KW36 DATA CHANNEL’S RSSI TRACING AND MONITORING DEMONSTRATION SYSTEM OF MULTIPLE CONNECTIONS

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP BLE Products for Automotive

Bluetooth in Automotive

- ## Smart Mobile Devices as the Digital Key
  - Secured information is sent to the vehicle to lock/unlock or start the engine, including RKE and PKE application.
  - Combined with NFC and UWB for full security, convenience and standard compliancy (CCC)
  - Enable Fleet management, Car Sharing and Car Rentals

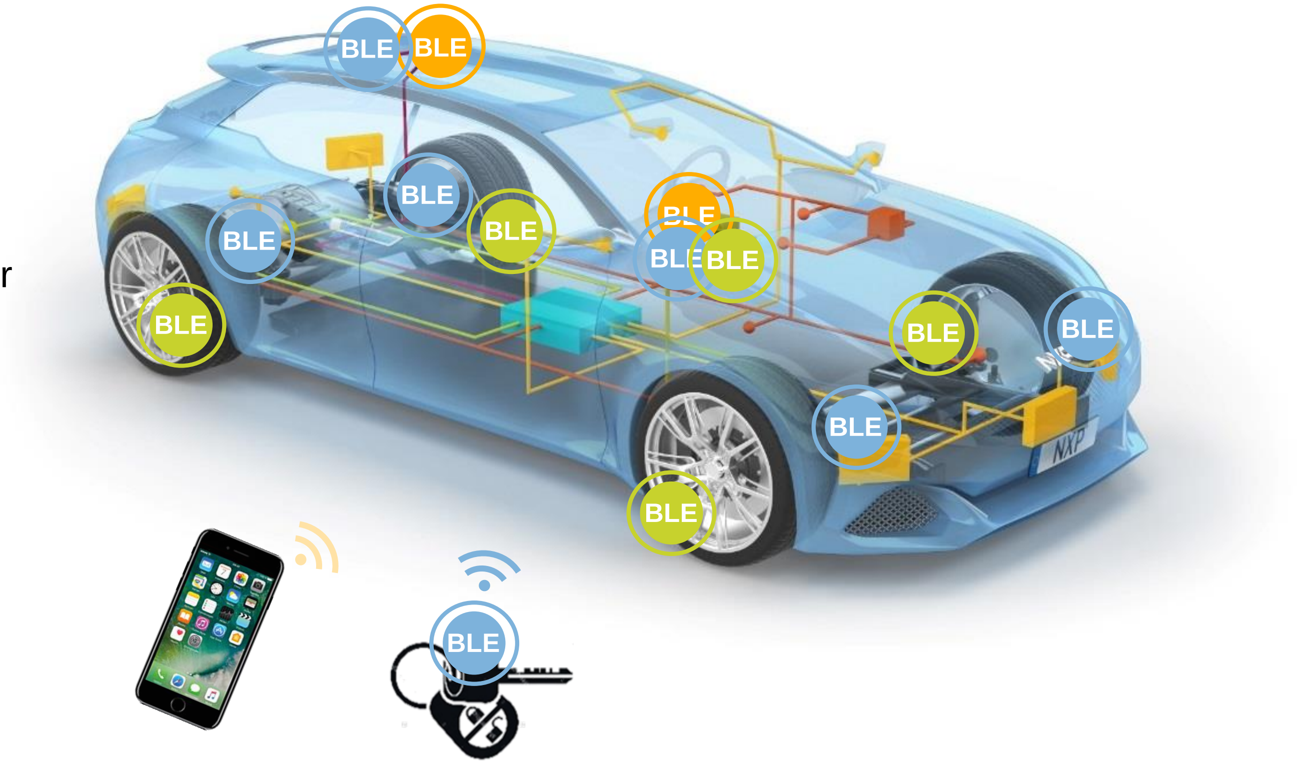
    The smartphone can communicate via BLE to the car either directly to the Body Control Unit or through the car key fob that acts like a gateway

- ## Secure Key Fobs
  - BLE is integrated in the Key Fob to communicate directly with the car replacing SubGhz communication
  - BLE can be use for location use case
    - Passive Entry Passive Start (PEPS)
    - Welcome light and vehicle customization settings
  - Combined with NFC and UWB for full security, convenience and standard compliancy (CCC)

- ## Vehicle Condition & Status Monitoring
  - Leverage BLE in the car for monitoring & updating vehicle status to Driver Information System & Smart Phone

    Tire Pressure Monitoring systems, customized seat settings, service reminders, trouble codes, etc.

- ## In Vehicle Connectivity

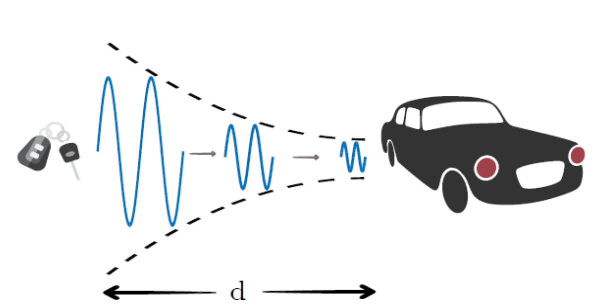


KW3x – Auto BLE for Smart Access

The Industry's First Automotive-Qualified Bluetooth 5-Ready Wireless Microcontrollers (MCU) with integrated CAN-FD

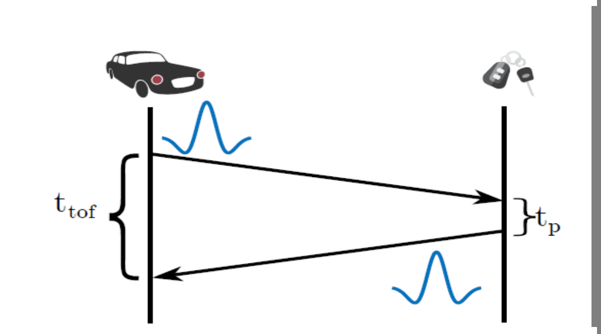
- ✓ Automotive and industrial qualified wireless MCUs (AECQ100-Grade 2 temperature range qualification)
- ✓ Simplified integration of Bluetooth connectivity in cars, enabling automotive manufacturers to deliver added convenience for consumers
- ✓ Complements NXP's automotive secure access portfolio (Classical with LF / Smart with NFC & UWB)

Wireless Ranging Techniques



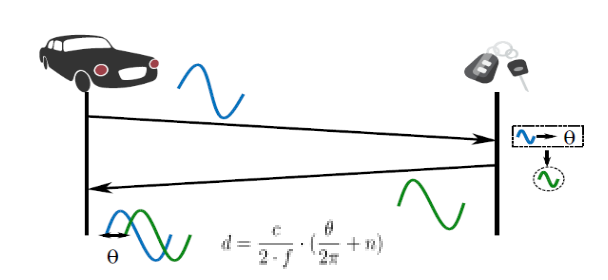
RSSI-Based distance estimation

- Distance is calculated based on the free space path loss equation
- Low accuracy, due to the unknown additional losses
- Examples: LF solution in Passive Keyless Entry key fob for cars
  Bluetooth-based proximity



Time-of-Flight based Ranging

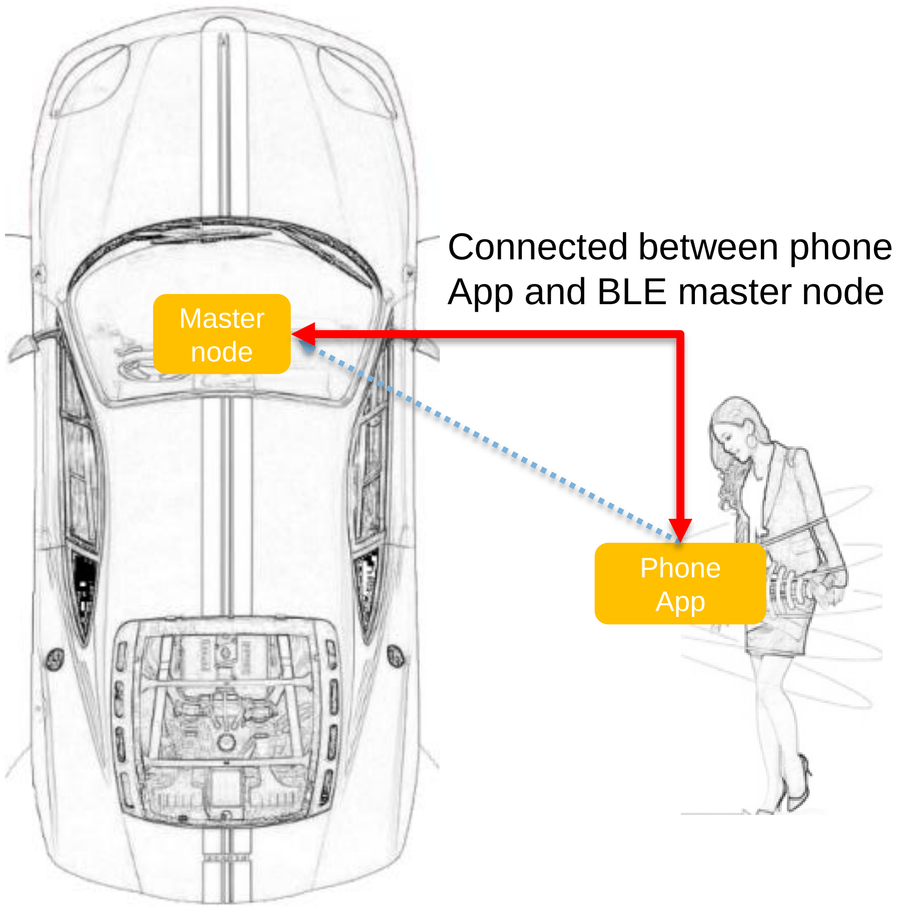
- One way Time-of-Flight: distance is *(t_{rx}-t_{tx})* Speed of light*
- Round-trip Time-of-Flight: Distance is *(t_{total}- t_{proc})* Speed of light*
- Angle-of-Arrival + Time-of-Flight (ToF) / Phase Based Ranging (PDE) can be used to provide 2D/3D positioning (not just ranging).



