ECEN 5023-001, -001B, -740

Mobile Computing & IoT Security

Lecture #11

21 February 2017

I2C bus analyzer demo

Agenda

- I2C bus analyzer demo
- Class Announcements
- Assigned reading
- Quiz 6 assigned
- Quiz 5 review
- Bluetooth Low Energy / Smart

Class Announcements

- Quiz #6 is due at 11:59pm on Sunday, February 26th, 2017
- Implementing an I2C Sensor assignment is due Wednesday, February 22nd, at 11:59pm
- Atmel ATSAMB11 dev kits will be distributed at the end of class today which will be required for the ATSAMB11 tutorial which will be assigned this Thursday the 23rd
- Mid-term will be held in class on Tuesday, March 7th, at 6:30 in class
    - For on campus students, you must be in class for the exam
    - For distant learners, the mid-term will be due by 6:00pm on Thursday, March 9th

Assigned Reading

ECEN5023-001, -001B, -740 – Reading List
Mobile Computing and the Internet of Things Security
Week 5

Note: Quiz for week 6 will be from the first 2 listed readings from the list below as well as the lectures.

1. "Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 2: Basic Concepts

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

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

Quiz 6: Assigned

- Will cover the assigned reading as well as lecture materials from January 17th thru February 23rd, 2017
- Quiz is due on Sunday, February 26th, at 11:59pm

Quiz 5 Review

What are the valid communication standards between different Bluetooth devices? (select all that apply)

- ☐ Single-Mode to Single-Mode in Bluetooth LE
- ☐ Single-Mode to Classic in Bluetooth LE
- ☐ Classic to Dual-Mode in Bluetooth Classic
- ☐ Dual-Mode to Dual-Mode in Bluetooth LE

In Dual-Mode to Dual-Mode, the Bluetooth devices will communicate in Bluetooth Classic
A Single-Mode device cannot communicate with a Bluetooth Classic device

Quiz 5 Review

Which type of Bluetooth radio would most likely be used in a new Client device?

- ✔ Dual-Mode
- Classic
- Single-Mode

Most client devices today like a cellphone or computer will have a dual-mode Bluetooth radio to enable communications with both BLE and Classic Bluetooth devices

Quiz 5 Review

Which Bluetooth radio was designed specifically to be used with coin cell batteries?

- ○ Bluetooth dual-mode
- ○ Bluetooth Classic
- ✔ Bluetooth Low Energy

Quiz Review

What were the design goals of the original Bluetooth radio? (select all that apply)

- ✗ Mesh Networking
- ✓ Short Range
- ✓ Worldwide operation
- ✓ Low Cost
- ✗ IP addressable devices

To reduce the radio packet size, the Bluetooth devices do not support direct IP addressability which would require large radio packets to support.

Quiz 5 Review

Bluetooth LE is targeting the same applications as Bluetooth Classic, but at a lower energy/power level.

- True
- False

Quiz Review

By limiting to only 3 radio frequencies for discoverability, the Bluetooth LE radio only needs to be on the air for a short period of time every second to be discovered.

To save energy, Bluetooth LE uses only 3 radio frequencies for discoverability out of the 40 radio channels.

- [x] True
- [ ] False

Quiz Review

Short packets are good for Bluetooth LE for what reasons? (select all that apply)

- [x] Short current pulses out of a button-cell battery is more efficient than long continuous current drain.
- [x] Short packet transmissions removes the requirement of constantly recalibrating the radio.
- [x] Efficient encoding enables larger quantity of data to be sent faster, thus using less energy.

Quiz 5 Review

A Bluetooth Smart Ready device is the same as a Bluetooth Low Energy radio?

- True
- False ✓

Quiz Review

A Bluetooth Smart Ready device is equivalent to a Bluetooth dual-mode device.

- True
- False

Quiz Review

Bluetooth Classic is architected for applications that need to transmit a few bytes of data every second.

- True
- False

Bluetooth Classic is designed to support audio, data, and voice streams which require many bytes per second.
Bluetooth Low Energy / Smart is architected to transmit state which requires only a few bytes per second.

Quiz Review

How long does it take a Bluetooth LE typically to make a connections?

- ○ 200-500 milli seconds
- ○ 200-500 micro seconds
- ✓ 2-4 milli seconds
- ○ 2-4 seconds

Quiz 5 Review

How long does it take a Bluetooth Classic typically to make a connections?

- ◯ 200-500 micro seconds
- ✔ 2-4 seconds
- ◯ 200-500 milli seconds
- ◯ 2-4 milli seconds

Quiz 5 Review

To save energy, a Bluetooth LE device can reduce its period on to save energy. What is the maximum period that the Bluetooth LE device can be off before a communication time-out occurs?

- 750 milli seconds
- 16 seconds
- 7.5 milli-seconds
- 6 seconds

Quiz Review

In the Bluetooth LE Generic Attribute Profile (GATT), what are the primary roles defined? (select all that apply)

- [ ] Central
- [x] Client
- [x] Server
- [ ] Peripheral

Quiz Review

Which concept most closely matches a peripheral role?

- ○ Central
- ○ Client
- ✓ Server

Both a peripheral and a server are most likely Bluetooth LE end points.

Quiz Review

Which Bluetooth LE term is most similar in functionality to a GATT Client?

- GAP Peripheral
- GAP Central ✓
- GAP Server

In most cases, a GATT Client will be the master device where the GATT Peripheral will be the slave. Similarly, in most cases, the GAP Central will be the master where the GAP Server will be the slave.

Quiz Review

What are the main strengths of Bluetooth Classic? (select all that apply)

- [x] Simultaneously handle both data and voice transmissions
- [x] Automatic service discovery
- [ ] Line of sight communications
- [x] Ad-hoc connections

Quiz Review

Bluetooth classic can be in the following network configurations? (select all that apply)

- Star network
- Hybrid Mesh and Star network
- Scatternet
- Mesh network

A Bluetooth Classic device can be in a standalone piconet which is configured as a star network or reside in two piconets which results in a scatternet.

