Direction Finding

nWP-036

White Paper

v1.1

1159720_173 v1.1 / 2020-08-24

NORDIC®
SEMICONDUCTOR

Contents

Revision history

Date	Version	Description
August 2020	1.1	Updated Angle of Arrival and Angle of Departure methods on page 5
August 2020	1.0	First release

1 Introduction

This white paper describes how to configure and enable the *Bluetooth*® Direction Finding features of nRF52 and nRF53 Series devices.

It is intended for developers and system integrators , and focuses on *Angle of Arrival (AoA)* implementation by providing instructions on how to get IQ samples. However, you can use the main principles in this white paper to create an *Angle of Departure (AoD)* system.

The configuration in this white paper only describes one part of the Direction Finding system. Stack and application software are required for this configuration to be Bluetooth compatible and certifiable.

Note: Nordic Semiconductor SoftDevices cannot be used with the Direction Finding system.

2 Direction Finding overview

Bluetooth Direction Finding is a major feature of the Bluetooth Core Specification. It is designed to enhance location services which previously only used signal strength based technology with received signal strength indication (RSSI).

Bluetooth Direction Finding offers a new and improved use case for real time location systems (RTLS) for asset tracking in a wide range of scenarios, from logistics and warehousing to value asset security in hospitals and factories. It also brings added user experiences in proximity-based scenarios for consumer awareness and contextual information.

Bluetooth Direction Finding can detect location in either 2D or 3D, dependent on the complexity of its implementation.

For more information on Bluetooth Direction Finding, see the following sections of the *Bluetooth Core Specification*:

- Direction Finding using Bluetooth Low Energy – Vol 1, Part A, Chapter 8
- Antenna Switching – Vol 6, Part A, Chapter 5
- Constant Tone Extension and IQ Sampling – Vol 6, Part B, Chapter 2.5

2.1 Angle of Arrival and Angle of Departure methods

Bluetooth Direction Finding is based on the two key concepts of *AoA* and *AoD*. This makes use of the angular phase-shifts that occur between antennas as they receive (*AoA*) or transmit (*AoD*) RF signals.

With the use of antenna arrays at either side of the communication link, phase shift data can be determined and from this the location can be calculated.

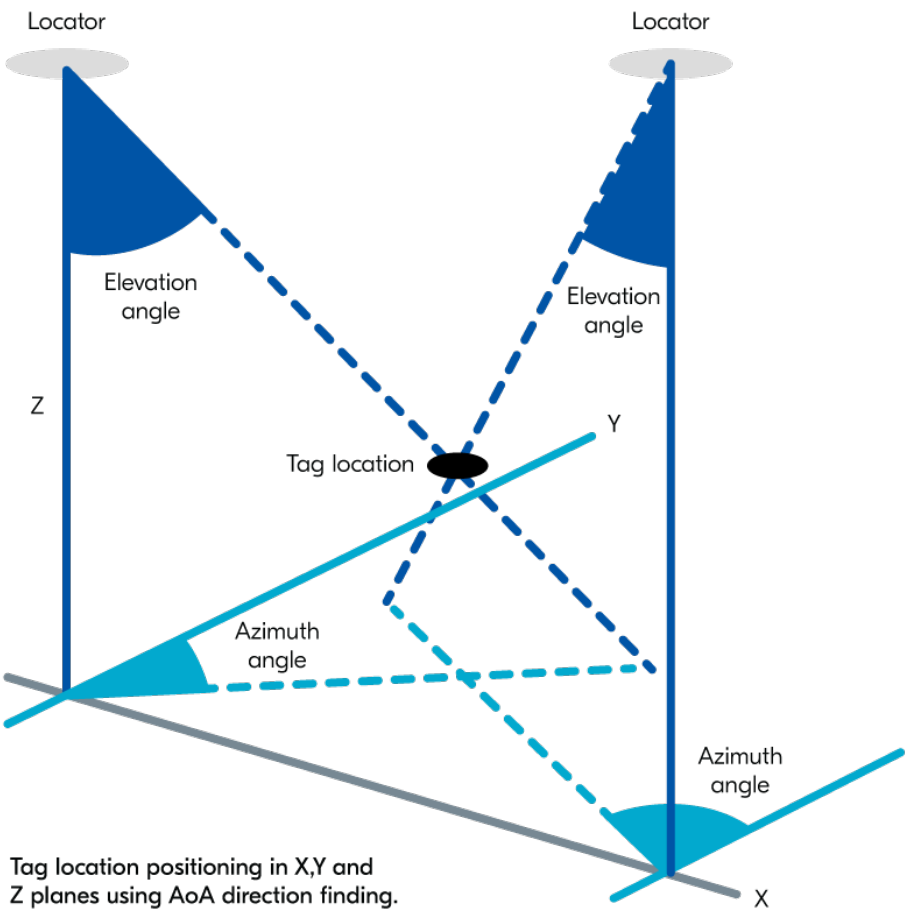


Figure 1: Tag location

An *AoA* system features the antenna array on the receiver side, so that by measuring the phase-shift of the incoming signal, the receiver can determine the direction of the incoming signal.

