360大学 | 飞扬

低功耗蓝牙（BLE）安全研究

针对特定BLE进行连接阻断和中继的研究探索

未来安全研究院　张伟
zhangwei13@360.cn

项目介绍

阻断

防止攻击，保证安全

特定设备

中继

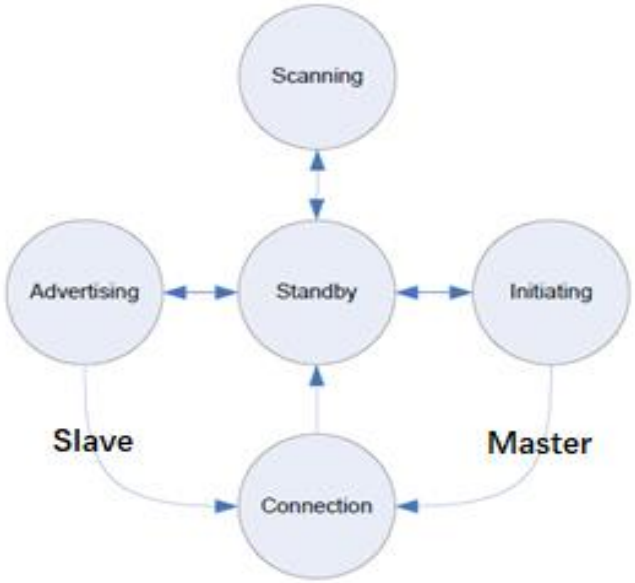
增加传输距离

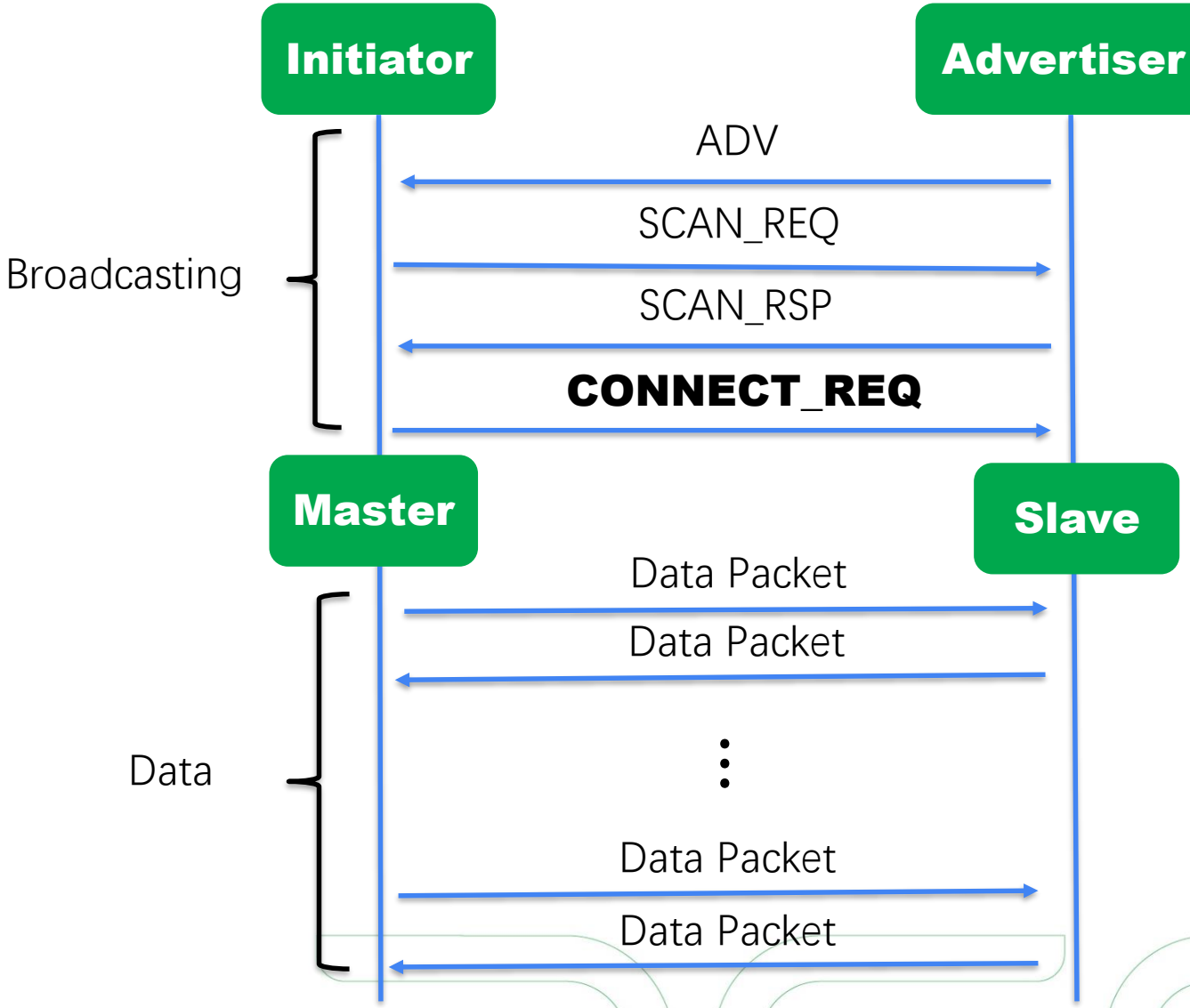
多时段多用户

BLE 阻断、中继

\

BLE 连接过程





BLE 阻断、中继

\

LLData： CONNECT_REQ

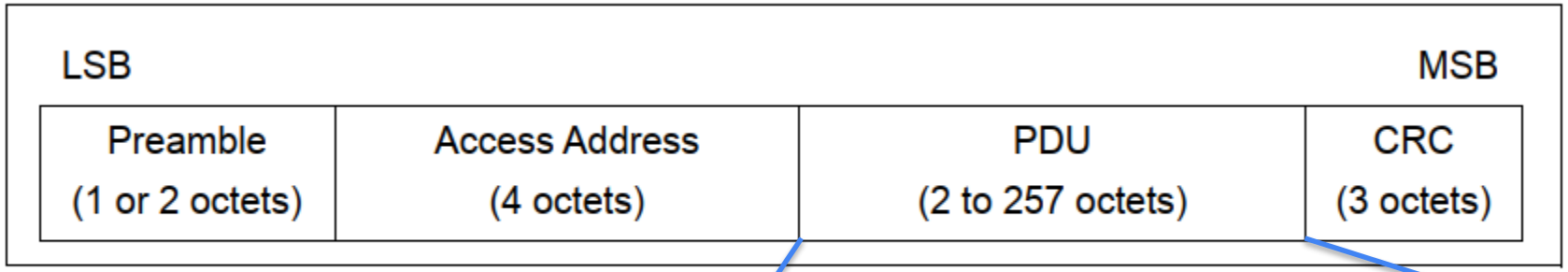


Figure 2.1: Link Layer packet format for the LE Uncoded PHYs

