ECEN 5823-001
Internet of Things Embedded Firmware

Lecture #11

02 October 2018

Be Boulder.

University of Colorado Boulder

Agenda

- Class Announcements
- Reading Assignment
- BLE Rubric
- Quiz 5 Review
- Bluetooth Low Energy / Smart

Class Announcements

- Quiz #6 is due at 11:59 on Sunday, October 6th, 2018
- Homework #4: BLE Server + MITM + LCD due on Sunday, October 7th, at 11:59pm
- Homework #5: Client flowchart due on Wednesday, October 10th, at 11:59pm
- Homework #6: Client-Server due on Wednesday, October 17th, at 11:59pm

Dynamically changing TX Power

1. the reference manual (http://www.silabs.com/documents/login/reference-manuals/BluetoothSmart_APIRefMan.pdf) says this "***should not*** be used while advertising, scanning, or during connection" (p176). "should not" is not very strong language, and I wonder what would be the negative side effects, since we would like to actually do this (essentially, we want to send out two different advertising messages on different transmission powers)

> It's not safe to change tx power during the RF usage, even the RF is transmitting a very short time at a time. We have done many tests and there is no error happened. But we still can't ignore the possibility that it could damage the PA. There is a workaround for this, which is a safe way to modify the tx power:
>
> gecko_cmd_system_halt(1)
> gecko_cmd_system_set_tx_power(new setting)
> gecko_cmd_system_halt(0)
>
> System halt will force the radio to idle, and connections stay alive if system is resumed before connection supervision timeout.

Reading Assignment

ECEN5823-001, -001B – Reading List
Internet of Things Embedded Firmware
Week 6

Note: The material in this reading as well as all lectures and assignments may be on this week's quiz, quiz 6.

1. "Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 5: Physical Layer

2. "Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 6: Direct Test Mode

3. "Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 10: Attributes

4. "Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 11: Security

HTP BLE Assignment Rubric

Did anyone not take temperature measurements while not connected to your phone app?

2. Functional code delivered per exercise. Max score is 2.0 pts.
    a. Provide screen shot verifying the Advertising period (0.25 pts)
    b. Provide screen shot verifying the connection interval setting (0.25 pts)
    c. Provide screen shot verify slave latency (0.25 pts)
    d. What is the average current between advertisements? (0.25 pts)
    e. What is the average current between connection intervals? (0.25 pts)
    f. What is the peak current of an advertisement? (0.25 pts)
    g. What is the peak current of a data transmission when the phone is placed next to the Blue Gecko? (0.25 pts)
    h. What is the peak current of a data transmission when the phone is placed 20 feet away from the Blue Gecko? (0.25 pts)

3. Functional code. Max score is 8.0 pts. (Note: Depending on iPhone or Android, the Advertisement or ConnInterval or Slave latency may be different. Base your timing on your phone)
    a. Correct temperatures updated to the phone update (1.0 pts)
    b. Advertisement period is 250mS (1.0 pts)
    c. ConnInterval either 75mS or 90mS (depending on phone) (1.0 pts)
    d. ConnInterval + Slave Latency 300mS or 360mS (1.0 pt)
    e. While advertising, between advertisements the average current < 4uA (1.0 pt)
    f. Between ConnIntervals while connected, average current < 4uA (1.0 pt)
    g. TX power auto adjusting (1.0 pt)
        i. You may need to disable TX power auto reset upon connection close to test out TX power auto adjusting
    h. TX power resets upon connection loss/close (1.0 pts)

4. Bonus item
    a. Only takes temperature measurements while Bluetooth is connected (+1.0 pt)

5. Best Practices
    a. Lack of Silicon Labs IP statement for sleep routines (-1.0 pts)
    b. Not following course documentation practices (-1.0 pts)
    c. Using for or while loop delays in I2C routines (-1.0 pts)

Quiz 5 Review

For which hop value would result in remapping due to WiFi channel 6 interference that corresponds to BLE channels 11-20 if at n=0, f = channel 7 at n = 8?

- hop = 12
- hop = 14
- hop = 7
- hop = 10

Quiz 5 Review

When connections are transient like in Bluetooth Low energy, the time to make a connection must be _____ (single word answer).