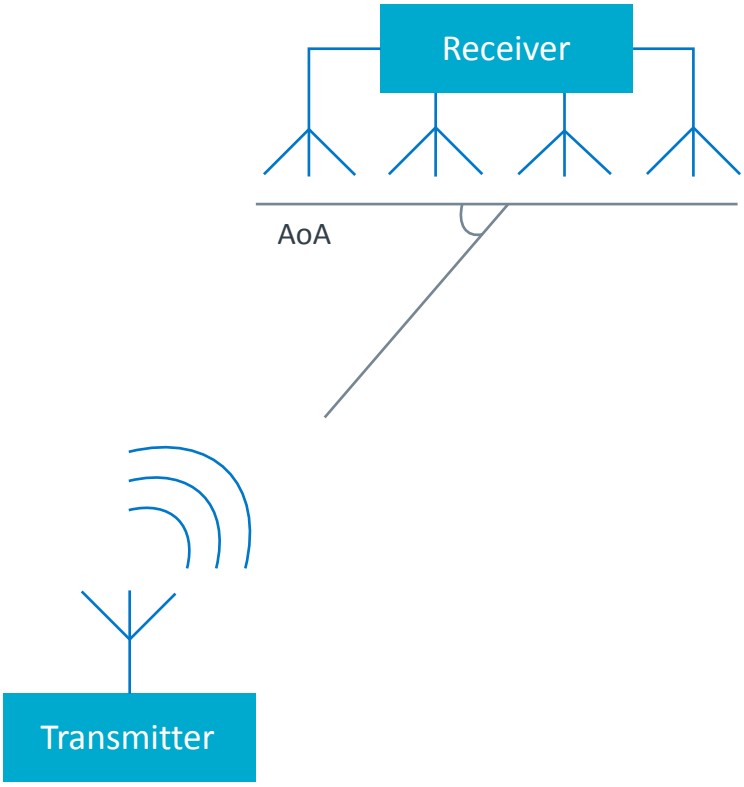


Figure 2: AoA method

AoD, as the name implies, uses the antenna array to direct the transmitted signal in a given angle.

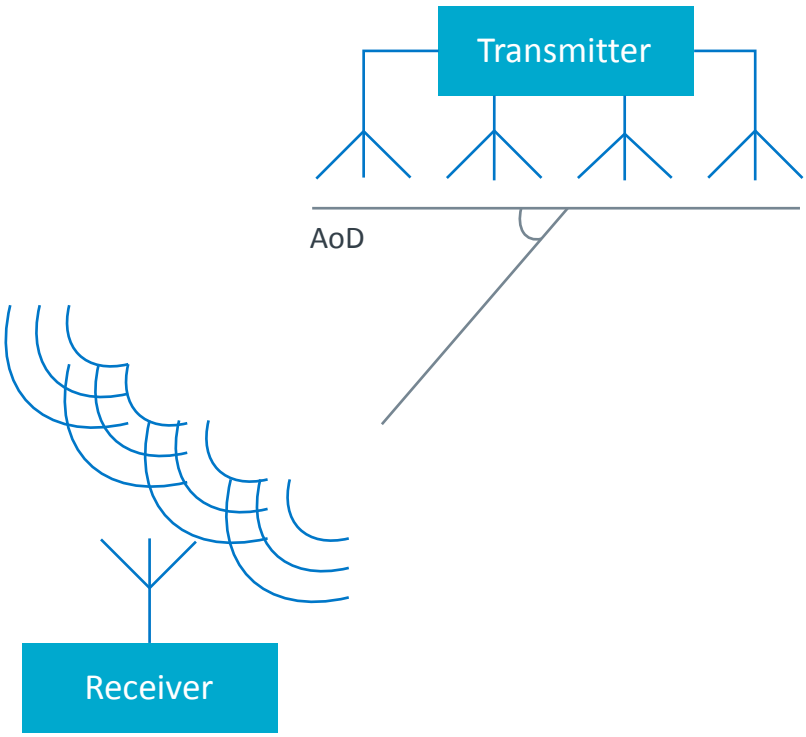


Figure 3: AoD method

The transmitter in *AoA* and the receiver in *AoD* does not need an antenna array, but the radio must still be able to append or sample the *Constant Tone Extension (CTE)* as described in Constant Tone Extension on page 9.

2.2 Determining the AoA/AoD by sampling phase and switching antennas

A signal transmitted by a Bluetooth Low Energy device has a frequency of approximately 2440 MHz, depending on the channel at a given transmission, resulting in a wavelength of approximately 12 cm in vacuum.

