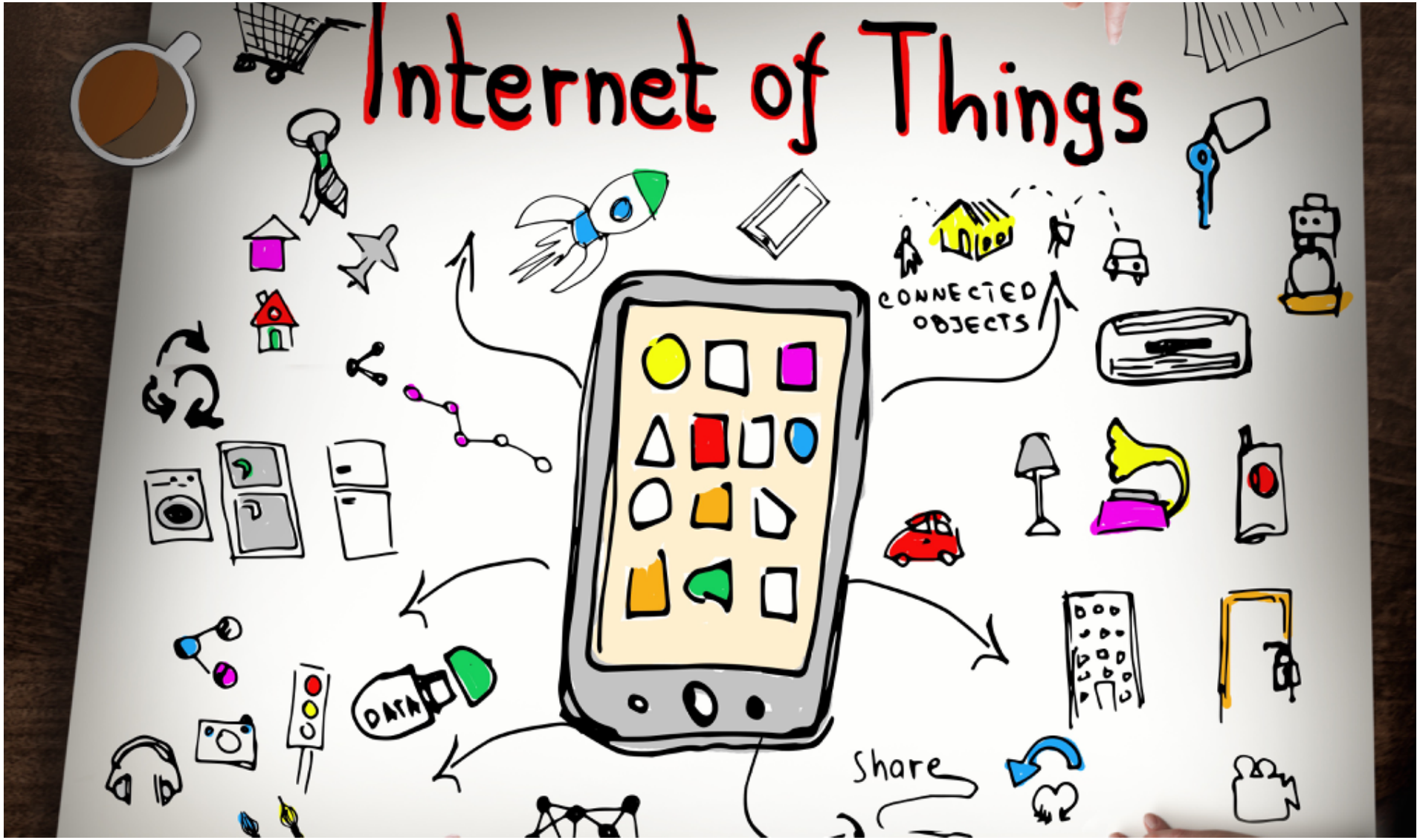


IoT Protocols

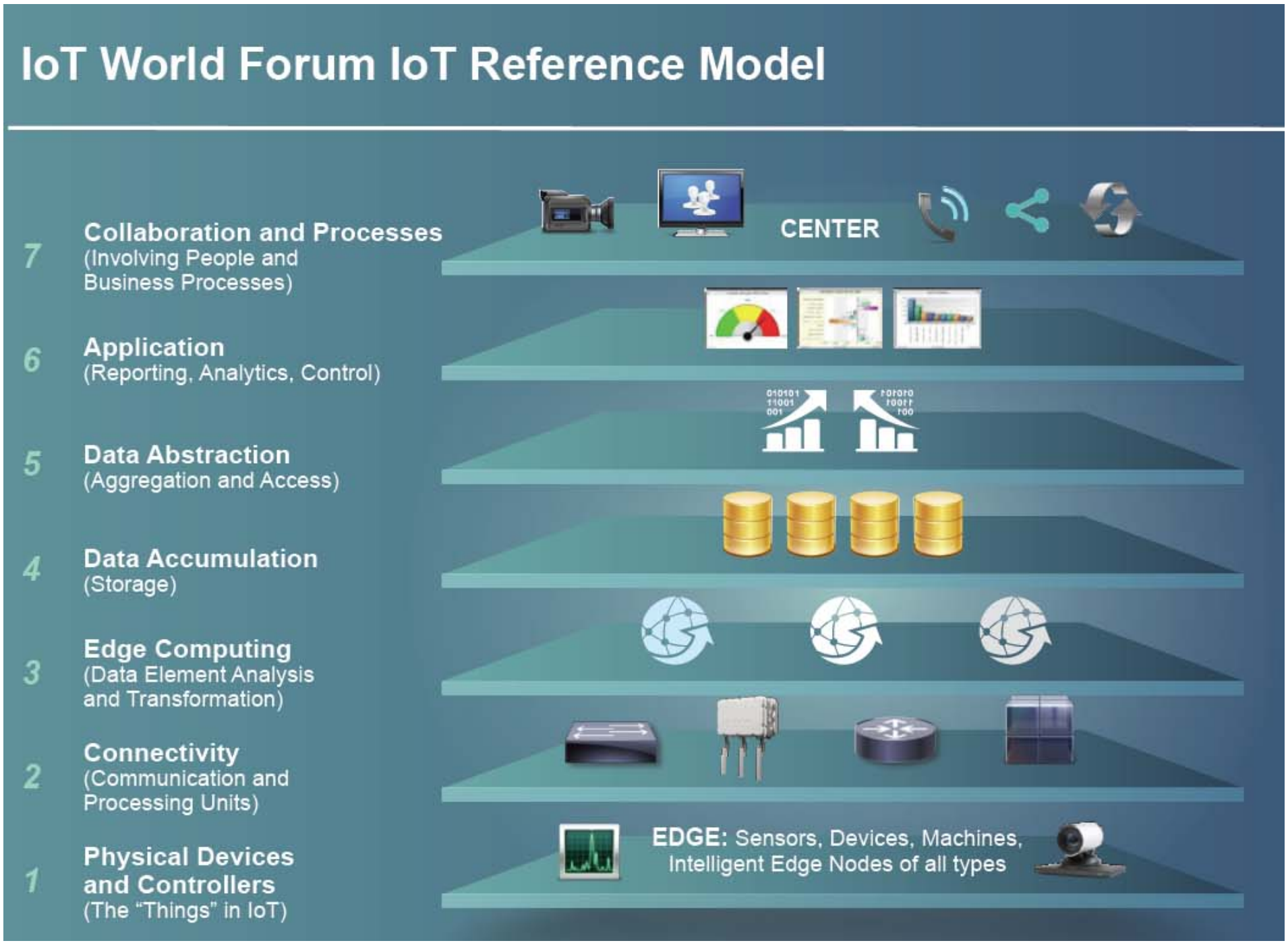
18-738 Sports Technology

Priya Narasimhan
ECE Department
Carnegie Mellon University
@yinzcampriya

Overview of Lecture

- Bluetooth
- Protocol basics
- Architecture
- Piconets, scatternets
- Service discovery

IoT World Forum IoT Reference Model



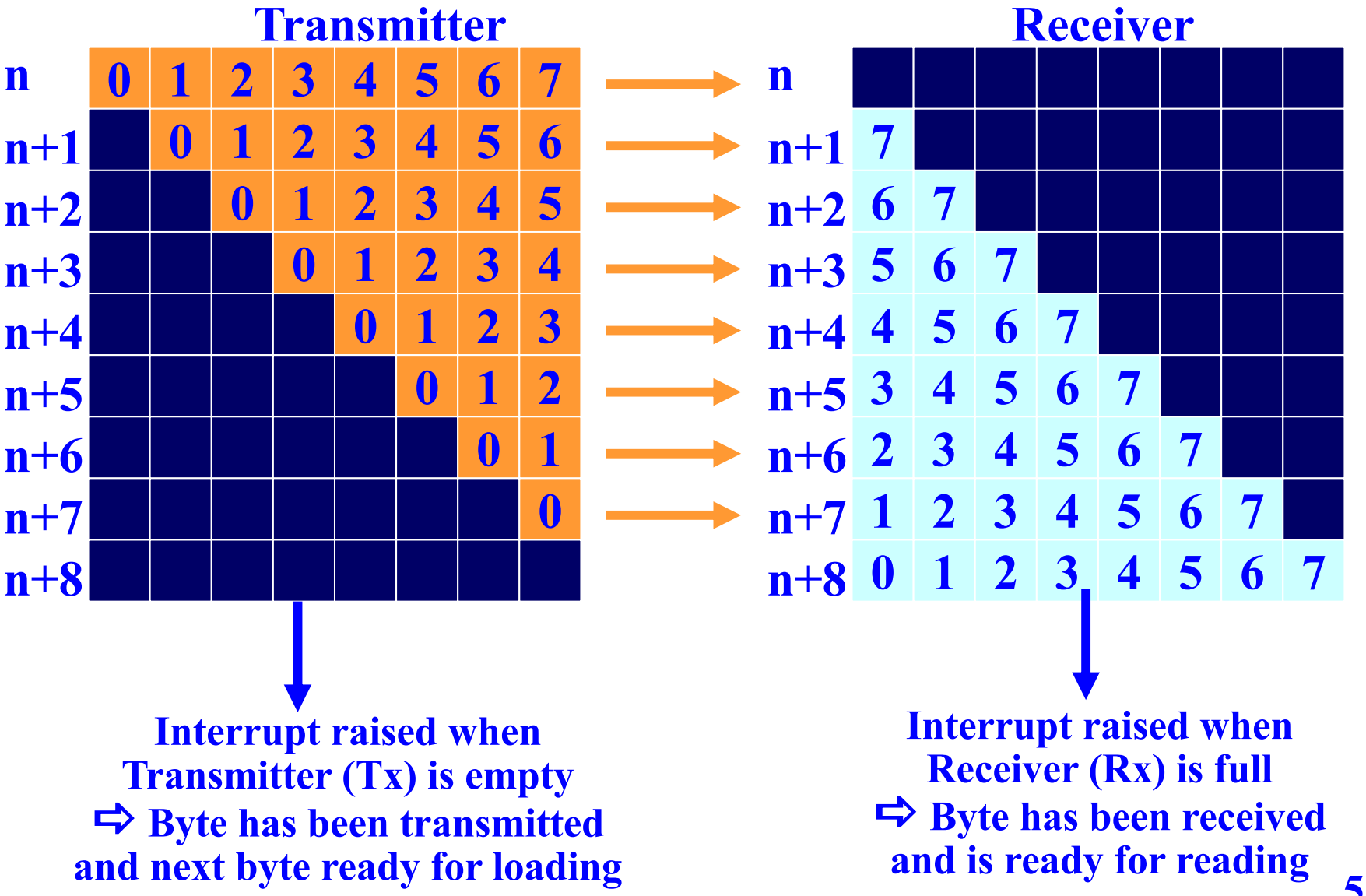
Why Serial Communication?