Phase-based distance estimation

- Distance is calculated based on the phase difference between a received continuous wave signal and a local reference signal
- Examples: LF solution in Passive Keyless Entry key fob for cars
  Bluetooth Phase Based Ranging

Smart BLE Car Key Application in Automotive

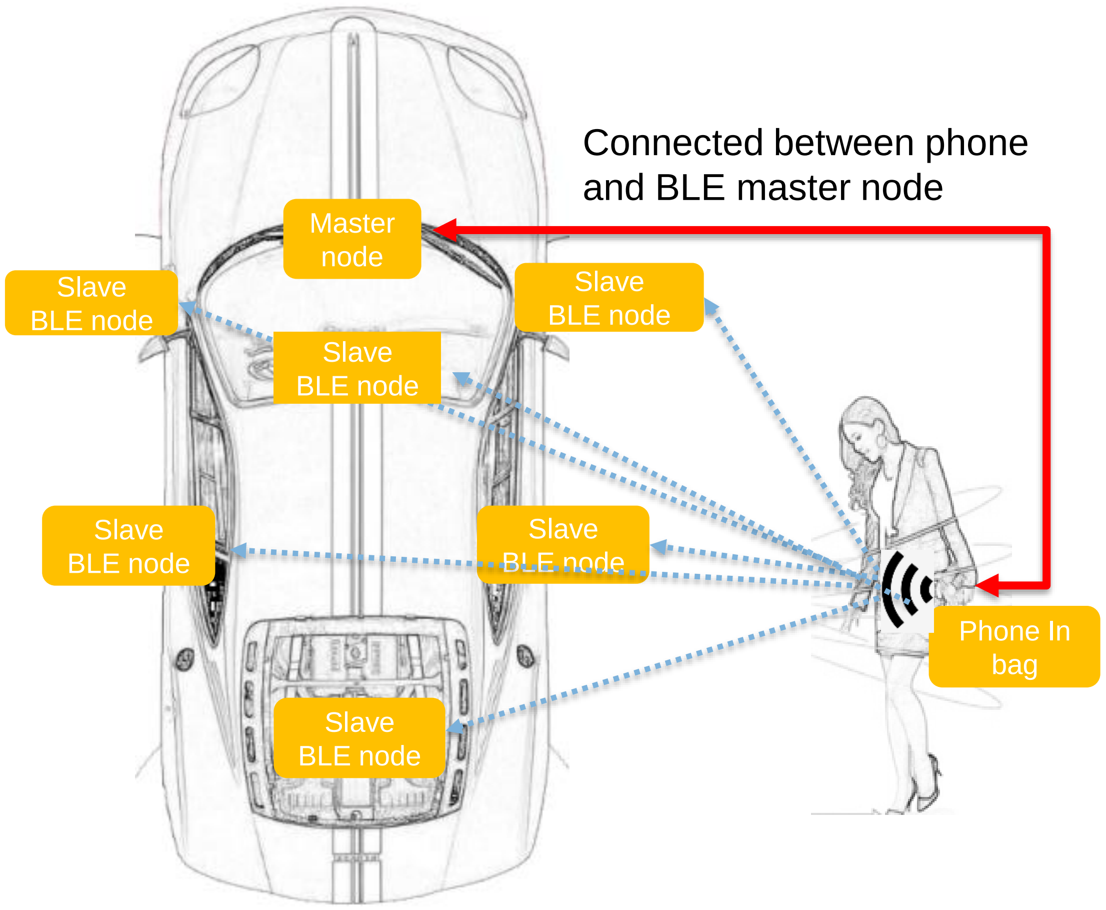


Connected between phone App and BLE master node

Master node

Phone App

RKE



Connected between phone and BLE master node

Master node

Slave BLE node

Slave BLE node

Slave BLE node

Slave BLE node

Slave BLE node

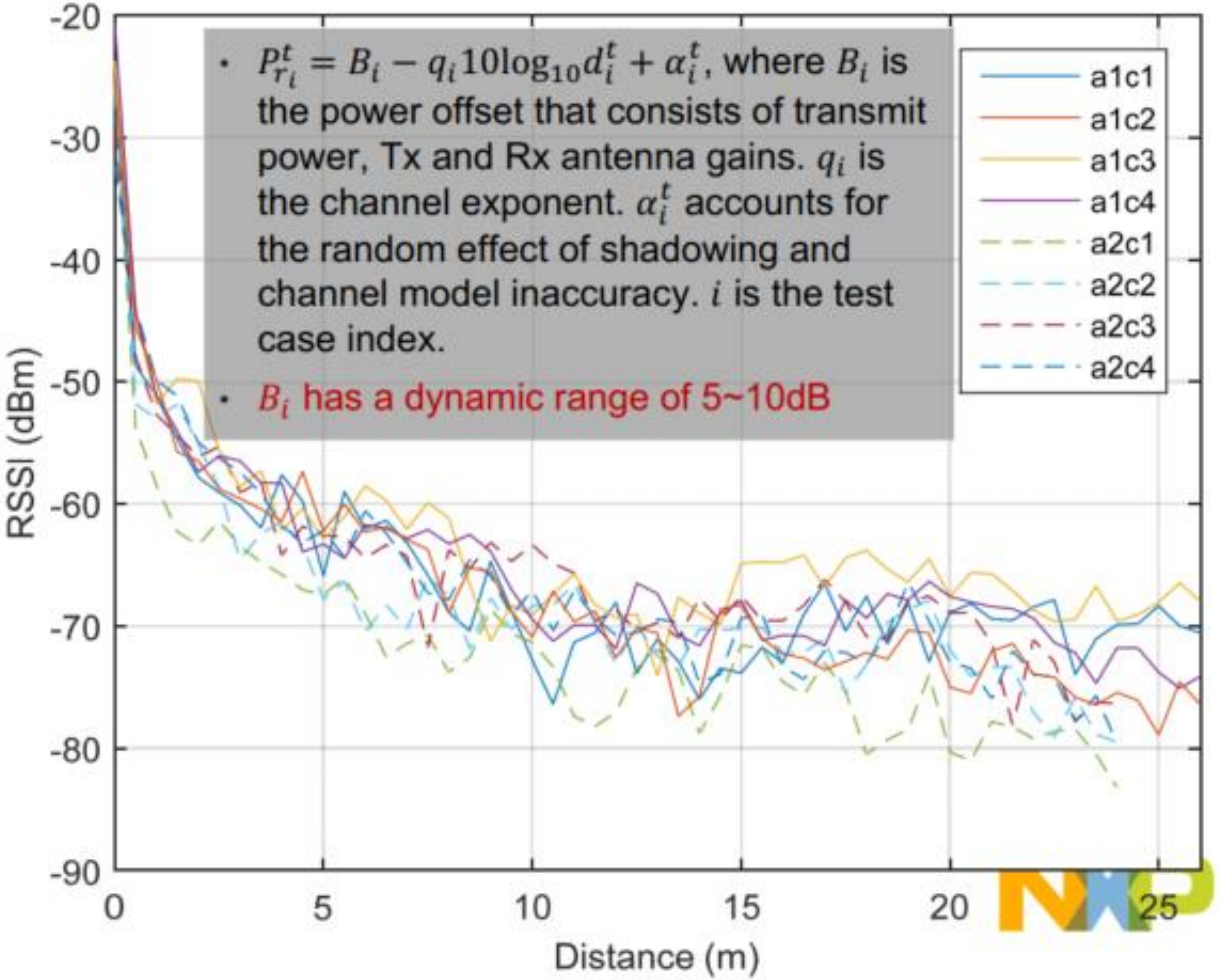
Slave BLE node

Phone In bag

PKE

Wireless Ranging Techniques – RSSI

- Multipath sensitive
  - Constructive or destructive superposition
- Antenna sensitive
  - Different radiation pattern and polarization
- Application
  - Appropriate for discovery
  - Auxiliary information for advanced localization technique.



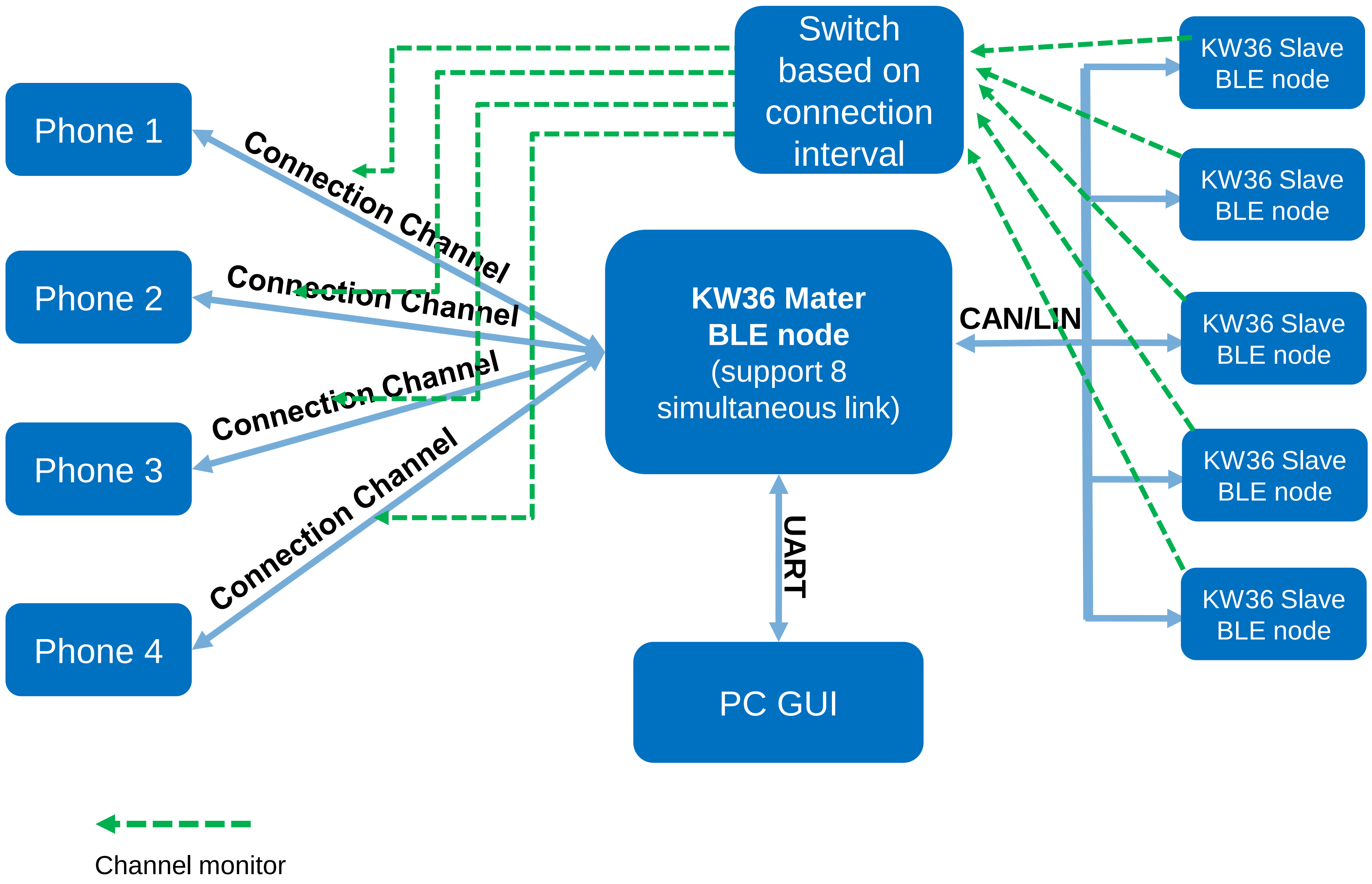
- $P_{r_i}^t = B_i - q_i 10\log_{10} d_i^t + \alpha_i^t$, where B_i is the power offset that consists of transmit power, Tx and Rx antenna gains. q_i is the channel exponent. α_i^t accounts for the random effect of shadowing and channel model inaccuracy. i is the test case index.
- B_i has a dynamic range of 5~10dB

Description

- **KW36 data channel's RSSI tracing and monitoring demonstration system of multiple BLE connections**

- More and more car OEM are considering to use phone as the car key, which need to localize the driver's position, most tier-1 customers prefer to use RSSI based solution as it can be supported by current phone directly, while PDE and AOA is not compatible with current phone.
- Common RSSI Localization method is acquiring advertising channels, It's easy, but it is hard to make authentication, can be attacked easily and have low anti-interference ability as it only have 3 channels. So customers are asking for a new method to monitor the data channels with hopping.
- This demonstration system implement data channel's RSSI tracing and monitoring of 4 BLE connections at the same time, and designed a GUI to simplify the steps to setup the demo system, and view the result visually.

