MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

DGA

Fingerprinting of Bluetooth BR/EDR devices using wideband SDR

Naomi WEIC
Margaux BOUGEARD
Arnaud RIGOLLÉ

Scope of study

❑ Bluetooth : Reference technology for radio connectivity usage

- Standardised [R0] from 1994 with several successive major evolutions : scope focused on BR/EDR only
- Devoted to short-range applications (WPAN)
- Information exchanged via Bluetooth : potentially sensitive

❑ Bluetooth specifications : supposed to guarantee the confidentiality

- Data encryption
- Strengthened by security mechanisms : frequency hopping (FH), whitening , physical address masking

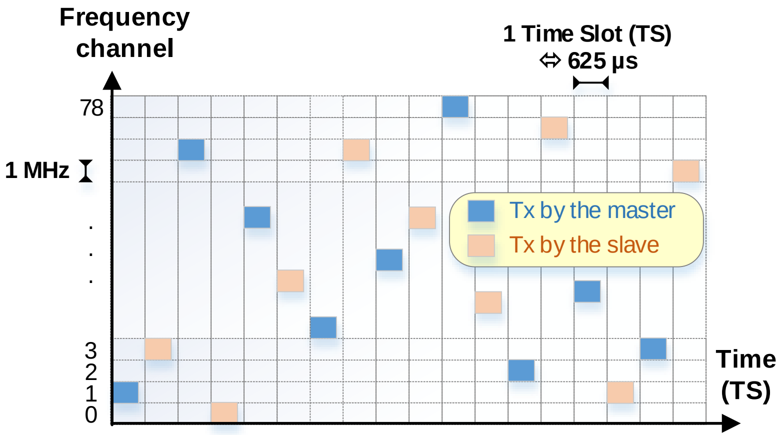
❑ Study goals

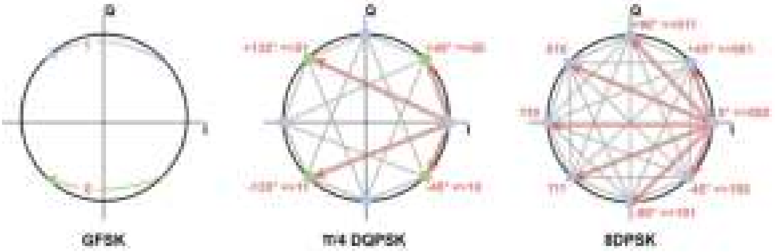
- Identifying Bluetooth users : fingerprinting
- Sniffing Bluetooth communications

Bluetooth overview

❑ Radio waveform & protocol

- 2.4 GHz ISM band
- FHSS communication system ⇒ difficult to sniff
  - 79 contiguous channels with 1 MHz unitary bandwidth
  - switch of channel every Time Slot (625 μs) □ 1600 hops / s
- 6-byte physical address assigned to each device
- 3 modulation schemes ⇒ bit rate of 1, 2 or 3 Mbps





❑ Security

- Diffie–Hellman key exchange (Secure Simple Pairing from Bluetooth v2.1)
- Data randomization by whitening
- Data symmetric encryption with E0 or AES-CCM

Security vulnerabilities exploitable via SDR

❑ Attacks published exploiting Bluetooth waveform security flaws

- Physical address can be revealed even though supposed to remain secret [R1], [R2]

  ⇒ identifying, locating and tracking Bluetooth equipments

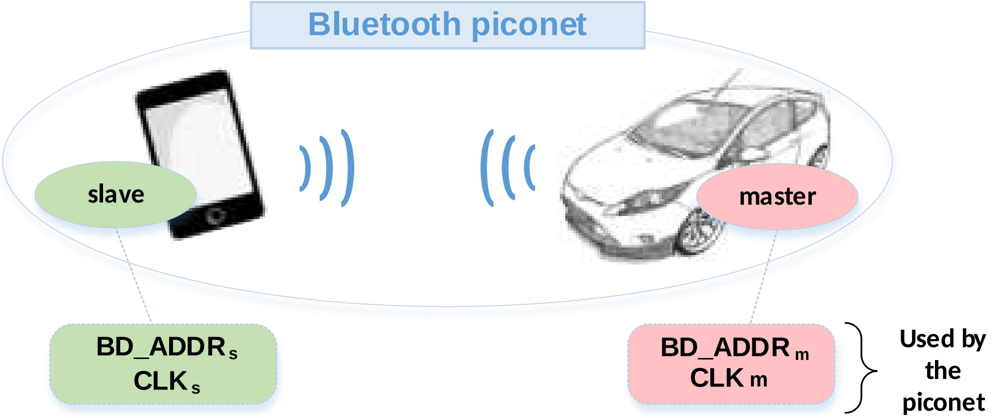
- Clock value can also be retrieved [R3]