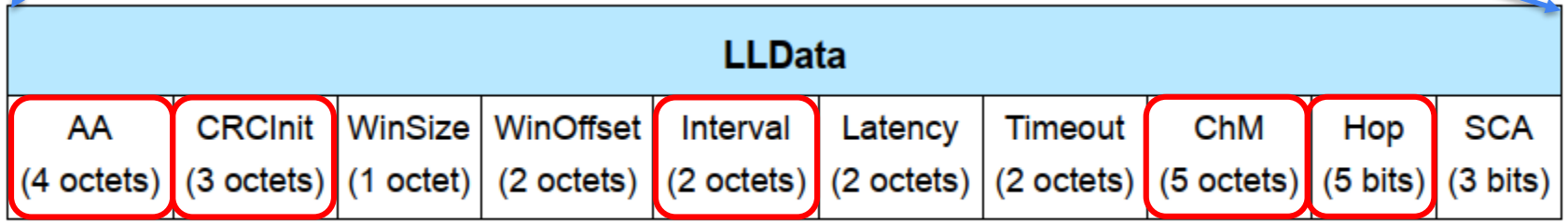


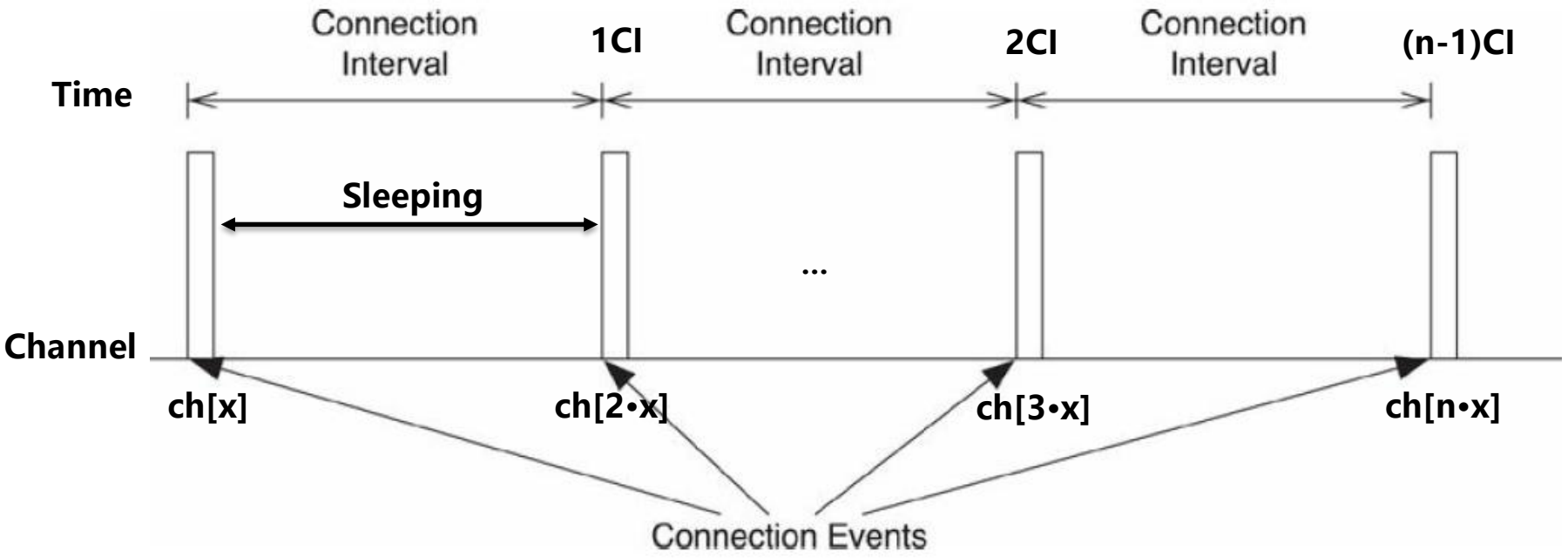
Figure 2.13: LLData field structure in CONNECT_IND and AUX_CONNECT_REQ PDU's payload

[1] Bluetooth Core Specification Core_v5.0[EB/OL]. Bluetooth SIG Proprietary. http://www.uni-obuda.hu/users/wuhrlt/MSc_Adatatvitel/Core_v5.0.pdf. 2016.12.06

BLE 阻断、中继

\

如何同步信道?