Usually Bluetooth LE devices are placed farther apart than this, meaning the signal undergoes multiple wave cycles as it propagates from the transmitter to the receiver. By measuring the phase difference of the signal as received by different antennas, the *AoA* receiver can determine the direction from which the signal is received. This is done with simple trigonometry, the phase difference yields a difference in travel time for the signal, and thus distance travelled.

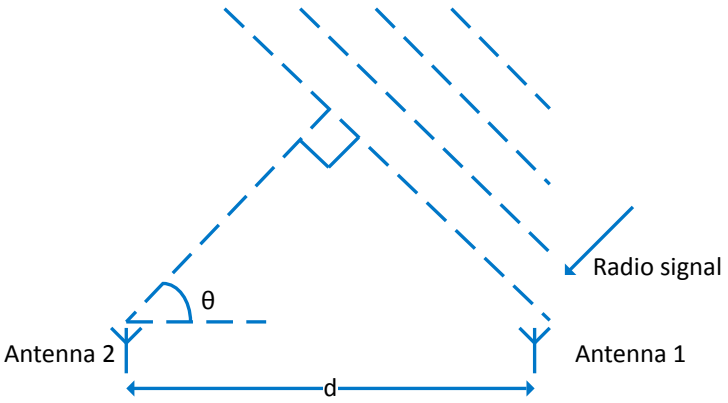


Figure 4: Measuring AoA

The angle can be calculated using the following equation.

$$\theta = \arccos\left(\frac{\psi\lambda}{2\pi d}\right)$$

Variable	Description
λ	The wavelength of the CTE signal.
ψ	The phase difference between the antennnas.
d	The distance between the antennas.

Table 1: AoA equation variables

The same principle applies to an *AoD* system. The only difference is that the transmitter is switching antennnas while adjusting the phase to cause constructive interference in the desired direction, and destructive interference in other directions.

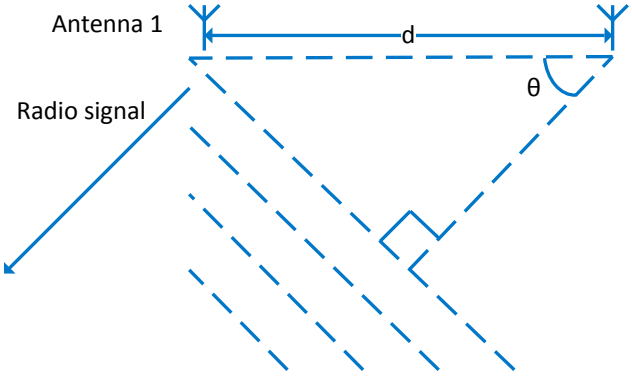


Figure 5: Measuring AoD

2.3 Constant Tone Extension

To enable *AoA* and *AoD*, Bluetooth Direction Finding uses a *CTE*.

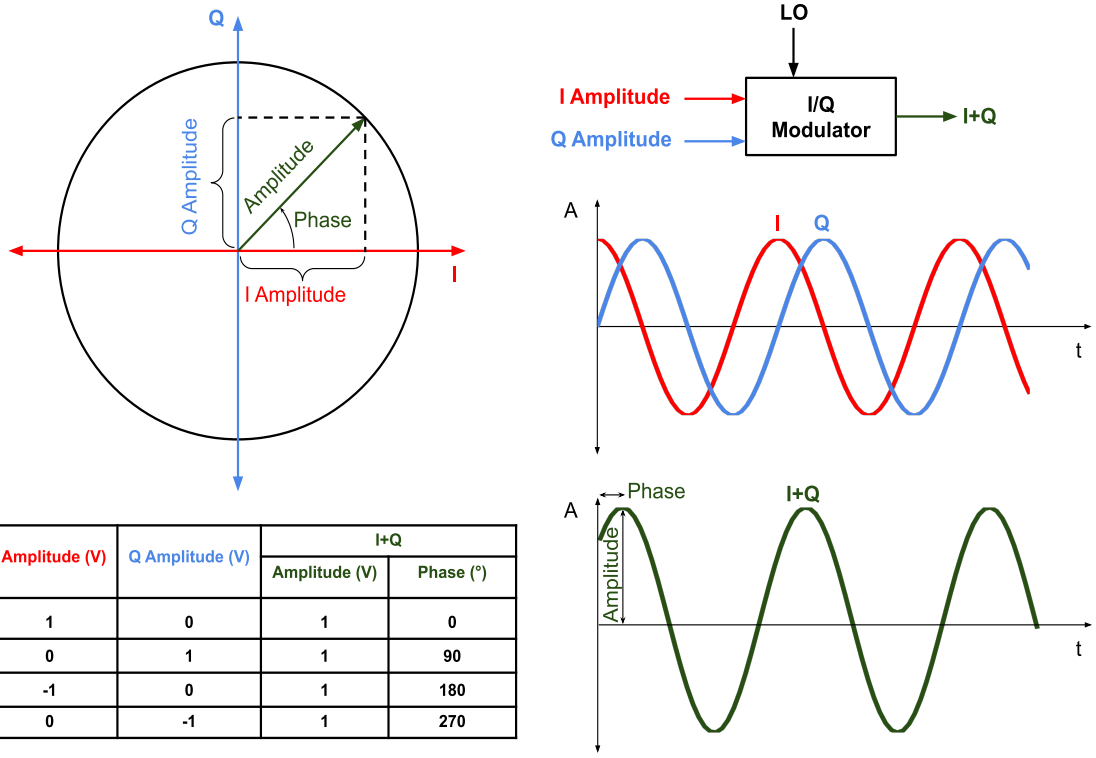
The *CTE* is appended to the packet, after the CRC, and appears as an offset unmodulated carrier, or an unwhitened sequence of modulated 1's. Because Bluetooth LE uses Gaussian Frequency Shift Keying (GFSK) modulation, the frequency is constantly changed throughout the packet to distinguish the different symbols, or 1's and 0's sent. Without the frequency being stable, the receiver will not be able to estimate the phase of the signal.