  ⇒ access to FH pattern

❑ Using commercial wideband Software Defined Radio (SDR) enables [R4]

- Instantaneous digitization of Bluetooth wideband radio signal (80 MHz)
- Overcoming FHSS techniques, supposed to ensure the security of the Bluetooth waveform
- Monitoring of different communications and channels in parallel
- Extract information much more quickly
- Interact (Rx/Tx) with target devices on the whole band

Bluetooth piconet



❑ Piconet composition

- 1 master
- Up to 7 slaves

❑ Piconet features

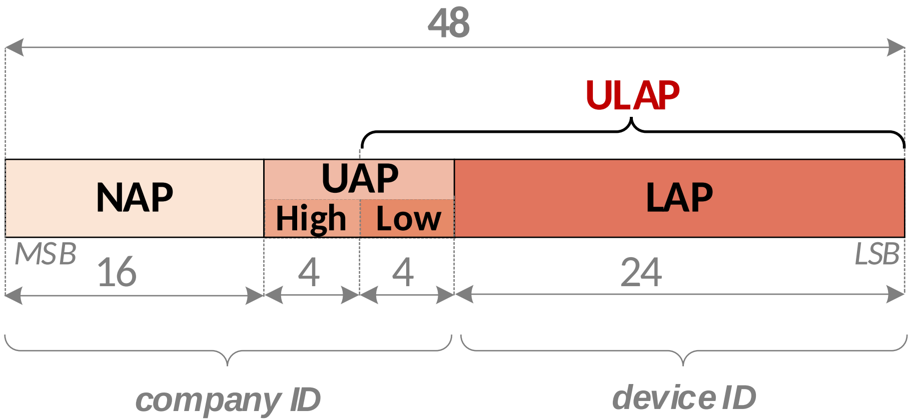
Settings used to control the piconet are derived from the master's characteristics :

- 48-bit physical address for unique identification
- Clock value (28-bit counter) with a 312.5 µs granularity

❑ Targeted information

- Get access to both piconet **secret** main features (master physical address and clock) controlling some key algorithms as the FH

Bluetooth Device physical Address (BD_ADDR)

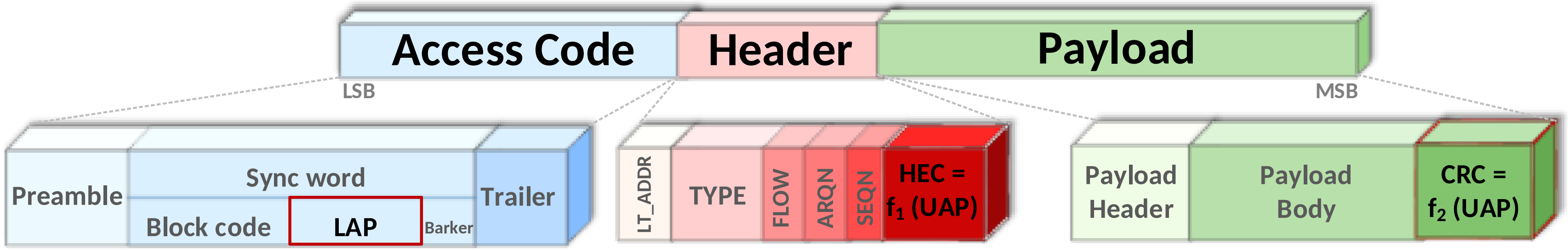


- **LAP**
  - 24-bit chip number assigned by manufacturer
- **UAP**
  - 8-bit value, used to control some algorithms in addition to LAP
- **NAP**
  - 16-bit non-significant part (unused by Bluetooth algorithms)
  - retrievable by BF (~128 trials) from UAP + OUI table [R5]