Quiz 5 Review

Which Bluetooth family profile specifies in detail the operation of both end points?

- Bluetooth Low Energy
- Bluetooth Classic
- Bluetooth Smart

Quiz 5 Review

For which Connection Events, n, would the frequency channel need to be remapped due to interference from WiFi's channel 6 which corresponds to BLE's channels 11-20? (select all that apply)

Assumptions:

at n=0, f(0) = channel 9, hop = 14

- [ ] n = 4
- [ ] n = 2
- [ ] n = 3
- [ ] n = 1
- [ ] n = 6
- [ ] n = 5

Quiz 5 Review

What are the primary methods that the Link Layer reduces power?

- [ ] Using offline encryption
- [ ] Keeping data packets short
- [ ] Using a high physical bid rate
- [ ] Single-channel connection events

Quiz 5 Review

_____ means that once a service is published, it cannot change.

Quiz 5 Review

How does short BLE packets and the 150uS dead time between transmit and receive save energy?

- [ ] Reduces peak current duration of the radio transmitter
- [ ] Radio stays cool
- [ ] Maximizes the duty cycle of transmitting data
- [ ] Reduces the time of the 2.4GHz oscillator being on

Quiz 5 Review

Select all that apply to Bluetooth Classic

- [ ] Each time slot is equal to 625uS
- [ ] Master transmits on odd time slots
- [ ] The 2.4GHz RF band is broken into 40 2MHz channels
- [ ] The Bluetooth radio hops 1600 times per second

Quiz 5 Review

Each element in a Bluetooth Mesh node must have which of the following unique addresses?

- virtual group address
- group address
- unassigned address
- unicast address

Quiz 5 Review

Bluetooth Smart is an asymmetric architecture where the resource rich devices perform the advertising.

- True
- False

Quiz 5 Review

In Bluetooth Low Energy, _____ means of or forming a singe irreducible unit of component of a larger system.

BLE: Offline Encryption

- Bluetooth Low Energy enables the encryption of the data and authentication code to be computed in the background
  - Before a packet is transmitted, the encryption of the data can be performed when the radio is still off
  - The encryption of the data does not depend on the sequence of the data, so it can be encrypted at anytime
    - The data can be retransmitted any number of times, and the encryption and the authentication code will not have to change
  - When receiving encrypted data, the CRC value is computed real time and is the only value that determines whether the data was received correctly.
    - The encrypted data can then remain in the Link Layer until the radio activity has stopped to decrypt the data

BLE: Peripherals

- For peripherals to operate extended time and possibly years on a button-cell battery, the states that the peripheral enters must be optimized
- This includes determining the optimal:
  - Advertising Interval
  - Connection Interval
  - Slave Latency
  - Access to attributes
  - Deciding to stay connected or to disconnect/reconnect

