Bluetooth & Zigbee

Some slides obtained from COMP327 Mobile computing

Personal Area Network

- Network for communicating between devices close to one's person
  - Range is typically a few meters
  - Wireless technologies now becoming ubiquitous:
    - IrDA - Infrared communication (less so these days)
    - Bluetooth Piconets
- Desirable requirements
  - "Plugging in" (automatic connection due to proximity)
  - Selective lock-out (prevent interference or unauthorised data access)

Bluetooth

- An open wireless protocol for exchanging data
- Development initiated in 1989 by Dr Nils Rydbeck, CTO at Ericsson Mobile
- Operates at frequencies in the globally unlicensed (but not unregulated) Industrial, Scientific and Medical (ISM) 2GHz short-range RF band.
  - Short range (1-100m) depending on class and power
  - Frequency hopping spread spectrum
    - Data is chopped up and transmitted as chunks over 79 separate frequencies.

Bluetooth

- Designed as a "cable replacement" technology
- Packet-based protocol with a master-slave structure
  - Establishes piconet, with one master and up to 7 slaves
  - Devices can switch roles by agreement
    - e.g. headphones initiating connection to a phone starts out as the master, but may switch to become a slave
  - Scatternets form when two or more piconets share members
    - Certain devices simultaneously the master in one piconet and a slave in another.

Bluetooth

- Dynamic discovery and connection mechanism
  - Security mechanisms employed through pairing
    - Uses the Service Discovery Protocol (SDP)
    - Devices can be in discoverable mode
      - Transmits name, class, list of services and technical information
    - Pairing is then performed using a link key (i.e. a shared code)
      - If stored by both devices, then they are bonded
    - Once paired, devices in range can be recognised and dynamically connected
  - Various security vulnerabilities have been identified
    - Bluejacking involves sending unsolicited messages to a device
    - Bluecasting is a variant, used for proximity marketing
      - e.g. Proxama

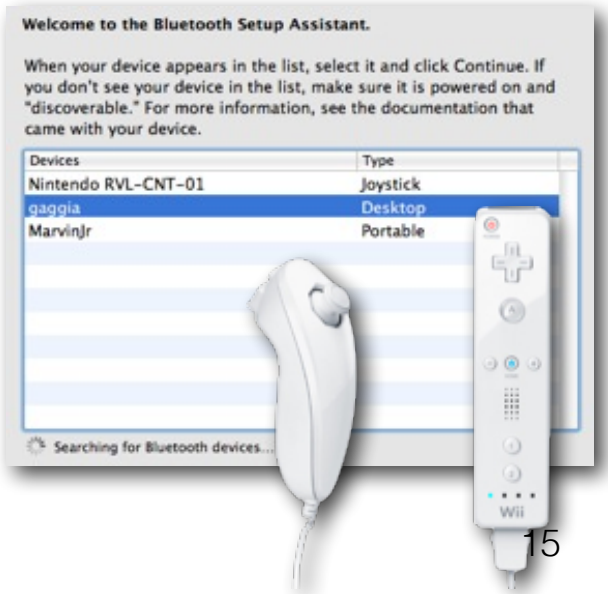
Proxama

Bluejacking and Bluecasting

- Bluejacking
  - Involves sending unsolicited messages via the OBEX protocol.
  - Sending a vCard with a message in the name field.
  - Usually harmless, but "victims" may not know what's happening to their device and may think it is malfunctioning
  - Not seen so much on Smartphones these days of SnapChat etc. (but still "a thing" in 2011).
- Bluecasting
  - A proximity marketing tool
  - Involves sending small digital media using OBEX protocol.
  - Doesn't have to be adverts - photos, audio, video etc.
  - Usually from a bluetooth kiosk.
  - Users can accept or reject content pushed to them.
- In both cases, proximity is key (Bluetooth is short range!)