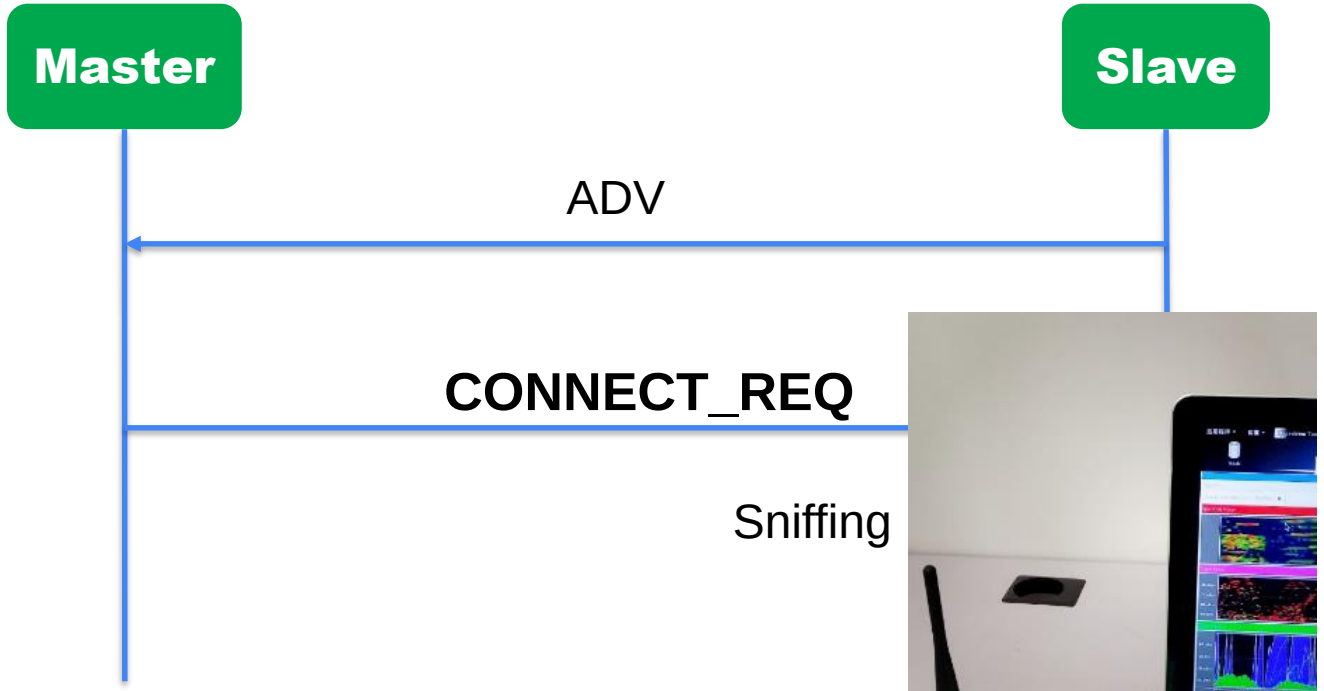
* CI = Connection Event + Sleeping

= (Connection Interval + Slave Latency + **Supervision Timeout**) + Sleeping

BLE 阻断、中继

\

BLE 数据包嗅探

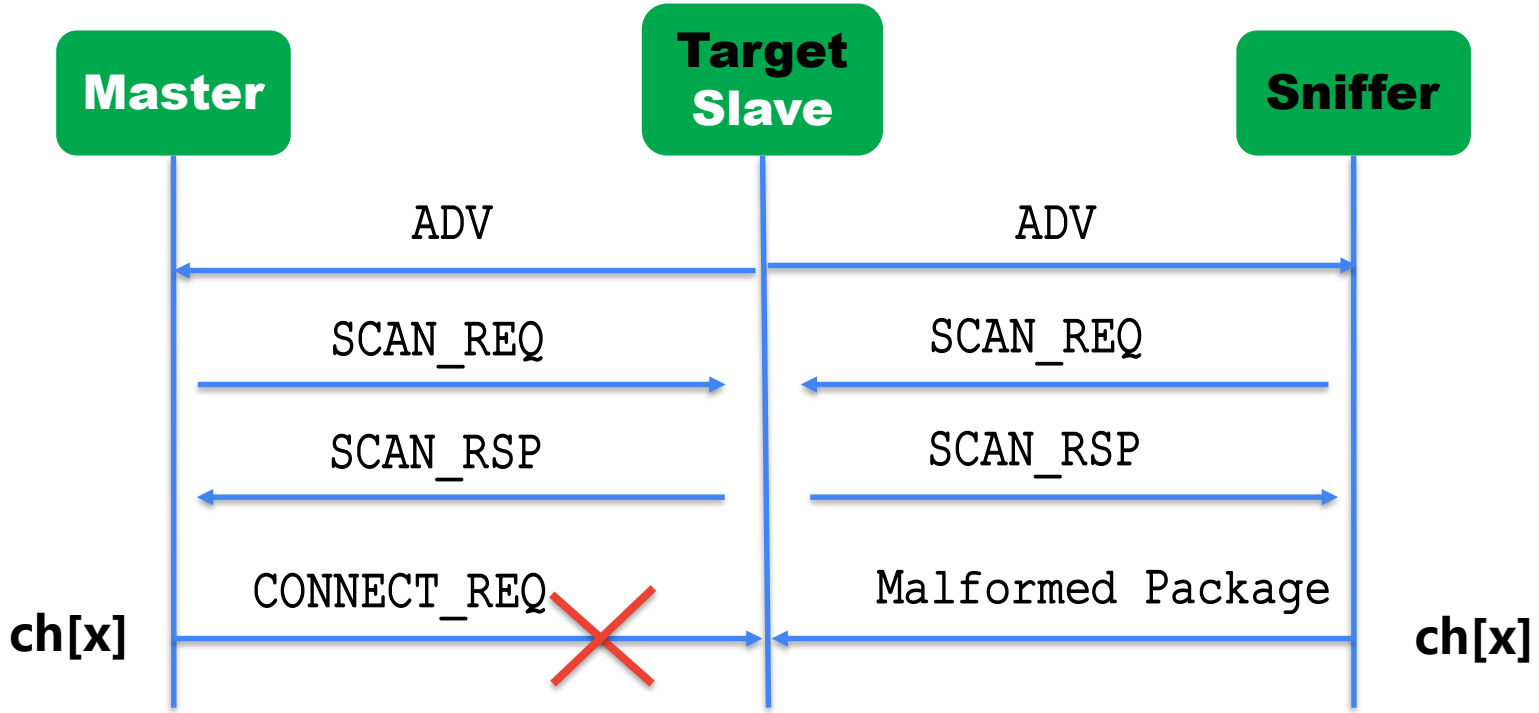


Ubertooth one

BLE 阻断

\

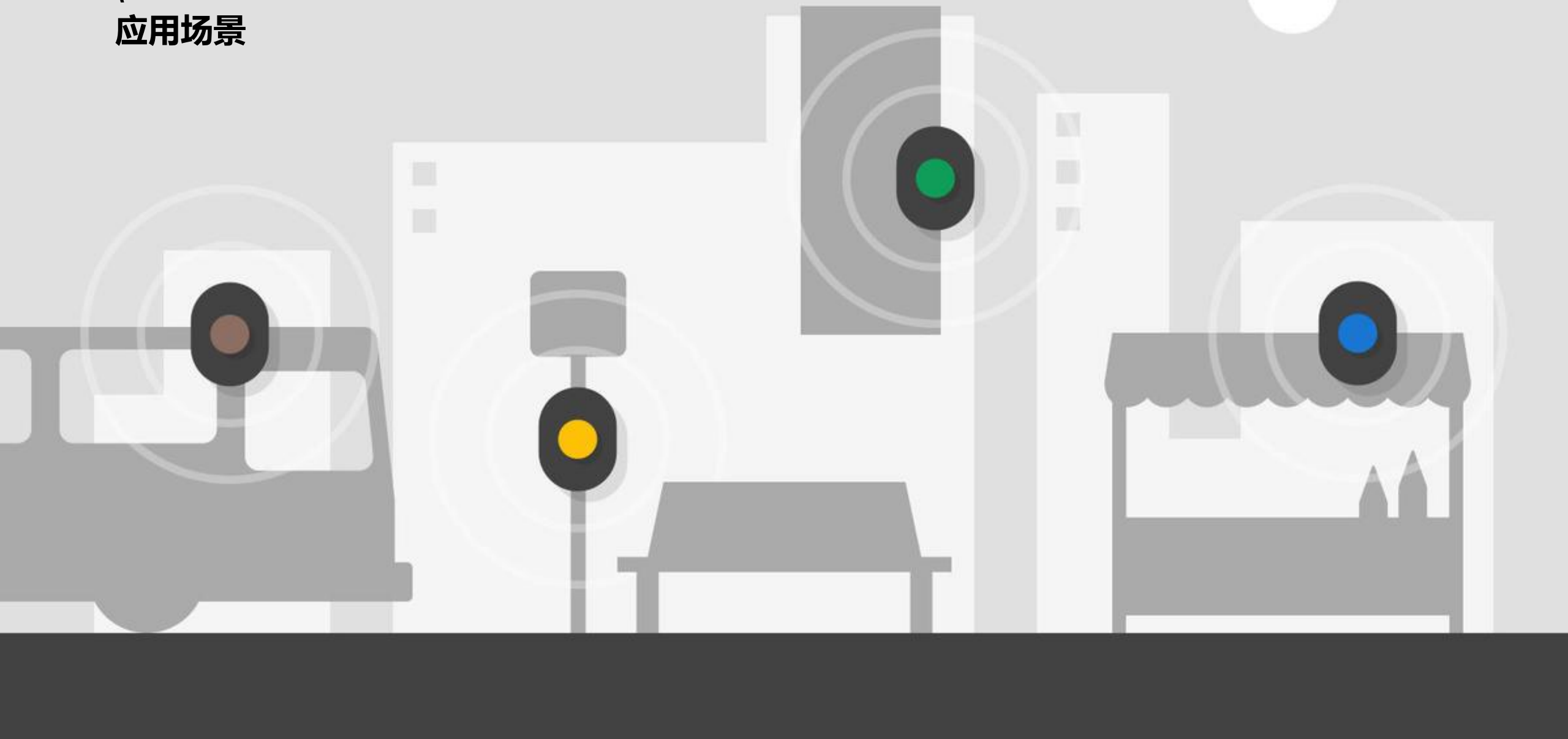
阻断方式


Master
Target Slave
Sniffer
ADV
ADV
SCAN_REQ
SCAN_REQ
SCAN_RSP
SCAN_RSP
CONNECT_REQ
Malformed Package
ch[x]
ch[x]