ULAP
⇒ 28-bit entropy used as secret input for FH algorithm

UAP + NAP = 24-bit public number [R5] assigned by IEEE and identifying Bluetooth manufacturer

Bluetooth BR/EDR : packet format



❑ Access code (AC)

- Identical for all packets Tx in the same piconet
- Constructed from master **LAP**

❑ Header

- Packet control information + **HEC** (integrity check bits)

❑ Payload

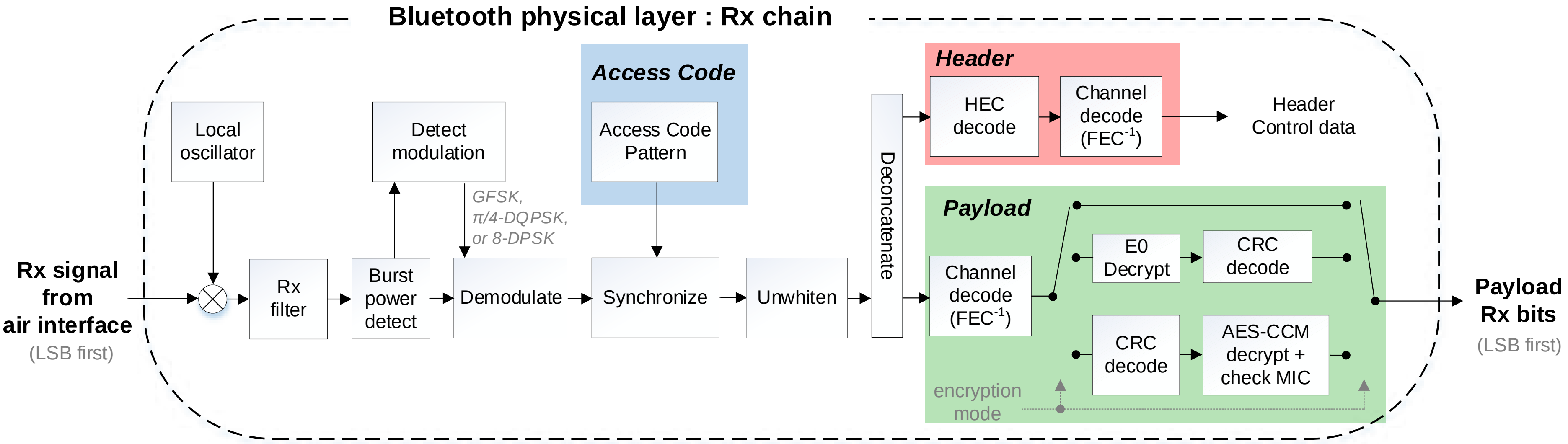
- User data from higher layers + **CRC** (integrity check bits)

Capture of a piconet packet can give access to significant parts of BD_ADDR (after tricky processing)

Accessing the Bluetooth physical layer

❑ Benefits of in-house physical layer development

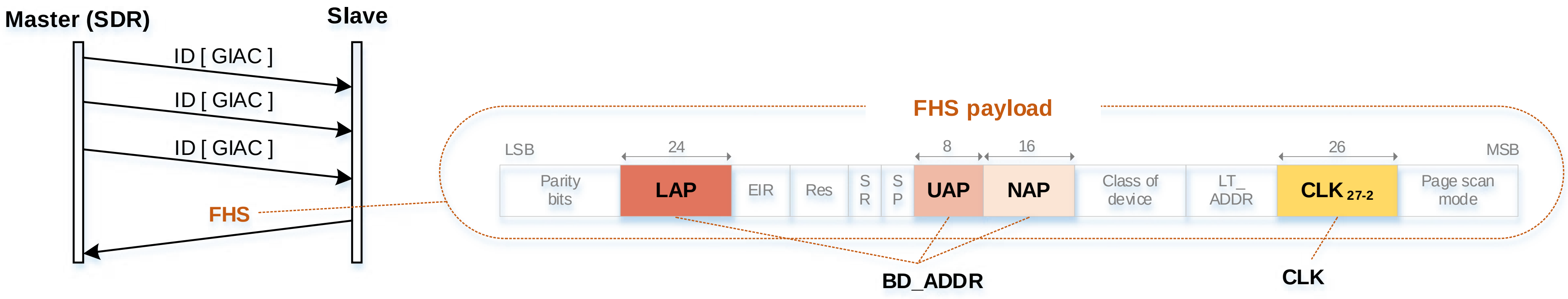
- Master the protocol
- Access messages managing connection establishment & security (LMP protocol)
- Extract supposedly inaccessible data