Bluetooth Profiles

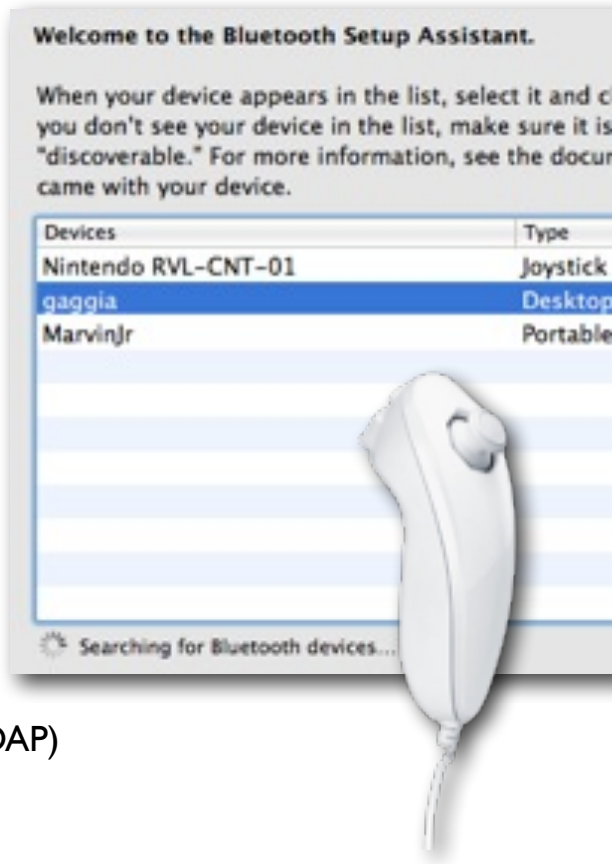
- Each profile corresponds to a class of devices, and defines:
  - Dependencies on other profiles
  - Suggested user interface formats
  - Parts of the Bluetooth stack used by the profile
- Several Major Device Classes, each with subclasses:
  - Computer: Desktops, Laptops, PDAs
  - Phone: Mobiles, Cordless, Payphones, Modems
  - LAN and Network Access Point
  - Audio: Headsets, Speakers and Stereos
  - Peripherals: Mouse, Joystick and Keyboards
  - Imaging: Printing, Scanner, Camera and Displays
  - +others!!



A good list of up-to-date profiles with further details can be found at: https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

Bluetooth Profiles

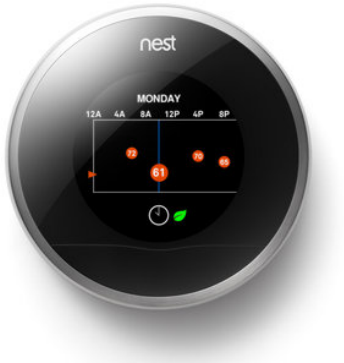
- Advanced Audio Distribution Profile (A2DP)
- Attribute Profile (ATT)
- Audio/Video Remote Control Profile (AVRCP)
- Basic Imaging Profile (BIP)
- Basic Printing Profile (BPP)
- Common ISDN Access Profile (CIP)
- Cordless Telephony Profile (CTP)
- Device ID Profile (DIP)
- Dial-up Networking Profile (DUN)
- Fax Profile (FAX)
- File Transfer Profile (FTP)
- Generic Audio/Video Distribution Profile (GAVDP)
- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Generic Object Exchange Profile (GOEP)
- Hard Copy Cable Replacement Profile (HCRP)
- Health Device Profile (HDP)
- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- Human Interface Device Profile (HID)
- Headset Profile (HSP)
- Intercom Profile (ICP)
- LAN Access Profile (LAP)
- Mesh Profile (MESH)
- Message Access Profile (MAP)
- OBject EXchange (OBEX)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP, PBA)
- Proximity Profile (PXP)
- Serial Port Profile (SPP)
- Service Discovery Application Profile (SDAP)
- SIM Access Profile (SAP, SIM, rSAP)
- Synchronization Profile (SYNCH)
- Synchronisation Mark-up Language Profile (SyncML)
- Video Distribution Profile (VDP)
- Wireless Application Protocol Bearer (WAPB)



A good list of up-to-date profiles with further details can be found at:
https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

Home and Health

- Entertainment:
  - Bluetooth is increasingly being used for
    - multi-player games
    - broadcasting music to speakers or headphones
- Lifestyle / Health:
  - Activity monitors allow users to track their lifestyle:
    - Jawbone's Up family of devices track activity, movement and sleep
  - Scales / Heart Rate / Blood Pressure monitors etc.