BLE 中继

\

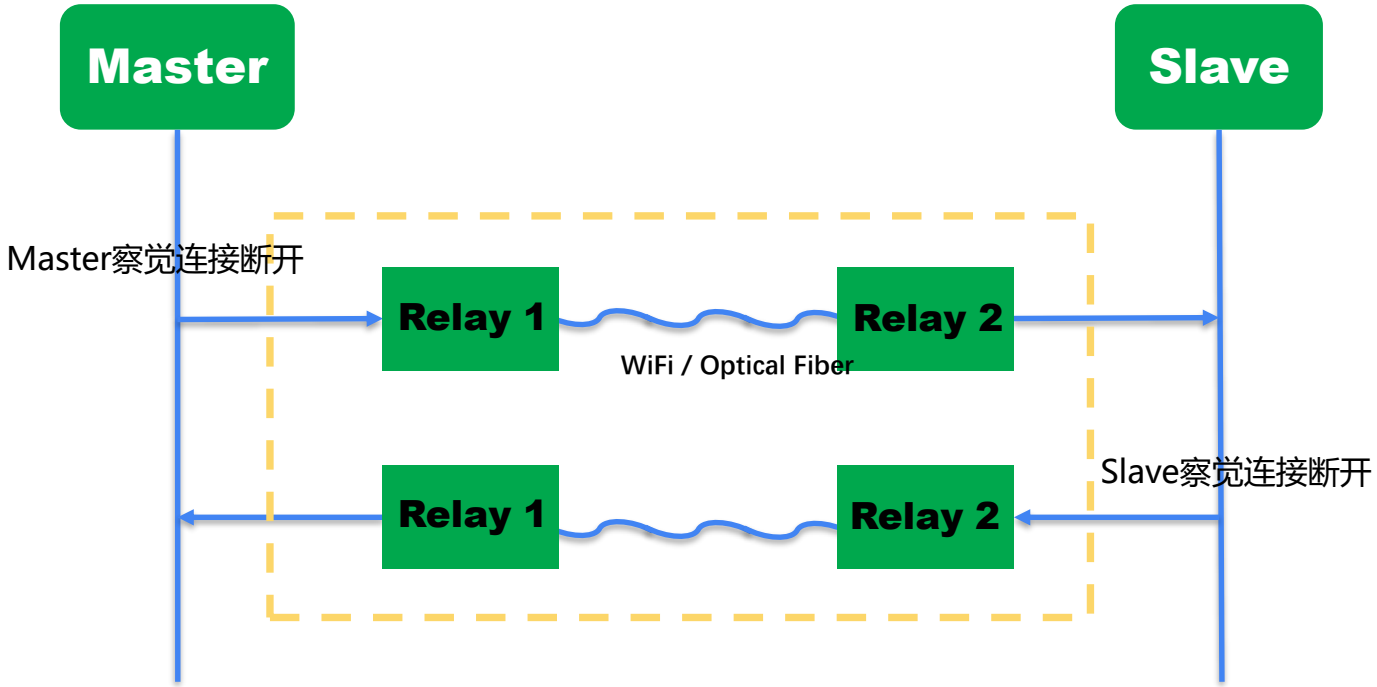
应用场景



BLE 中继

\

中继实现过程

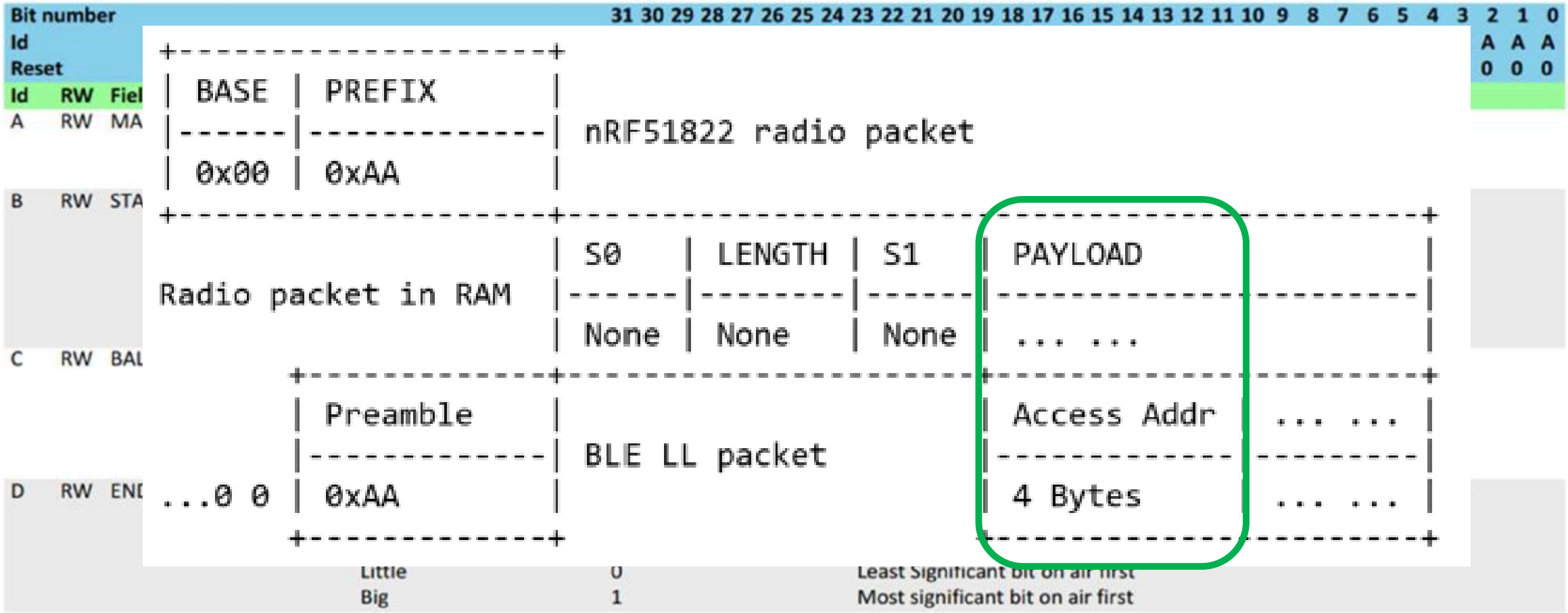


Now I wanna sniff some Bluetooth: Sniffing and Cracking Bluetooth with the UbertoothOne

破解 LLData

\

Access Address



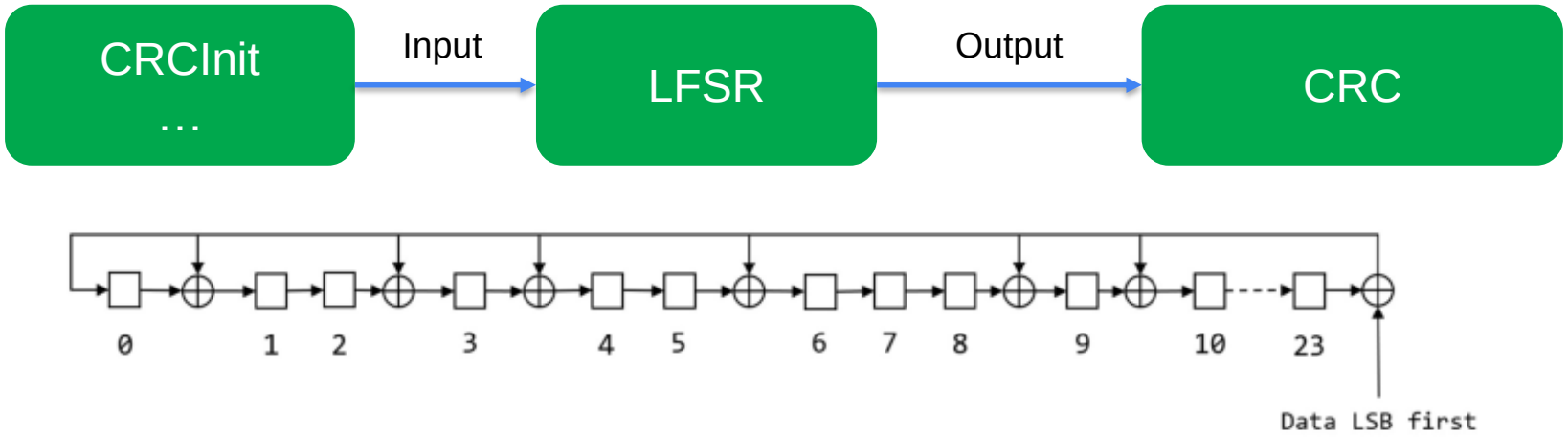
[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