Quiz 5 Review

A Bluetooth Classic device can be the following? (select all that apply)

- [ ] A master in one Piconet and a master in another Piconet
- [x] A master in one Piconet and a slave in another Piconet
- [x] A master in a Piconet
- [x] A slave in one Piconet and a slave in another Piconet
- [x] A slave in a Piconet

Quiz Review

What are the key specifications in determining a coin-cell battery life in a BLE application?

- [x] The duty cycle of the BLE device sleep mode
- [x] The duty cycle of the active radio RX/TX
- [x] Internal resistance of the battery
- [x] The peak current while the radio is in active mode

All of these specification of the BLE system are important in determining the life span of a coin cell in a BLE device.

Quiz 5 Review

Which device is the primary power source in a BLE device while in sleep mode?

- The capacitance
- The coin-cell battery

Quiz 5 Review

At what temperature is a coin-cell battery capacitor assisted power source more important?

- 70C
- 105C
- 0C
- 25C

Quiz 5 Review

Using the Leopard Gecko data sheet and reference manual, what would be the lowest sleep mode that the Leopard Gecko could enter after enabling the I2C as an I2C master and perform I2C operations after asuccessful BlockSleepMode()?

(Use the enumerations EM0, EM1, EM2, EM3, or EM4)

(em1, EM1)

Quiz 5 Review

Slaves on the I2C bus can pause communications to give them time to process information by ______ the SCL line.

(stretching, clock stretching, holding down, holding low, pull low, pulling low, pull down, pull low, hold low, hold down)

Quiz 5 Review

The Leopard Gecko I2C peripheral's obtain its clock from what source?

- [x] HFCLK
- [ ] ULFRCO
- [ ] LFA
- [x] HFPERCLK

Quiz 5 Review

In general, what is the preferred order of operation to enable an external device via Load Power Management using a GPIO pin as the power source?

2	Wait for power to stabilize and external device to boot
4	Initialize, program, the external peripheral
3	Enable GPIO I//O pins
1	Set GPIO power pin HIGH
5	Enable Interrupts if used

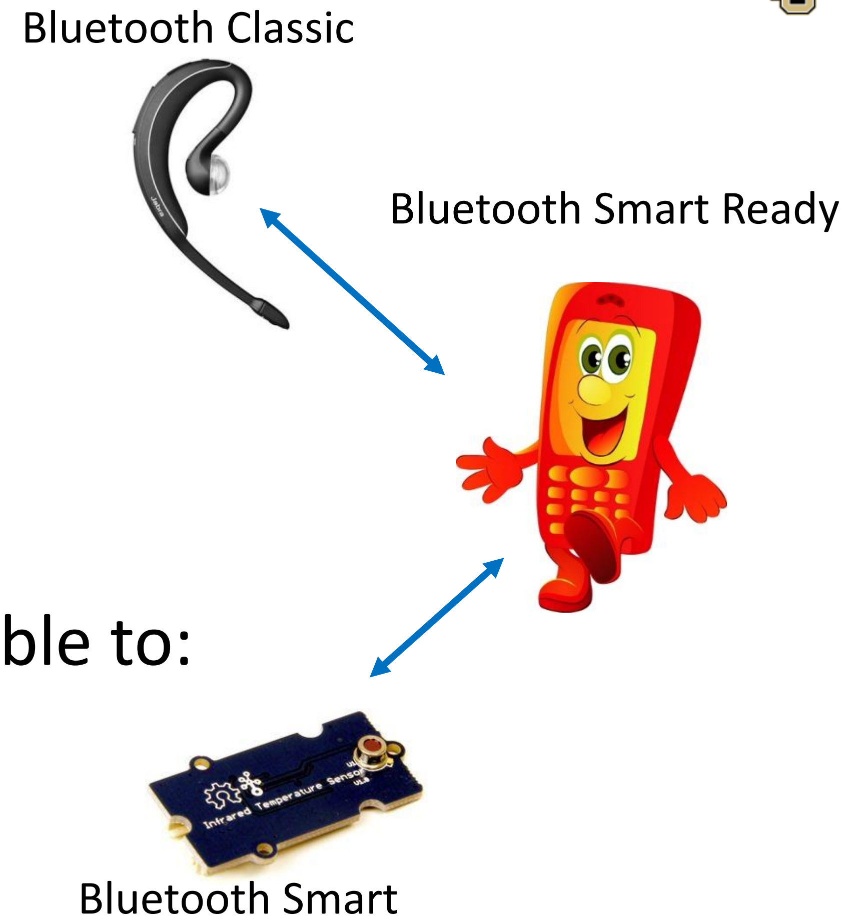
Bluetooth Low Energy / Smart

Bluetooth Low Energy = Bluetooth Smart

https://www.youtube.com/watch?v=Z08y-4S5O7s

Key take aways from the video

- Bluetooth Low Energy = Bluetooth Smart
- Bluetooth Smart != Bluetooth Classic
  - They are not compatible
- Bluetooth Smart Ready (Dual-Mode) is compatible to:
  - Bluetooth Smart (Single-Mode)
  - And,
  - Bluetooth Classic
- Bluetooth Smart Ready is a gateway between Bluetooth Smart and Bluetooth Classic



Bluetooth Low Energy / Smart

	Voice	Data	Audio	Video	State
Bluetooth ACL / HS	x	Y	Y	x	x
Bluetooth SCO/eSCO	Y	x	x	x	x
Bluetooth low energy	x	x	x	x	Y
Wi-Fi	(VoIP)	Y	Y	Y	x
Wi-Fi Direct	Y	Y	Y	x	x
ZigBee	x	x	x	x	Y
ANT	x	x	x	x	Y

State = low bandwidth, low latency data

Low Power

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth Low Energy / Smart

- What is traditional Bluetooth Classic used for?
  - Mobile phones, including ‘smart phones’
  - Wireless controllers for video games
  - Voice headsets and “Car kits”
  - Stereo speakers
  - PCs
  - M2M applications
    - credit card readers
    - industrial automation

Think of replacing wires

- Bluetooth Classic is mainly or more commonly used for Human I/O applications!

Bluetooth Low Energy / Smart

- How much energy does Bluetooth Classic use?
  - Bluetooth Classic is *connection oriented*
  - When a device is connected, a link, "pseudo wire," is maintained, even if there is no data flowing
  - Sniff modes allow devices to sleep, reducing power consumption to give months of battery life
  - Peak transmit current is typically around 25mA.

- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for coin cells and energy harvesting applications

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth BLE - What is Bluetooth Low Energy?

- A new radio, new protocol stack, new profile architecture and a new qualification regime
- It's designed to run from coin cells
- It is a radio standard enabling the Internet of Things
- Features:
  - Mostly new PHY; some parts derived from the Basic Rate (BR) radio
  - New advertising mechanism, for ease of discovery & connection
  - Asynchronous connection-less MAC: used for low latency, fast transactions (e.g. 3ms from start to finish)
  - New Generic Attribute Profile to simplify devices and the software that uses them.
  - Asynchronous Client / Server architecture
- Designed to be LOWEST cost and EASY to implement

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE - fact sheet

Range:	~ 150 meters open field
Output Power:	~ 10mW (10dBm)
Max Current:	~ 15mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current	~ 1µA
Modes:	Broadcast, Connection, Event Data Models Reads, Writes

Specification

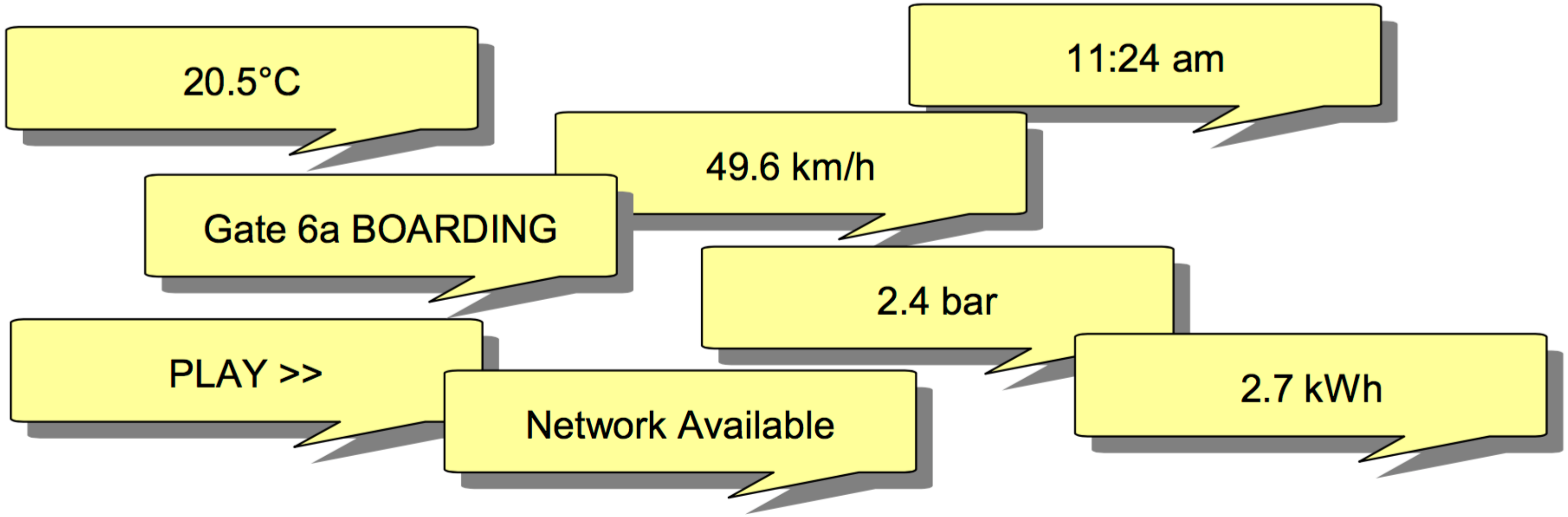
Implementation specific

BLE – fact sheet

- Data through put is missing
  - Data throughput is not a meaningful parameter for BLE
  - It does not support streaming
  - It has a data rate of 1Mbps, but is not optimized for file transfer.
  - It is designed for sending small chunks of data (exposing state).

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE – Exposing state

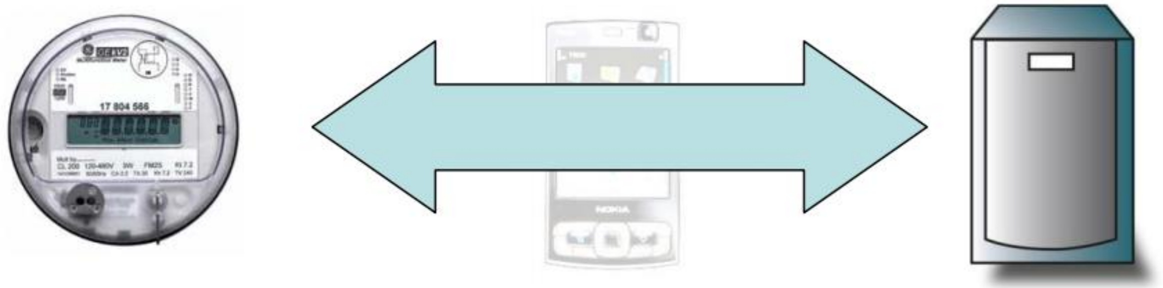


- It’s good at small, discrete data transfers
- Data can be triggered by local events
- Data can be read at any time by a client
- Interface model is very simple (GATT)
- Not targeted for Human I/O