- Serial communication is a **pin-efficient** way of sending and receiving bits of data one pin, one bit, at a time.
  - Sends and receives data one bit at a time over one wire
  - While it takes eight times as long to transfer each byte of data this way, only a few wires are required
  - Typically one to send, one to receive, and a common signal ground wire

    Data rate rely on clock frequency and # of bits being transmitted.

- **Simplistic** way to visualize serial port
  - Two 8-bit shift registers connected together
  - Output of one shift register (transmitter) connected to the input of the other shift register (receiver)
  - Common clock so that as a bit exits the transmitting shift register, the bit enters the receiving shift register
  - Data rate depends on clock frequency and number of bits transmitted

Simplistic View of Serial Port Operation



Protecting Against Data Loss

- How can data be lost?
  - If the transmitter starts to send the next byte before the receiver has had a chance to process/read the current byte
  - If the next byte is loaded at the transmitter end before the current byte has been completely transmitted

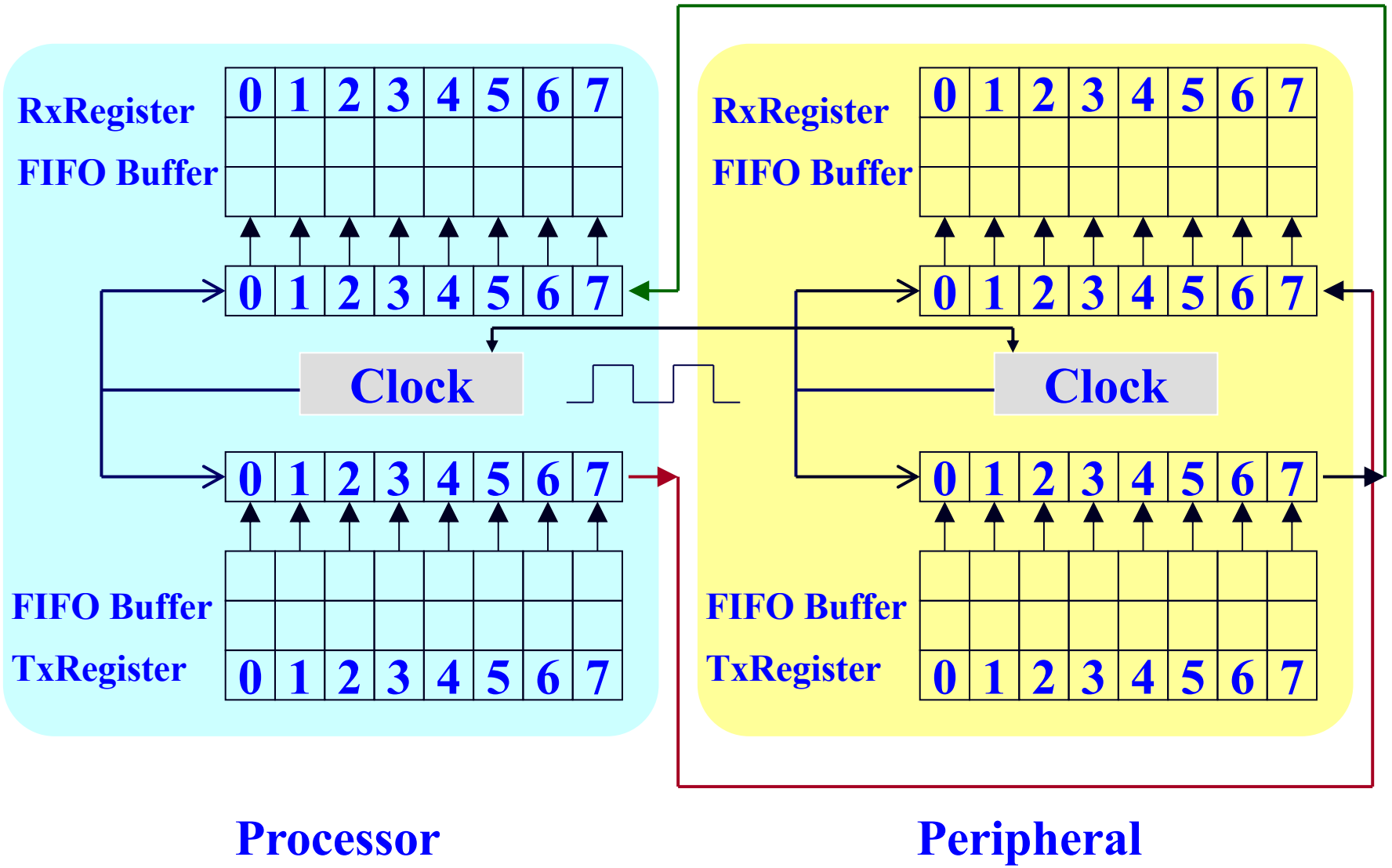
FIFO buffer prevents data losses.

- Most serial ports use FIFO buffers so that data is not lost
  - Buffering of received bytes at receiver end for later processing
  - Buffering of loaded bytes at transmitter end for later transmission
  - Shift registers free to transmit and receive data without worrying about data loss

- Why does the size of the FIFO buffers matter?

Serial Port

Make sure that TX and RX has common clock.



What is RS-232?

One-to-one, interference is rare.

- So far, we've talked about clocks being synchronized and using the clock as a reference for data transmission

  Clock need to be same clock.

  - Fine for short distances (e.g., within chips on the same board)

  Just like IR, even if there's a full room of receiver, it will only go to one.

- When data is transmitted over longer distances (off-chip), voltage levels can be affected by cable capacitance

  the pulse might be attenuated.

  - A logic "1" might appear as an indeterminate voltage at the receiver
  - Wrong data might be accepted when clock edges become skewed

- Enter RS232: Recommended Standard number 232
  - Serial ports for longer distances, typically, between PC and peripheral
  - Data transmitted asynchronously, i.e., no reference clock
  - Data provides its own reference clock

The data tells you how to digest the data.

1. Clock
2. Flow control

Synchronous = With Clock signal
Asynchronous = Without clock signal.

Types of Serial Communications

- Synchronous communication
  - All transmitted bits are synchronized to a common clock signal
  - The two devices initially synchronize themselves to each other, and then continually send characters to stay synchronized
  - Even when actual data is not really being sent, a constant flow of bits allows each device to know where the other is at any given time
    - Each bit that is sent is either actual data or an idle character
  - Faster data transfer rates than asynchronous methods, because it does not require additional bits to mark the beginning and end of each data byte
- Asynchronous communication
  - Each device uses its own internal clock resulting in bytes that are transferred at arbitrary times
  - Instead of using time as a way to synchronize the bits, the data format is used
  - Data transmission is synchronized using the start bit of the word, while one or more stop bits indicate the end of the word
    - Asynchronous communications slightly slower than synchronous
    - However, processor does not have to deal with the additional idle character

The asynchronous communication works by start and stop word.
Same as in human world: "hello.. I will start speaking now..."
"goodbye..." as in the end character.

Here's an Analogy

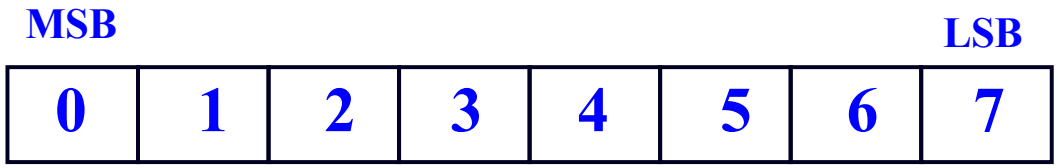
- With asynchronous communication
  - You would need to stop after every word to make sure the listener understood your meaning, and knew that you were about to speak the next word.
- With synchronous communication
  - You would establish with your listener that you were speaking English, that you will be speaking words at measured intervals, and that you would utter a complete sentence/paragraph, before pausing to confirm
  - You would establish with your listener beforehand that any extraneous noises (coughing) should be ignored.

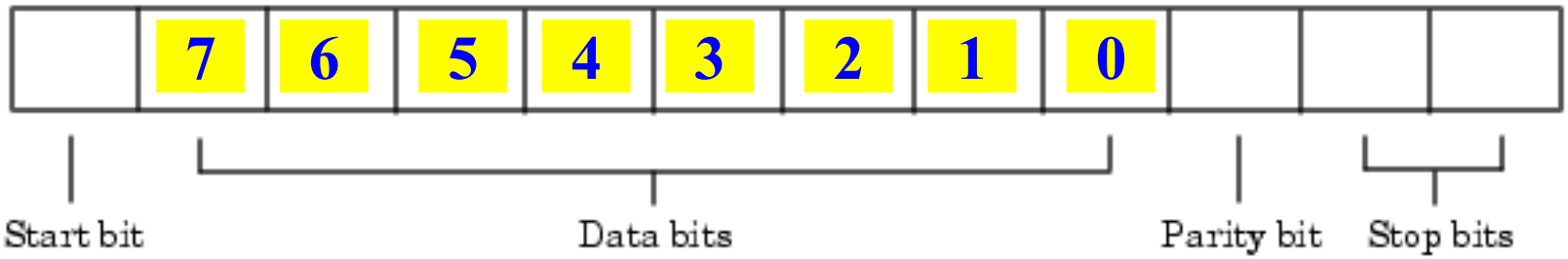
- Which is faster?
- Synchronous can be faster, even though initializing communication may take slightly longer

Synchronious is typicall faster because after the initialization, the flow control, start and stop word. It can also be slower, maybe it is always just syncing idle words.