Method #1 : active fingerprinting using inquiry

❑ Method : run inquiry procedure

- Usage of a WB SDR module in **active** mode
- Any Bluetooth device defined as "discoverable" must answer
- By sending a FHS packet with BD_ADDR full identity & clock



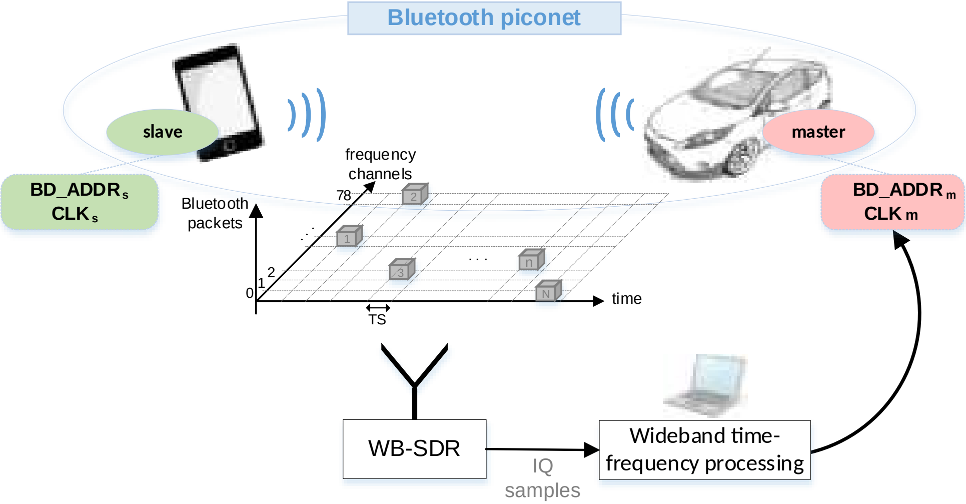
❑ Issues

- Unstealthy : radio transmissions required
- Unreliable : target user will never respond if configured as "non-discoverable"
- Many Bluetooth users may answer

Method #2 : passive fingerprinting by WB sniffing

❑ Goal = overcoming flaws of method #1

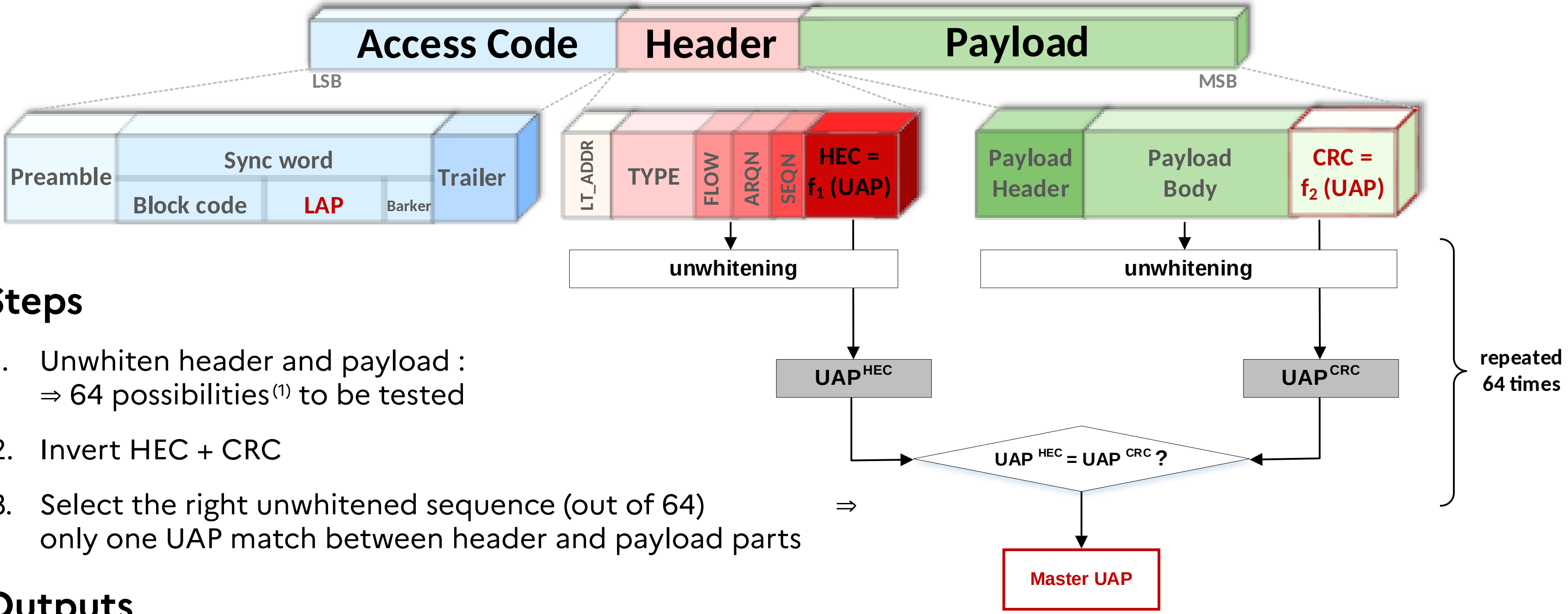
- Remaining stealthy **passive** mode
- Reliability : being able to identify a device, even if defined in “non-discoverable” mode