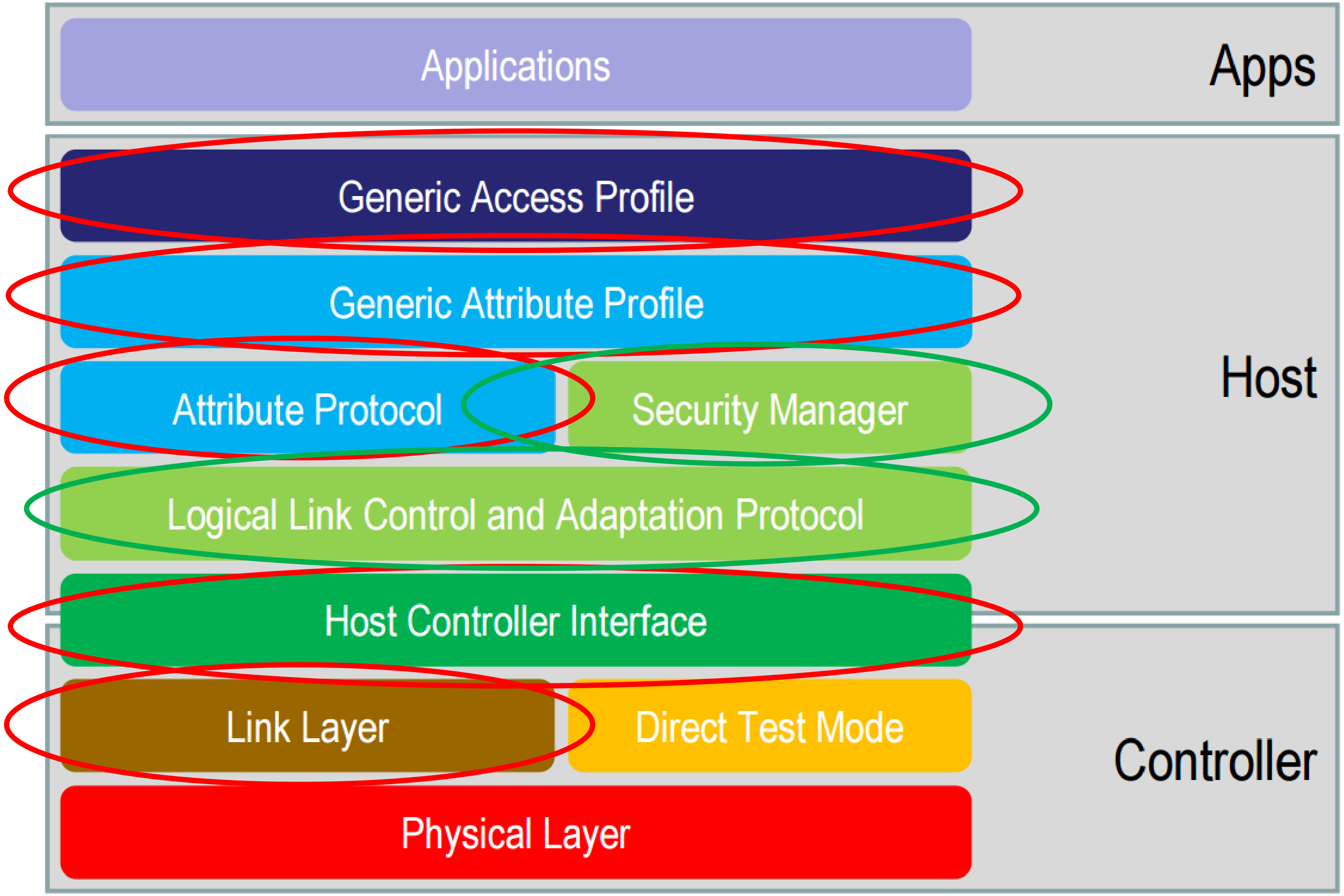
Bluetooth Low Energy is about ~~generic~~ gateways

Currently, hardware or vendor specific

- Devices that support Bluetooth low energy Gateway functionality provide a transparent pipe from a device to an IP address
- Middleware at the IP address can access the device directly as if it were a collector talking to it locally
- The Gateway device plays no part other than in acting as a pipe



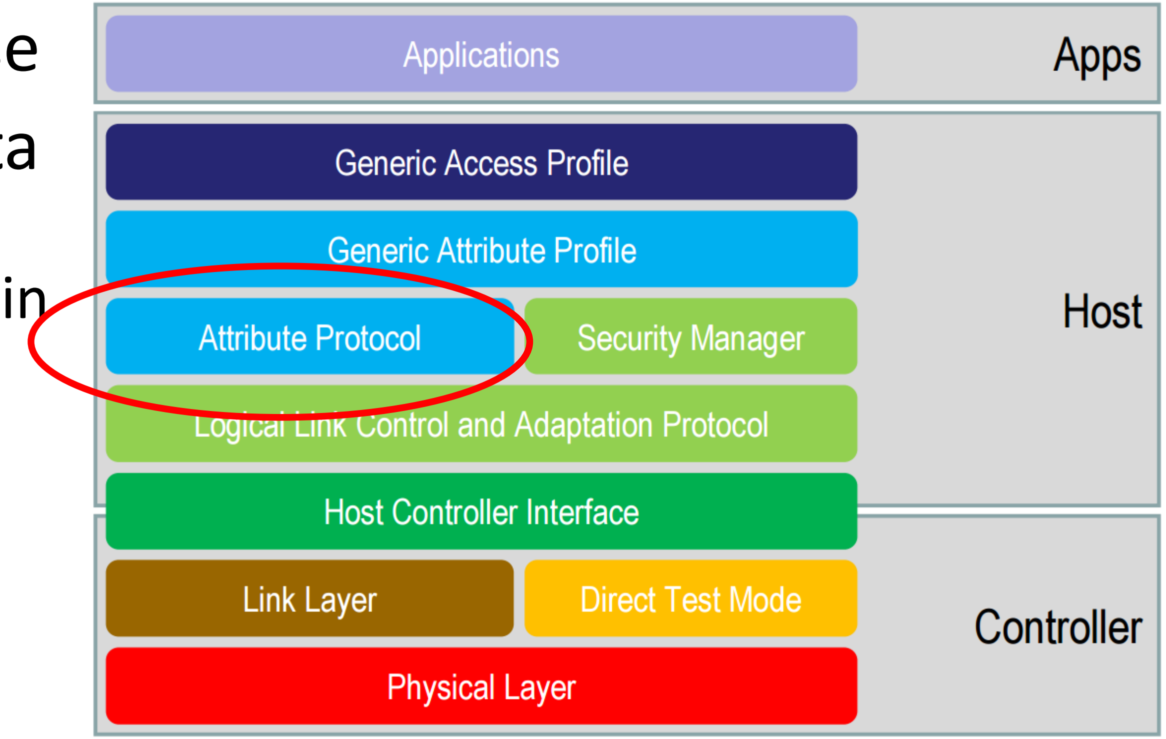
BLE: Stack



CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE: Attribute Protocol

- Only one protocol which is used for name discovery, service discovery, and for reading and writing information required to implement a given use case
- Defines a set of rules for accessing data on a peer device
  - The data is stored on an attribute server in “attributes” that an attribute client can read and write
  - The client sends requests to the server, and the server responds with response messages



Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf
Bluetooth Low Energy: The Developer’s Handbook By Robin Heydon

BLE: The Attribute Protocol

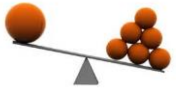
- Defines six types of messages:
  - Requests sent from client to the server
  - Responses sent from the server to the client in reply to request
  - Commands sent from the client to the server that have no response
  - Notifications sent from the server to the client that have no confirmation
  - Indications sent from the server to the client
  - Confirmations sent from the client to the server in reply to an indication
- Communications can be initiated by both the client and the server

BLE: The Attribute Protocol

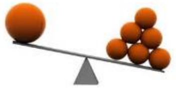
- Attributes are addressed, labeled bits of data
  - Each attribute has a unique handle that identifies that attribute
  - Type that identifies the data stored in the attribute
  - And a value
- For example, an attribute with type Temperature that has a value of 20.5C could be contained within an attribute with the handle 0x01CE
- The Attribute Protocol does not define any attribute types, although it does define that some attributes can be grouped, and their groups can be discovered via the Attribute Protocol
- The Attribute Protocol also defines that some attributes have permissions:
  - To allow a client to read or write an attribute's value
  - Or, to only allow access to the value of the attribute if the client has been authenticated itself or has been authorized by the server
- The Attribute Protocol is mostly stateless
  - Each individual transaction such as a read request and read response does not cause state to be saved on the server
  - The one exception is the prepare and execute write request. These store a set of values that are to be written in the server and then executed all in sequence in a singel transaction

BLE: Asymmetric Design

- A major philosophy of the Bluetooth Low Energy Architecture



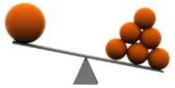
  - Devices with smaller energy sources be given less to do
  - Conversely, devices with larger energy sources be given more to do
- A fundamental assumption is the most resource-constraint device will be the one to which all others are optimized



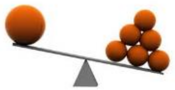
  - Advertising is less energy consuming than scanning
  - A slave has less energy than a master
    - A master has to manage the piconet timing, the adaptive frequency hopping set, encryption, and many other complex procedures

BLE: Asymmetric Design

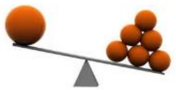
- At the Generic Attribute Protocol Layer, the two type of devices are:
  - Client
    - Determines what data the server has and how to use it
    - The client sends request to the server for data
  - Server
    - The Server holds data
    - Similar to the slave at the Link Layer, the server just does what it is told



- The security architecture works on a key distribution scheme by which the slave device gives a key to the master device to remember
  - The burden is on the master to remember the bonding information, not the slave



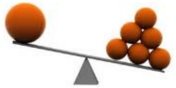
- This implies the most resource-constraint device will want to be the advertisers, slaves, and servers



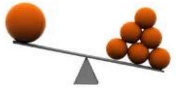
- Conversely, the devices with the most resources will be the scanners, masters, and clients

BLE: Asymmetric design

- Client-Server Architecture:
  - An IP address could have been specified to be given to each BLE device, but the simplest of IP stack takes more memory and energy than is desired on resourced constrained devices
    - The most resource-constraint device will be the one to which all others are optimized



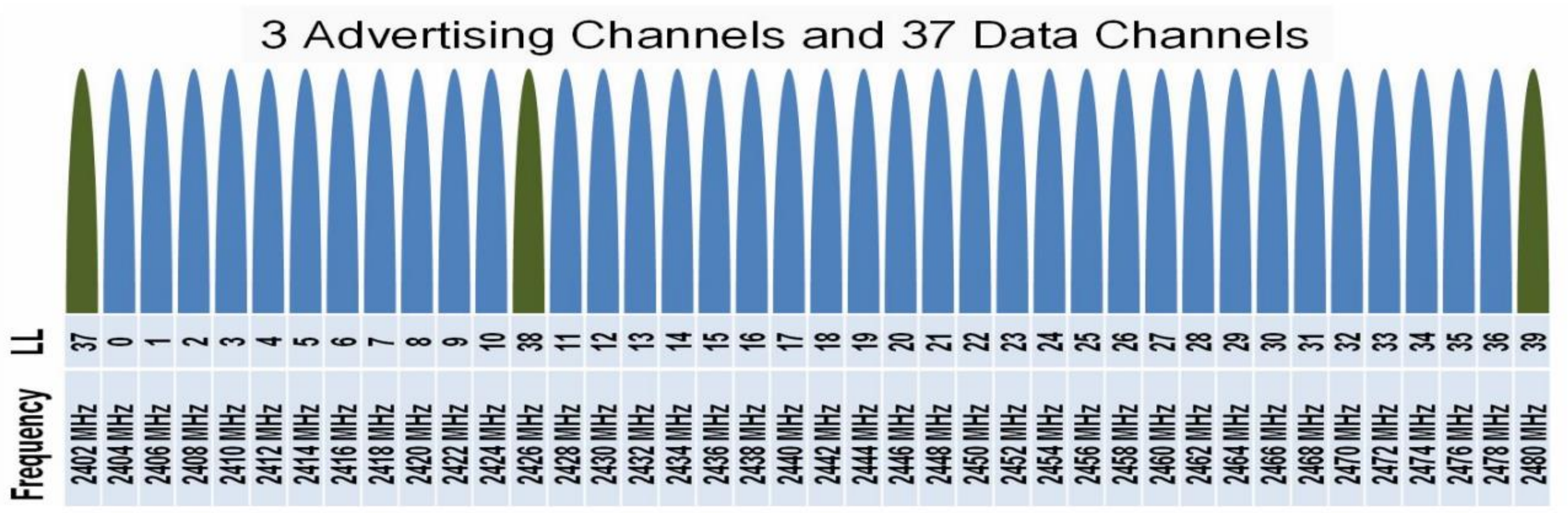
  - The client-server architecture makes possible smart gateways to connect the very efficient low-energy slaves to the internet