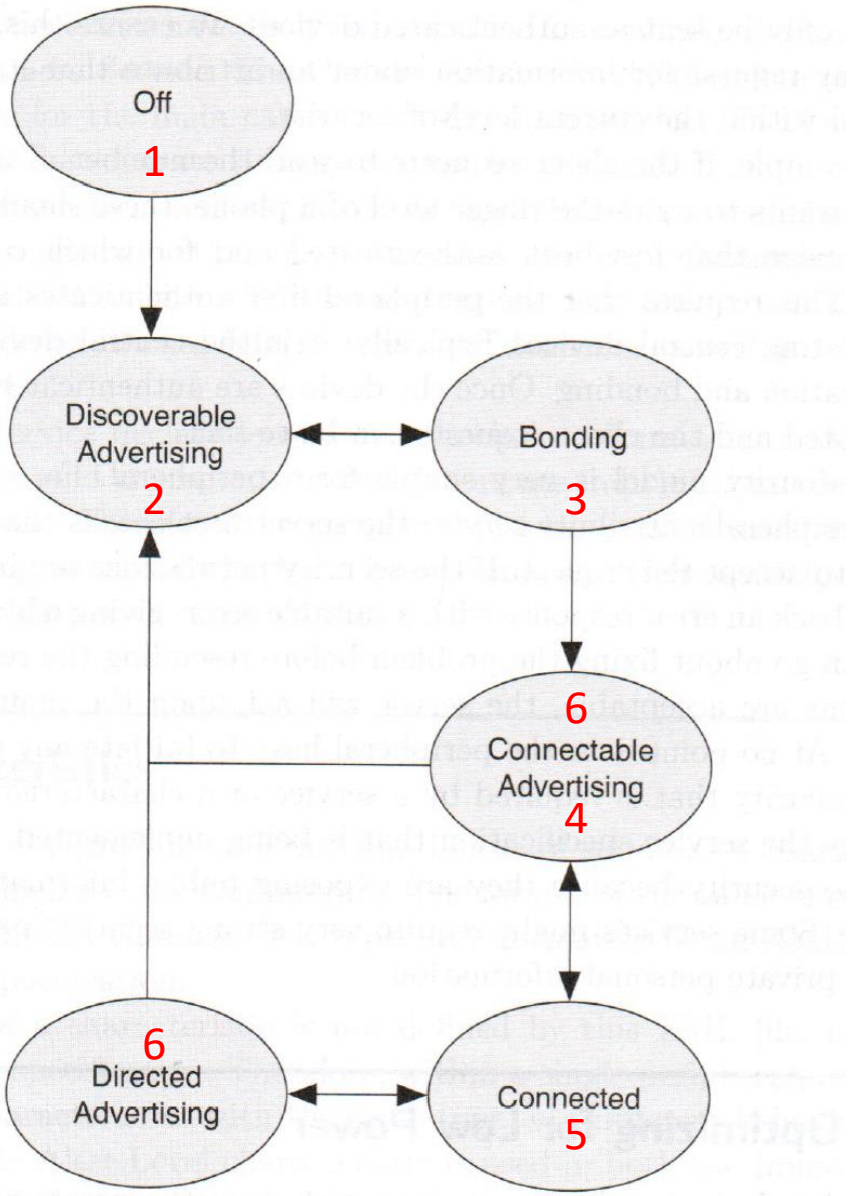


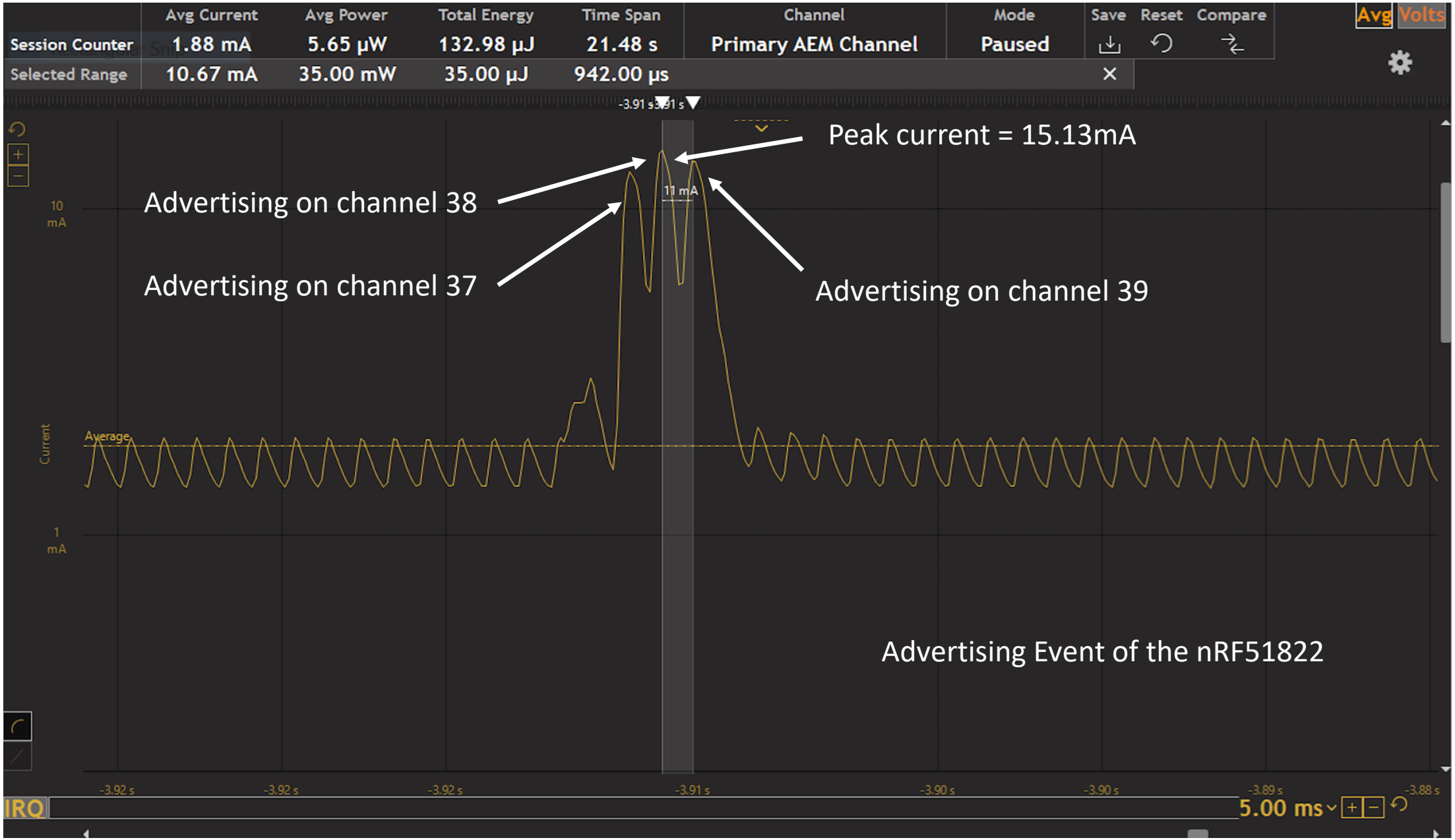
Figure 14–1 The typical states of a peripheral device