The exact frequency of the *CTE* also depends on the channel transmitted on at a given time. As the *CTE* is offset 250 kHz higher than the channel center frequency, this must be accounted for in order to calculate the correct difference in distance travelled.

2.4 Phase samples, I and Q components

Bluetooth Direction Finding uses IQ sampling, an in-phase and quadrature sampling technique, to measure the phase of incoming signals.

In IQ sampling, the receiver mixes the incoming signal with the local oscillator (LO) at 0 and 90 degree offsets. This creates two orthogonal functions known as the in-phase (I) and quadrature (Q) components. These components are plotted as the axes in the following diagram where the amplitude and phase of the main signal can be calculated as the magnitude and angle of the vector made up from the I and Q components.



I Amplitude (V)	Q Amplitude (V)	I+Q	
		Amplitude (V)	Phase (°)
1	0	1	0
0	1	1	90
-1	0	1	180
0	-1	1	270

Figure 6: IQ phasor diagram[1]

Thus, it is possible to estimate the phase of the signal by measuring the magnitude of the I and Q components. This is also the reason why the phase samples can be represented as I and Q values, or phase and magnitude, whichever is preferred for a given use case.

[1] IQ phasor diagram *by* Vigneshdm1990 *is licensed under* CC BY-SA 4.0

3 IQ sampling configuration

The *AoA* method uses a transmitter and receiver, where the receiver does the antenna switching to determine the direction to the transmitter.

This is enabled by the transmitter adding a *CTE* to the data packet causing a specified part of the packet to have a fixed and constant frequency. Knowing this, the receiver can sample the waveform IQ components and determine the phase of the waveform. And doing this for multiple antennas, the receiver can calculate from which angle the transmitter signal comes from.

According to the Bluetooth Core Specification, the *CTE* of the packet contains a guard period of 4 µs, a reference period of 8 µs, and a number of antenna samples. In particular, Vol 6, Part B, section 2.5.4 of the Bluetooth Core Specification states:

When receiving a packet that contains an AoA Constant Tone Extension, the receiver shall perform antenna switching at the rate and according to the switching pattern configured by the Host. In both cases, the receiver shall take an IQ sample each microsecond during the reference period and an IQ sample each sample slot (thus there will be 8 reference IQ samples, 1 to 37 IQ samples with 2 µs slots, and 2 to 74 IQ samples with 1 µs slots, meaning 9 to 82 samples in total).

This is illustrated in the following diagram.

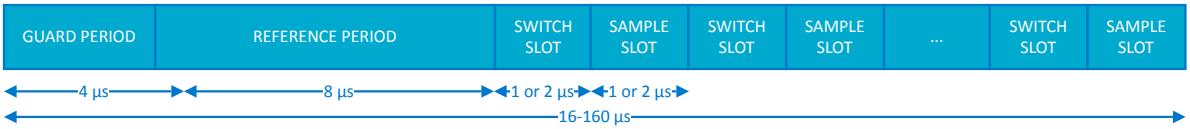


Figure 7: CTE structure

The duration for Guard Period and Reference Period is fixed and cannot be changed. The number of samples taken during the Reference Period is determined by 8 µs/TSAMPLESPACINGREF. However, the sample slot and switch slot duration can be changed using the settings in the following table.

