COMP327
Mobile Computing

Lecture Set 3 - Personal Area Networks and Wireless Connections

In this Lecture Set

- Wireless Connection Technologies
  - Wireless Personal Area Networks (WPAN)
    - InfraRed
    - Bluetooth
    - Zigbee
  - Wireless Local Area Networks (WLAN)
    - WiFi & WiMAX
  - Sensors
    - RFID

Oranges are not the only fruit!

- Mobile Devices do more than just make calls
  - They interact with a number of local devices, forming a Personal Area Network (PAN)
    - Printers, Audio Equipment, Input Devices
  - They also connect to other non-telephony networks to get Internet Access, through Local Area Networks (LAN)
    - WiFi, or the 802.11 standards
  - They may also detect sensor nodes in the environment and act based on their discovery
    - Tagging

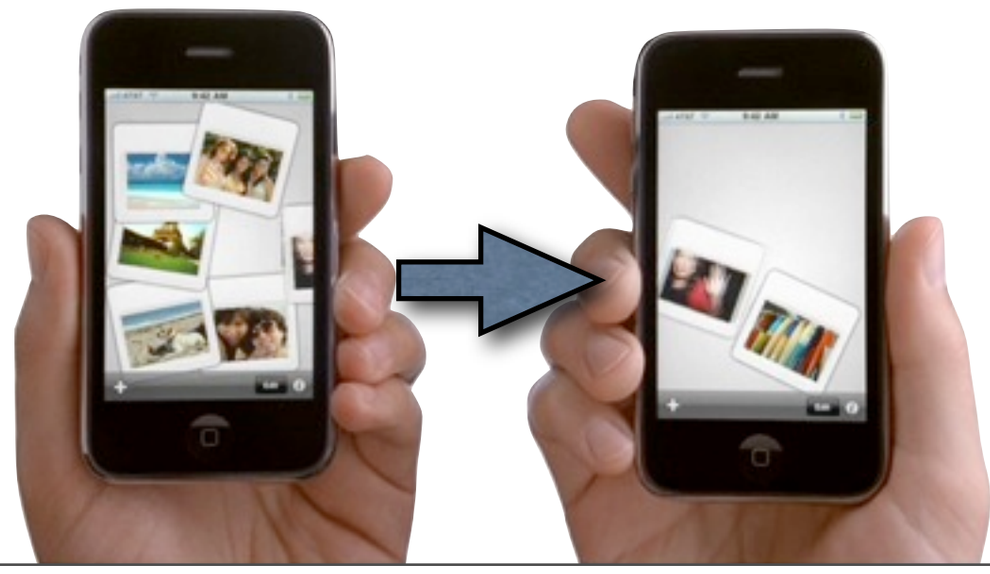
Master and Slave

- Mobile Phones can play both primary and secondary roles:
  - Primary Role
    - Other devices support the phone and its function
      - Output devices (e.g. Headsets, printers)
      - Input devices (e.g. keyboards, GPS devices, RFID tags)
  - Secondary Role
    - The phone acts as a comms device for another device
      - Modems (e.g. through tethering)
      - SMS transmitters/receivers (from a PC)

Peer relationships

- Mobile Phones can also have a peer-based relationship with other devices
  - Exchanging information
    - Typically with another user
      - Exchanging contact information, data, or multi-player games
  - Synchronising information
    - Typically with another device owned by the user
      - Address Books, Music, Images, Video
  - Receiving advertising
    - From wireless broadcast stations
      - Bluecasting!

To see three iPhone Apps that share data, see http://www.apple.com/iphone/gallery/ads/#share-large



The problem with wires

- Early mobile phone connectivity approaches used wired connections...
  - RS232, through bespoke connectors
  - USB and Firewire cables

- However, this can limit connectivity, and contradicts the mobile wireless ethos
- Various wireless approaches have emerged to facilitate connection between the phone and other user devices
  - Wireless PAN - Personal Area Network

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
    - Bluetooth Piconets
- Desirable requirements
  - "Plugging in" (automatic connection due to proximity)
  - Selective lock-out (prevent interference or unauthorised data access)