Block Diagram of Multiple Connections’ Monitor



Setup Procedures:

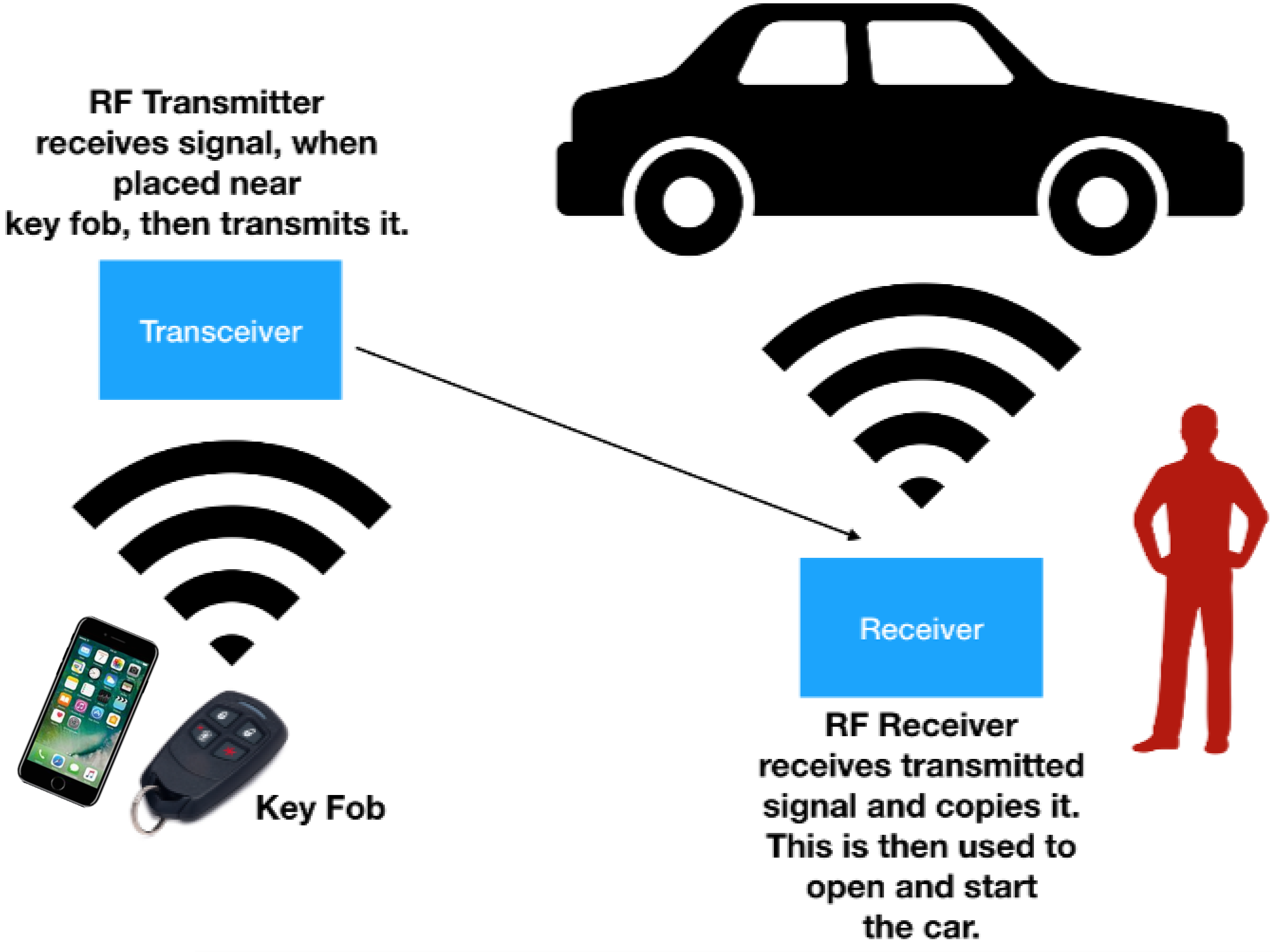
1. the master establishes a connection with the slave phone
2. the master distributes information needed to the monitors through LIN
3. the monitors starts monitoring connection
4. PC GUI was used to setup the system configuration and verify algorithm

CAN/LIN information:

1. Access Address
2. Connection Interval
3. Hop Increment
4. CRC Seed

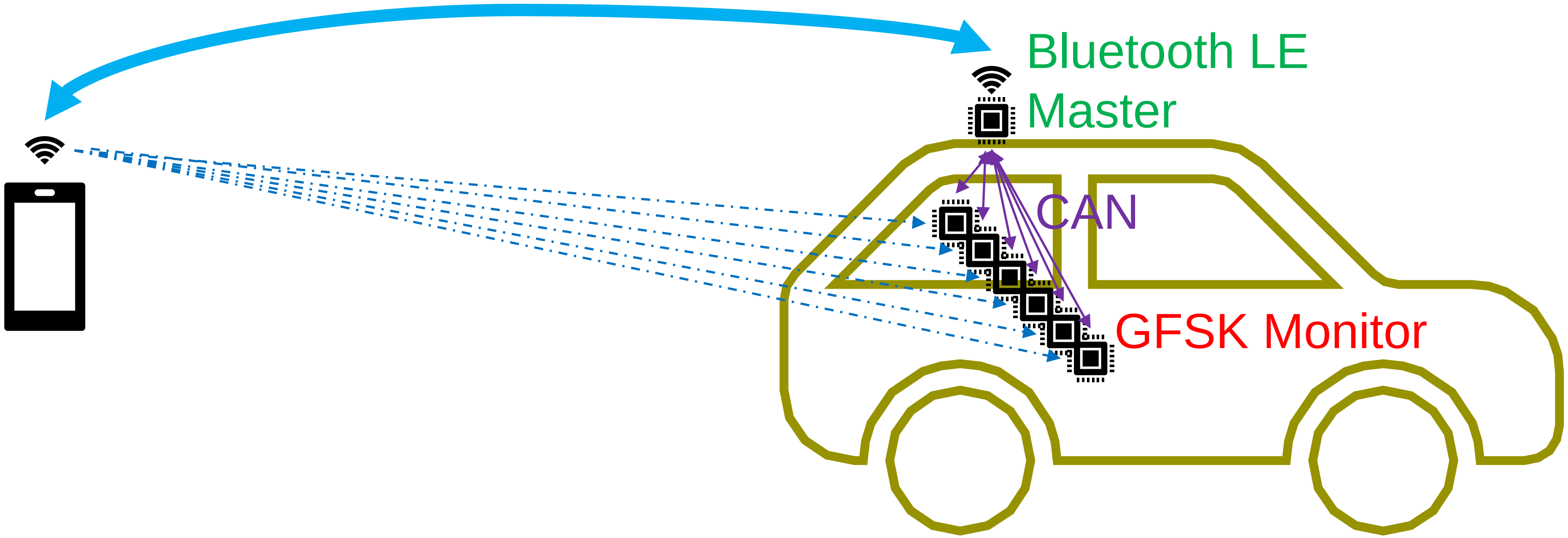
ANTI-RELAY SOLUTION

Typical Relay Attack



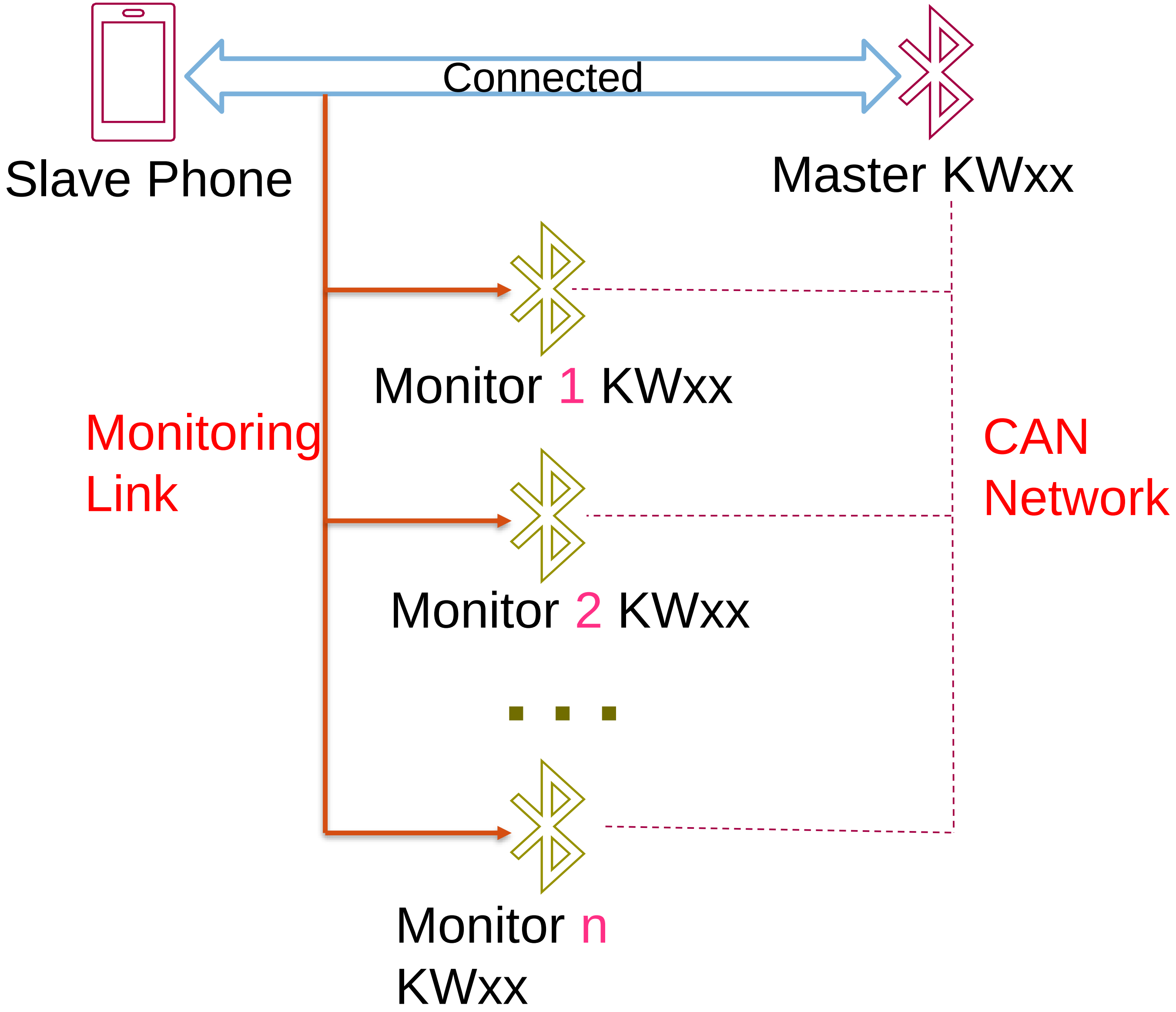
RF Transmitter receives signal, when placed near key fob, then transmits it.
Transceiver
Receiver
Key Fob
RF Receiver receives transmitted signal and copies it. This is then used to open and start the car.