Field	Value for 1 µs sample slots	Value for 2 µs sample slots	Description
TSAMPLESPACINGREF	1 µs	1 µs	Interval between samples in the reference period
TSAMPLESPACING	2 µs	4 µs	Interval between samples in the switching period
TSWITCHSPACING	2 µs	4 µs	Interval between every time the antenna is changed in the switching state

Table 2: Sample and switch slot duration settings

The following diagrams illustrate *AoA* configuration for 1 µs and 2 µs slots.

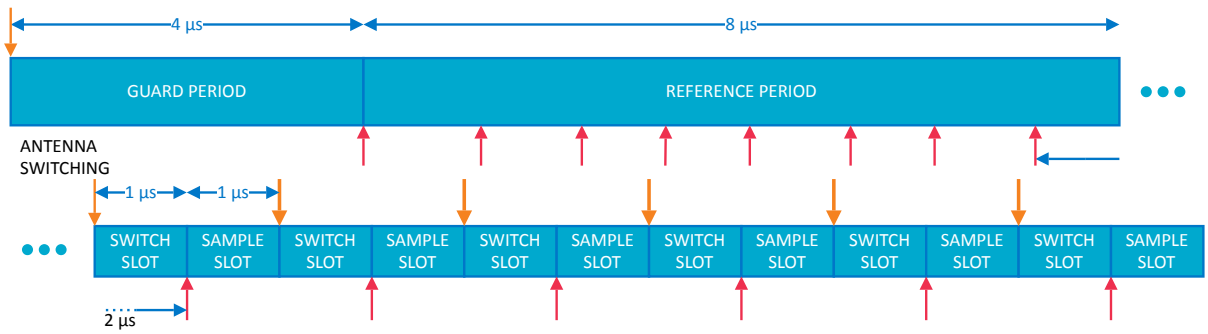


Figure 8: AoA configuration for 1 µs slots

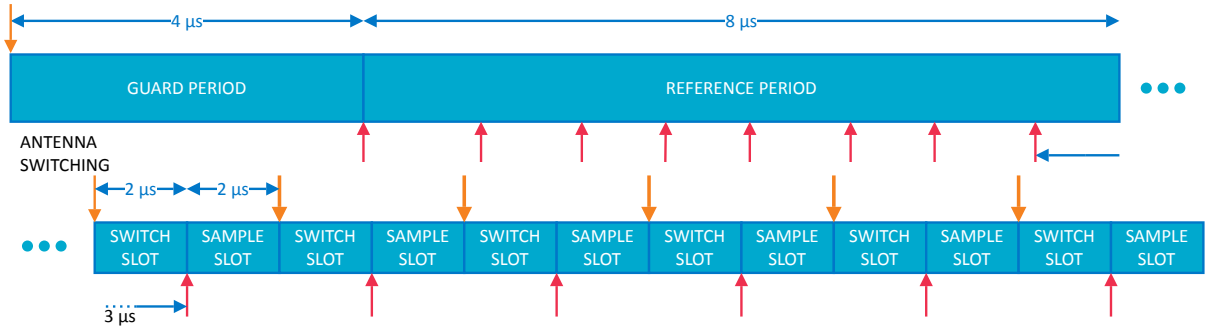


Figure 9: AoA configuration for 2 µs slots

3.1 TSAMPLEOFFSET

TSAMPLEOFFSET is a signed number for a relative offset of the sampling instant.

TSAMPLEOFFSET configures when the sample is taken, after an antenna switch has happened. It must be configured before starting the radio. The value should be chosen so that the signal through the receiver chain to the A/D converter has settled after the antenna switch before the sampling occurs. This delay varies for 1 Mbps and 2 Mbps data rates due to different filter settings. It may also depend on external components. The following values are recommended:

PHY (Mbps)	slotDuration (µs)	TSAMPLEOFFSET
1	1	1
1	2	15
2	1	6
2	2	20

The setting for 1Mbps, 1 µs causes the sampling to happen just before the next antenna switch. A signal with severe multipath may not have settled and can affect the quality of the IQ samples. This limitation stems from the bandwidth of the filters in 1 Mbps mode.

The ideal value of TSAMPLEOFFSET may be determined experimentally by sampling at a high rate and visually checking the impact from switching.