Bluetooth LE

- Aka Bluetooth v4
- Reduced Power version of Bluetooth, targeted at the health / well being / sport and fitness market:
  - Smaller size and lower cost
  - Low power requirement aimed at months or even years of use on a button (battery) cell
- Several new profiles:
  - Health Care
    - Health Thermometer Profile
    - Glucose Profile
    - Etc
  - Sports and Fitness
    - Heart Rate
    - Cycle Speed
    - Etc
  - Proximity Sensing
    - Find me profile
    - Proximity profile

Bluetooth LE - iBeacon

- iBeacon is a protocol developed by Apple
- Various vendors have made iBeacon BLE devices
- Closed, but Multi-platform
  - iOS iBeacon Monitoring API can wake up your app on your iPhone
- One type of data can be broadcast
  - iBeacon prefix + UUID + major & minor pair
- Battery life dependent on signal frequency
  - e.g. 1-3 months @ 100ms
  - 2-3 years @ 900ms

Works with Apple iBeacon

https://developer.apple.com/ibeacon/

Estimote Smart Beacons

https://www.youtube.com/watch?v=SrsHBjzt2E8

Estimote Sticker Beacons

https://www.youtube.com/watch?v=JrRS8qRYXCQ

Estimote Mirror

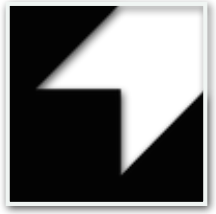
https://www.youtube.com/watch?v=FoVvPZRFd1I

Estimote Programming

```
let monitoringManager = ESTMonitoringManager()
monitoringManager.startMonitoringForIdentifier("7f6d1ab0", inProximity: .Near)

func monitoringManager(manager: ESTMonitoringManager,
                       didEnterRangeOfIdentifier identifier: String) {
    ESTRequestGetBeaconDetails(identifier: identifier).sendRequest { (details)
        if user.isFirstTimeIn(details.geoLocation) {
            showNotification("1st time in \(details.name)? Swipe here for our recommendations.")
        } else {
            showNotification("Welcome back to \(details.name)! Swipe here to learn what's new.")
        }
    }
}
```

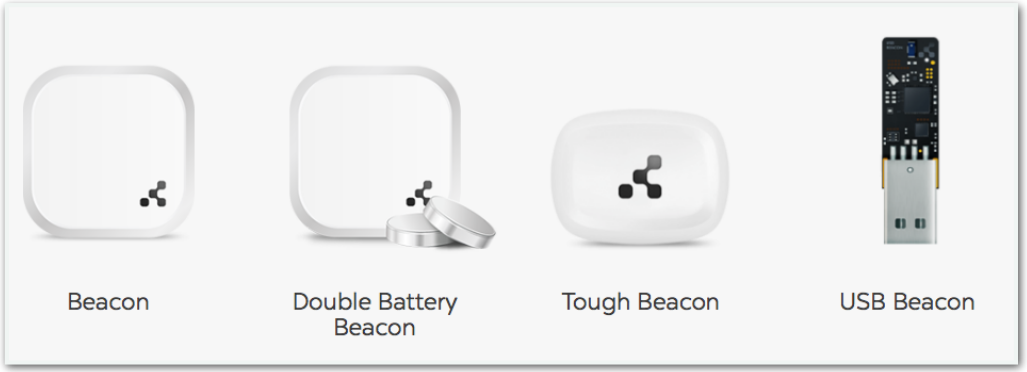
Bluetooth LE - Eddystone



- Eddystone is a format for a BLE beacon broadcast developed by Google
- Open and multi-platform (iOS & Android)
    - (better support on Android - on iOS no wake up + requires Chrome browser App installed)
- Specification published on the web:

  https://github.com/google/eddystone

- Three types of data can be broadcast
    - Eddystone-URL
    - Eddystone-UID
    - Eddystone-TLM