Bits and Serial Bytes

- Serial ports on IBM-style PCs support asynchronous communication only
- A "serial byte" usually consists of
  - *Characters:* 5-8 data bits
  - *Framing bits:* 1 start bit, 1 parity bit (optional), 1-2 stop bits
  - When serial data is stored on your computer, framing bits are removed, and this looks like a real 8-bit byte





- Specified as number of data bits - parity type - number of stop bits
  - 8-N-1 : eight data bits, no parity bit, and one stop bit
  - 7-E-2 : seven data bits, even parity, and two stop bits

Parity Bits

- Simple error checking for the transmitted data
- Even parity 00110011-0 1^1^1^1 = 0 -> even
  - The data bits plus the parity bit produce an even number of 1s
- Odd parity 00110011-1 1^1^1^1^1 = 1 -> odd
  - The data bits plus the parity bit produce an odd number of 1s

- Parity checking process
  1. The transmitting device sets the parity bit to 0 or to 1 depending on the data bit values and the type of parity checking selected.
  2. The receiving device checks if the parity bit is consistent with the transmitted data; depending on the result, error/success is returned

- Disadvantage
  - Parity checking can detect only **an odd number of bit-flip errors**
  - Multiple-bit errors can appear as valid data

    If there are two or four or eight ... bits flipped, single parity check cannot tell which one has gone wrong.

Data Modulation

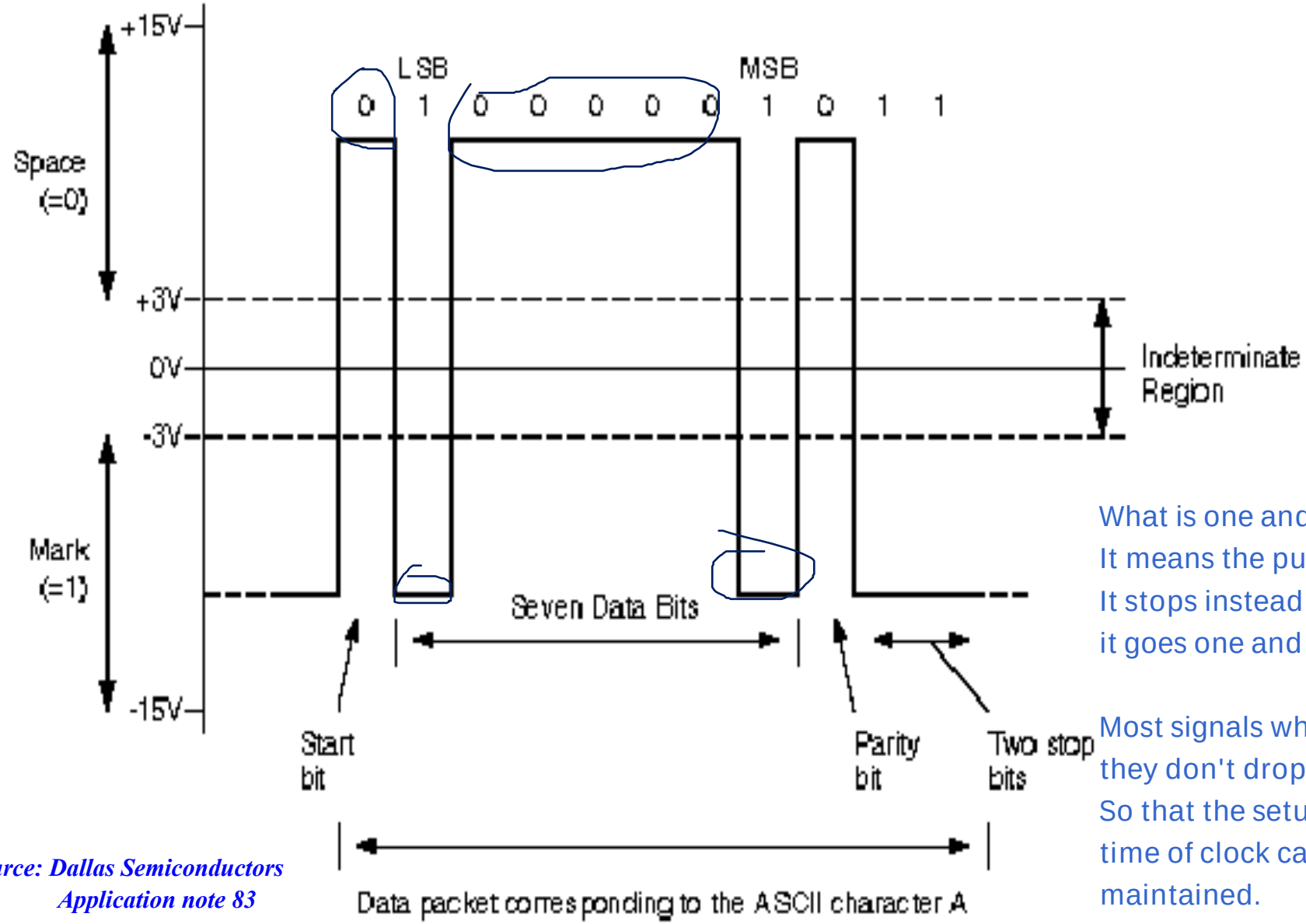
- When sending data over serial lines, logic signals are converted into a form the physical media (wires) can support

- RS232C uses bipolar pulses
  - Any signal greater than +3 volts is considered a space (0)
  - Any signal less than 3 volts is considered a mark (1)

    RS232 voltage is inverted. >3V = 0

    <3V = 1 -> RS232 voltage level is inverted from traditional TTL.
- Conventions
  - Idle line is assumed to be in high (1) state
  - Each character begins with a zero (0) bit, followed by 5-8 data bits and then 1, 11/2, or 2 closing stop bits
  - Bits are usually encoded using ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange)

RS-232 Signal Levels



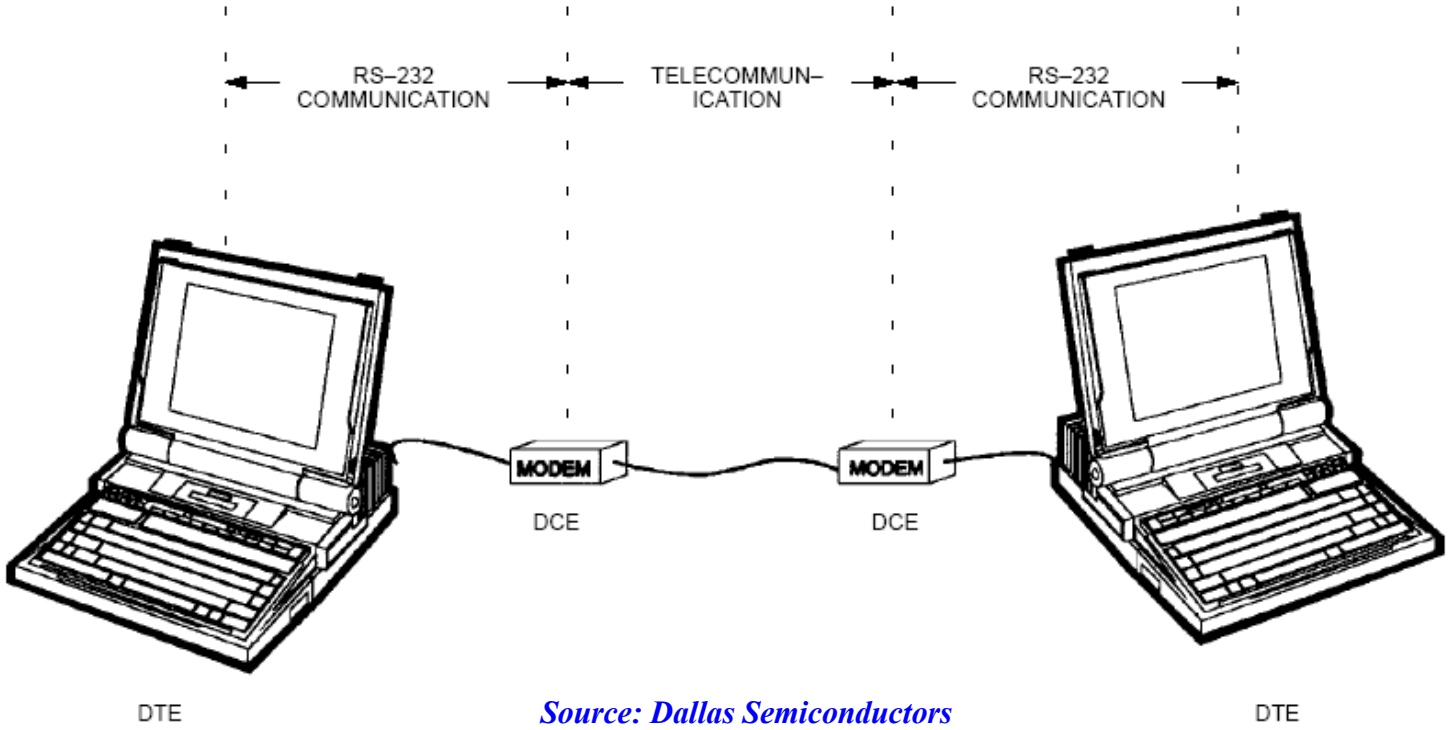
Source: Dallas Semiconductors Application note 83

What is one and half bits?
It means the pulse width.
It stops instead of one bits,
it goes one and half.

Most signals when they drop they don't drop abructly.
So that the setup and hold time of clock can be maintained.