    - The client, the more resource abundant device, can connect and handle the IP protocol
    - While, the server is just the repository of data
  - Full Internet security can be provided between the client to the gateway where the gateway performs access control, firewall, and authorization of the client before granting access to anything beyond the gateway
    - These gateways, routers and access points, are proven technologies used today

BLE: The Radio

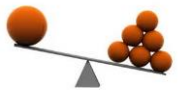
- 2.4 GHz ISM band
- 1 Mbps GFSK
  - Larger modulation index than Bluetooth BR (which means better range)
- 40 Channels on 2 MHz spacing:



CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE: The Radio

- Adaptive Frequency Hopping (AFH):
  - A technology where only a subset of available frequencies are used
  - Robust by detecting sources of interference quickly, and adapting to avoid them in the future
  - Quickly recovers from dropped packets caused by interference quickly by hopping to a new channel
- Short Range and Low Power:
  - Transmit power should be kept as low as possible
  - Receive sensitivity should be relatively high to pick up the transmitted signals
  - Transmit power and Receive amplification should match the device resources appropriately
    - Dual-Mode devices with larger batteries can transmit at a higher power
    - Dual-Mode devices with larger batteries can increase the gain of the receiver



BLE: Adaptive Frequency Hopping

Another representations of the BLE Advertising and Data Channels

Table 7–3 Complete List of Advertising and Data Channels, the Link Layer Channel Number, and Center Frequency

Frequency (MHz)	LL Channel Number	Type	Frequency (MHz)	LL Channel Number	Type
2402	37	Adv	2442	18	Data
2404	0	Data	2444	19	Data
2406	1	Data	2446	20	Data
2408	2	Data	2448	21	Data
2410	3	Data	2450	22	Data
2412	4	Data	2452	23	Data
2414	5	Data	2454	24	Data
2416	6	Data	2456	25	Data
2418	7	Data	2458	26	Data
2420	8	Data	2460	27	Data
2422	9	Data	2462	28	Data
2424	10	Data	2464	29	Data
2426	38	Adv	2466	30	Data
2428	11	Data	2468	31	Data
2430	12	Data	2470	32	Data
2432	13	Data	2472	33	Data
2434	14	Data	2474	34	Data
2436	15	Data	2476	35	Data
2438	16	Data	2478	36	Data
2440	17	Data	2480	39	Adv

BLE: Adaptive Frequency Hopping Managing Interference and Coexistence

- WiFi access point typically use one of three 802.11 channels
- BLE Advertising channels are strategically placed to not be interfered by these WiFi channels (1, 6, and 11)
- Three advertising channels are designed into the BLE specification to provide robustness
- Without an effective advertising channel, BLE would not be an effective wireless network