IrDA - Infrared Data Association

- Communicating data over infrared light
  - Short-range (< 1m), line of sight communication
    - Pair of LEDs focussed by a plastic lens into a narrow beam
    - Beam is modulated (switched on and off) to encode data
    - Filter is used to select rapid pulses and ignore ambient changes
    - Time Division Duplex Communication
      - Cannot transmit and receive simultaneously as receiver is blinded by the transmitter!
- Full stack exists supporting comms up to IrLAN
  - including IrSimpleShot for camera phones!
- Few security issues
  - no interference with other devices; works in "radio-noisy" environments

Bluetooth

- An open wireless protocol for exchanging data
  - 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.
- Designed as a “cable replacement” technology
  - Establishes piconet, with one master and up to 7 slaves
  - Scatternets form when two or more piconets share members
- Various specifications
  - Bluetooth 3.0 specification adopted in Apr 09
  - iPhone uses Bluetooth 2.0+EDR
    - EDR: Extended Data Rate of up to 3Mbit/s (x3 increase)

Bluetooth

- Dynamic discovery and connection mechanism
  - Security mechanisms employed through pairing
    - Uses the Service Discovery Profile (SDP)
    - Devices can be in discoverable mode
      - Transmits name, class, list of services and technical information
    - Paring is then performed using a link key (i.e. a shared code)
      - If stored by both devices, then they are bonded
    - Once pared, 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

Bluetooth Profiles

Minor Device Class for Audio/Video

Headset

Hands-free

Microphone

Loud-Speaker

Head Phones

Portable Audio

Car Audio

Set Top Box

HiFi Audio Device

VCR

Video Camera

Camcorder

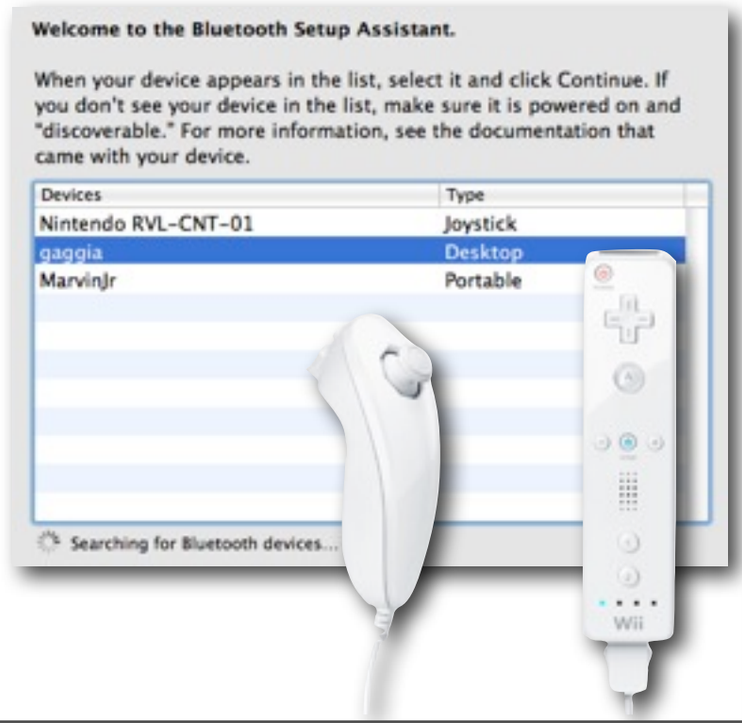
Video Monitor

Video Display and Loud Speaker

Video Conferencing

Gaming/Toy

- 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
  - Miscellaneous



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

ZigBee

- Simple, low-cost Radio Frequency (RF) mesh network
  - 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 to date
  - Main adoption in embedded applications
    - Building and home automation, and embedded sensors
  - Some use in mobile payment systems and m-security

Wireless Local Area Network (WLAN)

- Spread spectrum RF technology for data comms
  - Range typically in tens of meters
    - range of a network can be extended using several access points
  - Fast data rate
    - 802.11g provides 54Mbit/s
      - 802.11n increases this to 155Mbits/s using multiple antennas (MIMO)
    - Shared-key Encryption mechanisms include:
      - Wired Equivalent Privacy (WEP)
      - Wi-Fi Protected Access (WPA, WPA2)
- High adoption for home networks and HotSpots
  - Utilises unlicensed wavelengths