Terminology

- DTE: Data terminal equipment, e.g., PC
- DCE: Data communication equipment, e.g., modem, remote device
- Baud Rate
  - Maximum number of times per second that a line changes state
  - Not always the same as bits per second



Source: Dallas Semiconductors Application note 83

Serial Port Connector

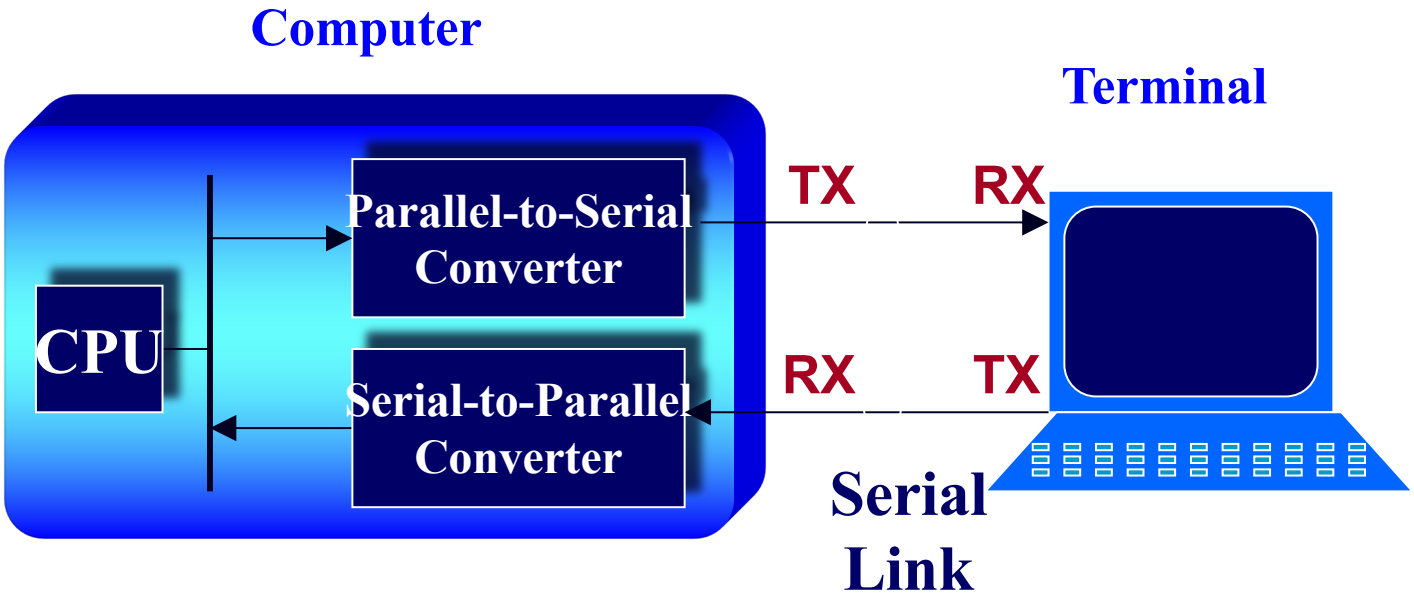
- 9-pin (DB-9) or 25-pin (DB-25) connector

  Hardware Flow Control

- Inside a 9-pin connector
  - **Carrier Detect** - Determines if the DCE is connected to a working phone line
  - **Receive Data** - Computer receives information sent from the DCE
  - **Transmit Data** - Computer sends information to the DCE
  - **Data Terminal Ready** - Computer tells the DCE that it is ready to talk
  - **Signal Ground** - Pin is grounded
  - **Data Set Ready** - DCE tells the computer that it is ready to talk
  - **Request To Send** - Computer asks the DCE if it can send information
  - **Clear To Send** - DCE tells the computer that it can send information
  - **Ring Indicator** – Asserted when a connected modem has detected an incoming call

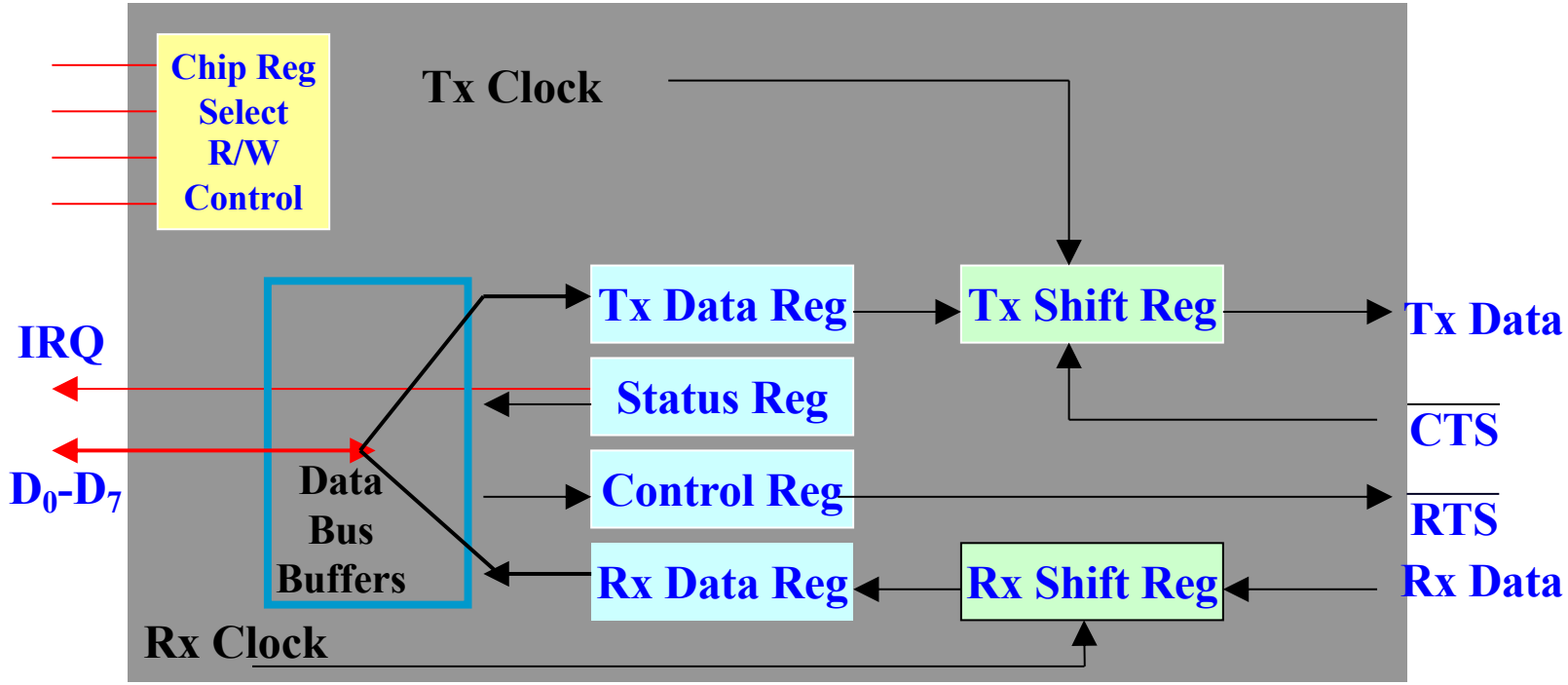
Data Communication

- Communications between computer and monitor over serial line
  - Data is converted from parallel (bytes) to serial (bits) in the bus interface
  - Bits are sent over wire (TX) to terminal (or back from terminal to computer)
  - Receiving end (RX) translates bit stream back into parallel data (bytes)



Interfacing Serial Data to Microprocessor

- Processor has parallel buses for data need to convert serial data to parallel (and vice versa)
- Standard way is with UART
- UART Universal asynchronous receiver and transmitter



Flow Control

- Necessary to prevent terminal from sending more data than the peripheral can consume (and vice-versa)
  - Higher data rates can result in missing characters (data-overrun errors)

- Hardware handshaking — Assert a line to say "stop"
  - Hardware in UART detects a potential overrun and asserts a handshake line to prevent the other side from transmitting
  - When receiving side can take more data, it releases the handshake line

- Software flow-control
  - Special characters XON and XOFF
  - XOFF stops a data transfer (control-S or ASCII code 13)
  - XON restarts the data transfer (control-Q or ASCII code 11)

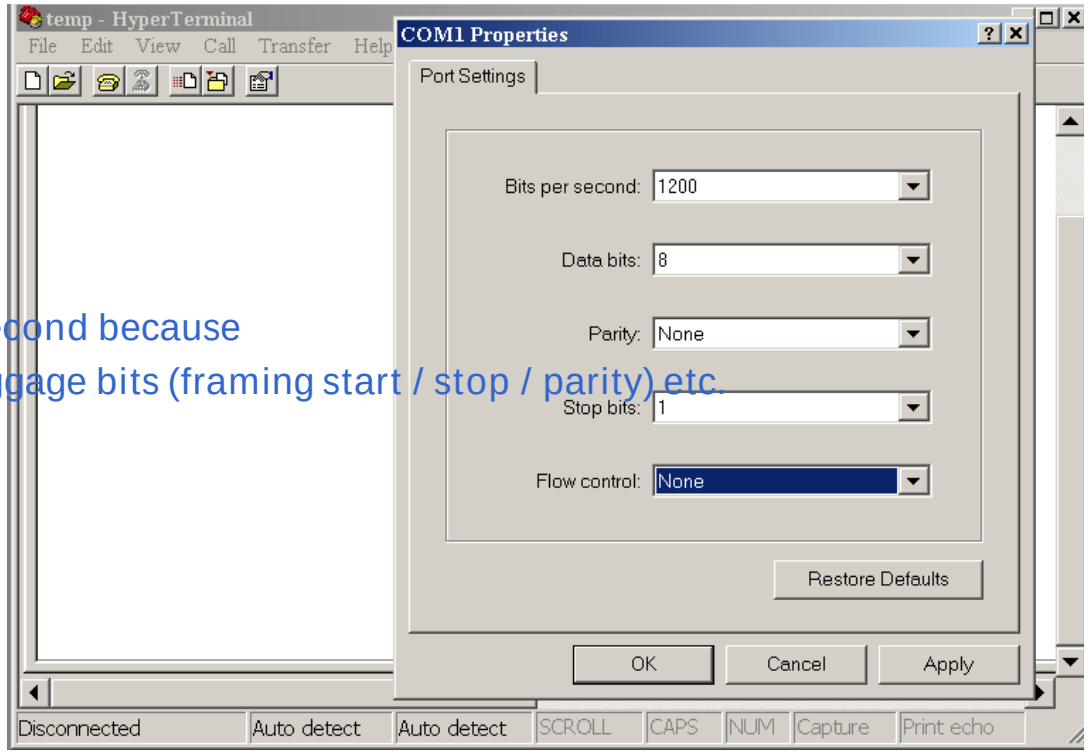
- Assumption is made that the flow-control becomes effective before data loss happens