❑ Setup

- Usage of a wideband SDR module (Rx only) + a PC for post-processing of digitized IQ samples
- Capture radio signals transmitted within one or several Bluetooth piconet(s)

Method #2 - challenge #1 : BD_ADDR extraction



❑ Steps

1. Unwhiten header and payload :
   ⇒ 64 possibilities(1) to be tested
2. Invert HEC + CRC
3. Select the right unwhitened sequence (out of 64) ⇒
   only one UAP match between header and payload parts

❑ Outputs

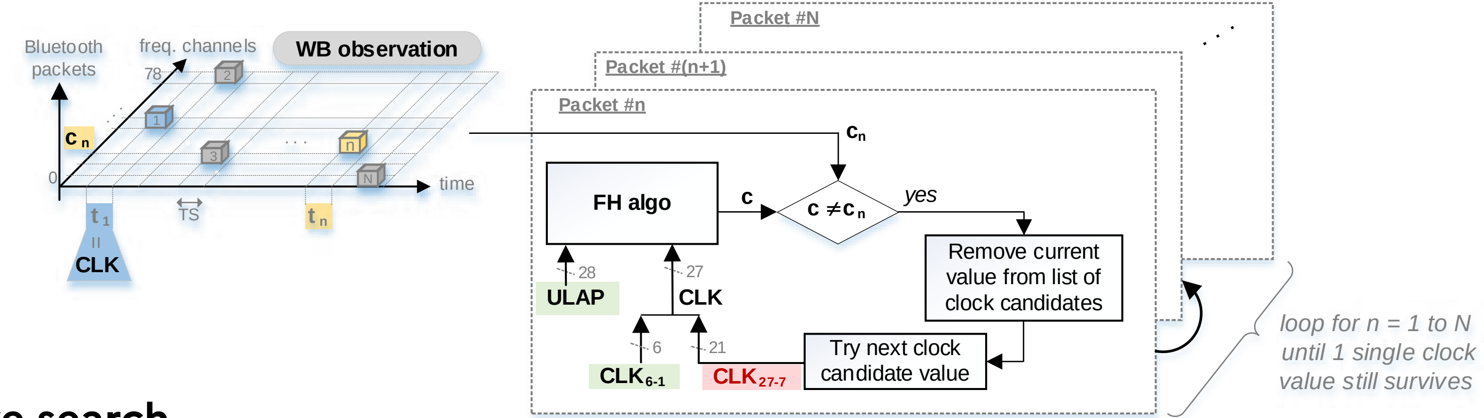
- Full 48-bit BD_ADDR : LAP + UAP + NAP derived from OUI table [R5]
- 6 bits ($CLK_{6\text{-}1}$) of the master clock

(1) Since whitening uses $CLK_{6\text{-}1}$ 6-bit secret value on the TX side

Method #2 - challenge #2 : extract piconet clock

❑ Principle [R3] : Brute force the Frequency Hopping algorithm

- FH algorithm : known from Bluetooth specs
- ULAP and CLK_{6-1} : secret values extracted from challenge #1
- CLK 21 missing bits (CLK_{27-7}) can be found by BF