RSSI based solution– Monitoring one connection



Single-Connection Monitoring

- Single Bluetooth LE Connection
- Multiple monitoring devices
- Synchronize the first monitoring point by constantly monitoring specific channel



Information Needed

- Access Address
- Connection Interval
- Hop Increment
- CRC Seed

Operating Procedures

- 1. the master establishes a connection with the slave phone
- 2. the master distributes information needed to the monitors through LIN/CAN
- 3. the monitors starts monitoring connection

Hardware Prerequisites

Hardware requirements
=====================
- 3 Mini/micro USB cables
- 3 FRDM-KW36 boards
  - B1 as master
  - B2 as slave or a phone
  - B3 as monitor
- Personal Computer
- Power adapter 12 V
- Three Dupont female-to-female wire

Board settings
==============
- Connect 12 V adapter to J32 of board B3
- Unmount R34 and R27 resistors of board B3
- Connect J13-1 of the board B1 and B3
- Connect J13-2 of the board B1 and B3
- Connect J13-4 of the board B1 and B3

Note: When using autobaudrate feature connect J1-5 and J2-9

Prepare the Demo
================

1. Connect a mini/micro USB cable between the PC host and the OpenSDA USB port on the boards.
2. Open a serial terminal on PC for OpenSDA serial device with these settings:
    - 115200 baud rate
    - 8 data bits
    - No parity
    - One stop bit
    - No flow control

6. Download the program to the target board.

Software Prerequisites

Project Wireless_UART - B1 as master Located at

SDK\boards \ frdmkw36 \ wireless_examples \ bluetooth \ w_uart_c-lin_m\ freertos

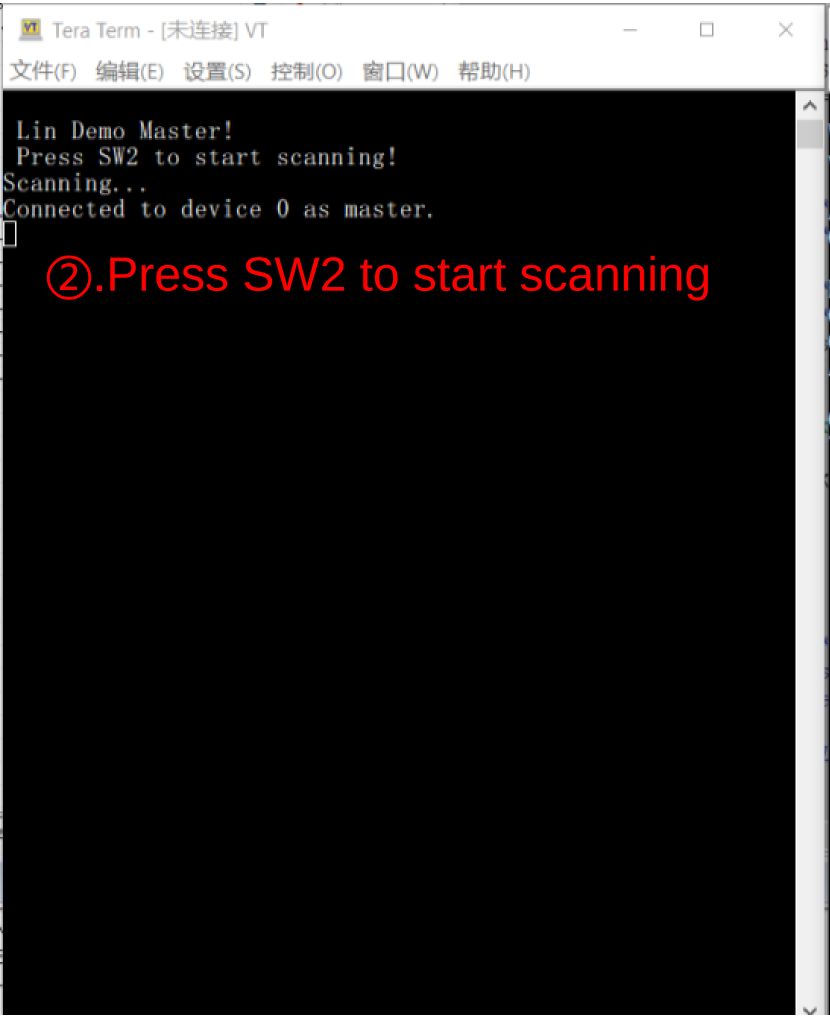
- Project Wireless_UART - B2 as slaveLocated at

SDK\boards \ frdmkw36 \ wireless_examples \ bluetooth \ w_uart\ freertos

- Project Link_Monitor - B3 as monitor Located at

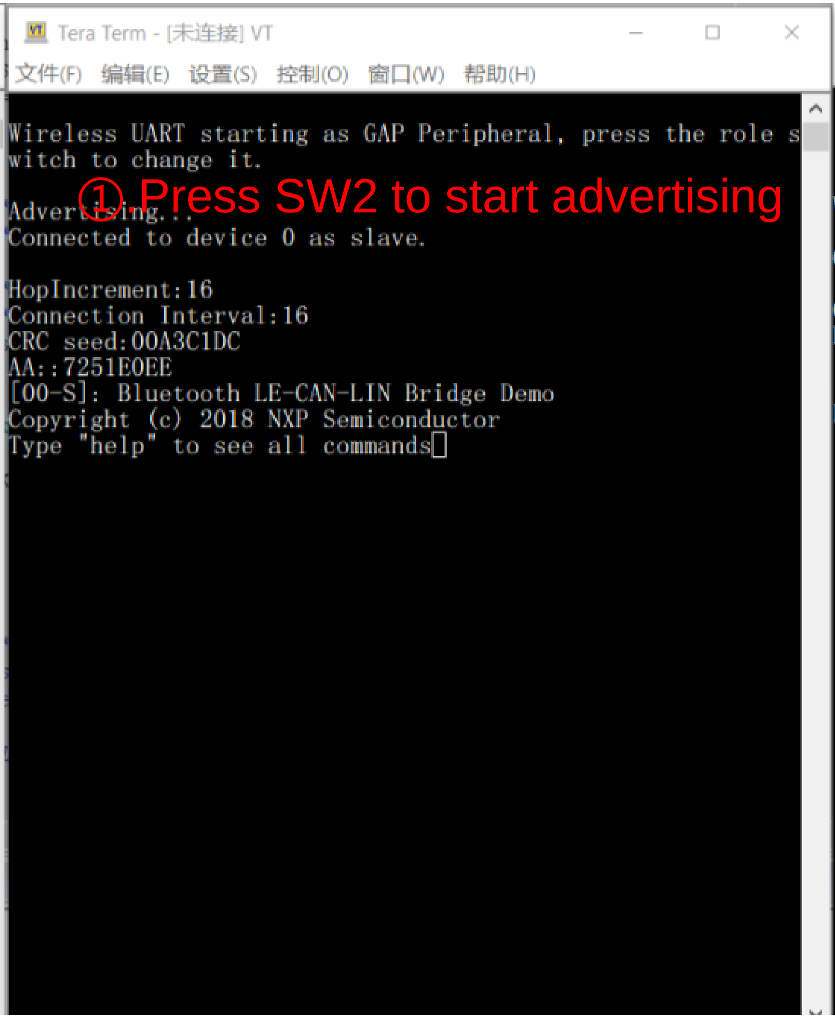
SDK\boards\frdmkw36\wireless_examples\genfsk\conn_test\freertos

Software log information print



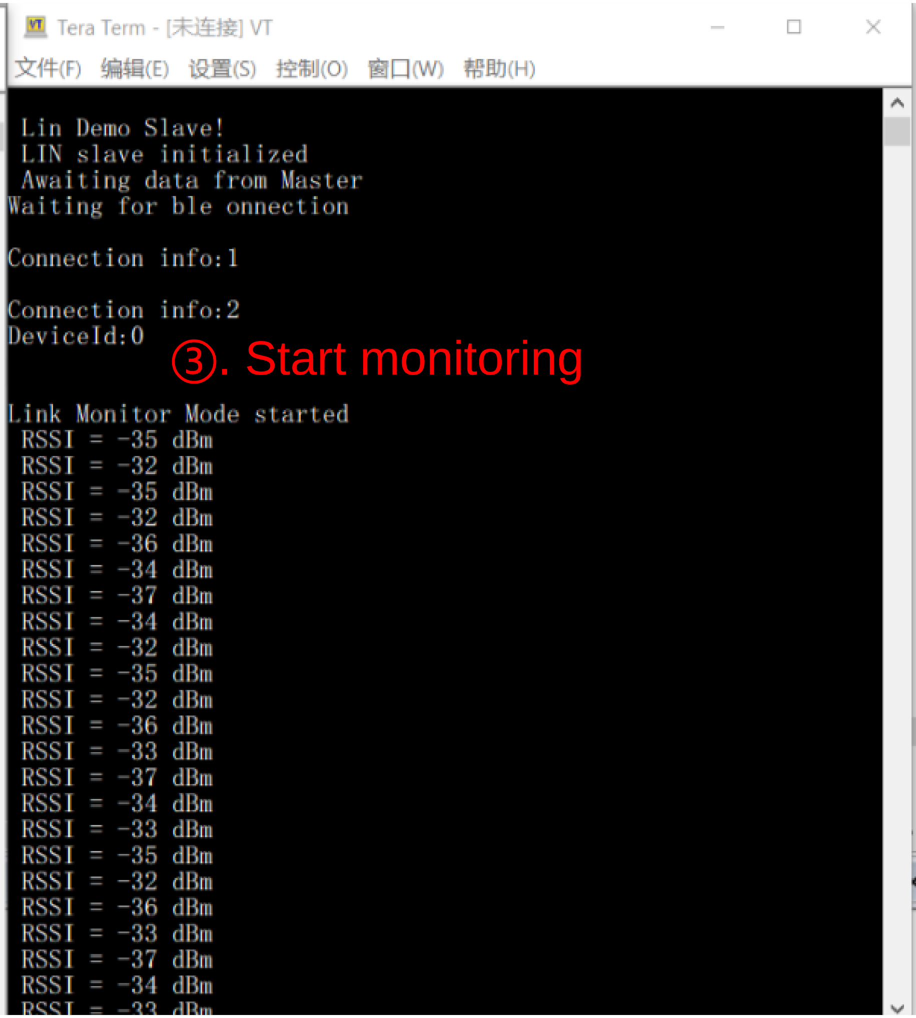
```
 Lin Demo Master!
 Press SW2 to start scanning!
Scanning...
Connected to device 0 as master.
```

②.Press SW2 to start scanning



```
Wireless UART starting as GAP Peripheral, press the role s
witch to change it.

Advertising...
Connected to device 0 as slave.

HopIncrement:16
Connection Interval:16
CRC seed:00A3C1DC
AA::7251E0EE
[00-S]: Bluetooth LE-CAN-LIN Bridge Demo
Copyright (c) 2018 NXP Semiconductor
Type "help" to see all commands
```