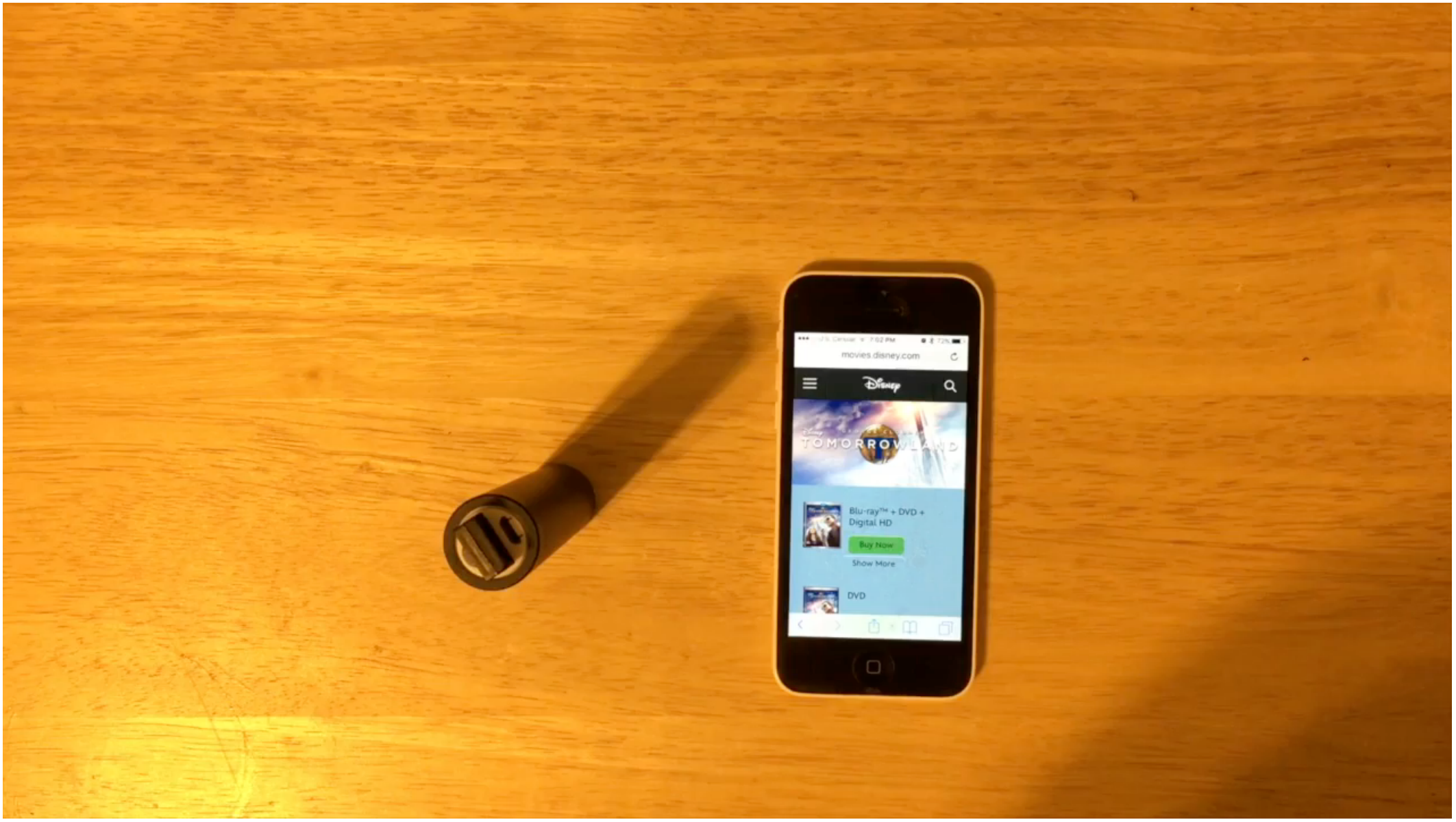


https://kontakt.io

Meet Eddystone

https://www.youtube.com/watch?v=jSDnf4In6QI

Setup Your Beacon to Broadcast Eddystone URL



https://www.youtube.com/watch?v=ntwRxCGO-Is

Case Study: Proxama

- The UK's largest independent network of Bluetooth beacons
- Specialise in transport based mobile proximity services, using beacons to engage users via mobile in moments of high dwell.
- Mobile technology platform, TapPoint, enables brands to interact more effectively with consumers across transport networks and high footfall destinations, such as shopping malls, stadiums and city centres and events.

https://proxama.com/

Proxama

Case Study: Proxama

- Partnered with Mapway in March 2016 to provide *contextually relevant mobile engagement* with consumers travelling on London buses and *experiencing times of high dwell.*
- Combined Mapway's Bus Time London App alongside it's network of iBeacons on buses.
- Allows brands to engage with users based on their physical context.
- Average London commuter spends £44 a week buying stuff during their commute.

https://proxama.com/

ZigBee

- Simple, low-cost Radio Frequency (RF) mesh network
- Intended to be simpler and less expensive than e.g. Bluetooth
  - Low data rate, but also low power
    - e.g. lifetime of 1-2 yrs on one battery
  - Three types of ZigBee device
    - ZigBee Coordinator (ZC): Root of network; maintains topology info
    - ZigBee Router (ZR): Can route data as well as act as an end device
    - ZigBee End Device (ZED): low power, low memory end node
- Low mobile phone adoption
  - Main adoption in embedded applications
    - Building and home automation, and embedded sensors
  - Some use in mobile payment systems and m-security
- More than 2,200 certified devices & 100's of millions of products deployed (as of Nov 2017)

ZigBee