破解 LLData

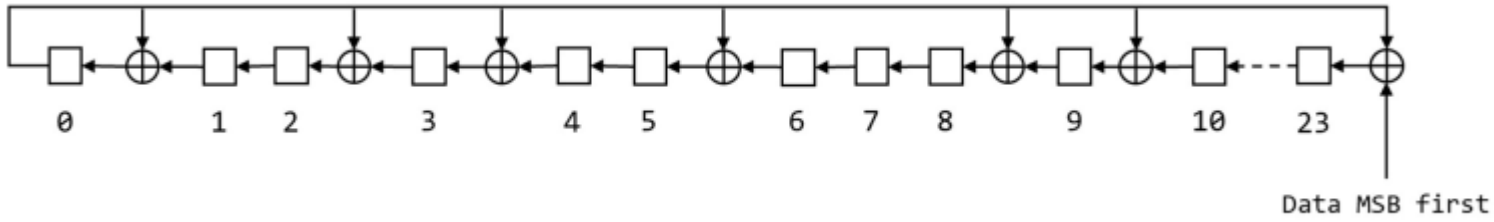
\

CRC Init

- **CRC**生成过程：



- 反转生成 **CRC** 所用的 **LFSR** 而得到的新 **LFSR**：

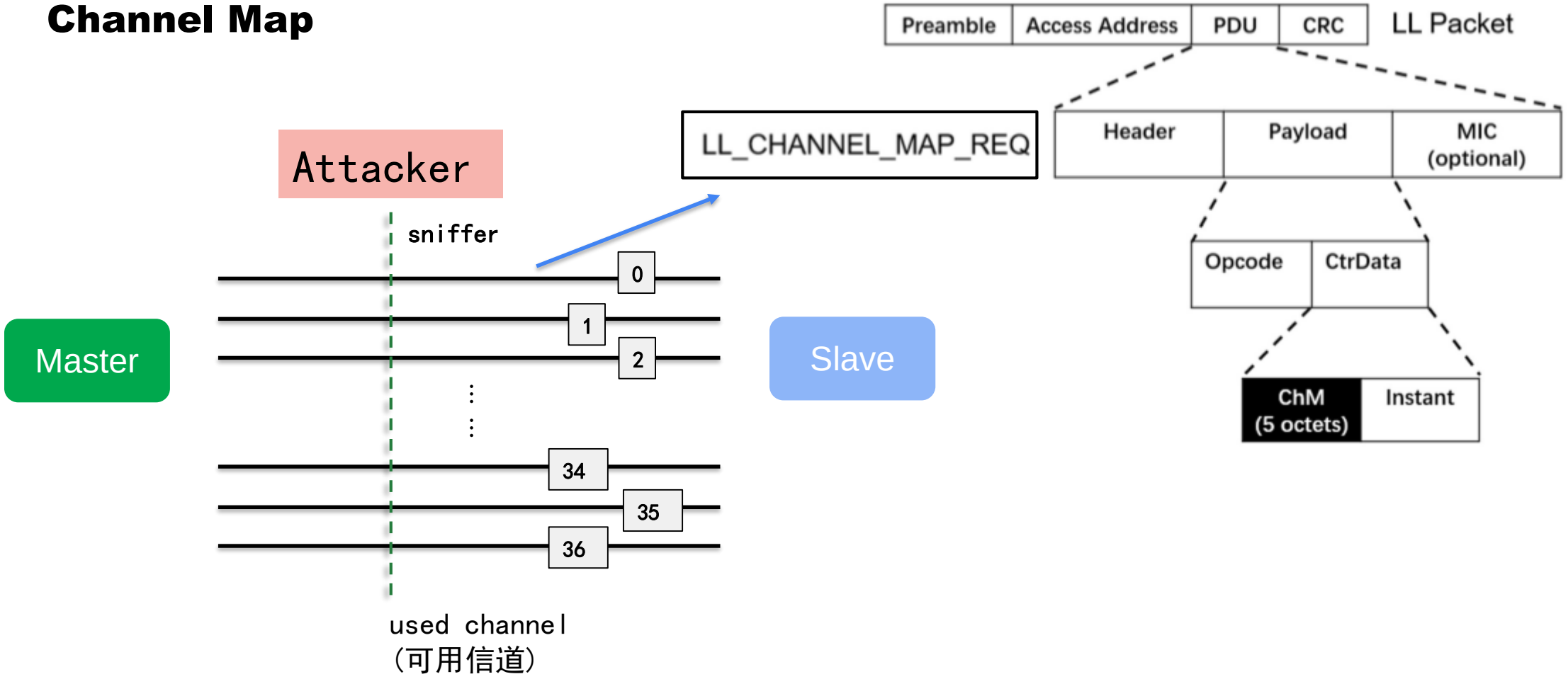


[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

破解 LLData

\

Channel Map

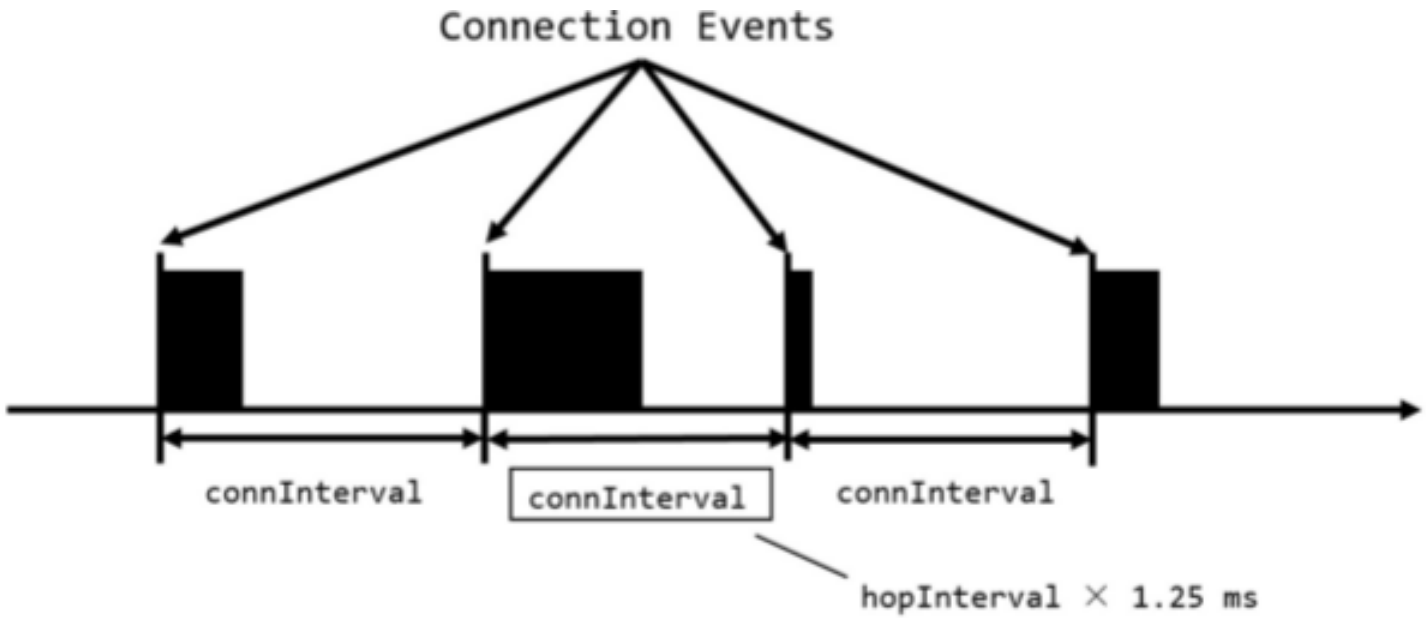


[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

破解 LLData

\

Hop Interval



* Connection Interval=Hop Interval* **1.25ms**

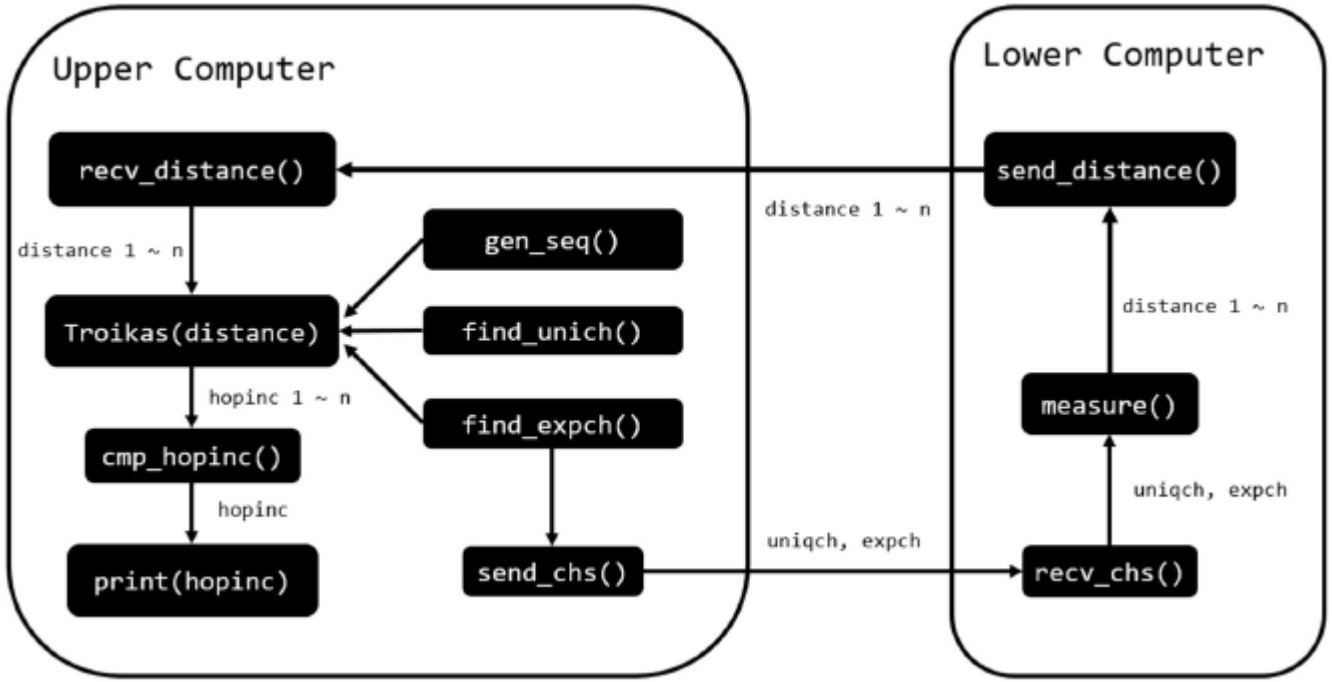
[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