BLE: Peripherals (Discoverable Advertising)

- One of the fundamental ways to optimize for low power is to appropriately choose the intervals for advertising and connection intervals
  - The choice could be the difference between a few weeks of operation to years
- Typically, the first state that a peripheral performs is discoverable advertising so that a central device can find it
  - The time that a peripheral is in this state of operation is typically very short in the lifetime of the device since in most applications, the user will want to connect a device shortly after installation
  - Once bonded to a central device, it will move into connectable advertising

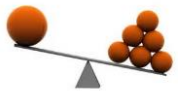
BLE: Peripherals (Discoverable Advertising)

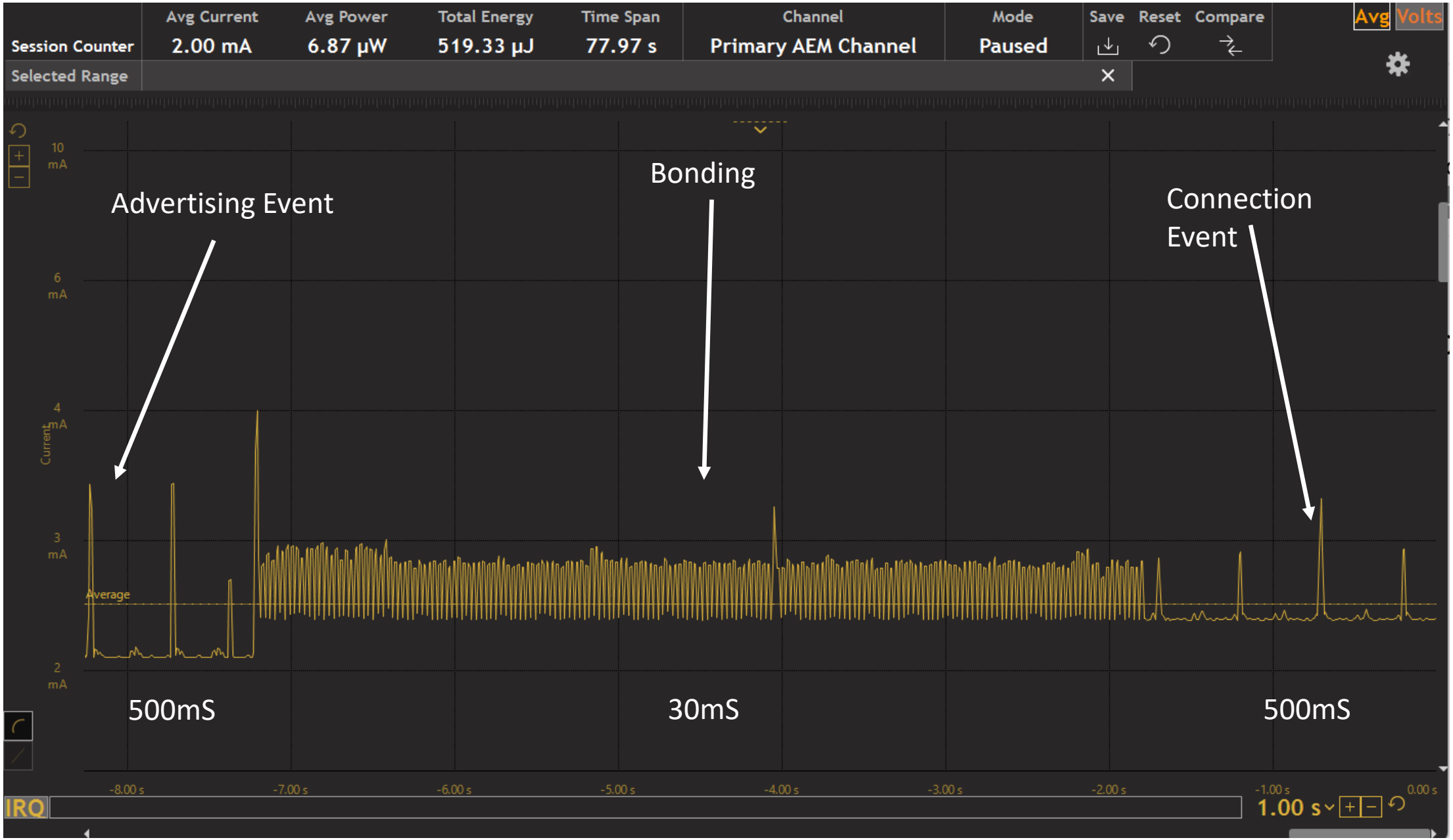
- With the idea that the peripheral will be in the discoverable advertising state for a very short period of its life cycle and to provide a good user experience of a quick connect, the advertising interval of 250mS would be a good compromise between speed of discovery and power savings


Avg Current
Avg Power
Total Energy
Time Span
Channel
Mode
Save
Reset
Compare
Avg
Volts
Session Counter
1.88 mA
5.65 µW
132.98 µJ
21.48 s
Primary AEM Channel
Paused
Selected Range
10.67 mA
35.00 mW
35.00 µJ
942.00 µs
Peak current = 15.13mA
Advertising on channel 38
Advertising on channel 37
Advertising on channel 39
11 mA
10 mA
1 mA
Current
Average
Advertising Event of the nRF51822
IRQ
5.00 ms

BLE: Peripherals (Bonding)

- After the peripheral makes a connection from the discoverable advertising state, the device enters bonding and the connection interval can be set very short (or fast)
  - A fast connection interval of 7.5mS to 25mS can use a lot of power, but it also allows the central device to discover the set of services and characteristics that the peripheral has to offer as well as provide prompt feedback to the user about how it can interact with the peripheral
  - If the connection interval is very slow, 1 to 4S, it can be an extremely long time before a central device can determine how to utilize the peripheral
- Once the appropriate bonding information has been exchanged, the connection interval timing can be long (or slow) to conserve energy




Session Counter
Avg Current
2.00 mA
Avg Power
6.87 µW
Total Energy
519.33 µJ
Time Span
77.97 s
Channel
Primary AEM Channel
Mode
Paused
Save
Reset
Compare
Avg
Volts
Selected Range
10 mA
6 mA
4 mA
3 mA
2 mA
Current
Average
Advertising Event
Bonding
Connection Event
500mS
30mS
500mS
-8.00 s
-7.00 s
-6.00 s
-5.00 s
-4.00 s
-3.00 s
-2.00 s
-1.00 s
0.00 s
IRQ
1.00 s