- ZigBee protocols support two types of networks: beacon and non-beacon enabled.
- In non-beacon-enabled networks, ZigBee Routers typically have their receivers continuously active, requiring a more robust power supply.
    - allows for heterogeneous networks in which some devices receive continuously while others only transmit when an external stimulus is detected.
    - e.g. wireless light switch
        - ZigBee node at lamp may be set to constantly receive. How?
        - battery-powered light switch would remain asleep until the switch is thrown.
        - Switch wakes up, sends a command to the lamp, receives an acknowledgment, and returns to sleep.

ZigBee

- In beacon-enabled networks, special network nodes called ZigBee Routers transmit periodic beacons to confirm their presence to other network nodes.
    - Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life.
    - Beacon intervals depend on data rate
    - In general, ZigBee protocols minimize the time the radio is on, so as to reduce power use.
- In beaconing networks, nodes only need be active while a beacon is being transmitted.
- In non-beacon-enabled networks, power consumption is decidedly asymmetrical: Some devices are always active while others spend most of their time sleeping.

ZigBee
example

Zigbee Vibration Sensor

Vibration sensor is small enough to fit into just about anywhere. Place it with unsafe items such as medications and chemicals to protect them from young hands.

Power Supply: 3V, CR2016 battery (6 month battery life)
Distance: 150m open space
Work Temperature: -25~65° C
Size: 34*39*15mm & 15*46*15mm
Function: End Point
Firmware: Zigbee Pro, Home Automation, Intruder Alarm System (IAS)

ZigBee

example

ZigBee

- Many Zigbee devices are used in the Smart Home and Smart Energy domains.
- The devices themselves don't advertise that they use Zigbee technologies.
- Not a technology in the public eye (unlike Bluetooth)