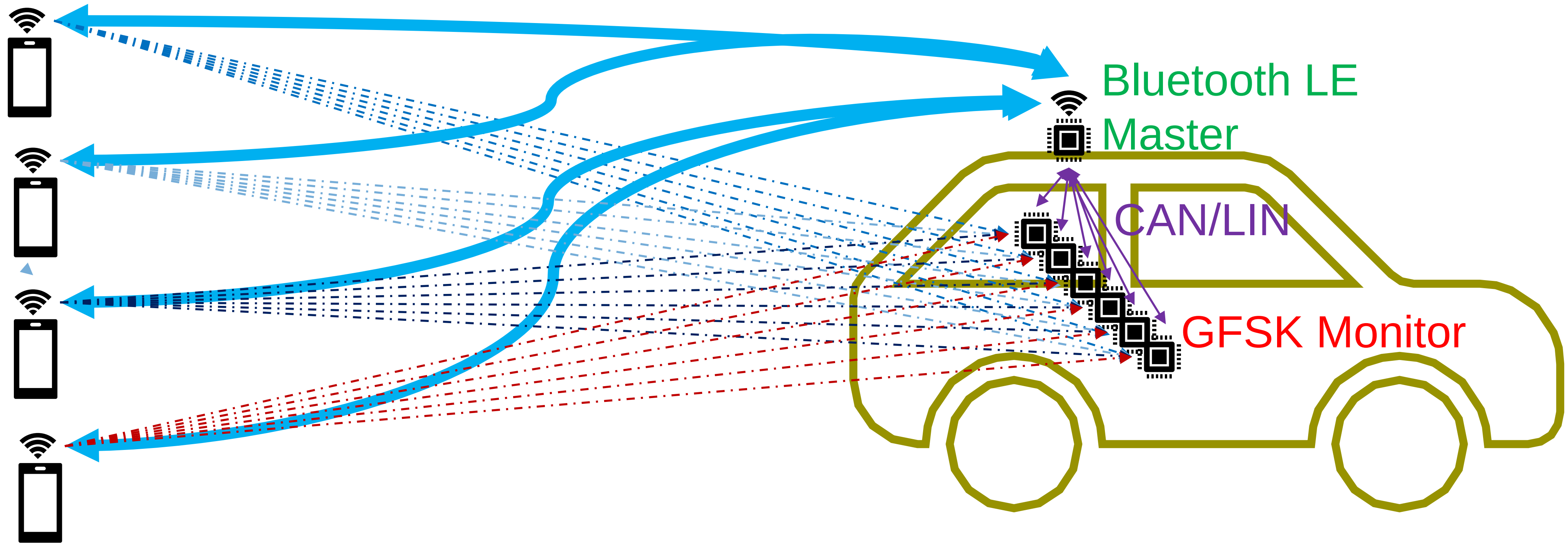
①.Press SW2 to start advertising



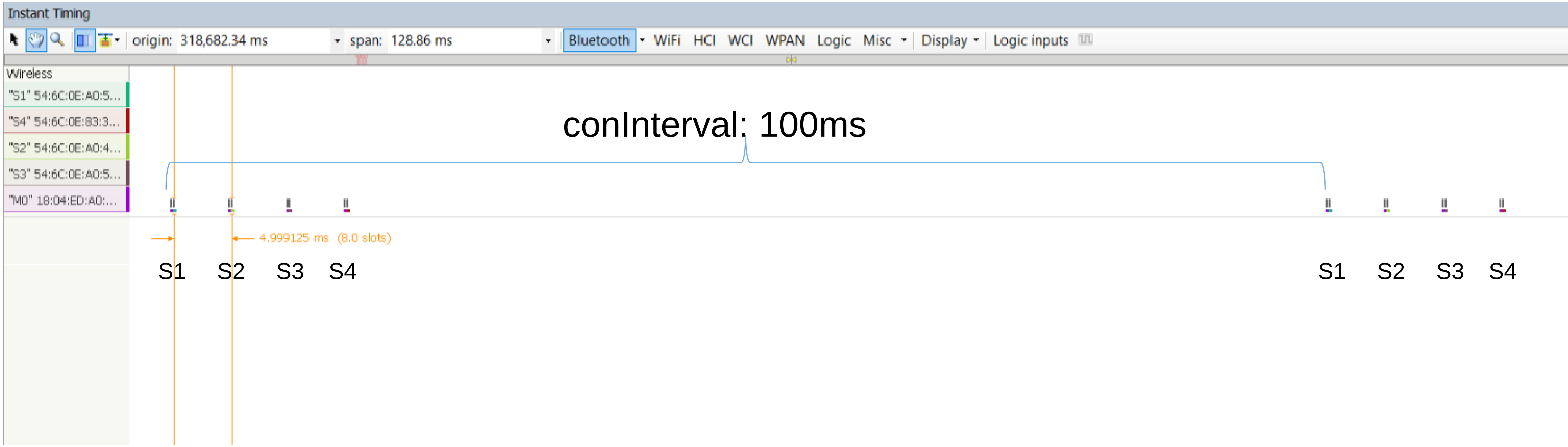
```
 Lin Demo Slave!
 LIN slave initialized
 Awaiting data from Master
Waiting for ble onnection

Connection info:1

Connection info:2
DeviceId:0

Link Monitor Mode started
 RSSI = -35 dBm
 RSSI = -32 dBm
 RSSI = -35 dBm
 RSSI = -32 dBm
 RSSI = -36 dBm
 RSSI = -34 dBm
 RSSI = -37 dBm
 RSSI = -34 dBm
 RSSI = -32 dBm
 RSSI = -35 dBm
 RSSI = -32 dBm
 RSSI = -36 dBm
 RSSI = -33 dBm
 RSSI = -37 dBm
 RSSI = -34 dBm
 RSSI = -33 dBm
 RSSI = -35 dBm
 RSSI = -32 dBm
 RSSI = -36 dBm
 RSSI = -33 dBm
 RSSI = -37 dBm
 RSSI = -34 dBm
 RSSI = -33 dBm
```

③. Start monitoring

RSSI based solution– Monitoring multiple connection



Multi-Connection Monitoring - **Continuous processing**



origin: 318,682.34 ms

span: 128.86 ms

4.999125 ms (8.0 slots)

conInterval: 100ms

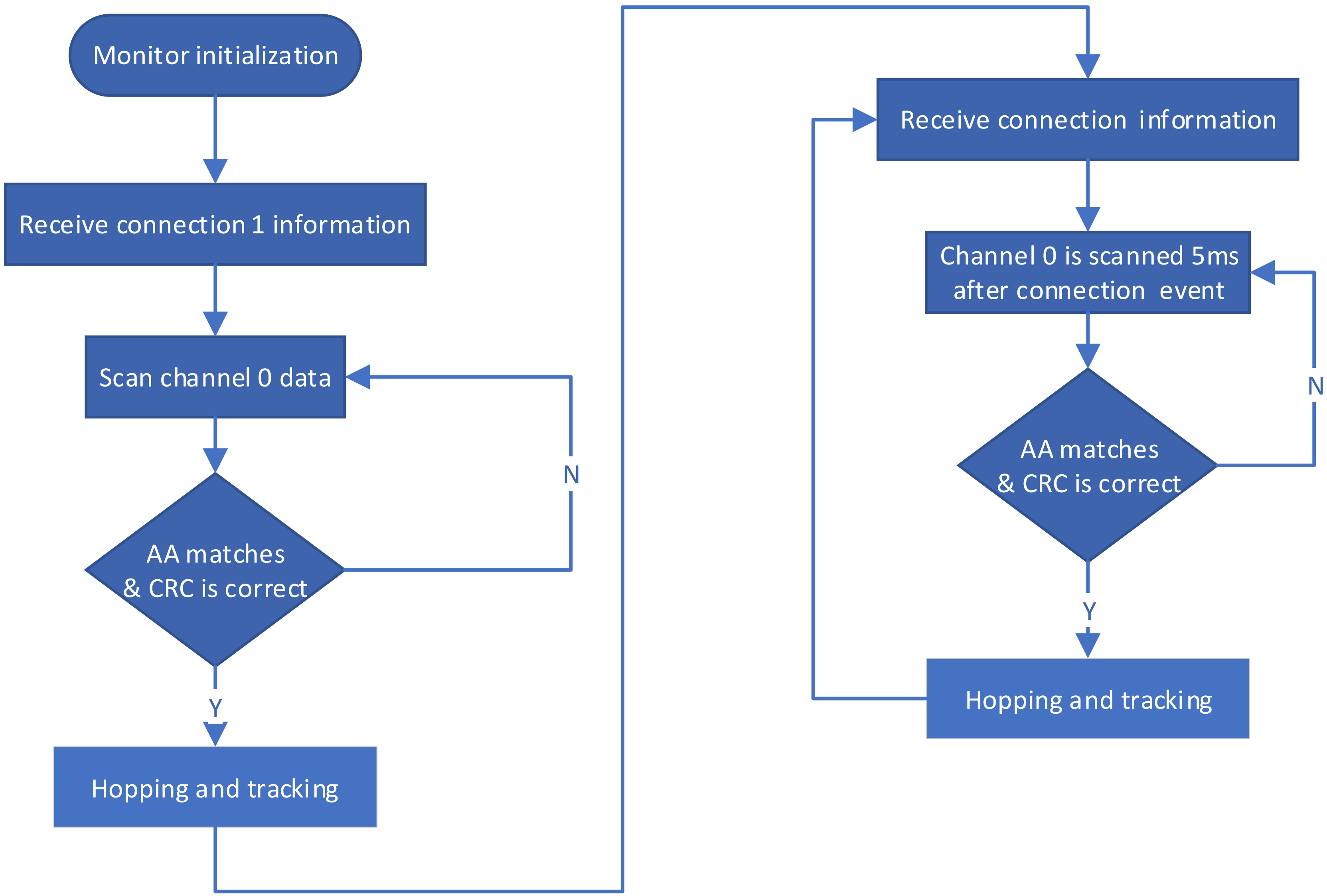
S1 S2 S3 S4

S1 S2 S3 S4

Multi-Connection Monitoring - **Operating Procedures**

- 1. the master establishes a connection with the slave phone 1;
- 2. the master distributes information needed to the monitor through CAN;
- 3. the monitors starts monitoring by constantly monitoring specific channel;
- 4. the master establishes a connection with the slave phone 2;
- 5. the master distributes information needed to the monitor through CAN;
- 6. the monitors starts monitoring connection 2 by monitoring a specific channel 5ms after connection 1 event;
- 7. same processing from connection 3 to connection n

