Protocol	Length	Info
localhost (********** A80)	SamsungE_23:8f:b7 (Galaxy Fit2 (8FB…	SMP	16	Sent Pairing Request

Source	Destination	Protocol	Length	Info
SamsungE_23:8f:b7 (Galaxy Fit2 (8FB7))	localhost (********** A80)	SMP	16	Rcvd Pairing Response

```
Bluetooth Security Manager Protocol
    Opcode: Pairing Request (0x01)
    IO Capability: Keyboard, Display (0x04)
    OOB Data Flags: OOB Auth. Data Not Present (0x00)
  AuthReq: 0x2d, Secure Connection Flag, MITM Flag, Bonding Flags: Bonding
      001. .... = Reserved: 0x1
      ...0 .... = Keypress Flag: False
      .... 1... = Secure Connection Flag: True
      .... .1.. = MITM Flag: True
      .... ..01 = Bonding Flags: Bonding (0x1)
    Max Encryption Key Size: 16
  Initiator Key Distribution: 0x0f, Link Key, Signature Key (CSRK), Id Key (IRK), Encryption Key (LTK)
      0000 .... = Reserved: 0x0
      .... 1... = Link Key: True
      .... .1.. = Signature Key (CSRK): True
      .... ..1. = Id Key (IRK): True
      .... ...1 = Encryption Key (LTK): True
  Responder Key Distribution: 0x0f, Link Key, Signature Key (CSRK), Id Key (IRK), Encryption Key (LTK)
      0000 .... = Reserved: 0x0
      .... 1... = Link Key: True
      .... .1.. = Signature Key (CSRK): True
      .... ..1. = Id Key (IRK): True
      .... ...1 = Encryption Key (LTK): True
```

Pairing

Rules for using OOB and MITM flags

		Initiator			
		OOB Set	**OOB Not Set**	**MITM Set**	**MITM Not Set**
Responder	**OOB Set**	Use OOB	Check MITM		
	OOB Not Set	Check MITM	Check MITM		
	MITM Set			Use IO Capabilities	Use IO Capabilities
	MITM Not Set			Use IO Capabilities	Use Just Works

in Legacy Pairing

		Initiator			
		OOB Set	**OOB Not Set**	**MITM Set**	**MITM Not Set**
Responder	**OOB Set**	Use OOB	Use OOB		
	OOB Not Set	Use OOB	Check MITM		
	MITM Set			Use IO Capabilities	Use IO Capabilities
	MITM Not Set			Use IO Capabilities	Use Just Works

in Secure Connection

Pairing

Mapping of 10 Capabilities to Key Generation Method

	Initiator				
Responder	**DisplayOnly**	**Display YesNo**	**Keyboard Only**	**NoInput NoOutput**	**Keyboard Display**
Display Only	Just Works Unauthenticated	Just Works Unauthenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry: responder displays, initiator inputs Authenticated
Display YesNo	Just Works Unauthenticated	Just Works (For LE Legacy Pairing) Unauthenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): responder displays, initiator inputs Authenticated
		Numeric Comparison (For LE Secure Connections) Authenticated			Numeric Comparison (For LE Secure Connections) Authenticated

	Initiator				
Responder	**DisplayOnly**	**Display YesNo**	**Keyboard Only**	**NoInput NoOutput**	**Keyboard Display**
Keyboard Only	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator and responder inputs Authenticated	Just Works Unauthenticated	Passkey Entry: initiator displays, responder inputs Authenticated
NoInput NoOutput	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated
Keyboard Display	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated
		Numeric Comparison (For LE Secure Connections) Authenticated			Numeric Comparison (For LE Secure Connections) Authenticated

Pairing

Public Key Exchange

- Legacy Pairing과 Secure Connecion의 가장 큰 차이점
- Pairing Request & Response의 Auth Req 필드의 Secure Connection값이 둘 다 1일 때 사용한다.
- Diffie-Hellman Key exchange를 사용한다.
- Just Works, Numeric Comparion을 진행하기 이전에 Pairing Public Key를 통해 서로 공개키를 교환하여 비밀키를 계산한 후 이후 과정에서 이를 사용한다.

Pairing


```
Bluetooth Security Manager Protocol
    Opcode: Pairing Public Key (0x0c)
    Public Key X: 0479c015303b047ccd82ac9a68b9c1ab1d1fa7664be26310a57b4ee2b8f53f78
    Public Key Y: 62ce7146d60a0b23c27081421a9f93e52a1027dbec3958223b9d0001ab3cb5a8
```

```
Bluetooth Security Manager Protocol
    Opcode: Pairing Public Key (0x0c)
    Public Key X: 3760bc694d8b087bc45b79bcb821f7d8f8bc3b97895d6b3d8621a1d9c5d365e4
    Public Key Y: 74ffe85c0cd18ca0a0ad31fdd3bf37ee1bec39a531849677ba25edd5f9fe7eba
```

Q & A