Wi-Fi Architectures

- Three typical architectures
  - Peer-to-peer
    - Two clients can communicate without the need for an access point
  - Bridge
    - Clients connect with Access point, which acts as a bridge / router to a wired ethernet
  - Wireless Distribution System
    - Multiple access points provide wider coverage without the need for wired backbone
      - Each access point is either a main, relay or remote base station
      - All nodes share same radio channel, and WEP or WPA keys

Wi-Fi Benefits

- **Convenience**
  - Provides network access from any location within range
    - Good as the number of home wi-fi gadgets increases
- **Mobility**
  - Users can browse outside home/work environment
    - Coffee Shops, Airports, Hotels
- **Productivity**
  - Employee can work from several locations without impediment
- **Deployment**
  - Initial setup requires single access point
- **Expandability**
  - Easy to add new clients without the need for additional infrastructure
  - WDS can be used to extend range
- **Cost**
  - Increase over a wired equivalent is modest

Wi-Fi Disadvantages

- **Security**
  - Poor antennas mean that signal propagate further than stated range
    - Can be intercepted by good antenna, and hence hacked
  - Encryption helps, but well known weaknesses exist in WEP
- **Range**
  - Suitable only for small areas
  - Metropolitan coverage can be costly
- **Reliability**
  - Signal quality affected by interference from devices on similar wavelengths
- **Speed**
  - Reasonably slow compared to wired connections
  - Faster than most wireless counterparts
- **Radio Emission**
  - Can affect nearby devices
  - Questionable affect on human health

WiFi vs UMTS

- WiFi is often perceived as better than UMTS...
  - Wifi is not always faster
    - *"WiFi hotspots offer up to 54Mbit/s but early UMTS R99 offers only 3Mbit/s"*
  - Wifi often limited by backhaul link to the Internet
    - DSL limits downlink speed to 1-8Mbit/s; uplink to < 1Mbit/s
    - UMTS has large coverage, with GPRS fallback
      - WiFi covers small area, limiting roaming ability
- UMTS has a well-established billing solution
  - Payment for commercial Wifi access is ad-hoc
    - Scratch cards, online Credit-card payment, or billing through subscription

WiFi vs UMTS

- Technical realisation of lawful interception
  - Well established for Telecommunications
  - Still evolving for Wifi access
- Wifi designed for small coverage
  - WDS can extend coverage, but with limitations
    - Handover problematic when roaming to a new area
  - UMTS designed for national coverage
    - Seamless roaming over long periods at high speed (<500km/h)
- Security
  - UMTS through SIM encryption & key management
  - Wifi exposes IP subnet, and key handling can be combersome