HyperTerminal

- A (hyper) terminal program is an application that will enable a PC to communicate directly with a serial port
  - Can be used to display data received at the PC's serial port

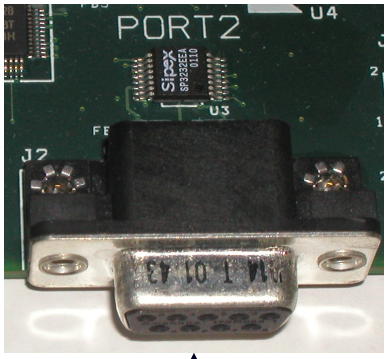
- Can be used to configure the serial port
  - Baud rate Baud rate = number of time the wire change rate.
  - Number of Data bits
  - Number of parity bits
  - Number of stop bits
  - Flow control

The number of time it change state.
Baud rate = bits per second. Not real bits per second because
not only we have data bit, we also have the baggage bits (framing start / stop / parity) etc.
bit rate = useful bites.



Example: When You Press a Key

- Pressed key generates a specific ASCII code which represents the character being pressed
- Code converted to a bit pattern for transmission via the serial port
- Converted bit pattern encapsulates start bits, stop bits, parity, etc.
- Bit pattern is sent down the serial line by a UART at a specific baud rate



Serial vs. Parallel

- Serial ports
  - Universal Asynchronous Receiver/Transmitter (UART): controller
  - Takes the computer bus' parallel data and serializes it
  - Transfer rate of 115 Kbps
  - Example usage: Modems
- Parallel ports
  - Sends/receives the 8 bits in parallel over 8 different wires
  - 50-100 KBps (standard), upto 2 MBps (enhanced)
  - Example usage: Printers, Zip drives

02-24-2022 Lecture Ends Here

Bluetooth: Why the Name?

- Harald Blaatand (910-986 AD) was a Danish Viking king in late 10th century
  - "Blaatand" = Bluetooth
- United Denmark and part of Norway into a single kingdom
- Introduced Christianity into Denmark
- Left behind a large monument, the Jelling rune stone, in memory of his parents
- Why the name "Bluetooth"?
  - Indicates how important this standard is to Nordic industries (companies in Denmark, Sweden, Norway and Finland) are to the communications industry)
  - Aimed at the unification of computing and telecom industries

Introduction

- Intended as a replacement for short-range cables
- Essentially, replacement for RS-232 cables
- 30,000 companies belong to the Bluetooth Special Interest Group (SIG)
- Developed a standard or a set of specifications
- Some implementation details left open to the developer—a manufacturer must meet Bluetooth SIG standards to market something as a Bluetooth device
- IEEE standardized it as IEEE 802.15.1 (but does not maintain it)

Bluetooth opens doors to a new generation of "connectionless" devices

On 6 December 2016, Bluetooth took a massive leap forward to deliver advanced beacon and location-based capabilities in home, enterprise and industrial environments. Bluetooth 5 quadruples the range, doubles the speed, and boosts broadcast messaging capacity by 800%—the key to enabling robust, reliable Internet of Things (IoT) connections that make full-home and building and outdoor use cases a reality.

Bluetooth Everywhere (Source: Bluetooth SIG)

As a trusted standard for wireless connectivity, *Bluetooth*® is integrated into more than 8.2 billion products produced by over 30,000 Bluetooth SIG members. Discover how Bluetooth is helping to transform the way people and devices connect across a variety of markets.

Automotive

Consumer Electronics

Home Automation

Medical & Health

Mobile Phones & Smart Phones

PC & Peripherals

Wearables

Sports & Fitness

Retail & Location-based Services

Relevant Detour: Let's talk Infrared (IR)

- Also a replacement for short-range cables
- Using light waves of a lower frequency than the human eye can interpret
- Inexpensive as well, but a couple of drawbacks
- Line-of-sight technology, e.g., point the remote-control at the TV to operate it
- One-to-one technology—only send data between two devices at a time
- However, interference between devices is rare
- Message only goes to the intended recipient (the one-to-one nature of the tech), even in a room full of IR receivers

- Bluetooth—also inexpensive, also replacement for short-range cables—but addresses the limitations of IR systems

Introduction

- [1994] Ericsson started to look at alternatives to connect their mobile phones to accessories
  - Cable replacement that could connect devices such as mobile phone handsets, headsets and portable computers
  - Looked at option of using radio – not directional, no line of sight, many-to-one
- [1998] Original Bluetooth SIG: Ericsson, Intel, IBM, Toshiba, Nokia
- [1999] Version 1.0 of an open, global specification that defines a complete protocol, from the underlying physical (radio) layer to the application level
  - Bluetooth 1.0 has a maximum transfer speed of 1 megabit/s (Mbps)
  - Bluetooth 2.0 can handle up to 3 Mbps (and is backward-compatible with 1.0 devices)

- Standardized wireless communications between electrical devices in proximity
  - Location independent – devices do not need to know each other's specific locations
  - Low-cost, low-power, short-range radio technology
- Notion of a Personal Area Network (PAN) – a close-range wireless network
- Protocol usually implemented partly in hardware and partly as software

Speeds

- Bluetooth 1.0 has a maximum transfer speed of 1 megabit/s (Mbps)
- Bluetooth 2.0 can handle up to 3 Mbps (and is backward-compatible with 1.0 devices)
- Bluetooth 3.0 can handle up to 25 Mbps
- Bluetooth 4.0 can handle up to 25 Mbps
- Bluetooth 5.0 can handle up to 50 Mbps

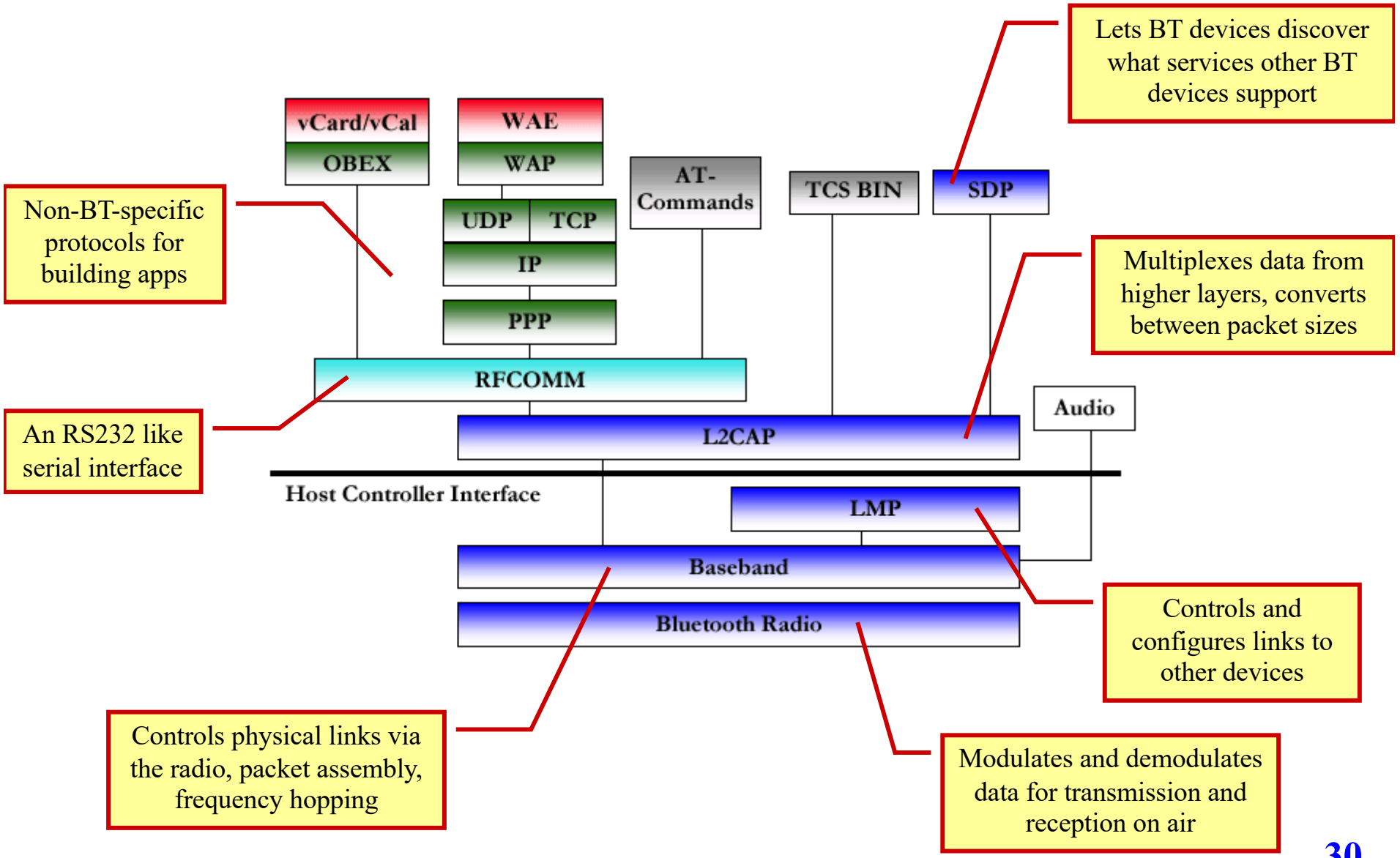
- The Bluetooth Core Specification specifies minimum range of 10m (33 ft), but there is no upper limit on actual range

Some Implicit Requirements

- Bluetooth envisioned as a cable-replacement technology – this imposes some requirements

- Cost
  - Can't be more expensive than a cable
- Battery-operated
  - Target market was mobile devices
  - Must be low power
  - Must be able to run on low voltages
  - Must be lightweight and compact enough not to intrude on the design of mobile devices
- Ease of use
  - Must be as simple as (if not simpler than) plugging in a cable
  - Must be as reliable as a cable, must cope with errors (resilience)
  - Must not be captive to a vendor