破解 LLData

\

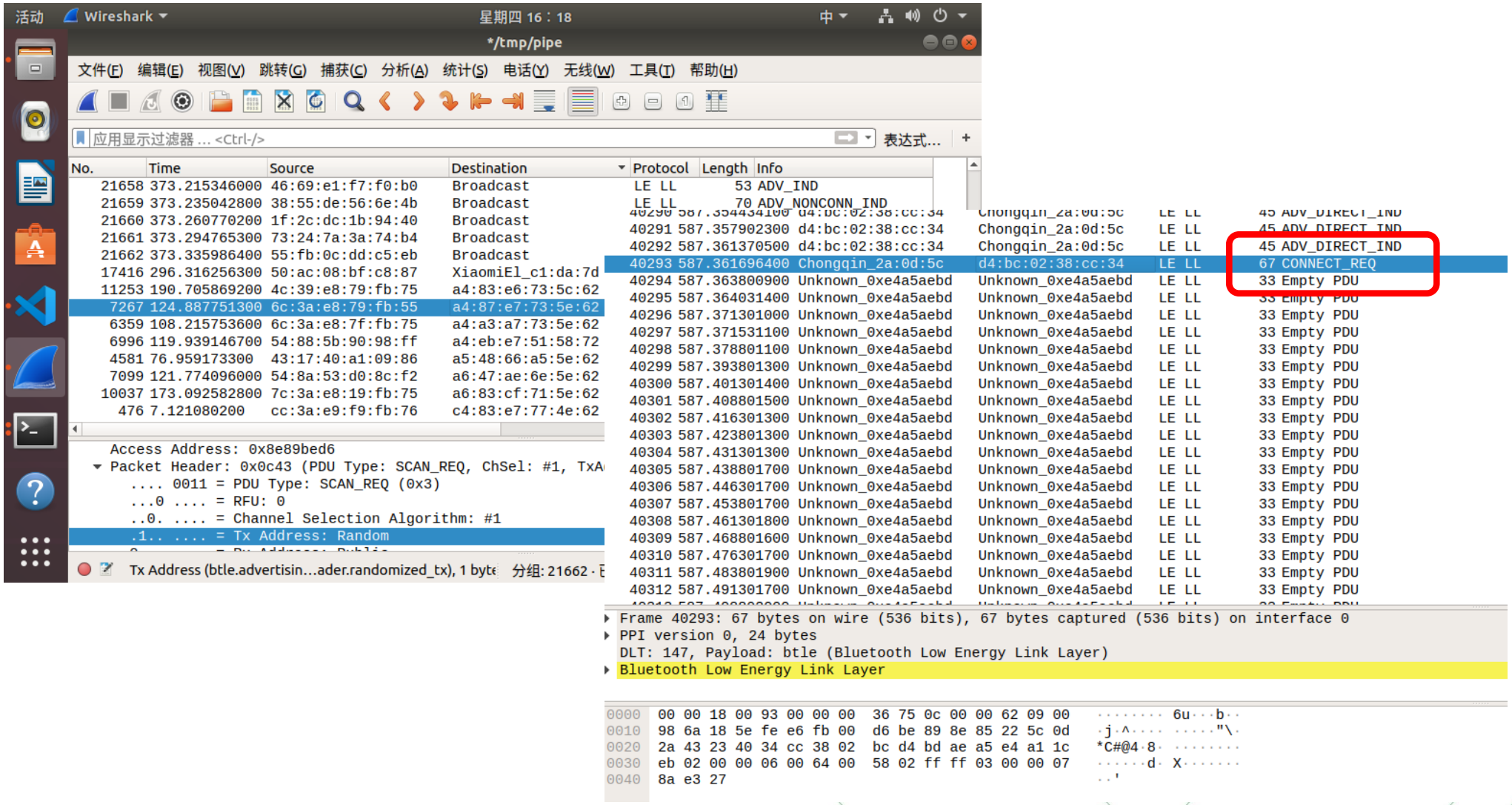
Hop Increment

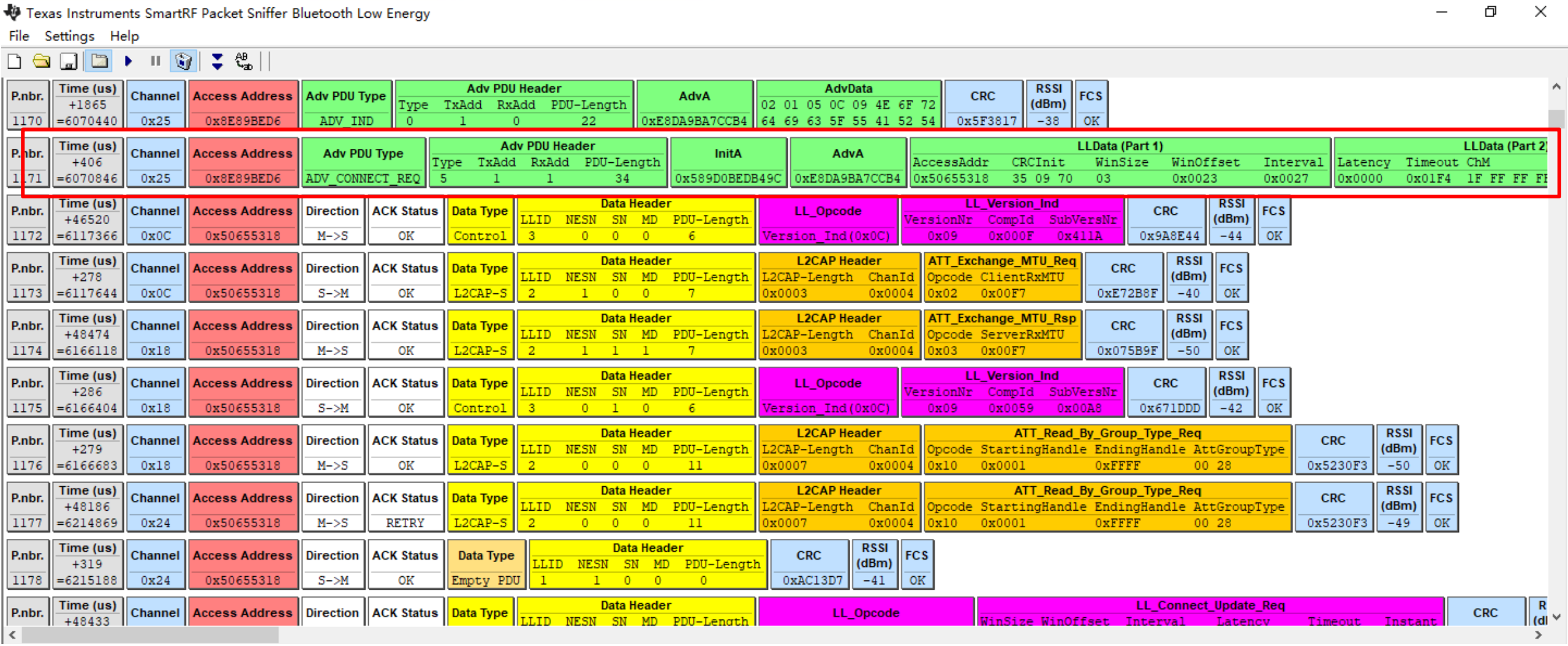
破解Hop Increment → 12种 → 确定目标BLE连接选择用的跳频信道序列 → exploitable → 确定目标BLE连接exploitable信道与unique信道之间的距离牙



[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

实验结果


活动
Wireshark
星期四 16：18
*/tmp/pipe
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
No. Time Source Destination Protocol Length Info
21658 373.215346000 46:69:e1:f7:f0:b0 Broadcast LE LL 53 ADV_IND
21659 373.235042800 38:55:de:56:6e:4b Broadcast LE LL 70 ADV_NONCONN_IND
21660 373.260770200 1f:2c:dc:1b:94:40 Broadcast
21661 373.294765300 73:24:7a:3a:74:b4 Broadcast
21662 373.335986400 55:fb:0c:dd:c5:eb Broadcast
17416 296.316256300 50:ac:08:bf:c8:87 XiaomiEl_c1:da:7d
11253 190.705869200 4c:39:e8:79:fb:75 a4:83:e6:73:5c:62
7267 124.887751300 6c:3a:e8:79:fb:55 a4:87:e7:73:5e:62
6359 108.215753600 6c:3a:e8:7f:fb:75 a4:a3:a7:73:5e:62
6996 119.939146700 54:88:5b:90:98:ff a4:eb:e7:51:58:72
4581 76.959173300 43:17:40:a1:09:86 a5:48:66:a5:5e:62
7099 121.774096000 54:8a:53:d0:8c:f2 a6:47:ae:6e:5e:62
10037 173.092582800 7c:3a:e8:19:fb:75 a6:83:cf:71:5e:62
476 7.121080200 cc:3a:e9:f9:fb:76 c4:83:e7:77:4e:62
Access Address: 0x8e89bed6
Packet Header: 0x0c43 (PDU Type: SCAN_REQ, ChSel: #1, TxA
.... 0011 = PDU Type: SCAN_REQ (0x3)
...0 .... = RFU: 0
..0. .... = Channel Selection Algorithm: #1
.1.. .... = Tx Address: Random
Tx Address (btle.advertisin…ader.randomized_tx), 1 byte
分组: 21662 ·
40291 587.357902300 d4:bc:02:38:cc:34 Chongqin_2a:0d:5c LE LL 45 ADV_DIRECT_IND
40292 587.361370500 d4:bc:02:38:cc:34 Chongqin_2a:0d:5c LE LL 45 ADV_DIRECT_IND
40293 587.361696400 Chongqin_2a:0d:5c d4:bc:02:38:cc:34 LE LL 67 CONNECT_REQ
40294 587.363800900 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40295 587.364031400 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40296 587.371301000 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40297 587.371531100 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40298 587.378801100 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40299 587.393801300 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40300 587.401301400 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40301 587.408801500 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40302 587.416301300 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40303 587.423801300 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40304 587.431301300 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40305 587.438801700 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40306 587.446301700 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40307 587.453801700 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40308 587.461301800 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40309 587.468801600 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40310 587.476301700 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40311 587.483801900 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
40312 587.491301700 Unknown_0xe4a5aebd Unknown_0xe4a5aebd LE LL 33 Empty PDU
Frame 40293: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
PPI version 0, 24 bytes
DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
Bluetooth Low Energy Link Layer
0000 00 00 18 00 93 00 00 00 36 75 0c 00 00 62 09 00 ···· ···· 6u···b··
0010 98 6a 18 5e fe e6 fb 00 d6 be 89 8e 85 22 5c 0d ·j·^···· ·····"\·
0020 2a 43 23 40 34 cc 38 02 bc d4 bd ae a5 e4 a1 1c *C#@4·8· ····
0030 eb 02 00 00 06 00 64 00 58 02 ff ff 03 00 00 07 ····· d· X·····
0040 8a e3 27 ··'