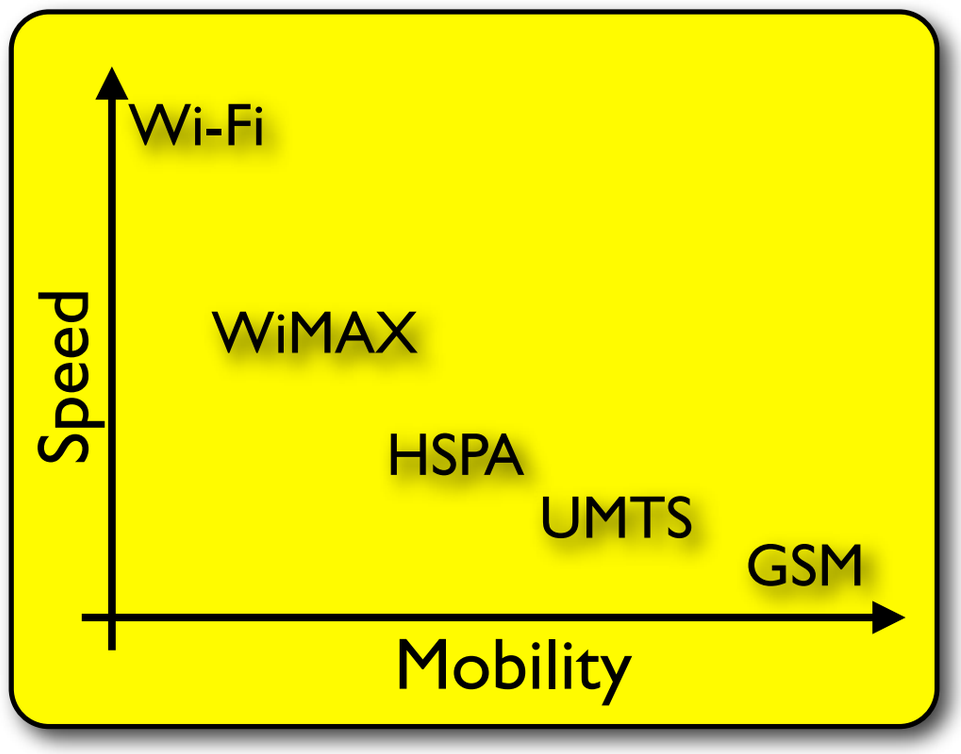
WiFi vs UMTS

- Telephony and VoIP
  - UMTS provides circuit switched links for voice
    - IMS architecture supports VoIP
  - VoIP clients exist over WLAN
    - Quality of Service can be poor; uplink speeds problematic

- Mobile Phones are increasingly appearing with both WiFi and UMTS capability
  - WiFi used when available, but fallback to UMTS (and GSM) when roaming

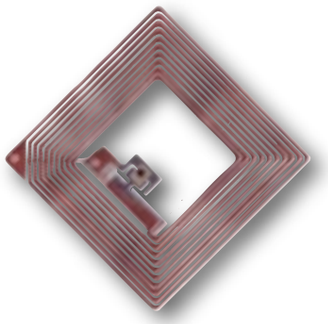
WiMAX (802.16e)
Worldwide Interoperability for Microwave Access

- Fast wireless broadband
  - Speeds "theoretically" faster than 70Mbit/s
  - Offers "last mile" access as alternative to DSL or Cable
  - Connect Wi-Fi hotspots to the Internet
  - Data and Telecoms services (alternative to UMTS)
  - Backhaul for 3G networks in less developed areas
- More similar to 3G technologies than WiFi
  - Licensed frequencies
  - Long Range (<50 miles)
    - Lower speed at longer distances
- Operates in various modes
  - *Point-to-point* - acts as a bridge
  - *Point-to-multipoint* - consumer data access



Sensors: RFID

- Radio-frequency Identification (RFID) uses a tag with a unique ID for tagging "things"
  - Three tag types



    - Passive: no battery - coiled antenna induces current which powers the tag and and encoded information is transmitted
    - Active: battery operated - can transmit signals autonomously
    - Battery Assisted Passive: requires external power to wake, but has greater range
- Used mainly in inventory and supply-chain management
  - Increasing used in:
    - Contactless Mobile Payment (e.g. Nokia's RFID shells)
    - Location-based services (e.g. in museums)
    - Bar code replacement
  - Can be used as external cues by mobile devices

Exercises...

- If periodic, peer-to-peer transmission of data is required between two devices (e.g. a camera-phone and a printer), which of the following technologies would you use: IrDA or Bluetooth?
  - Explain why, and the limitations of each approach for this application.
- Discuss ethical issues of Bluecasting and Bluejacking
- Compare and contrast the use of WiFi technology with 3G standards, and illustrate two scenarios where one may be better than the other.

To Recap...

- In this lecture set, we covered:
  - The notion of Personal Area Networks
    - Discussed why these should be wireless
    - How such technologies are used by Mobile Phones
  - Wireless Local Area Networks
    - How Wifi compares to 3G technology
    - How WiMAX augments existing infrastructures
  - Sensing using RFID

Further Reading

- ***Ubiquitous Computing: Smart Devices, Environments and Interactions***
  Stefan Poslad (Wiley, 2009)
  - Chapter 11

- ***Communication Systems: for the Mobile Information Society***
  Martin Sauter (Wiley, 2006)
  - Chapters 4, 5 and 6

- ***Wikipedia !!!***