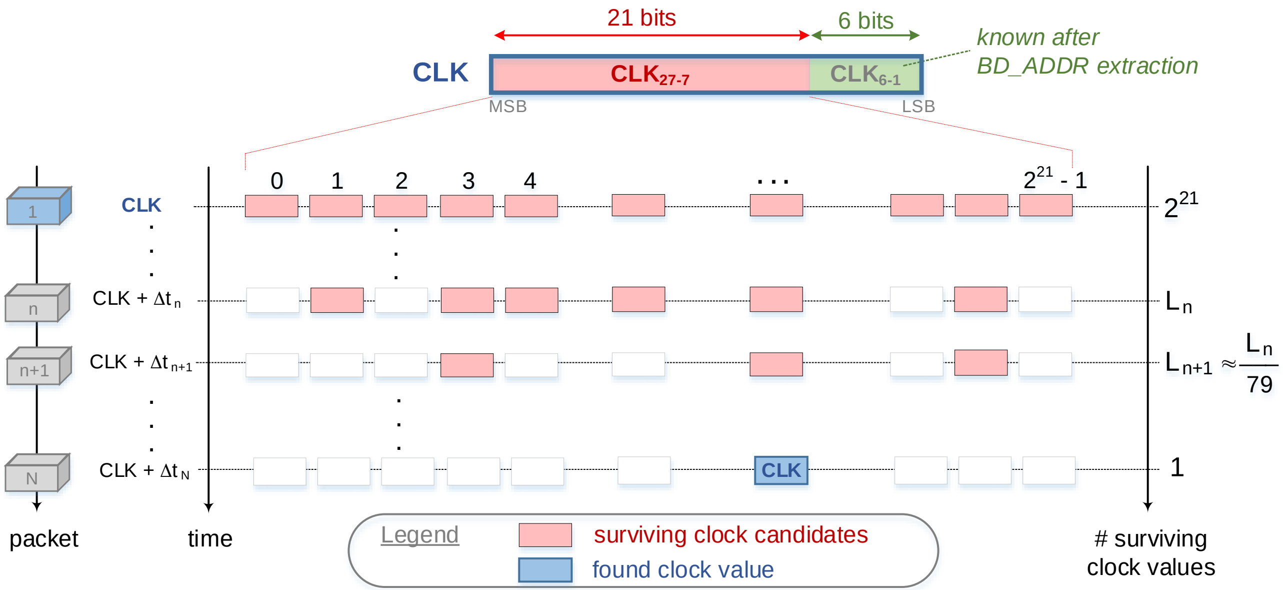
❑ Iterative search

- The list of clock candidates is initialized with all 2^{21} possible values
- For each n^{th} new packet, list is reduced to clock values able to explain the whole observation (from 1 to n)
- Once the list is reduced to 1 single element (after N packets), the piconet clock value is uniquely identified

Method #2 - challenge #2 : extract piconet clock

❑ Algorithm convergence

- High initial entropy (21 bits)
- But geometrical progression at each iteration : geometric factor = 79 (2)
  ⇒ N = 4 iterations only typically required to find the (unique) piconet clock value (3)



(2) 79 being the number of Bluetooth frequency BR/EDR frequency channels that are all selected equiprobably

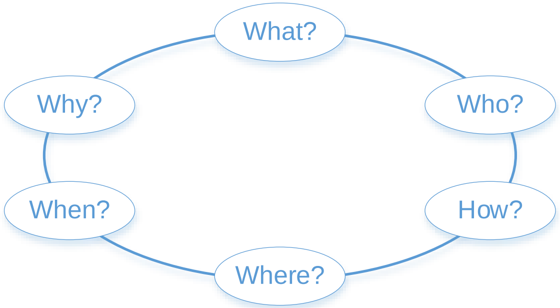
(3) since $79^4 > 2^{21}$

Conclusion

❑ Achievements

- Some published attacks on Bluetooth BR/EDR sucessfully replayed
  - Physical address extraction
  - Piconet clock extraction
- Some enhancements implemented and made possible by wideband SDR
  - Faster extraction of targeted information (BD_ADDR and piconet clock)
  - Extension of attacks with RX/TX interaction possible on the whole Bluetooth band between WB-SDR module and targeted devices

❑ Questions ?