Bluetooth Protocol Stack

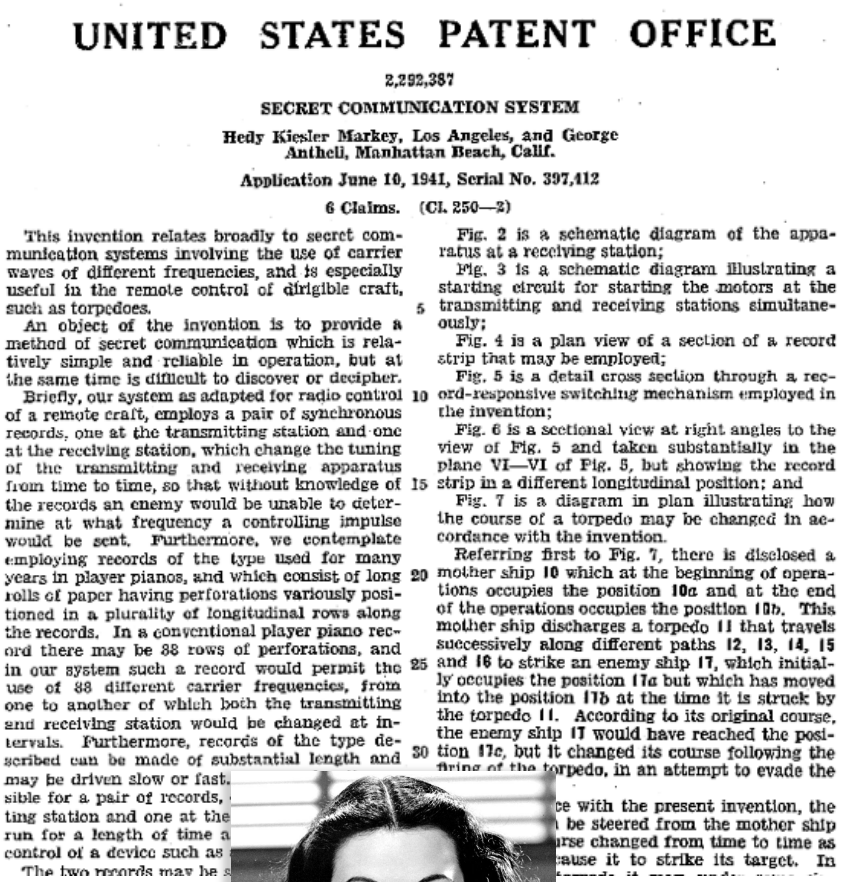


Physical Radio Layer

- Bluetooth devices operate in the globally available, unlicensed ISM band situated at 2.4 GHz
  - General use by Industrial, Scientific and Medical (ISM) applications
  - Has restrictions in some countries – Bluetooth SIG is lobbying to harmonize these regulations
- ISM band
  - Occupied by a variety of other RF emitters
  - Car security, cordless headphones, baby monitors, garage-door openers, random-noise generators (microwave ovens, sodium vapor street lamps)
- The 2.4 GHz is not a terribly stable or reliable medium
  - But its worldwide availability ensures widespread acceptance of Bluetooth
  - Coping with interference becomes a huge issue
- To cope with the hostile environment, Bluetooth employs special means
  - Frequency hopping, adaptive power control, short data packets
- Three different power ranges
  - Provide transmission ranges of 10m (lowest power), 20m or 100m

Hedy Lamarr and Frequency Hopping

- Lamarr worked on a jam-proof radio guidance for torpedoes during the World War
- Lamarr and Antheil worked on a frequency-hopping spread-spectrum technology
  - Continually change the radio signals sent to the torpedo
  - Underlies Wi-Fi, CDMA and Bluetooth
- Posthumously inducted into the National Inventors Hall of Fame



UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.

An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

Briefly, our system as adapted for radio control of a remote craft, employs a pair of synchronous records, one at the transmitting station and one at the receiving station, which change the tuning of the transmitting and receiving apparatus from time to time, so that without knowledge of the records an enemy would be unable to determine at what frequency a controlling impulse would be sent. Furthermore, we contemplate employing records of the type used for many years in player pianos, and which consist of long rolls of paper having perforations variously positioned in a plurality of longitudinal rows along the records. In a conventional player piano record there may be 88 rows of perforations, and in our system such a record would permit the use of 88 different carrier frequencies, from one to another of which both the transmitting and receiving station would be changed at intervals. Furthermore, records of the type described can be made of substantial length and may be driven slow or fast. sible for a pair of records, ting station and one at the run for a length of time a control of a device such as

The two records may be s

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the transmitting and receiving stations simultaneously;

Fig. 4 is a plan view of a section of a record strip that may be employed;

Fig. 5 is a detail cross section through a record-responsive switching mechanism employed in the invention;

Fig. 6 is a sectional view at right angles to the view of Fig. 5 and taken substantially in the plane VI—VI of Fig. 5, but showing the record strip in a different longitudinal position; and

Fig. 7 is a diagram in plan illustrating how the course of a torpedo may be changed in accordance with the invention.

Referring first to Fig. 7, there is disclosed a mother ship 10 which at the beginning of operations occupies the position 10a and at the end of the operations occupies the position 10b. This mother ship discharges a torpedo 11 that travels successively along different paths 12, 13, 14, 15 and 16 to strike an enemy ship 17, which initially occupies the position 17a but which has moved into the position 17b at the time it is struck by the torpedo 11. According to its original course, the enemy ship 17 would have reached the position 17c, but it changed its course following the firing of the torpedo, in an attempt to evade the

ce with the present invention, the be steered from the mother ship rse changed from time to time as ause it to strike its target. In

Frequency Hopping

- The operating band, 2.4 GHz ISM, band is 2400 - 2483.5 MHz
- The 79 RF channels are ordered from channel number 0-78 and are spaced 1 MHz apart, starting at 2402 MHz
  - Each channel signals data at 1 Megasymbol per second
- GFSK (Gaussian Frequency Shift Keying) modulation
  - Binary 1 gives rise to a positive frequency deviation from the nominal carrier frequency
  - Binary 0 gives rise to a negative frequency deviation
  - Effective on-air data rate is 1Mb/s
- After each packet, both devices return their radio to a different frequency, effectively hopping from one radio channel to another
  - FHSS: frequency hopping spread spectrum
- Why?
  - Bluetooth devices will end up using the whole of the available ISM band
  - If a transmission is compromised by interference on one channel, the retransmission will occur on a different (hopefully clear) channel
- Each Bluetooth time-slot is 625 microseconds – devices hop once per packet (which can be 1, 3 or 5 time slots)

Master-Slave Organization

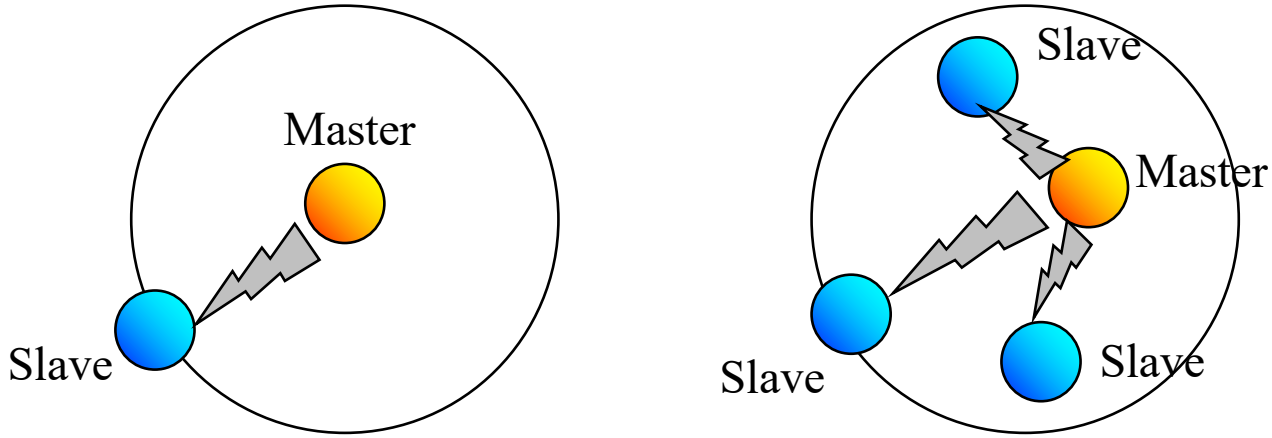
- If devices are to hop to new frequencies after each packet, they must all agree on the sequence of frequencies that they will use
- BT devices can operate in two modes: Master or Slave
- All devices share the Master's clock
- The Master sets the frequency-hopping sequence
- The Slave synchronizes to the Master in time and frequency by following the Master's hopping sequence
- Every BT device has a unique BT device address and a BT clock
- The devices can switch roles, by agreement, and the Slave device can become the Master device
  - For example, a headset initiating a connection to a phone necessarily begins as a Master device—as initiator of the connection—but may subsequently operate as a Slave device
- Being a Master of 7 Slaves is possible; being a Slave of more than one Master is possible

Master Controls Multiple Things

- Frequency-hopping: When Slaves connect to a Master, they are told the BT device address and clock of the Master
  - The frequency-hop sequence can be calculated from this BT device address and a BT clock
  - Because all Slaves use the Master's clock and address, they are all synchronized to the Master's frequency-hop sequence
- Transmission: The Master also controls when devices are allowed to transmit
  - Master allows Slaves to transmit by allocating slots for voice/data traffic
  - In data-traffic slots, Slaves can transmit only when responding to a transmission sent to them by the Master
  - In voice-traffic slots, Slaves are required to transmit regularly in reserved slots whether or not they are responding to the Master
- Bandwidth: Master controls how total bandwidth is divided up amongst the Slaves
  - By deciding when and how often to communicate with each Slave
  - Time Division Multiplexing (TDM)
  - How many slots each Slave gets depends on its data-transfer needs