Multi-Connection Monitoring – Flow Chart



Monitor initialization

Receive connection 1 information

Scan channel 0 data

AA matches & CRC is correct

N

Y

Hopping and tracking

Receive connection information

Channel 0 is scanned 5ms after connection event

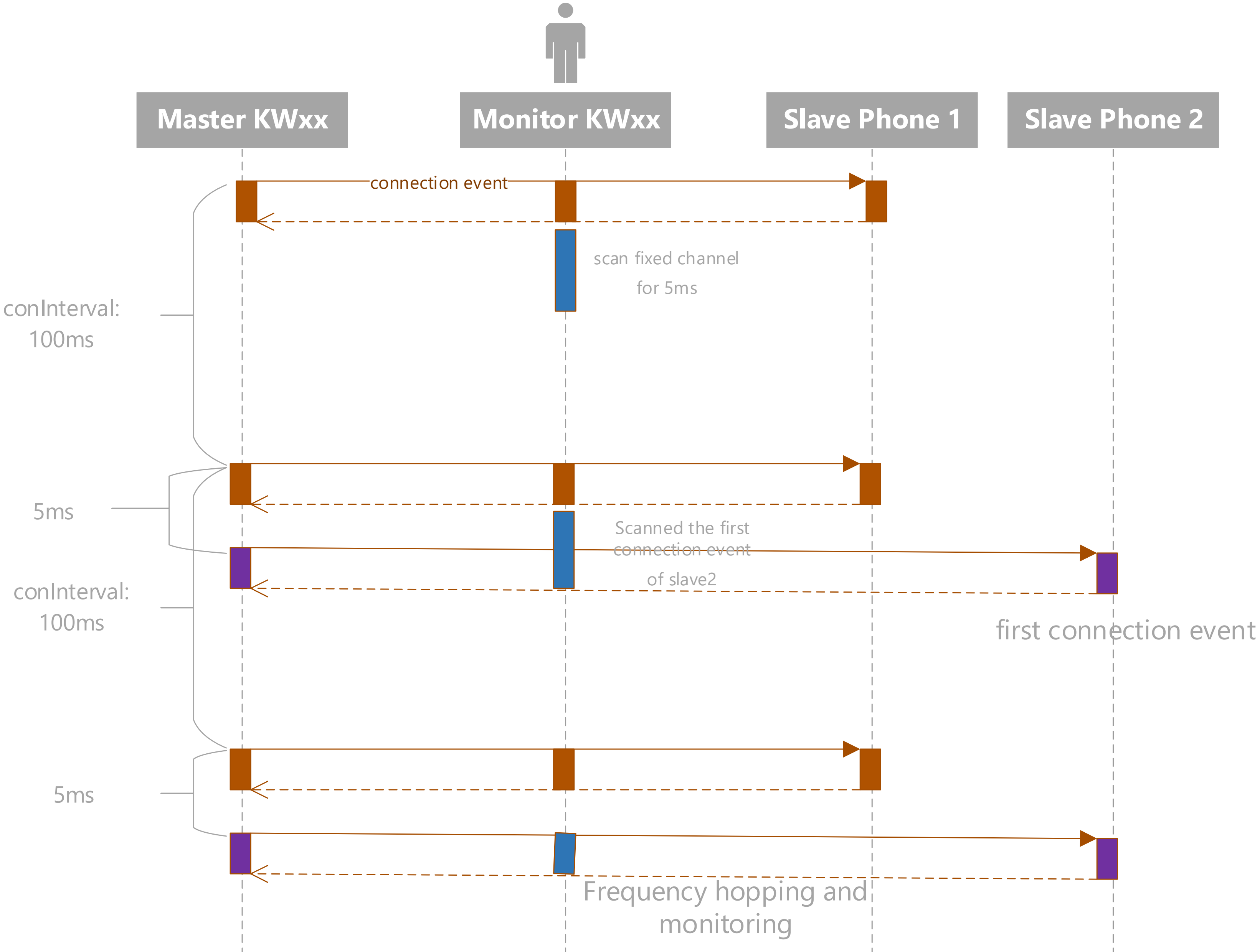
AA matches & CRC is correct

N

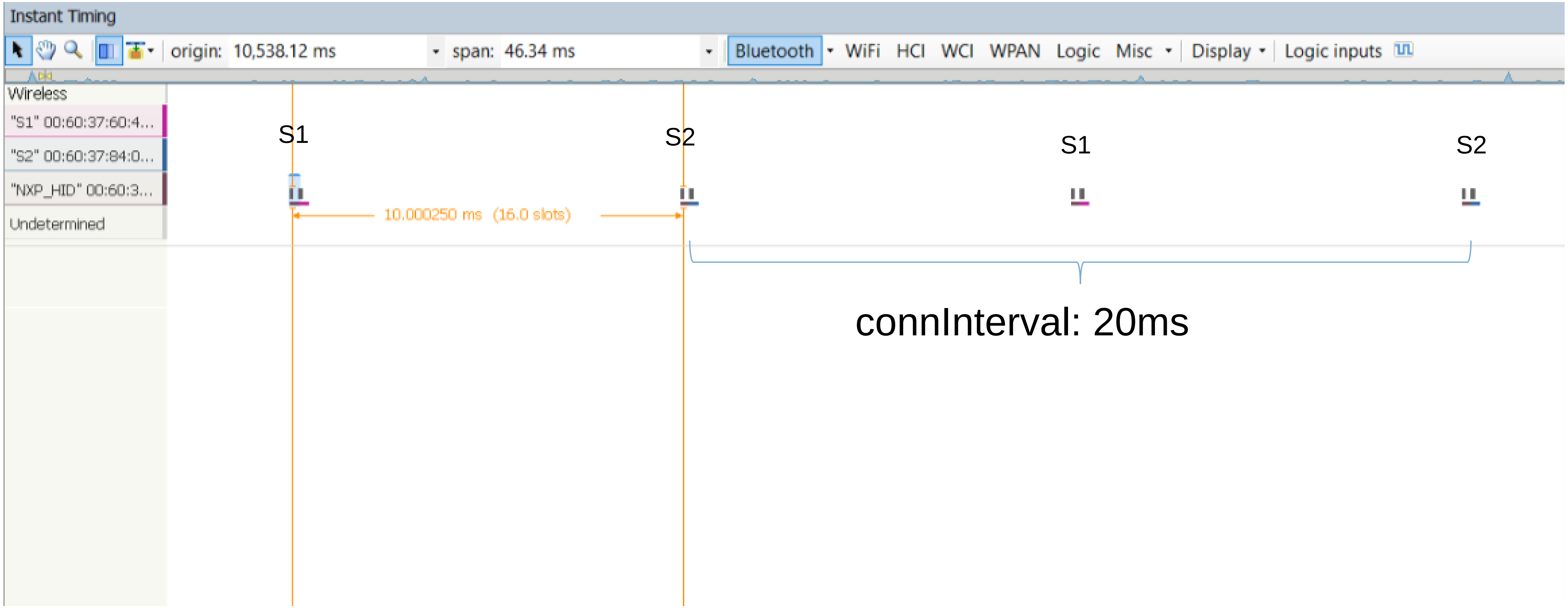
Y

Hopping and tracking

Multi-Connection Monitoring - **Continuous processing**



Multi-Connection Monitoring - **Split processing**



origin: 10,538.12 ms

span: 46.34 ms

10.000250 ms (16.0 slots)

S1

S2

S1

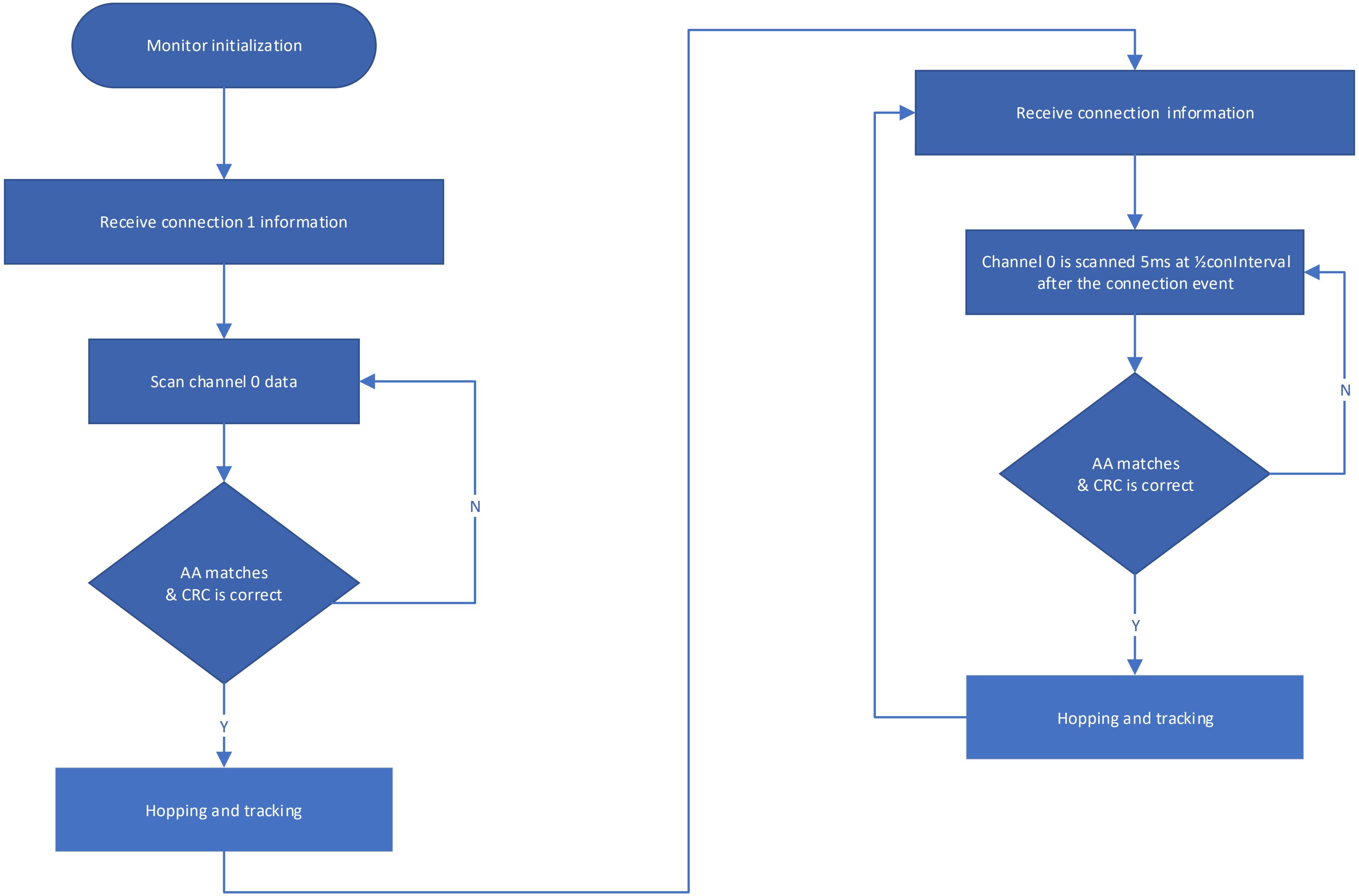
S2

connInterval: 20ms

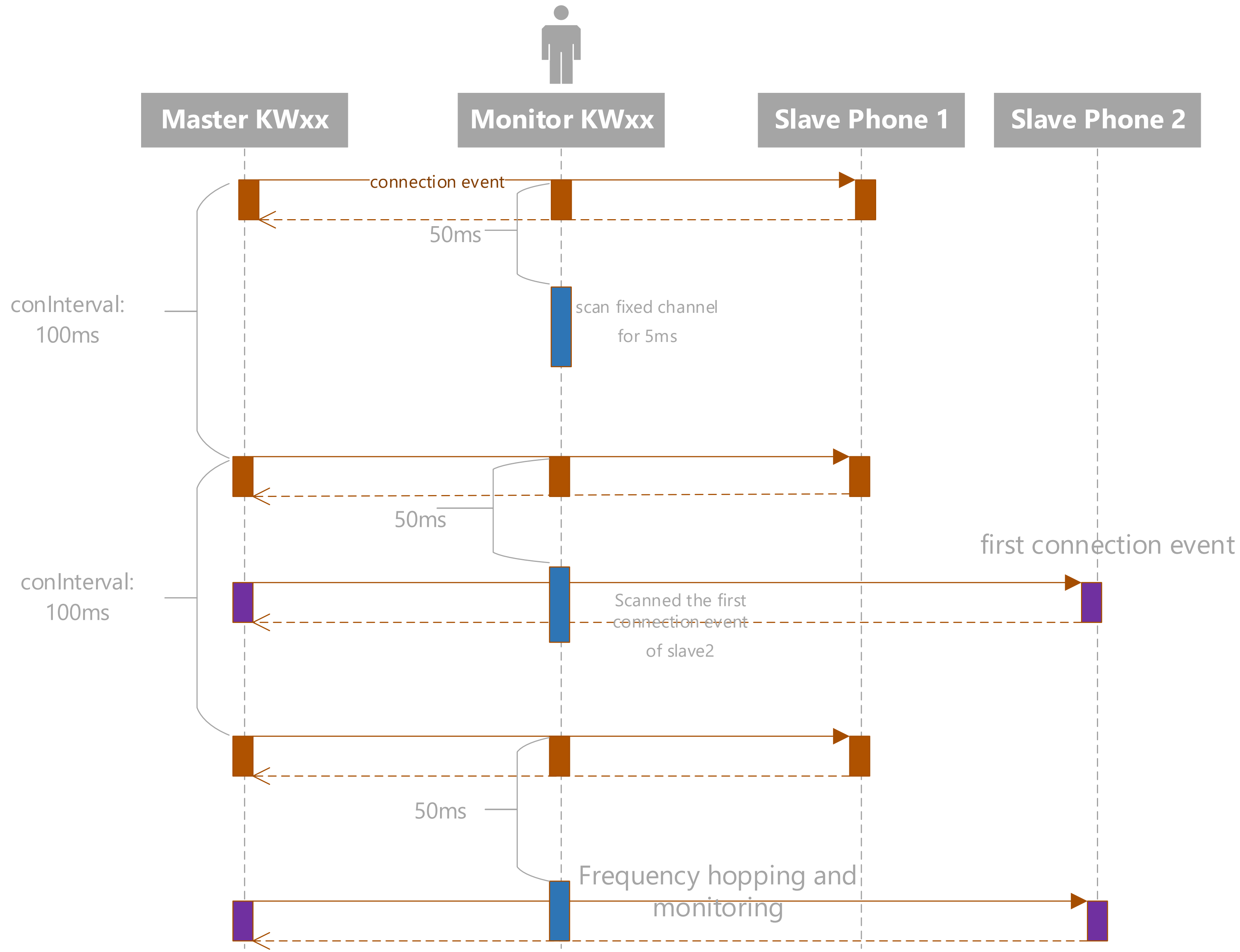
Multi-Connection Monitoring - **Operating Procedures**