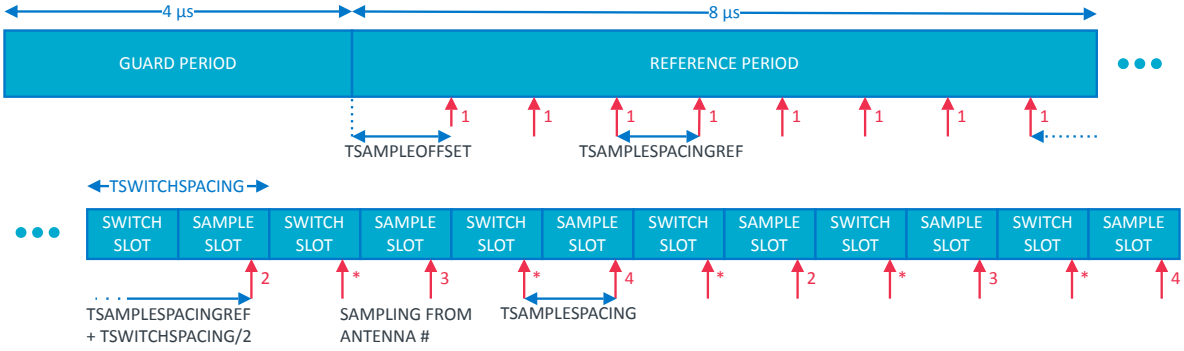


Figure 10: Parameters affecting switching and sampling

3.2 First IQ sample

The hardware always aligns the first IQ sample in the first sample slot.

The duration between the first sample of the reference period and the first sample of the first sample slot is independent from TSAMPLESPACINGREF. However, as a consequence, the duration between the last sample in the reference period and the first sample in the first sample slot is not independent from TSAMPLESPACINGREF. The following diagram illustrates this behavior.

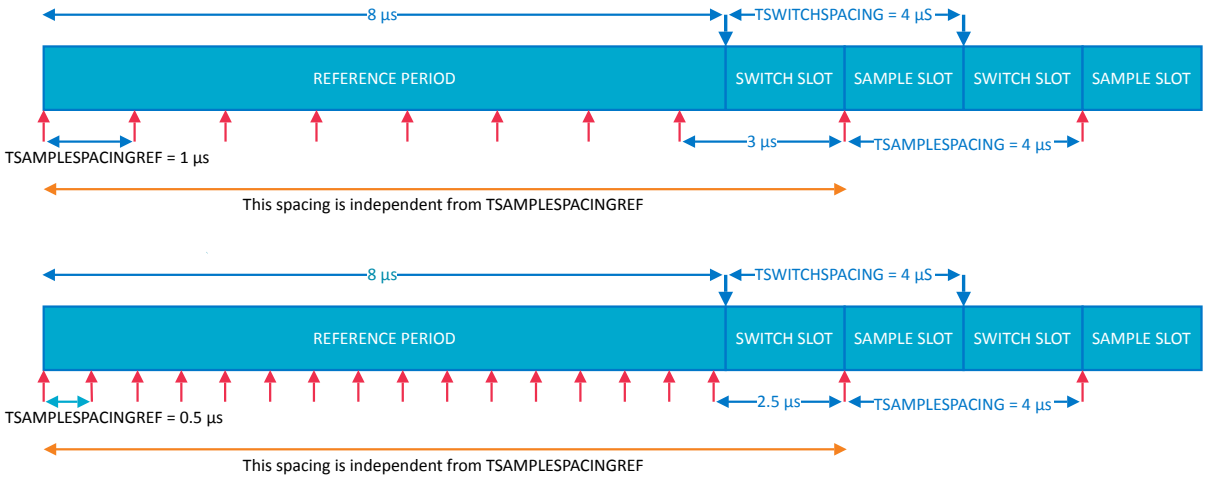


Figure 11: First sample slot

3.3 Frequency offset

The *CTE* is an unmodulated carrier consisting of unwhitened, modulated 1's where the receiver samples a waveform offset of 250 kHz from the channel center in 1 Mbps mode, and in 2 Mbps mode samples a waveform offset of 500 kHz from the channel center.

However, there is generally a frequency offset between the transmitter and receiver. This frequency offset can be calculated from the IQ samples in the reference period and be compensated by software for all IQ samples.

The frequency offset estimate can be refined by switching back to the reference antenna in one or several later switch slots.

3.4 Sample buffer configuration

The RADIO uses DMA to write IQ samples recorded during the *CTE* to RAM.

Alternatively, the magnitude and phase of the samples can be recorded using the DFECTRL1.SAMPLETYPE field. The samples are written to the location in RAM specified by DFEPACKET.PTR. The maximum number of samples to transfer are specified by DFEPACKET.MAXCNT and the number of samples transferred are given in DFEPACKET.AMOUNT.

MAXCNT is defined as number of words and must be determined from the length of the CTE and the sample intervals. This can be calculated as:

```
MAXCNT = 2*(8/TSAMPLESPACINGREF + (8*NUMBEROF8US-12)/TSAMPLESPACING)
```

For typical values of TSAMPLESPACINGREF and TSAMPLESPACING, this can be simplified as:

		TSAMPLESPACING	
		2 µs	4 µs
TSAMPLESPACINGREF	0.5 µs	20 + 8*NUMBEROF8US	26 + 4*NUMBEROF8US
	1 µs	4 + 8*NUMBEROF8US	10 + 4*NUMBEROF8US

Table 3: Typical sample buffer sizes

4 Antenna switching configuration

The following parameters are needed to configure antenna switching.