Texas Instruments SmartRF Packet Sniffer Bluetooth Low Energy
File Settings Help
P.nbr. 1170 | Time (us) +1865 =6070440 | Channel 0x25 | Access Address 0x8E89BED6 | Adv PDU Type ADV_IND | Adv PDU Header Type 0 TxAdd 1 RxAdd 0 PDU-Length 22 | AdvA 0xE8DA9BA7CCB4 | AdvData 02 01 05 0C 09 4E 6F 72 64 69 63 5F 55 41 52 54 | CRC 0x5F3817 | RSSI (dBm) -38 | FCS OK
P.nbr. 1171 | Time (us) +406 =6070846 | Channel 0x25 | Access Address 0x8E89BED6 | Adv PDU Type ADV_CONNECT_REQ | Adv PDU Header Type 5 TxAdd 1 RxAdd 1 PDU-Length 34 | InitA 0x589D0BEDB49C | AdvA 0xE8DA9BA7CCB4 | LLData (Part 1) AccessAddr 0x50655318 CRCInit 35 09 70 WinSize 03 WinOffset 0x0023 Interval 0x0027 | LLData (Part 2) Latency 0x0000 Timeout 0x01F4 ChM 1F FF FF FF
P.nbr. 1172 | Time (us) +46520 =6117366 | Channel 0x0C | Access Address 0x50655318 | Direction M->S | ACK Status OK | Data Type Control | Data Header LLID 3 NESN 0 SN 0 MD 0 PDU-Length 6 | LL_Opcode Version_Ind(0x0C) | LL_Version_Ind VersionNr 0x09 CompId 0x000F SubVersNr 0x411A | CRC 0x9A8E44 | RSSI (dBm) -44 | FCS OK
P.nbr. 1173 | Time (us) +278 =6117644 | Channel 0x0C | Access Address 0x50655318 | Direction S->M | ACK Status OK | Data Type L2CAP-S | Data Header LLID 2 NESN 1 SN 0 MD 0 PDU-Length 7 | L2CAP Header L2CAP-Length 0x0003 ChanId 0x0004 | ATT_Exchange_MTU_Req Opcode 0x02 ClientRxMTU 0x00F7 | CRC 0xE72B8F | RSSI (dBm) -40 | FCS OK
P.nbr. 1174 | Time (us) +48474 =6166118 | Channel 0x18 | Access Address 0x50655318 | Direction M->S | ACK Status OK | Data Type L2CAP-S | Data Header LLID 2 NESN 1 SN 1 MD 1 PDU-Length 7 | L2CAP Header L2CAP-Length 0x0003 ChanId 0x0004 | ATT_Exchange_MTU_Rsp Opcode 0x03 ServerRxMTU 0x00F7 | CRC 0x075B9F | RSSI (dBm) -50 | FCS OK
P.nbr. 1175 | Time (us) +286 =6166404 | Channel 0x18 | Access Address 0x50655318 | Direction S->M | ACK Status OK | Data Type Control | Data Header LLID 3 NESN 0 SN 1 MD 0 PDU-Length 6 | LL_Opcode Version_Ind(0x0C) | LL_Version_Ind VersionNr 0x09 CompId 0x0059 SubVersNr 0x00A8 | CRC 0x671DDD | RSSI (dBm) -42 | FCS OK
P.nbr. 1176 | Time (us) +279 =6166683 | Channel 0x18 | Access Address 0x50655318 | Direction M->S | ACK Status OK | Data Type L2CAP-S | Data Header LLID 2 NESN 0 SN 0 MD 0 PDU-Length 11 | L2CAP Header L2CAP-Length 0x0007 ChanId 0x0004 | ATT_Read_By_Group_Type_Req Opcode 0x10 StartingHandle 0x0001 EndingHandle 0xFFFF AttGroupType 00 28 | CRC 0x5230F3 | RSSI (dBm) -50 | FCS OK
P.nbr. 1177 | Time (us) +48186 =6214869 | Channel 0x24 | Access Address 0x50655318 | Direction M->S | ACK Status RETRY | Data Type L2CAP-S | Data Header LLID 2 NESN 0 SN 0 MD 0 PDU-Length 11 | L2CAP Header L2CAP-Length 0x0007 ChanId 0x0004 | ATT_Read_By_Group_Type_Req Opcode 0x10 StartingHandle 0x0001 EndingHandle 0xFFFF AttGroupType 00 28 | CRC 0x5230F3 | RSSI (dBm) -49 | FCS OK
P.nbr. 1178 | Time (us) +319 =6215188 | Channel 0x24 | Access Address 0x50655318 | Direction S->M | ACK Status OK | Data Type Empty PDU | Data Header LLID 1 NESN 1 SN 0 MD 0 PDU-Length 0 | CRC 0xAC13D7 | RSSI (dBm) -41 | FCS OK
P.nbr. | Time (us) +48433 | Channel | Access Address | Direction | ACK Status | Data Type | Data Header LLID NESN SN MD PDU-Length | LL_Opcode | LL_Connect_Update_Req WinSize WinOffset Interval Latency Timeout Instant | CRC

总结

优势

- 方案具有很强的可行性；
- 相对2018 BtleJack 优化了嗅探 access address 的效率；
- 可以快速切换嗅探信道，避免固件在一个信道上长时间停留

不足

- PDU抓包困难；
  破解效率有待提高
- 方案仅适用于首次连接的蓝牙设备，对于二次连接的两个设备不适用

创新

- 阻断和中继方案具有很强的创新性，首次提出

下一步研究

- 破解过程需进一步优化；
  需要提高破解效率
- 需要根据特定应用场景调整抓包策略

参考资料

[1] Bluetooth Core Specification Core_v5.0[EB/OL]. Bluetooth SIG Proprietary. http://www.uni-obuda.hu/users/wuhrlt/MSc_Adatatvitel/Core_v5.0.pdf. 2016.12.06

[2] Michael Ossmann, Dominic Spill, Mike Ryan, Will Code, Jared Boone. Ubertooth[CP/OL]. https://github.com/greatscottgadgets/ubertooth/, 2018.12.20.

[3] Damien Cauquil. Btlejack firmware[CP/OL]. https://github.com/virtualabs/btlejackfirmware/tree/e664385437068c5bbcb9ac9dc67c883de9754997, 2018.9.17.

[4] 徐井源. 低功耗蓝牙连接阻断与设备接管方法研究[D].华中科技大学,2019.

[5] Damien Cauquil. BtleJack: a new Bluetooth Low Energy swiss-army knife[CP/OL]. https://github.com/virtualabs/btlejack, 2019.2.11.

[6] Mahyar Taj Dini. Volodymyr Sokolov. Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio[C]. arXiv preprint arXiv 1902.08595, 2019.2.

[7] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg. Meltdown[C]. arXiv preprint arXiv:1801.01207, 2018.1.3.

[8] Kocher, Paul, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution[C]. arXiv preprint arXiv:1801.01203, 2018.1.3.

360大学 | 飞扬

Thanks for Your Listening

未来安全研究院　张伟
zhangwei13@360.cn