BLE: Peripherals (Connectable Advertising)

- After a peripheral has bonded with a central device, it can disconnect and at a later time advertise to allow the central device to reconnect
- The advertising interval used in this state is a compromise between how fast at central device can reconnect to the peripheral and the power consumption that the peripheral will use when disconnected
  - Example: A heart-rate belt used by a runner might only be connected for the 3 hours a week while the runner is using it while the remaining 165 hours a week it remains in the connectable advertising state. It also does not need to connect instantaneously, so using a longer connectable advertising interval would be advisable or even disconnect when the belt is not worn
  - A connectable advertising interval of 1 second would allow a central device to be able to connect within a few seconds, and if the peripheral requires a faster connection time, than a connectable advertising interval of 0.5s or less would be required

BLE: Peripheral (Directed Advertising)

- Directed Advertising is used when a peripheral needs to connect directly to a central device usually based on an event happening
- And, when the time between the event and sending notification to the central device must be as short as possible
  - Example: A fire or smoke alarm
- A peripheral burns a lot of power/energy when executing Directed Advertising because the peripheral transmit lots of advertising packets very quickly to a single central device
  - If the central device is available to initiate a connection to this peripheral, it will immediately connect, allowing the peripheral to send its data quickly

BLE: Peripheral (Directed Advertising)

- Directed advertising is the quickest way for a peripheral to make a connection to a central device
  - Connection times + sending the required data can be less than 3 milliseconds
- There is no interval configuration in Directed Advertising
  - Every 3.75mS, the peripheral will send its advertising packets on each of the 3 advertising channels
  - Resulting in one directed advertising packet every 1.25mS or 800 packets per second
  - If there is no central device to respond, directed advertising could consume 250+ times more energy per second compared to a device sending connectable advertising packets once per second
- Directed Advertising could be very useful for peripherals that rarely need to be connected, but when the need arises, connected very quickly

BLE: Peripheral (Connected)

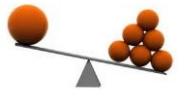
- When connected, the central device has complete control over the connection intervals and latency used by the peripheral
- The peripheral does not have away to signal to the central device that the current connection values being used are appropriate
  - But, the peripheral can request or suggest alternative settings after connection has been made
- There are two configurable values for the connection parameters that relate to power consumption
  - Connection Interval (connInterval): The time that determines how often the central will transmit and synchronize with the peripheral. The connInterval is a multiple of 1.25mS
  - Slave Latency (slavelatency): The number of master connection intervals that the slave can ignore. This value can be 0 to 500

BLE: Peripheral (Connection)

- Example 1:
  - connInterval is set to 12.5mS (10 times 1.25mS)
  - slaveLatency is set to 0
  - How often would the slave need to listen to the client?
    - This would result in the slave required to listen every 12.5mS to determine if the master has a request and consuming a lot of energy
- Example 2:
  - connInterval is set to 12.5mS (10 times 1.25mS)
  - slaveLatency is set to 1
  - How often would the slave need to listen to the client?
    - This would enable the slave to skip one of the reserved connection events for the peripheral, but must listen to the second connection event
    - This would result in a 50% power reduction due to halving the time that the peripheral listens and transmits data to the central device
    - The peripheral could listen and transmit to the first 12.5mS connection event if required

BLE: Peripheral (Connection)

- IMPORTANT: Slave Latency also sets the latency of the central device to the peripheral
  - For example: If a keyboard has an LED indicator that needs to be turned on within 500mS for the desired user experience, the connInterval X slavelatency must be less than 500mS
  - The slave has the option of jumping onto a connection event early, but the master does not!