Setting	Description
TSWITCHSPACING	This setting is the interval between every time the antenna is changed in the switching state.
TSWITCHOFFSET	This setting lets you fine-tune the switching instant (e.g., if an external antenna switch has a long switch delay).
DFEGPIO[n] (n=0..7)	This setting configures the GPIOs used in switching antennas, determined by the SWITCHPATTERN setting.
SWITCHPATTERN	Writing adds a GPIO configuration to the switching pattern to be used. Each configuration contains 8 bits, one for each GPIO, where bit 0 indicates DFEGPIO[0], bit 1 indicates DFEGPIO[1] and so on. A switch pattern is generated by writing multiple configurations consecutively to SWITCHPATTERN. The first configuration is used in the data part of the packet, the second configuration is used in the guard and REFERENCE periods, and each subsequent configuration is applied at the beginning of the next switch slot.

Table 4: Antenna switching settings

The *GPIO*s must be configured as outputs in the *GPIO* peripheral (e.g. with the DIRSET register) in addition to the DFEGPIO register. The radio only controls these *GPIO*s while it is enabled, so to avoid uncontrolled toggling of these *GPIO*s it is recommended to set configuration 1 as default output for these *GPIO*s (e.g. using the OUT register in the *GPIO* peripheral).

When the last switch pattern is reached and IQ sampling continues, the switch pattern loops back to the one used in the first SWITCH slot. The following diagram shows five antenna patterns that have been loaded.

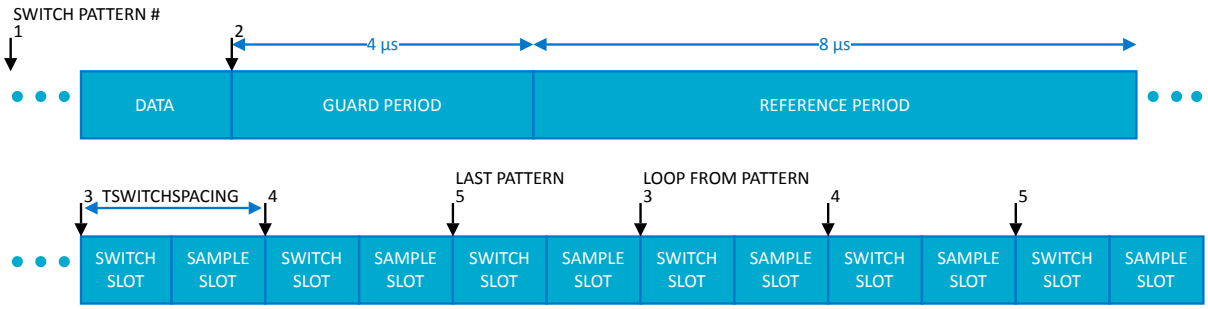


Figure 12: Antenna switching

5 Example configuration

This section describes the implementation of a sample *AoA* system.

This system includes the following configuration:

- nRF52811 in 48 pin QFN
- 4 antennas at the receiver with a SP4T RF switch
- Advertising channel *Protocol Data Unit (PDU)*s
- CTE inline mode
- Output buffer set to 0x20004000
- 0x1C buffer size (28 words)

The following procedures only cover the Direction Finding configuration and does not include general PHY settings. However, you can add this configuration to an existing non-SoftDevice system.

5.1 Setting up the transmitter

Configure the *CTE* to set up the *AoA* transmitter.

1. Enter **`DFEMODE.DFEOPMODE=3`** to set the *AoA* mode.
2. Enter **`DFECTRL.NUMBEROF8US=3`** to set the length of the *CTE* to 24 µs.
3. Enter **`DFECTRL.DFEINEXTENSION=1`** (default) to add the *CTE* after the CRC.
4. Write the TX data to the RAM.

   The frame shall match the required format for an advertising channel *PDU* (CP bit set and CTEInfo=0x18).
5. If the SHORTS.READY_START register is enabled, enter **`TASKS_TXEN=1`** to start the transmitter.

5.2 Receiver configuration

Several configuration procedures must be done before the receiver is started.

5.2.1 Setting up the receiver

The receiver must be configured before it is started.

1. Enter **`DFEMODE.DFEOPMODE=3`** to set the *AoA* mode.
2. Enter **`CTEINLINECONF.CTEINLINECTRLEN=1`** to enable the *CTE* inline mode.
3. Enter **`CTEINLINECONF.CTEINFOINS1=0`** because the Advertising Channel *PDU* has the CP in `S0`.
4. Set the `S0` configuration and mask according to the expected format by entering the following commands:

   a) **`CTEINLINECONF.S0CONF=0x07`**

   b) **`CTEINLINECONF.S0MASK=0x0F`**

Note: The following configurations are used for the Data Channel PDU:

- **`CTEINLINECONF-CTEINFOINS1=1`**
- **`CTEINLINECONF.S0CONF=0x20`**
- **`CTEINLINECONF.S0MASK=0x20`**

5.2.2 Setting up antenna switching for the AoA receiver

Configure *GPIO* toggling for antenna switching.