Piconet

- Another term for a Bluetooth Personal Area Network (PAN)
- A collection of Slave devices operating together with one common Master
- All devices on a piconet follow the Master's frequency hopping & timing
- Slaves in a piconet only have links to the Master
- There are no direct links between the Slaves in a piconet
- Specification mandates a maximum of 7 Slaves in a piconet – why 7?
- Typical range of a piconet is 10m, but can be more with higher power
- Larger coverage can be hand by linking piconets into a scatternet

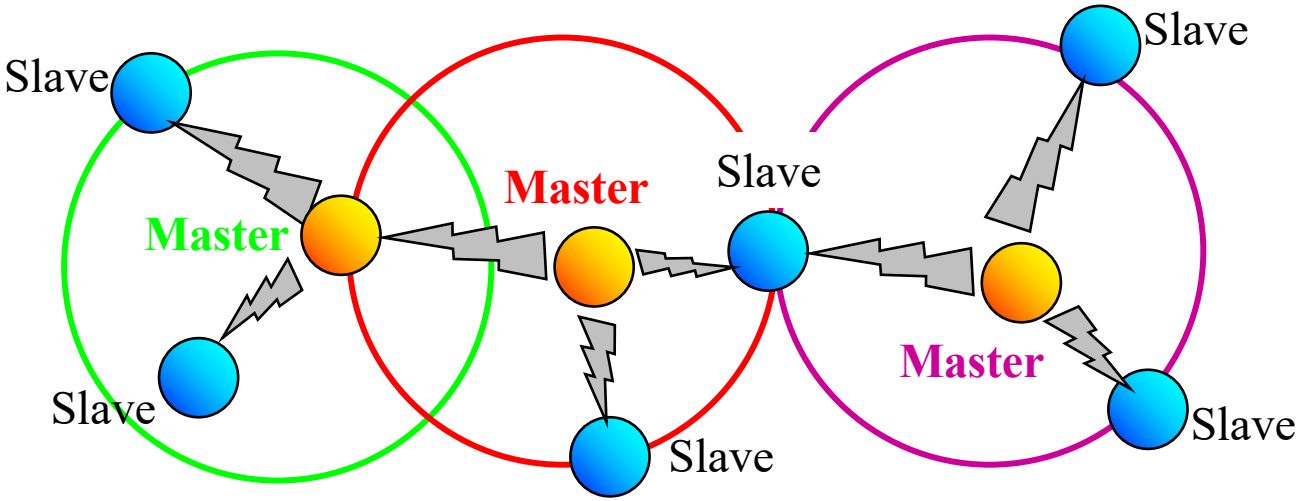


Side-Story

- The BlueSniper rifle from Flexilis can scan and attack Bluetooth devices (called BlueSnarfing) from more than a mile away
- The first version of the gun showed up at Defcon 2004
- John Hering, from Flexilis: *"The parts are easily available for a few hundred dollars and you can make this gun in a long afternoon."*

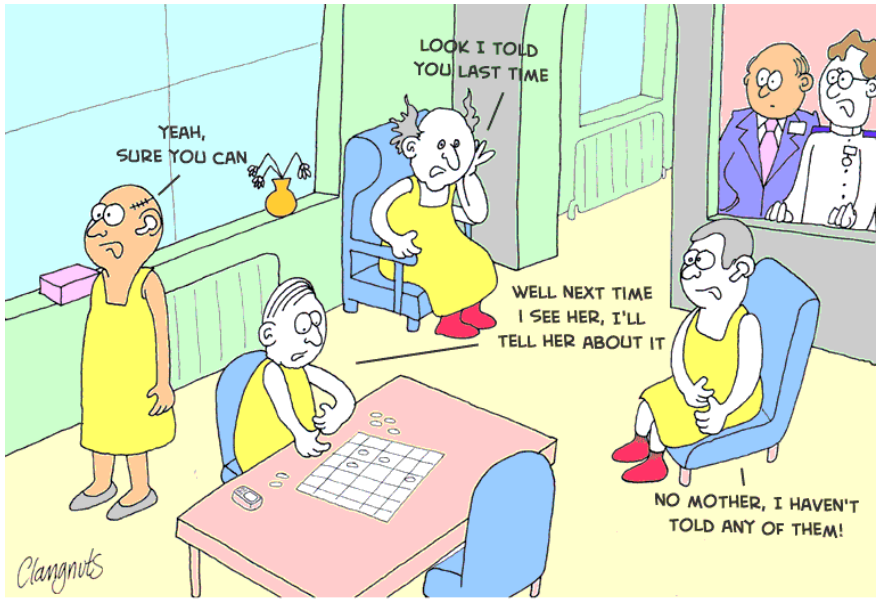
Scatternet

- Some devices are members of more than one piconet
- When a device belongs to more than one piconet, it must time share
  - Spends few slots on one piconet, and then a few other slots on the other piconet
- Slave in one piconet can be a Master in the other
- Slave in one piconet can be a Slave in the other as well (Slave has two Masters, one in each piconet)
- What is not possible?
  - To have a device that is a Master of two different piconets since all Slaves in a piconet are synchronized to the Master



Piconet

- Slaves in a piconet are synchronized to avoid interference with each other
  - But, other unsynchronized piconets in the area might randomly collide on the same frequency
  - If there is a collision on a particular channel, those packets will be lost and will need to be retransmitted
  - The more piconets in an area, the more retranmissions that will occur, causing data rates to fall (can also happen in a scatternet)



"SINCE THEY ALL GOT BLUETOOTH, IT'S HARD TO TELL WHO'S HEARING VOICES!"

Radio Power Classes

- Three types of radio power classes
  - Class 1: 100mW (range 100m)
  - Class 2: 2.5mW (range 20m)
  - Class 3: 1mW (range 10m)
- Most manufacturers produce Class 3 devices
  - Ideal range is 10m
  - Because human bodies, furniture, etc. absorb waves, practical range is ~5m
- Also a minimum range for Bluetooth devices
  - If radios are too close together, the receiver saturates
  - Minimum range for a BT radio link is 10cm
- Possible to create piconets with a mixture of high and low power devices at different operating ranges (e.g., Class 1 Master can have a Class 3 Slave, but the range is now dictated by the lower-class device)

Communication

- Supports data and voice traffic

- Asynchronous Connectionless (ACL) links
  - Data communication
  - Packet: 72-bit access code, 54-bit packet header, 16-bit CRC + payload
  - Largest packet size (DH5 packet) can carry 339 bytes (2712 bits) of payload and needs 142 bytes of overhead (72+54+16 bits)
  - DH5 packet takes 5 time-slots to send and a minimum of 1 time-slot for reply
  - **Effective** max data rate in one direction = (2712 bits)/ (6 time-slots * 625 μs/slot) = 723.2 kb/s
  - Using more packets for reply reduces this effective data rate
  - Higher layers can add more protocol overhead, so max data rate might drop

- Synchronous Connection Oriented (SCO) links
  - Voice communication
  - Work at 64 kb/s
  - Possible to have three full-duplex links at once (to mix voice and data)
  - Audio quality not really sufficient for delivery of music, for good enough for modern cellular phone system
  - Perhaps use ACL for audio delivery using compression

Error Correction

- Cyclic Redundancy Check (CRC)
  - Performed on all packet headers and on payload data
  - CRC will flag any errors in the data
  - 16-bit CRC over the payload header + payload data
- ARQ (Automatic Repeat Request)
  - For data or voice packets
  - Error detection through CRC at receiver
  - Receiver discards packets in error
  - Receiver returns a positive ACK for received error-free packets
  - Receiver returns a NACK to packets in error; sender retransmits such packets
  - Retransmission occurs after a time-out
- Whitening or Bit Randomisation
  - Mixing a pseudo random bit sequence with the data bitstream to randomize the data
  - Greatly reduces the possibility of long sequences of 0s or 1s (basically, DC bias)
  - Avoids offsets that might build up
  - Avoids problems that might cause certain radio architectures to drift off channel

Forward Error Correction (FEC)

- By adding extra parity bits created from the input data
- Can detect (and sometimes correct) bit errors

- Three FEC options decided based on packet type: non, 1/3 and 2/3

- **1/3 FEC** – strongest
  - For high quality voice packets
  - Transmits 3 copies of each bit
  - Decoded at the receiver through a majority function
- **2/3 FEC**
  - For data or voice packets
  - Packet header uses 1/3 FEC since it is the most critical part
  - Uses Hamming code
    - For every 10 bits, 15 bits are generated to allow detection of 2 bit errors in the 10-bit input and correct 1 bit error in the 10-bit input
    - Input needs to be padded to ensure multiple of 10

Bluetooth Profiles

- Bluetooth specification includes a profiles document
- Describes how a particular application can be implemented using BT
- Specifies which parts of the core BT protocol should be used for these applications

- Version 1.0 provides profiles for connecting
  - Mobile cellphone to public switched telephone network (PSTN) through an access point
  - Mobile cellphone to a notebook PC
  - Mobile cellphone to a headset
  - LAN access points for laptops or palmtops
  - Notebook, palmtop or other Internet access device to the Internet via a PSTN access point or access modeul
  - Laptops and palmtops

Example Bluetooth Profiles

- Bluetooth profiles save time in communicating parameters when the profiles are interpreted
- A2DP (Advanced Audio Distribution Profile)
  - Streaming music
- HID (Human Interface Device Profile)
  - Bluetooth-enabled mice and keyboards
- BIP (Basic Imaging Profile)
  - Send photos and images to Bluetooth-enabled printers, picture frames, etc.
- GATT (Generic Attribute Profile)
  - Build your own Bluetooth-enabled thing!