BLE: Peripheral (Connection)

- IMPORTANT: Extremely long Slave Latency can actually consume more energy than they actually save due to the accuracy of the central and peripheral clocks
  - In worst case, the clock inaccuracies could be 500 parts per million on each device, and possibly in opposition directions
  - If a device was set with a connection interval of 15mS and a slave latency of 500, the slave only would be required to listen every 7.5s
  - At the end of 7.5s, the two devices could be out of synch by 3.75mS and possibly up to 7.5mS if the two devices are off in different directions
  - To resolve this possible timing synchronization issue, the peripheral would need to begin to listen 7.5mS before its expected connection time and possibly 7.5mS afterwards . This is called window widening.
    - For every 7.5s, the peripheral would have to listen from 7.5 to 15.0mS to synchronize
    - Resulting in significant energy loss

BLE: Peripheral (Connection)

- For practical purposes in terms of saving energy, it does not make sense to set the slave latency to have a maximum time between connections greater than 1s or fewer than 300mS.
- Why setting the slave latency less than 300mS does not generally save energy?
  - Below 300mS, the power used to repeatedly synchronize is higher than it would be to wait long
- Why setting the slave latency greater than 1S does not generally save energy?
  - Above 1s, the power used by window widening does not save any significant amount of power, and the user experience is enhanced with a smaller slave latency

BLE: Peripheral (Stay Connected or Disconnect)

- Two main questions to answer:
  - Can the central device reconnect back to the peripheral in a reasonable latency if the peripheral starts to advertise?
  - If the peripheral does stay connected, can the peripheral inquire the connection latency being used or ask for a connection latency to enable an acceptable battery life?
- The peripheral can obtain from the central device the connection latency that it will honor to the peripheral when reestablishing a connection if the peripheral exposes the Scan Parameters Service
  - The central device that connects to this peripheral will discover the scan parameter service and provide to the peripheral its latency


kasa
SMART LIGHTING
veho
0:07 / 1:55
powered by veho
CC
HD

Bluetooth-Classic: Profiles

- High level description to differentiate between Bluetooth-Classic and BLE profiles
- Why are there Bluetooth-Classic profiles?
  - They provide an interoperability between the master and slave
  - For example, enabling a Bluetooth-Classic headset to work with any Bluetooth-Classic or dual-mode phone
- How does the Bluetooth-Classic profile enable interoperability?
  - Clearly defines and states the responsibility of the master and its commands to the slave within a given profile
  - Clearly defines and states the responsibility of the slave and how it responses to the master within a given profile

Bluetooth-Classic: Profiles

- Are there any drawbacks to the Bluetooth-Classic Profiles?
  - It does not allow, or at least easily, the change of roles or use cases
  - For example:
    - Bluetooth-Classic headsets support the Headset Profile (HSP) which enables interoperability with all Bluetooth-Classic phones
    - As an audio engineer, you discover a new way to send data to the headset that would increase audio fidelity
    - You develop the code on your phone, but since the definition of how the master (phone) operates with the slave (headset) is defined, your new and improved communications scheme will not work on any of the older HSP headsets
    - You will need to convince the headset manufacturers to support a new profile to enable your improved product to market

BLE: Profiles

- First, what is BLE service?
  - Defined state information on a server
  - Standard defined services on the server are immutable
- What are BLE profiles?
  - Client defined use of server services
  - The profile could use multiple server services or services across multiple servers
  - Note: No specification of what the server must do in support of a BLE profile

BLE: Profiles

- What is the advantage of moving the responsibility of the profile from both end points to the client?
  - Enabling the server to be used in a “limitless” number of profiles that exist today and in the future
  - Minimize the code and responsibility of the server to save energy on the resource limited device
- For example:
  - A device provides the following services:
    - Temperature
    - Air quality
  - The client uses this devices services with a profile to provide an application with data on the temperature and air quality of a particular room in a building
  - Someday in the future, a new profile could be developed on the client that could take these device services and make it a fire or smoke alarm
- Moving the role to the client enables servers to be used in new roles that may not even be thought of today

BLE: Central (Discovering Devices)

- The first thing that a newly commissioned central device will do is to discover other devices
  - Passive Scanning: a central device passively listens to advertisement packets that peripherals are transmitting
  - Active Scanning: a central device, after hearing a peripheral, asks for more information
- If the Central device is only looking for what devices are around, such as when you open your mobile phone Bluetooth connections, it should only use passive scanning
  - Reduces the energy of the central and peripheral devices
  - If active scanning is used, the peripheral will need to listen to the central device and respond to request which will increase the radio active time consuming energy