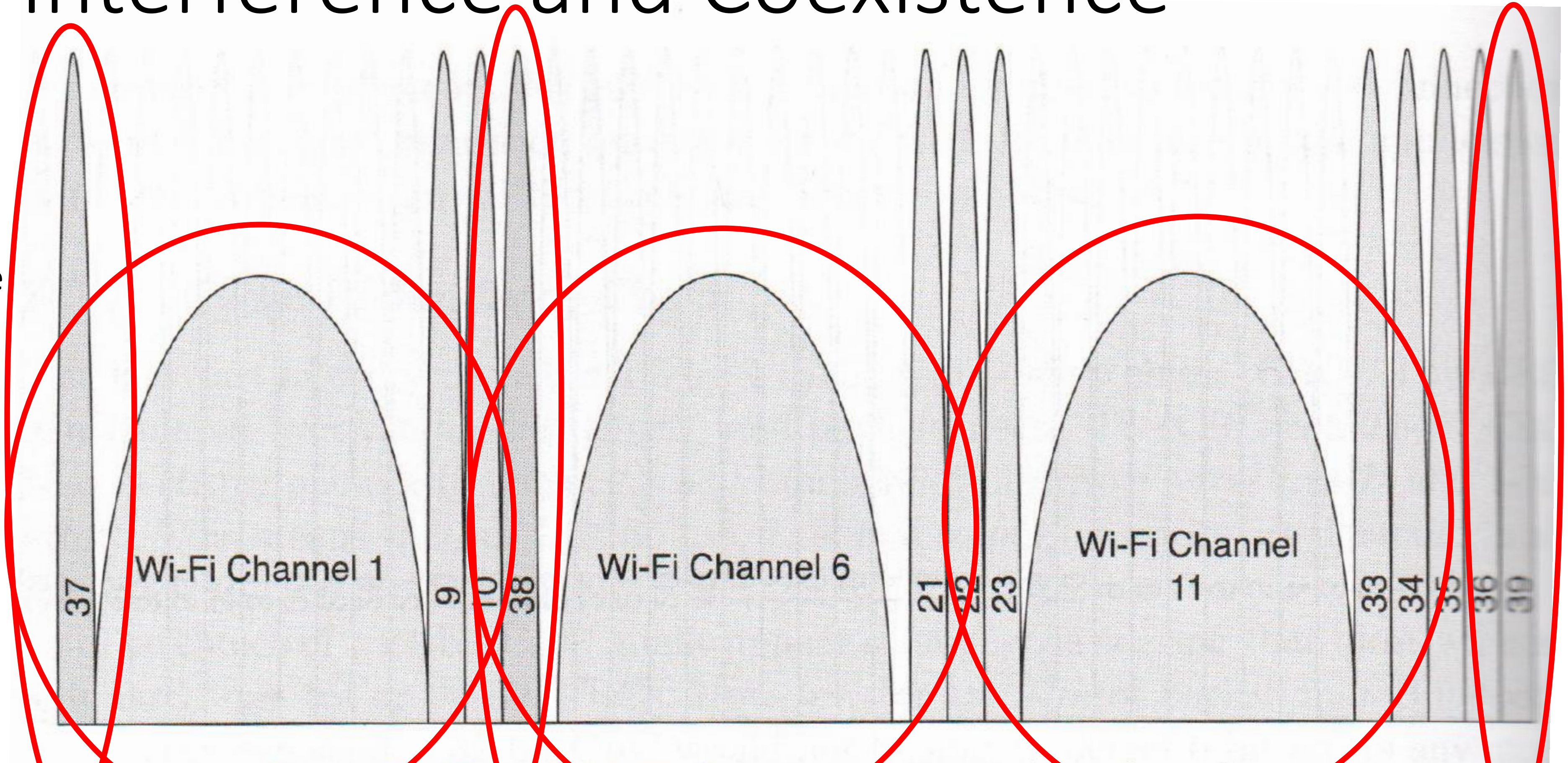


Figure 7–13 Link Layer channels and Wi-Fi channel coexistence

BLE: Frequency Hopping

- When in data connection, a frequency-hopping algorithm is used. Since there are 37 data channels which is a prime number, the hopping sequence is very simple
  - f_{n+1} = (f_n+hop) mod 37
  - The hop value can range from 5 to 16
  - This will result in every frequency be used with equal priority
- Notice, that the advertising channel numbers are greater than 37, so they will never be used in the data connection hop sequence

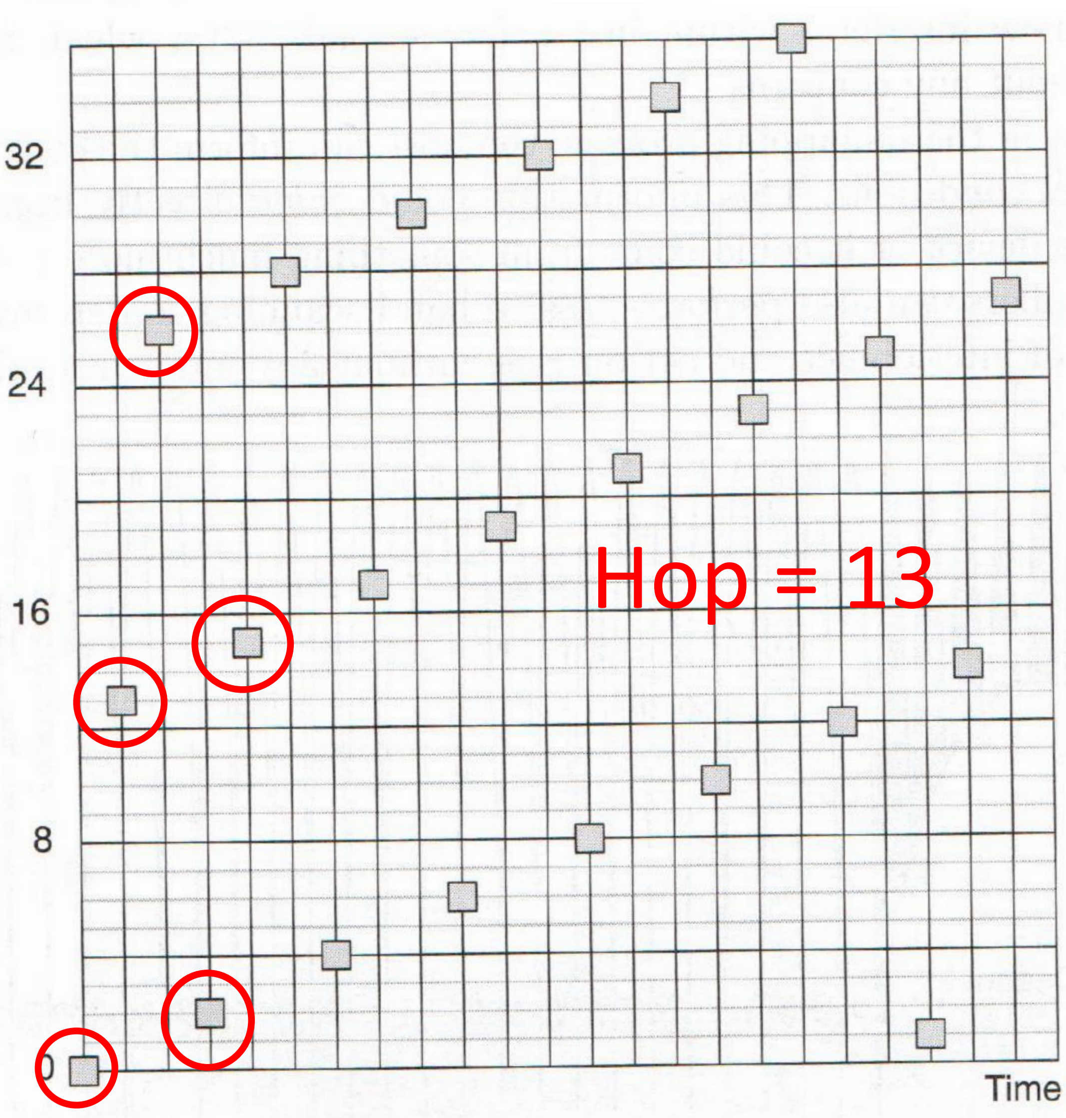


Figure 7–14 Frequency hopping of data channels over time

BLE: Adaptive Frequency Hopping

- Adaptive frequency hopping makes it possible for a given packet to be remapped from a known bad channel to a know good channel
- In the example to the right, the data channels 0-8 are known bad channels due to the WiFi Channel 1 interference
- Channels 0-8 should be remapped to channels 9-36

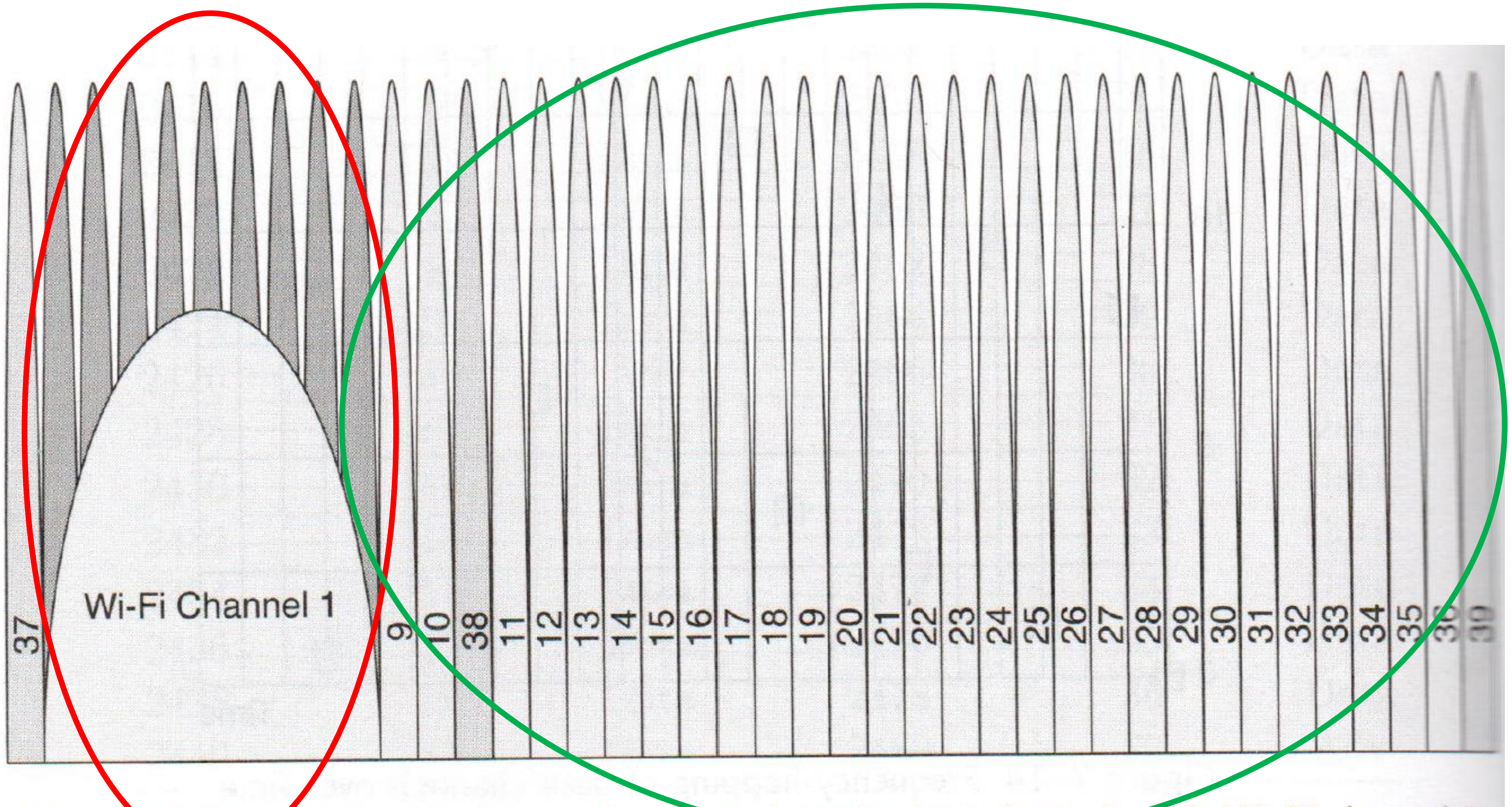


Figure 7–15 Link Layer adaptive frequency-hopping bad channels with Wi-Fi channel 1

BLE: Adaptive Frequency Hopping

Hop = 13

Table 7–4 An Example of Adaptive Frequency Channel Remapping

Original Channel	Good/Bad	Remapped Channel
0	Bad	9
13	Good	13
26	Good	26
2	Bad	11
15	Good	15
28	Good	28
4	Bad	13
17	Good	17
30	Good	30
6	Bad	15
19	Good	19
32	Good	32
8	Bad	17

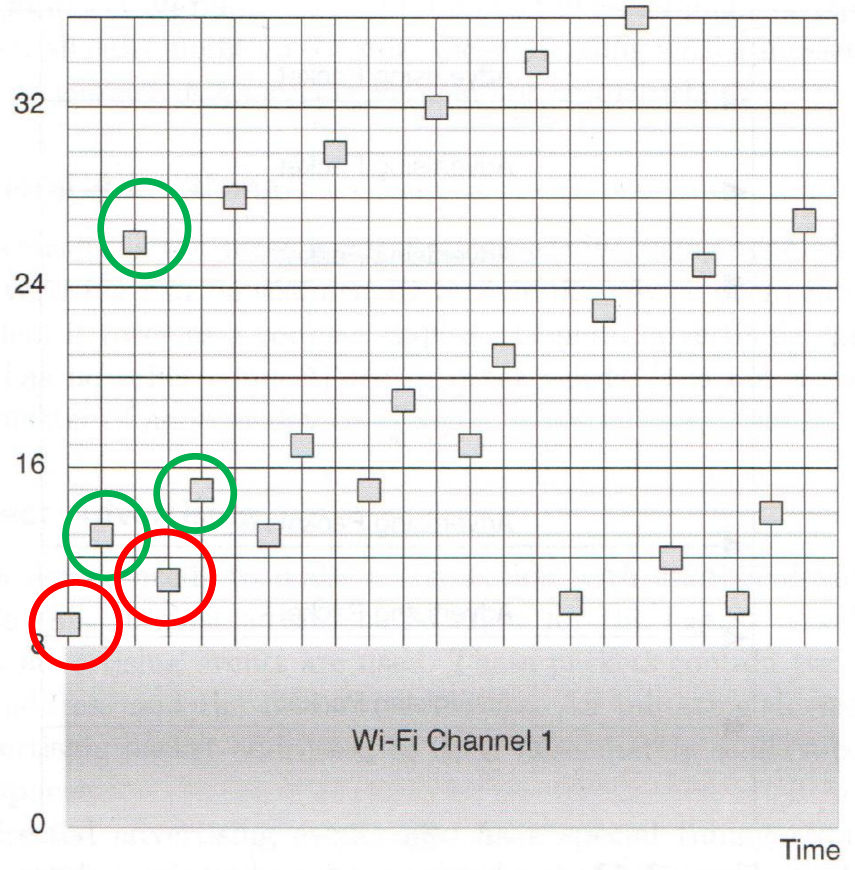


Figure 7–16 Adaptive frequency-hopping remapping