1. Enter **`DFECTRL1.TSWITCHSPACING=2`** (default) to configure antenna switching every 2 µs.
2. Set the switch pattern that controls the *GPIO*s connected to the antenna switches by entering the following:

   ```
   SWITCHPATTERN=0x1
   SWITCHPATTERN=0x1
   SWITCHPATTERN=0x2
   SWITCHPATTERN=0x4
   SWITCHPATTERN=0x8
   ```

   This step performs five writes to the same register:

   - antenna 1 (data)=0001
   - antenna 1 (guard/reference)=0001
   - antenna 2=0010
   - antenna 3=0100
   - antenna 4=1000
3. Configure the four *GPIO*s (e.g., Pins 37 to 40 on the QFN48 package, P0.25-P0.28):

   ```
   PSEL.DFEGPIO[0]=0X19
   PSEL.DFEGPIO[1]=0X1A
   PSEL.DFEGPIO[2]=0X1B
   PSEL.DFEGPIO[3]=0X1C
   ```
4. Enter **`DFECTRL2.TSWITCHOFFSET=0`** to set the switch offset to zero.
5. Enter **`DIRSET=0x1E00000`** to configure the four *GPIO*s as Output in the *GPIO* peripheral.
6. Enter **`OUT=0x0200000`** to set switch pattern 1 as the default output of the four antenna switching *GPIO*s.

5.2.3 Setting up IQ sampling for the AoA receiver

Complete the following steps to configure the *AoA* receiver for IQ sampling.

1. Enter **`DFECTRL1.SAMPLETYPE=0`** (default) to set the sample type to IQ format.
2. Enter **`DFEPACKET.PTR=0x20004000`** to configure the DMA pointer to RAM.
3. Enter **`DFEPACKET.MAXCNT=0x1C`** to configure the size of the reserved buffer.
4. Enter **`DFECTRL1.TSAMPLESPACINGREF=3`** (default) to set the sample spacing to 1 µs for the reference period.
5. Enter **`DFECTRL1.TSAMPLEOFFSET=3`** to set sample offset to `1`.

   Note: `1` is the recommended value based on Radio Frequency testing.
6. Enter **`CTEINLINECONF.CTEINLINERXMODE1US=2`** (default) to set sample spacing to 2 µs for the sample slots with *CTE* inline mode.
7. If the SHORTS.READY_START register is enabled, enter **`TASKS_RXEN=1`** to start the receiver.

Glossary

Angle of Arrival (AoA)

The relative direction at which a propagating RF wave that was transmitted using an antenna array is incident on another antenna.

Angle of Departure (AoD)

The relative direction from which a propagating RF wave that was transmitted using an antenna array is incident on another antenna.

Constant Tone Extension (CTE)

A field with a constantly modulated series of unwhitenened 1's.

GPIO

General-Purpose Input/Output

Protocol Data Unit (PDU)

Information transferred as a single unit between peer entities of a computer network and containing control and address information or data. PDU mode is one of the two ways of sending and receiving SMS messages.

Acronyms and abbreviations

These acronyms and abbreviations are used in this document.

AoA
Angle of Arrival

AoD
Angle of Departure

CTE
Constant Tone Extension

PDU
Protocol Data Unit

GPIO
General-Purpose Input/Output

Legal notices

By using this documentation you agree to our terms and conditions of use. Nordic Semiconductor may change these terms and conditions at any time without notice.

Liability disclaimer

Nordic Semiconductor ASA reserves the right to make changes without further notice to the product to improve reliability, function, or design. Nordic Semiconductor ASA does not assume any liability arising out of the application or use of any product or circuits described herein.

Nordic Semiconductor ASA does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. If there are any discrepancies, ambiguities or conflicts in Nordic Semiconductor's documentation, the Product Specification prevails.

Nordic Semiconductor ASA reserves the right to make corrections, enhancements, and other changes to this document without notice.

Life support applications

Nordic Semiconductor products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury.

Nordic Semiconductor ASA customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nordic Semiconductor ASA for any damages resulting from such improper use or sale.

RoHS and REACH statement

Complete hazardous substance reports, material composition reports and latest version of Nordic's REACH statement can be found on our website www.nordicsemi.com.

Trademarks

All trademarks, service marks, trade names, product names, and logos appearing in this documentation are the property of their respective owners.

Copyright notice

COMPANY WITH
QUALITY SYSTEM
CERTIFIED BY DNV GL
= ISO 9001 =