Computer Networks

Topic 3:

Wireless Networking Standards

V1.0

Computer Networks

Topic 3 – Lecture 1:

Wireless Devices

V1.0

Scope and Coverage

This topic will cover:

- Wireless devices
- Wireless networking standards
- Issues for wireless networks
- Wireless networking protocols

Learning Outcomes

By the end of this topic, students will be able to:

- Explain the function and rationale of wireless networking standards
- Explain a range of contemporary wireless standards and their relevant applications

Wireless Networks

- Wireless Networks are networks in which electromagnetic waves carry the signal over part or all of the communication path.
- This is in contrast to networks that utilise physical media, such as fibre-optic cable, coaxial cable, etc.

Advantages of Wireless

- Increased mobility
- Increased flexibility
- Convenience
- Opportunities to provide new services

History of Wireless

- Wireless technology has been around for a few decades.
- Take up was initially slow:
  - Low data transfer rates
  - Little interoperability between different devices
  - High cost
- Great increase in number of wireless networks due to standardisation, greater speeds and reduced costs

Wireless Devices

- Computer peripherals
- Wireless LANs
- Bluetooth devices
- RFID
- Many others, e.g. mobile telephones, TV remote control, GPS, etc.

Wireless Computer Peripherals - 1

- Devices include mouse, printer, keyboard, scanner, etc.
- Can allow multiple devices to use the same peripheral
- Removes the need for cumbersome cables
- Limited flexibility by operating a little distance away from the PC

Wireless Computer Peripherals - 2

- Use two technologies:
  - ***Infrared*** (IR) is cheaper, has less interference, but requires direct optical contact between the peripheral and receiver.
  - ***Radio frequency*** (RF) works in all angles relative to the receiver, even with objects between the peripheral and receiver, but it is more expensive.

Wireless LAN (WLAN)

- Wireless networking relies on a broadcast signal.
- Suitably configured devices contain receivers that pick up and understand the broadcast signal.
- Devices can process data and broadcast signals as well.

WLAN Components - 1

- ***Wireless Adapters*** (WA)
  - Capable of transmitting and receiving wireless digital signals and are usually contained in the user device
  - Modern PCs, laptops, smartphones, etc. all come with a wireless adapter.

WLAN Components - 2

- ***Access Points*** (AP)
  - Acts as a base station that receives and transmits signals via radio waves
  - It provides the link between the devices and the network.

Hotspots

- A wireless client may be any device (computer or peripheral) designed to use the same wireless protocol as the access point.
- A client must be in range of the access point.
- The area within range of an AP is known as a “hotspot”.
- Overlapping hotspots allow a wireless network to cover a wide area.

Bluetooth

- A short range radio link with a range of around 10 metres
- Allows a number of devices to link together in an ad-hoc network
- Does not require line of sight
- Can provide communication links between phones, PDAs, computers, peripherals, etc
- Can transmit voice and data

Piconets

- The Bluetooth ad-hoc networks
- Can have up to eight devices on the same piconet
- Each piconet is synchronised to the clock of one device on it (the master).
- Other devices are slaves
- Several piconets may be active in the same location.
- Each device can be a part of several piconets, but only master of one.

RFID Tags

- A radio frequency identification tag is a small object that is attached to another object in order to identify it via radio waves
- Has two main components:
  - An integrated circuit that modulates and demodulates a radio signal, stores data and processes information
  - Antenna for transmitting/receiving

RFID Tag Uses

- A wide range of uses including:
  - Passports
  - Travel cards
  - Wildlife tracking
  - Stocktaking in shops

Other Wireless Devices

- There are many devices in common use that are wireless:
  - Mobile telephones
  - TV
  - Satellite communications
  - Pagers (e.g. hospital)
  - Remote alarms
  - GPS
  - Remote controls (TV, model aircraft)
  - Two-way radio …..

Computer Networks

Topic 3 – Lecture 2:

Wireless Networking Standards

V1.0

Wireless Standards

- IEEE 802.11 series – Wireless LAN
- Bluetooth/IEEE 802.15 - Wireless Personal Area Network
- IEEE 802.16 - Wireless Metropolitan Area Networks
- IEEE 802.20 - Mobile Broadband Wireless

Why Do We Need Standards?