Device Discovery

- Suppose I have two Bluetooth devices
  - Cellphone capable of acting as a modem using a BT dialup networking profile
  - Laptop running an application that needs a BT dialup networking connection
- Cellphone will periodically scan to see if anyone needs to use it

- Laptop will perform an inquiry to look for any BT devices nearby
  - Through a series of inquiry packets
- Cellphone responds (eventually) with a Frequency Hop Synchronization (FHS) packet
  - Contains all the info that the laptop needs to connect to the cellphone
  - Plus, the device class – the fact that this is a phone and specifically, a cellphone
- Every other Bluetooth-enabled device nearby will also respond with an FHS packet – laptop accumulates a list of all nearby devices
- Laptop can now
  - Present the user with this list, allowing the user to decide what to do next
    - User will only know about the devices, but not their services
  - Take the next step of discovering which of these devices support the dialup networking profile that is needed

Service Discovery – I

- To find out whether a device supports a specific service, the Service Discovery Protocol (SDP) needs to be used
- Laptop pages the cellphone, using the information gathered during inquiry
- If the cellphone is scanning for pages, it responds
  - An ACL baseband connection can be set up to transfer data between the two devices
- Once ACL connection is set up, an L2CAP connection can be established
  - Used whenever data has to be transferred between Bluetooth devices
  - Allows many protocols and services to piggyback onto one ACL link
    - Protocol and Service Multiplexor (PSM) embedded in every L2CAP packet to distinguish the specific protocol/service using the ACL link
    - Different PSMs for different protocols or services
  - PSM=0x0001 ⇨ service discovery protocol is using the ACL link

Service Discovery – II

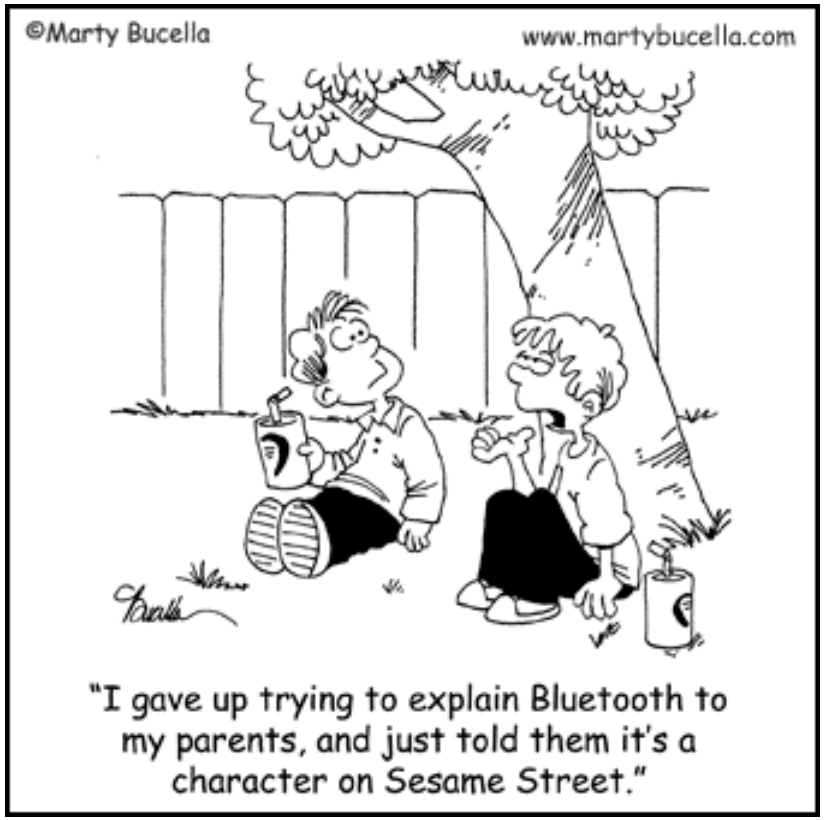
- Laptop uses L2CAP channel to connect to the service discovery *server* on the cellphone
  - Laptop runs a service discovery *client*
  - Client asks the server to send any and all information related to a dialup networking profile
  - Server looks through its database and returns attributes related to dialup networking
- Laptop receives this information
  - Can decide to tear down connection to the cell phone
  - Particularly the case if there are many devices in the area – no sense in waiting with open connections while collecting service information
- At the end of this service discovery phase
  - It's up to the application what to do – can let the application decide for itself or can involve the user in deciding which device to select

Connecting to a Service

- Same initial process as establishing an ACL connection
- Except the connection might have specific quality-of-service requirements this time
  - Basically, a link configuration phase
- Now, an L2CAP connection on top of the ACL connection
  - Dialup networking uses RFCOMM, an RS-232 emulation layer
  - PSM=0x0003 ⇨ RFCOMM is using the ACL link
- RFCOMM can also multiplex several protocols or services, each with its own channel number
  - Knows which channel number to use from the service discovery information
- Finally, the Dialup Networking (DUN) connection is set up over the RFCOMM connection and the laptop can use the dialup networking services of the cellphone
- If cellphone goes out of the laptop's range, the laptop will need to repeat the entire process and find another device
- Important
  - Both ends of the connection have to be willing to connect
  - Some devices might be set up not to scan for inquiries
  - Others might be set up to not be discoverable – effectively, these are invisible

Bluetooth Limitations

- Does not address routing, most network functions are pushed into the link layer
- Does not support multi-hop multicasting
- Does not necessarily cope with mobility
- The Master node is often the bottleneck
- The number of nodes in a piconet is limited to 8
- Does not incorporate or exploit power-saving methods done at upper layers, above the link-layer

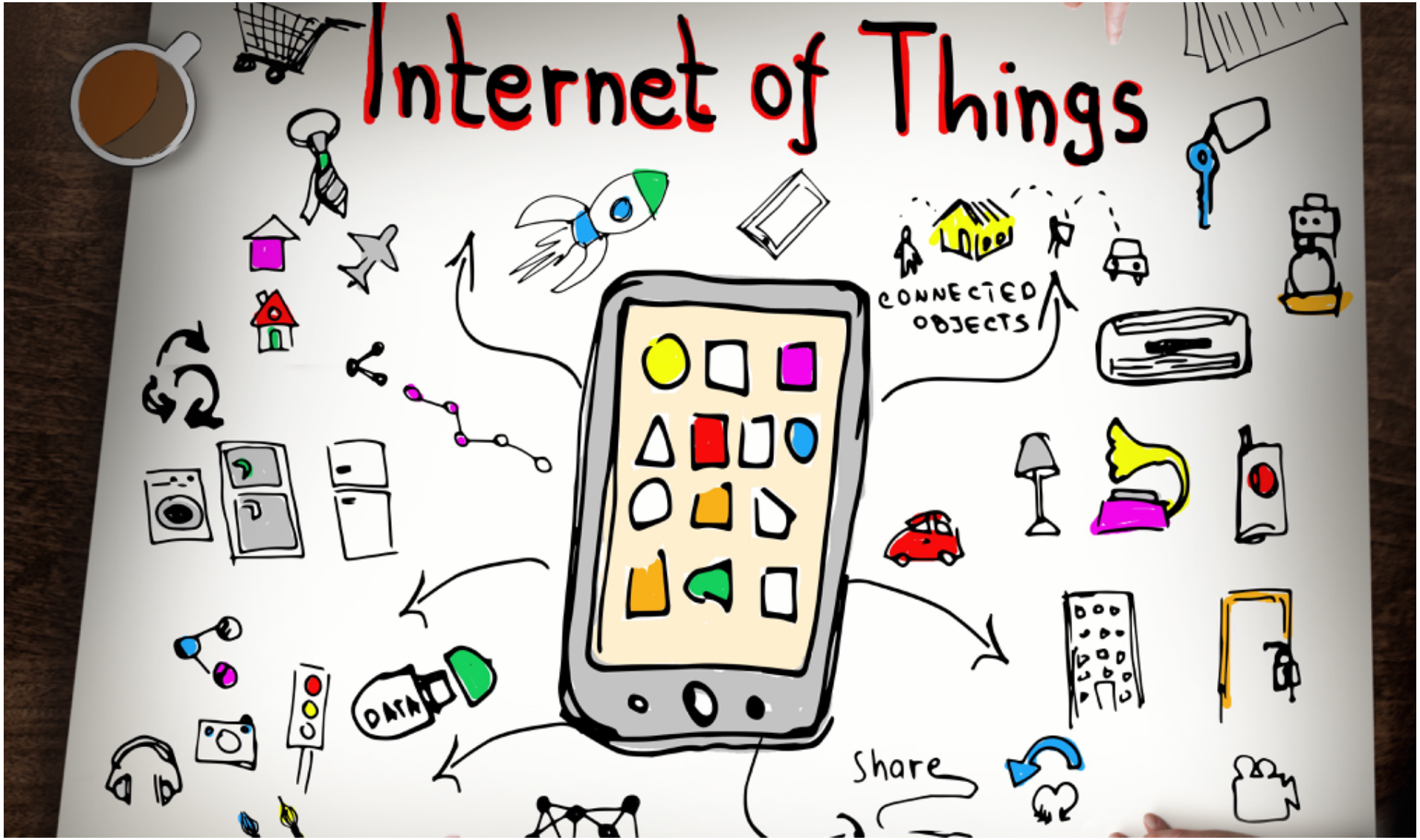


Zigbee vs. Bluetooth

- Two different technologies with very different areas of application and different means of designing for those applications
  - ZigBee (IEEE 802.15.4) is focused on control and automation
  - Bluetooth is focused on connectivity between laptops, PDA's, and the like, as well as more general cable replacement
- ZigBee uses low data rate, low power consumption, and works with small-packet devices
- Bluetooth uses a higher data rate, higher power consumption, and works with large-packet devices
- ZigBee networks can support a larger number of devices and a longer range between devices than Bluetooth
- Bluetooth must rely on fairly frequent battery recharging, while the whole goal of ZigBee is for a user to be able to put a small number of batteries in the devices and forget about recharging for months to years
- In timing-critical applications, ZigBee is designed to respond quickly, while Bluetooth takes much longer and could be detrimental to the application

Zigbee vs. Bluetooth

Characteristic	ZigBee	Bluetooth
Range		
As designed	10–100 metres	10 metres
Special kit or outdoors	up to 400 metres	100+ metres dep. on radio
Data rate	20-250 Kbps	1 Mbps
Network Latency (typical)		
New slave enumeration	30ms	20s
Sleeping slave changing to active	15ms	3s
Active slave channel access	15ms	2ms
Power profile	Years Optimizes slave power requirements	Days Maximises adhoc functionality
Security	128 bit AES and application layer user definable	64 bit, 128 bit
Operating Frequency	868 Mhz, 902-928 MHz, 2.4 GHz ISM	2.4 GHz ISM
Complexity	Simple	Complex
Network Topology	Adhoc, star, mesh hybrid	Adhoc piconets
Number of devices per network	2 to 65,000	8
Scalability/Extendability	Very High/Yes	Low/No
Flexibility	Very High	Medium, profile dependent
Resilience and reliability	Very High	Medium



IoT Protocols

18-738 Sports Technology

Priya Narasimhan
ECE Department
Carnegie Mellon University
@yinzcampriya