Bibliography

❑ Standards

[R0] Bluetooth SIG, 2023-01-31 Bluetooth Core Specification V5.4

❑ IEEE publications

[R1] D. Spill & A. Bittau, 2007 : Bluesniff : Eve meets Alice and Bluetooth

[R2] M. Cominelli et al., 2020 : Even Black Cats Cannot Stay Hidden in the Dark : Full-band De-anonymization of Bluetooth Classic Devices

[R3] A. Tabassam & S. Heiss, 2008 : Bluetooth Clock Recovery and Hop Sequence Synchronization Using Software Defined Radios

❑ SDR tutorial

[R4] National Instruments / Ettus Research USRP Hardware Driver and USRP Manual https://files.ettus.com/manual/page_usrp_x3x0.html

❑ IEEE table

[R5] OUI assignment table https://standards-oui.ieee.org/oui/oui.txt

Glossary

AC Access Code (first temporal part of a Bluetooth packet,used to detect and synchronize a piconet)

AES Advanced Encryption Standard (symmetric encryption)

BD_ADDR Bluetooth Device Address (physical address of a Bluetooth device, coded on 6 bytes)

BF Brute Force

BLE Bluetooth Low Energy (waveform evolution introduced in 2010 in V4.0 standard version and out of scope of this presentation)

BR Basic Rate (1st official version – V1.0 - of the standardised Bluetooth waveform, with a unique modulation rate of 1 Mbps)

CCM Counter with Cipher block chaining Message authentication code

CLK Clock (clock value of the considered Bluetooth piconet, imposed by the master)

CRC Cyclic Redundancy Check (error detection code applied to payload bits)

E0 Bluetooth legacy encryption algorithm

EDR Enhanced Data Rate (Bluetooth waveform evolution introduced in 2004 – V2.0 version - enabling 2 higher data rates of 2 and 3 Mbps)

EUI Extended Unique Identifier

FEC Forward Error Correction

FH Frequency Hop(ping)

FHS FH Synchronization (a type of Bluetooth control packet)

FHSS FH Spread Spectrum

Fingerprinting Identification of the BD_ADDR physical address of a Bluetooth radio device

GIAC General Inquiry AC (predefined AC value used to call all Bluetooth devices during the inquiry phase)

GFSK Gaussian Frequency Shift Keying (modulation used for Bluetooth BR @ 1 Mbps)

Header Second temporal part of a Bluetooth packet

HEC Header Error Check (error detection code applied to Header bits)

ID Identity (a type of Bluetooth control packet)

IEEE Institute of Electrical and Electronics Engineers

Inquiry Procedure used by a Bluetooth device to identify other discoverable Bluetooth equipments within its radio range

ISM Industrial, Scientific and medical (frequency band)

IQ Name of the complex signal samples digitized by the SDR module, I designating the in-phase real channel and Q the quadrature imaginary channel

LAP Lower Address Part (3-byte low order portion of a BD_ADDR address)

LMP Link Manager Protocol

LSB Least Significant Bit

Mbps Mega bits per second

MIC Message Integrity Check

MSB Most Significant Bit

NAP Non-significant Address Part (2-byte high order portion of a BD_ADDR address)

OUI Organisationally Unique Identifier (number assigned by IEEE identifying the Bluetooth device manufacturer)

packet Message from the Bluetooth physical layer transiting on the radio channel

Payload Third and final temporal part of a Bluetooth packet containing data from upper layers

π/4-DQPSK π/4 Differential Quadrature Phase Shift Keying (modulation used for Bluetooth EDR waveform @ 2 Mbps)

Rx Reception

SDR Software Defined Radio (electronic module)

TS Time Slot (TS duration is equal to 0.625 ms for Bluetooth radio waveform)

Tx Transmission

UAP Upper Address Part (1-bye central portion of a BD_ADDR address)

ULAP 28 LSB bits of BD_ADDR (4 UAP LSB bits + LAP) (used to control FH algorithm)

WB Wideband

WPAN Wireless Personal Area Network

8-DPSK 8-state Differential Phase Shift Keying (modulation used for Bluetooth EDR waveform @ 3 Mbps)