- There are a number of key reasons for creating and adhering to standards for wireless networking.
- Interoperability
  - Different devices work together
- Many equipment manufacturers
  - Customers can switch for better price or features
- Allocation of frequencies
  - The radio wave spectrum is used for many applications

The IEEE 802.11 standards

- WLAN or WiFi
- Wireless LAN Media Access Control and Physical Layer specification
- Contains a number of revisions and interpretations:
  - 802.11a,b,g,etc. are amendments to the original 802.11 standard
- Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified”.

The Original IEEE 802.11

- Data rates of up to 2 Mbps
- Uses Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) signalling techniques
- 2.4 GHz frequency range

IEEE 802.11 Revisions - 1

- 802.11a
  - Uses Orthogonal Frequency-Division Multiplexing (OFDM)
  - Enhanced data speed to 54 Mbps
  - 5 GHz frequency range

- 802.11b
  - Added higher data rate modes to DSSS
  - Data speeds up to 11 Mbps
  - 22 MHz Bandwidth yields 3 non-overlapping channels in the frequency range of 2.4 GHz frequency band.

IEEE 802.11 Revisions - 2

- 802.11d
  - Enhancement to 802.11a and 802.11b allows for global roaming
  - Particulars can be set at ***Media Access Control*** (MAC) layer
- 802.11e
  - Enhancement to 802.11 includes quality of service features
  - Facilitates prioritisation of data, voice, and video transmissions

IEEE 802.11 Revisions - 3

- 802.11g
  - Extends the maximum data rate in the 2.4 GHz band, permits interoperation with 802.11b devices
  - Uses OFDM
  - 54 Mbps, with fall-back speeds that include the b speed
- 802.11h
  - Deals with interference
- 802.11i
  - Deals with security

IEEE 802.11 Revisions - 4

- 802.11n
  - High speed WLAN
  - Can theoretically operate at bandwidths up to 600 Mbps
  - Applications supporting 100 Mbps using the TCP/IP protocol are available.
  - Uses ***Multiple-Input Multiple-Output*** (MIMO) technology
  - Uses 5 GHz band

Which Version?

- Most modern wireless routers will support 802.11n plus 802.11b and 802.11g
- Older routers may only support 802.11b and 802.11g
- Higher speed networks should use 802.11n

IEEE 802.15/Bluetooth

- IEEE 802.15 covers ***Wireless Personal Area*** Networks (WPAN).
- Working Group1 (IEEE 802.15.1) is a standard based upon Bluetooth version 1.1.
- The Bluetooth ***Special Interest Group*** (SIG) is a separate non-profit organisation that oversees the Bluetooth standards.
- The Bluetooth SIG and IEEE are not related
  - No IEEE standards match recent Bluetooth standards

Bluetooth

- Open wireless technology standard
- Exchanges data over short distances
- Uses short wavelength radio transmissions
- Used in fixed and mobile devices
- Creates ***Personal Area Networks*** (PANs)

Bluetooth Range

- The range is specific to the application.
- The Core Specification states a minimum range of 10 metres or 30 feet.
- However, there is no set limit.
- Manufacturers are allowed to tune their devices to provide the range they require.

Bluetooth Spectrum

- Operates in the unlicensed industrial, scientific and medical (ISM) band
- Frequencies 2.4 to 2.485 GHz are used
- Uses a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec.
- The 2.4 GHz ISM band is available and unlicensed in most countries.

Bluetooth Interference

- Adaptive frequency hopping (AFH) reduces interference between wireless technologies sharing the 2.4 GHz spectrum.
- The technology detects other devices in the spectrum and avoids the frequencies they are using.

Bluetooth Range

- Range depends on class of radio used:
  - Class 3 radios have a range of up to 1 metre or 3 feet
  - Class 2 radios, most commonly found in mobile devices, have a range of 10 metres or 33 feet
  - Class 1 radios, used primarily in industrial devices, have a range of 100 metres or 300 feet

IEEE 802.16

- Mobile Broadband Wireless Access
- Also known as ***WiMAX*** (from "Worldwide Interoperability for Microwave Access")
- Provides up to 40 Mbps
- Currently working on the IEEE 802.16m update
  - Expected to offer up to 1 Gbps fixed speed
  - Required for 4G networks

WiMAX Usage

- Provides mobile broadband or at-home broadband connectivity across whole cities or countries.
- Deploying a WiMAX network has low cost in comparison to DSL or Fibre-Optic.
- Can provide broadband in remote locations

Comparison with WiFi

- WiMAX covers many km and uses an unlicensed spectrum to provide access to a local network.
- Wi-Fi is more popular in end user devices.
- 802.11 supports direct, ad hoc or peer-to-peer networking between end user devices without an access point, while 802.16 end user devices must be in range of the base station.