- 1. the master establishes a connection with the slave phone 1;
- 2. the master distributes information needed to the monitor through CAN;
- 3. the monitors starts monitoring by constantly monitoring specific channel;
- 4. the master establishes a connection with the slave phone 2;
- 5. the master distributes information needed to the monitor through CAN;
- 6. the monitors starts monitoring connection 2 by monitoring a specific channel 10ms after connection 1 event;
- 7. same processing from connection 3 to connection n

Multi-Connection Monitoring – Flow Chart



Multi-Connection Monitoring - **Split processing**

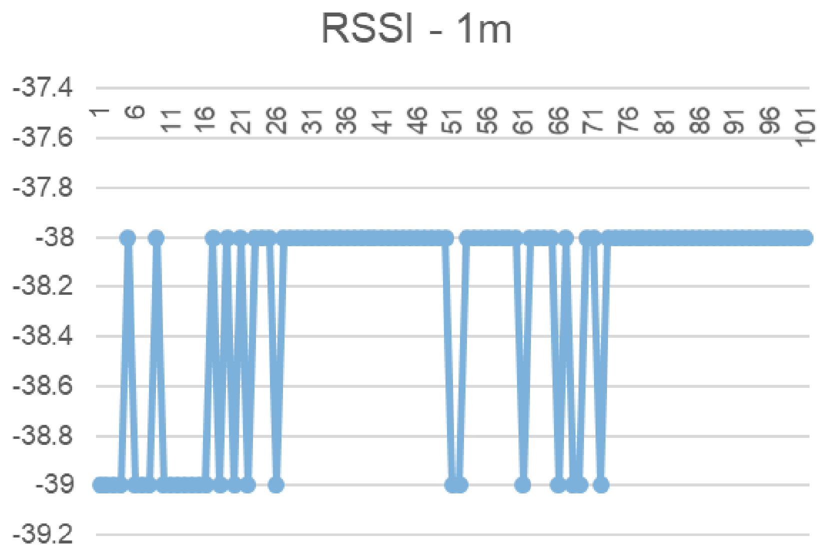


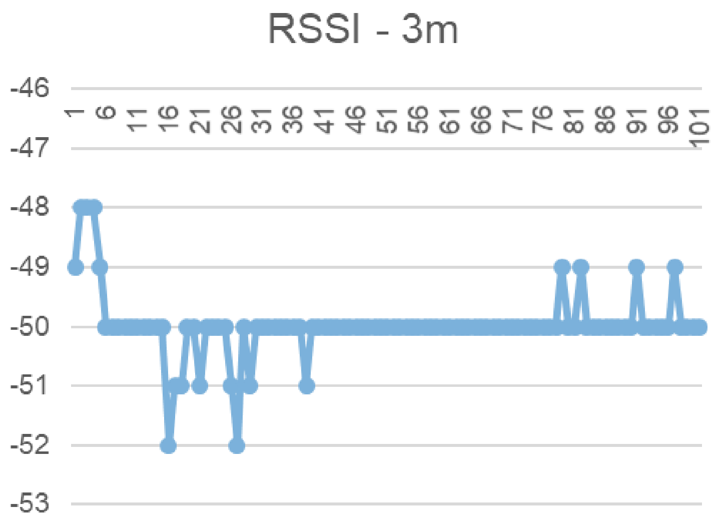
RSSI LOCALIZATION SOLUTION

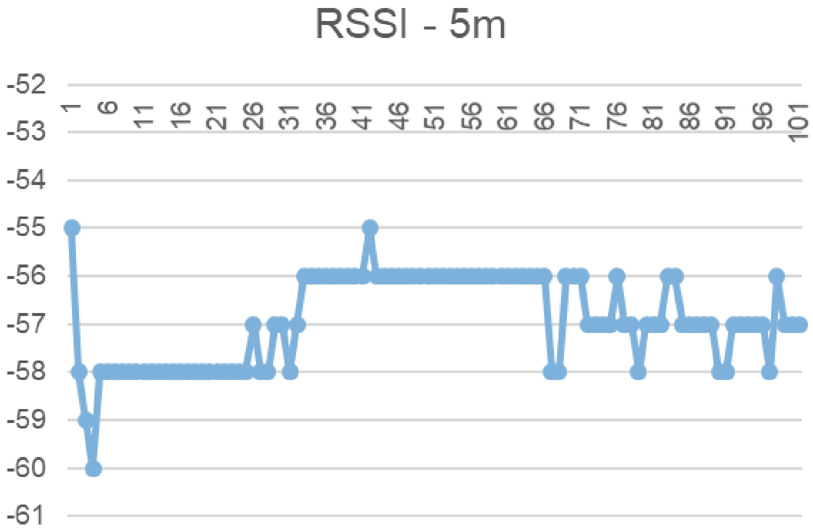
KW36 Advantages

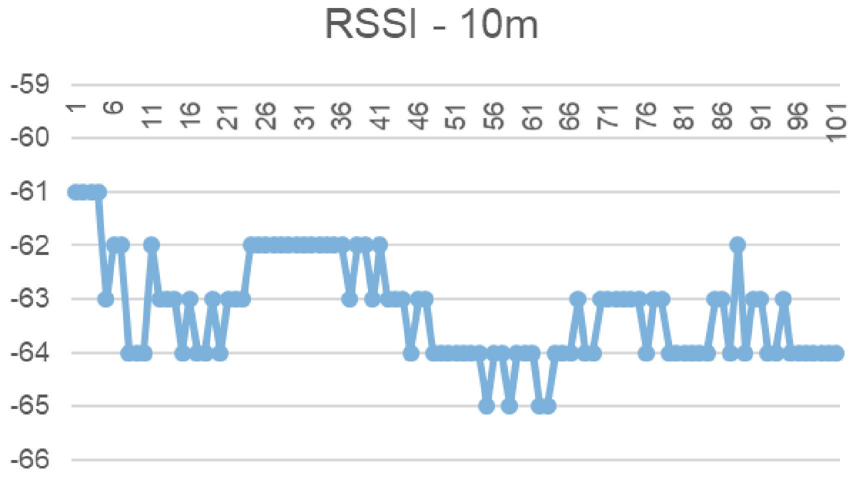
- RSSI indication associated with channel number in scanning event
- Support RSSI reporting in data packet in connection event
- Good RSSI accuracy, -3 to 3 dBm

KW36 RSSI Accuracy（-3dBm to 3dBm)


RSSI - 1m


RSSI - 3m


RSSI - 5m

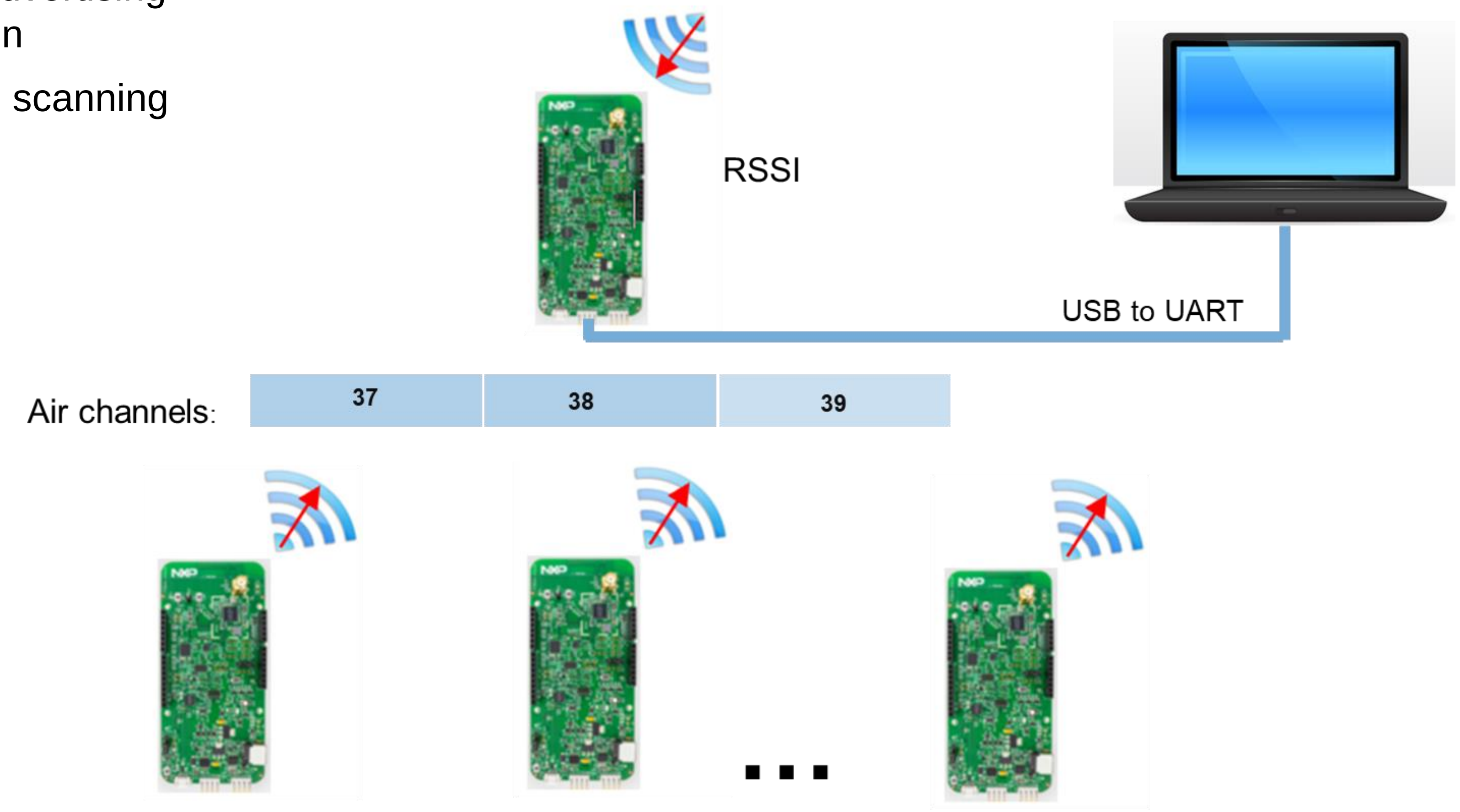

RSSI - 10m

KW36 RSSI Localization Schemes

- Typical RSSI based localization schemes
  - Acquiring RSSI from advertising channels, no connection
    - Anchor scanning, tag advertising
    - Anchor adverting, tag scanning
  - Acquiring RSSI from data channel, with connection

KW36 RSSI Localization Schemes - Advertising

- Acquiring RSSI from advertising channels, no connection
- Anchor advertising, tag scanning