IEEE 802.20

- Mobile Broadband Wireless Access (MBWA)
- Aims to enable worldwide deployment of interoperable mobile broadband wireless access networks, including:
  - Mobile and ubiquitous Internet access
  - Transparent support of Internet applications
  - Access to enterprise intranet services
  - Transparent access to infotainment and location services

IEEE 802.20 Detail

- Bandwidths of 5, 10, and 20 MHz
- Peak data rates of 80 Mbps
- Uses MIMO
- Supports low-bit rates efficiently, carrying up to 100 phone calls per MHz
- Allows network access whilst travelling at speeds of 250 km/h

Computer Networks

Topic 3 – Lecture 3:

Issues for Wireless Networks

V1.0

Wireless Issues

- There are a number of issues that may cause concern for those using radio frequencies for network media rather than physical cables, these include:
  - Range
  - Interference
  - Security

Range

- The range where wireless signals can be reliably transmitted and received is a key parameter for a wireless network.
- In ideal conditions, a WLAN can have a range of 300m or more.
- Real world conditions are not ideal.
- In an office/home, range can drop as low as 10m.

Indoor Range

- WLANs are normally implemented indoors and a number of factors will affect the range of the network:
  - Building design
  - Construction materials
  - Room layout
  - The location and type of other electrical devices

Installation

- Technically simple regarding installation and configuration

- Installation does need to take into account the location of:
  - access points
  - networked devices
  - obstacles

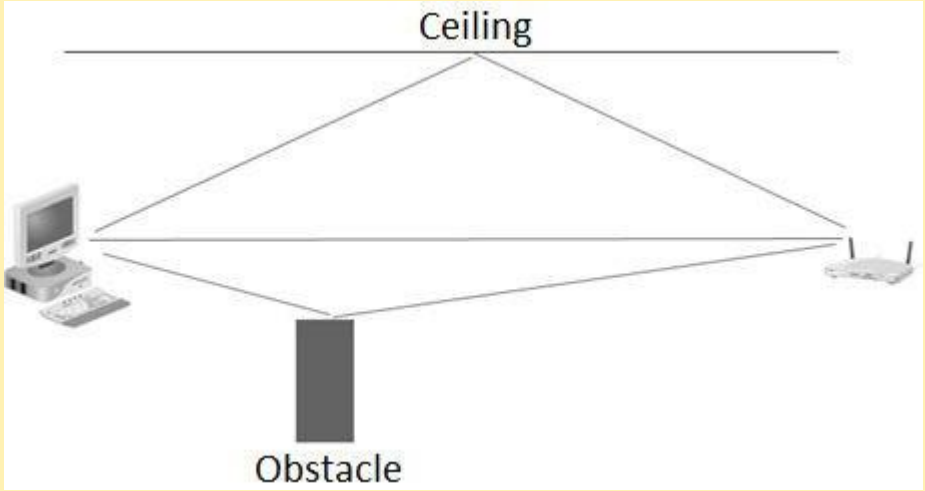
Interference

- Radio frequency signals can be negatively affected by other radio signals in the same frequency band.

- There are two main sources of such signals:
  - Reflected signals from the wireless network itself
  - Other electrical equipment

Multipath

- Radio frequency signals can be affected by signals bouncing off building surfaces and other obstacles
- Signals can come from multiple directions (multipath)
- May cancel or reduce signal strength



Eliminating Multipath

- Most access appointments include software tools that analyse signal strength.
- These can be used to test signal strength of networked computers.
- Most networked equipment can be moved to improve signal strength.

External Interference

- Radio emissions from other devices using the same frequency band are a source of interference
- There are particular industries where this is a problem
  - Hospitals use a lot of monitoring equipment that may use the same frequency
- Equipment may need to be isolated to prevent the interference.

Security Issues

- Security can be compromised in different ways from hard-wired networks.
- Radio transmission cannot be limited to within the network premises.
- Therefore, the transmitted signals can be intercepted by devices outside of a building and this data could include sensitive business or personal data.

Drive–by Hacking

- Any IEEE 802.11 receiving device using the relevant standard could pick up a transmitted signal.
- A hacker could be located near a business premises and pick up these signals.
- As the signals are broadcast, there would be no way of knowing that an unauthorised person had accessed the signal.

Wired Equivalent Privacy (WEP)

- The first major attempt to make wireless networks as secure as wired networks
- Susceptible to eavesdropping
- Has been deprecated by IEEE as it does not meet its security goals
- Still widely in use

WiFi Protected Access (WPA)

- Brought in as an improvement on WEP
- WPA is more secure and comes in two forms
  - A form using pre-shared keys for home networks
  - A more secure form using an authentication server for business networks
- WPA has also been cracked and been replaced by WPA2 which is more secure.

Bluetooth Security

- There are a number of known security flaws with Bluetooth devices and these include:
  - Bluejacking
  - Bluesnarfing
  - Bluebugging
  - Bluetoothing

Bluejacking

- The hacker sends a phone contact or business card to another nearby phone.
- The ‘name' field of the contact can be misused by replacing it with a suggestive text.
- This is equivalent to spam email since both are unsolicited messages displayed on recipients' end without consent.

Bluesnarfing

- Accesses or steals data like messages, such as a calendar or phone book from the target device.

- There have been reports of the tools that use methods such as device address guessing and brute force in order to break-in, even when device is configured as ‘invisible‘.

Bluebugging

- The target device is controlled by the attacker who sends commands as if they had physical access.
- Similar to a ***trojan***

Bluetoothing

- Short range social networking
- Harassment of individuals within range

Securely Using Bluetooth

- Keep devices in the disabled state, enable it only when needed
- Keep the device in non-discoverable mode
- Do not accept any unknown and unexpected request for pairing your device
- Use non regular patterns as PIN keys
- Keep a check of all paired devices and delete any paired device which you are not sure about
- Register your device at the manufacturer site

Computer Networks

Topic 3 – Lecture 4:

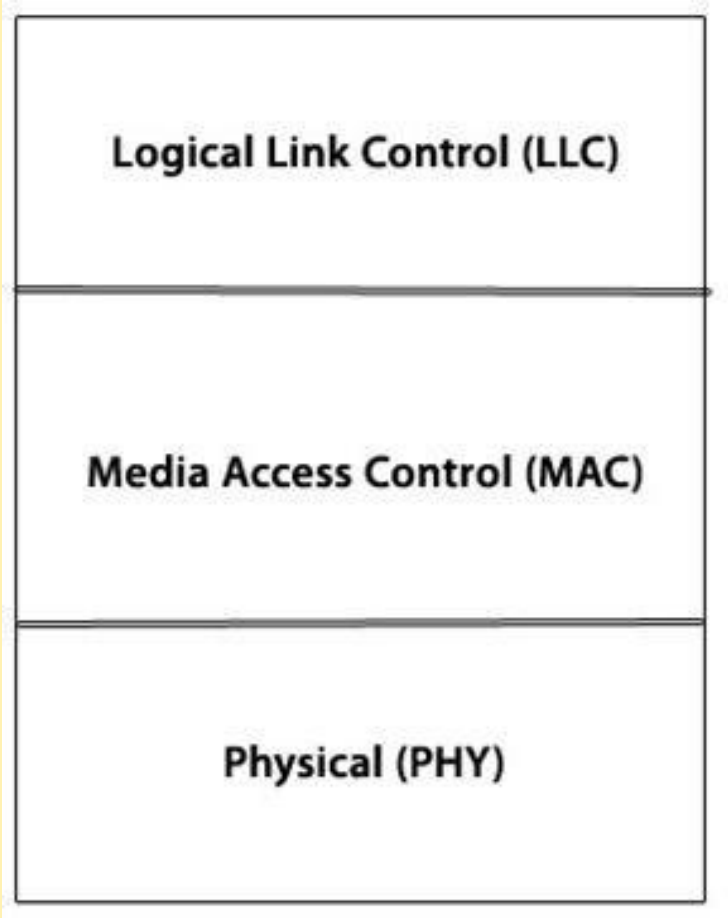
Wireless Networking Protocols

V1.0

Protocol Stacks

- Wireless networks have layered protocol stacks like other networks.
- We will not deal with the higher level layers.
- We will examine protocol stacks and specific technologies of:
  - WLAN
  - Bluetooth

WLAN Protocol Stack



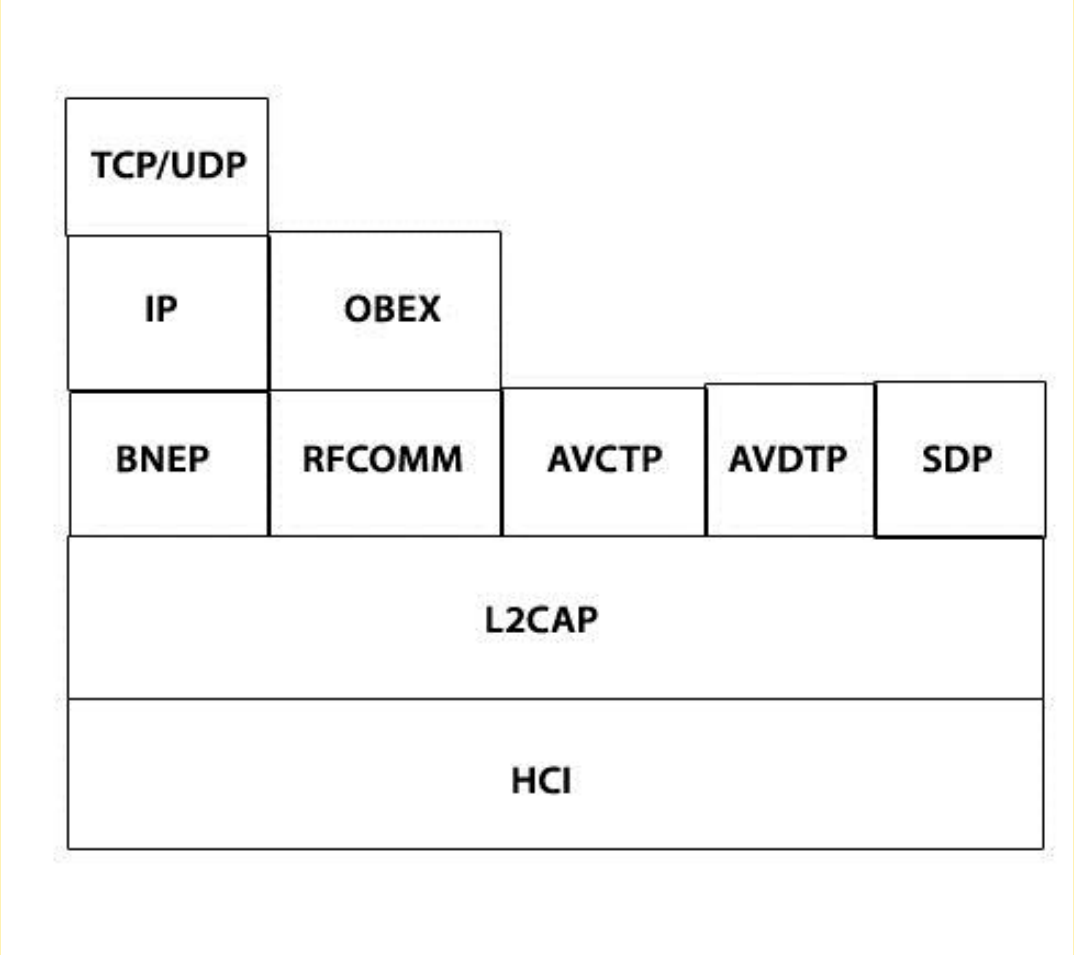
WLAN LLC & MAC Layers

- LLC designed to provide the functionality of the High-Level Data Link Control protocol of the standard TCP/IP protocol stack
- LLC allows an 802.11 protocol stack to be grafted underneath any TCP/IP implementation with little or no change to the upper layers
- MAC provides the same functions as in other protocol stacks

WLAN PHY Layer

- Original 802.11 standard defined three specific physical network protocols:
  - An infrared communications standard
  - A ***Direct-Sequence Spread Spectrum*** (DSSS) RF protocol
  - A ***Frequency-Hopping Spread Spectrum*** (FHSS) RF protocol
- Later versions of the 802.11 standard redefined the physical layer to be DSSS only.

Bluetooth Protocol Stack - 1



Bluetooth Protocol Stack - 2

- The bottom layer of the stack is the HCI, the ***Host Controller Interface***
  - This is the interface between the host (e.g. a computer) and the controller (e.g. a Bluetooth device).
- The layer above is L2CAP, the ***Logical Link Controller Adaptation Protocol***
  - This acts as the data multiplexer for other layers.

Bluetooth Protocol Stack - 3

- ***Bluetooth Network Encapsulation Protocol*** (BNEP)
  - Allows the running of other networking protocols, such as IP, TCP, and UDP, over Bluetooth
- ***RFCOMM*** is the virtual serial port protocol
  - Allows a Bluetooth device to simulate the functions of a serial port
- ***Service Discovery Protocol*** (SDP)
  - Used whenever you want to find services on a remote Bluetooth device

Bluetooth Protocol Stack - 4

- ***The Object Exchange layer*** (OBEX) protocol layer
  - Implemented above the RFCOMM layer and is useful when you want to transfer data as an object, such as files

Bluetooth Protocol Stack - 5

- ***Audio/visual control transport protocol*** (AVCTP) and ***Audio/visual data transport protocol*** (AVDTP)
  - Used to control and distribute audio and video over Bluetooth
  - Used when you want to control the functions of a media player or if you want stream audio in stereo

Wireless Technologies

- Orthogonal Frequency Division Multiplexing
- Multiple Input Multiple Output
- Frequency Hopping Spread Spectrum
- Adaptive Frequency Hopping
- Direct Sequence Spread Spectrum

FDM

- Frequency division multiplexing (FDM) is a technology that allows transmission of multiple signals simultaneously over a single transmission cable or wireless system.

- Each signal travels within its own unique frequency range (carrier), which is modulated by the data (text, voice, video, etc.).

OFDM

- Orthogonal FDM is a spread spectrum technique.
- Data is distributed over a large number of carriers, spaced apart at precise frequencies.
- Demodulators only pick up their own frequencies and not other frequencies.
- The benefits of OFDM are:
  - high spectral efficiency
  - resiliency to interference
  - less distortion

MIMO

- Multiple Input, Multiple Output OFDM
- Uses multiple antennas to simultaneously transmit/receive data
- This ***spatial multiplexing*** increases data-transmission speed by a factor equal to the number of transmitting antennae
  - 4 antennae = 4 x speed
- All data is transmitted in the same frequency band, which utilises the spectrum very efficiently.

FHSS

- Bluetooth
- Transmitter hops from frequency to frequency hundreds of times per second
- Pseudo-random number generation is used to produce the sequence of frequencies.
- All stations use the same seed and hop to the same frequency at the same time, thus staying synchronised.
- May use TDMA or CDMA

Time Division Multiple Access

- Frequencies divided into time slots allocated to individual users.
- A user is allocated a slot on a single frequency and then moved to another frequency
- Several different data streams will be transmitted on one frequency in short bursts with an allocated timeslot

Code Division Multiple Access

- Each transmitter may transmit over the whole frequency spectrum all of the time.
- Coding theory is used to separate all of the multiple and simultaneous transmissions.
- Comparison of TDMA and CDMA
  - TDMA is like a classroom where each person takes a turn to speak.
  - CDMA is like a classroom of people all speaking at the same time but in different languages, so the messages are only heard by people who speak that language.

AFH

- Adaptive frequency hopping reduces interference between Bluetooth and other devices.
- Transmission does not occur on channels that have significant interference.
- Devices in the same frequency band and physical area detect the presence of each other and adjust their communication systems to reduce the amount of frequency overlap.

DSSS

- WLAN
- Data is divided into small pieces
- Each piece is allocated to a frequency channel on the available spectrum
- Data is combined with a '***chipping code***'.
- Chipping code helps resist interference and allows for data recovery.

DSSS v FHSS

- FHSS advantages:
  - Devices are usually cheaper
  - Uses less power
- DSSS advantages
  - Better performance
  - More reliable transmission

References

- Tanenbaum, A.S. & Weatherall, D.J. (2010). *Computer Networks,* 5th edition. Pearson Education.
- Rysavy, P. (2002). *Networking Standards and Wireless Networks*. Netmotion Wireless.
- IEEE website: http://grouper.ieee.org/groups/802/
- Bluetooth website: https://www.bluetooth.org
- IBM website: http://www.ibm.com

Topic 3 – Wireless Networking Standards

Any Questions?