RSSI

USB to UART

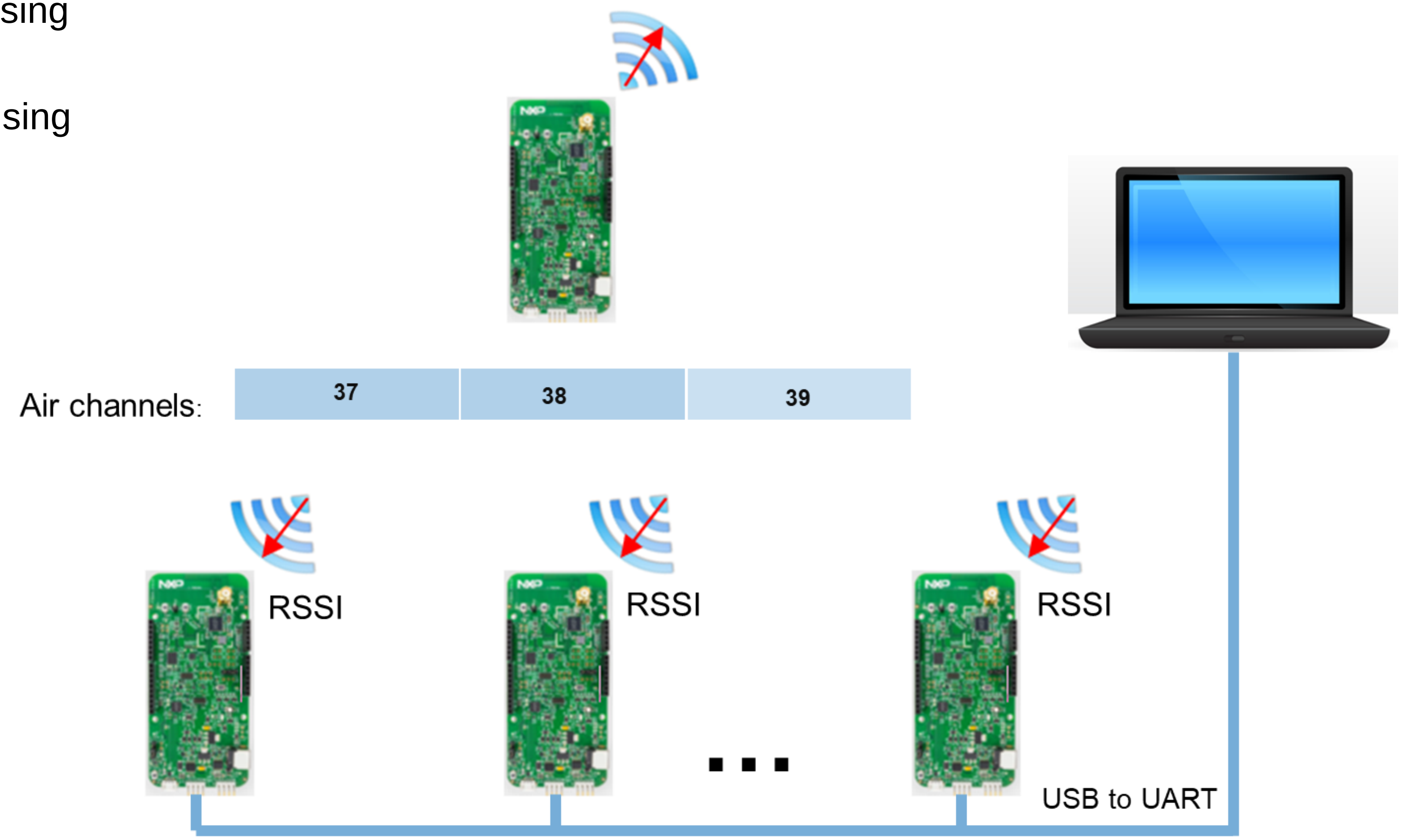
Air channels:

37	38	39

...

KW36 RSSI Localization Schemes - Advertising

- Acquiring RSSI from advertising channels, no connection
- Anchor scanning, tag advertising



Air channels:

37	38	39

RSSI

RSSI

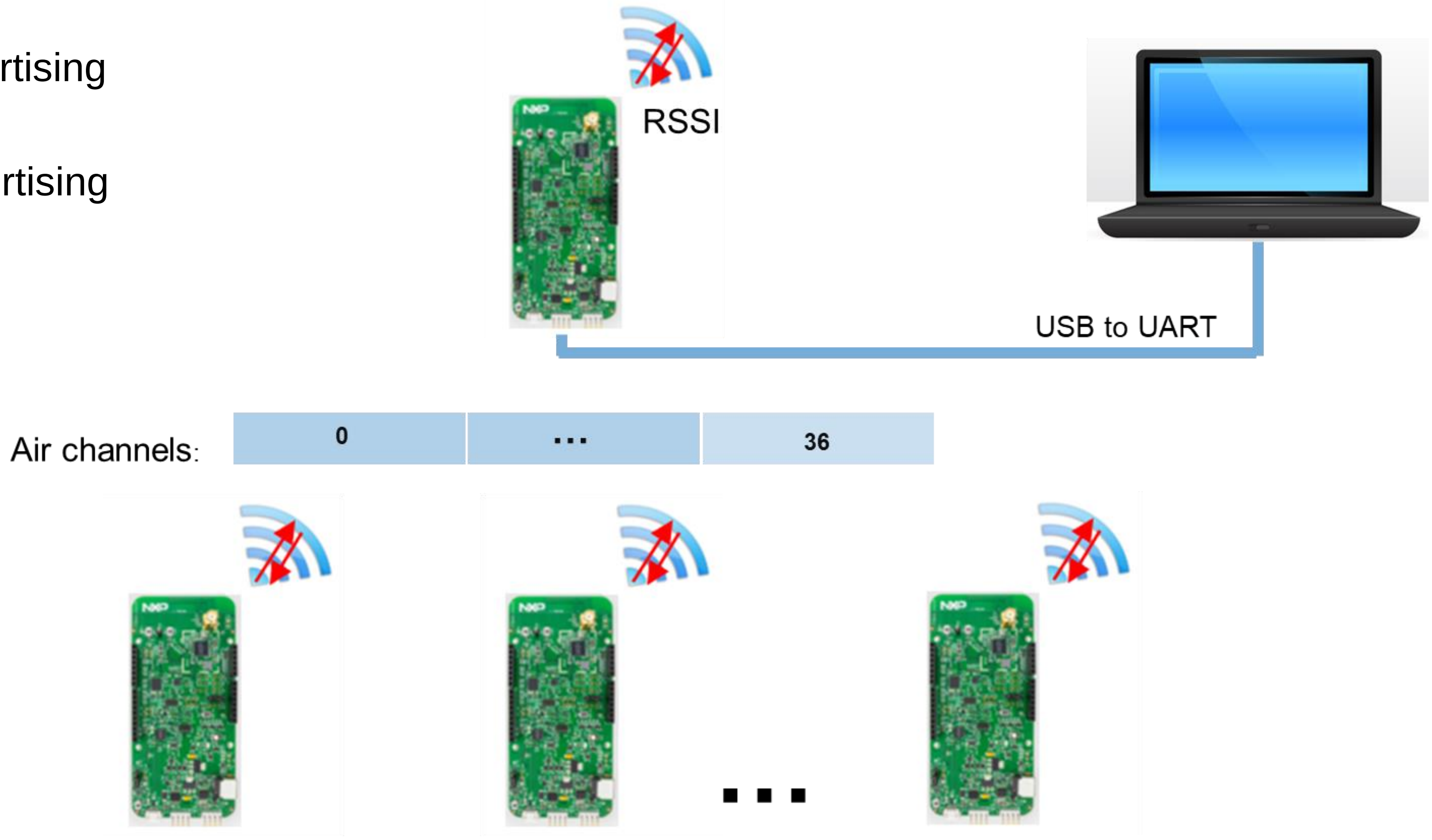
RSSI

. . .

USB to UART

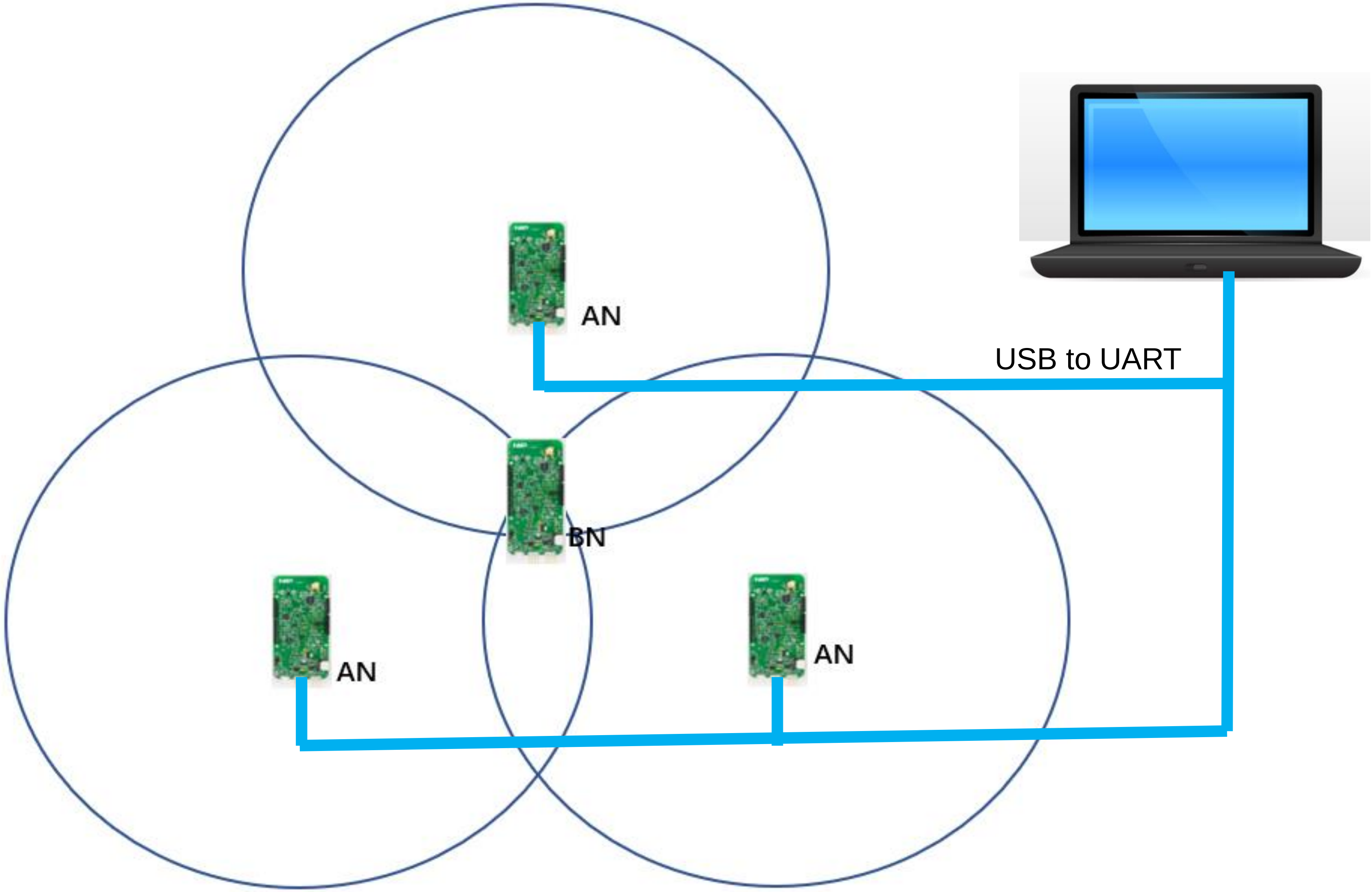
KW36 RSSI Localization Schemes - Connection

- Acquiring RSSI from advertising channels, no connection
- Anchor scanning, tag advertising



KW36 based RSSI Localization Solution

- Advertising based scheme
- Anchor scanning
- Tag advertising
- Algorithm running on PC



NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD