Wireless Communications and Mobile Internet

刘栋 5140309415

Chapter 1 Overview of Wireless Networks

1) Faraday: Electromagnetic induction(1831) →Morse : Telegraph(1837) →Maxwell: Electromagnetic Field Theory → Bell: Telephone(1876) → Marconi: wireless telegraphy(1895) →Fessenden: AM Modulation(1906) → TV broadcast(1927) → Public Mobile Phone System(1946) → Communication Satellite（1958）→ NMT: Analog Cellular System（1981）→ GSM: Digital Cellular System（1988）→Wireless LAN（1997）
2) Cellular System、Mobile Management、Mobile IP、Wi-Fi、WiMAX、Ad Hoc Networks、Security of Wireless Networks、Wireless Personal Area Network、Wireless Sensor Network、Internet of Things(IOT)、Software Defined Network(SDN)

Chapter 2 Radio Propagation

1) Differences: Different transmission medium (Wireless media uses air while Wired use different transmission medium); Stability (Wireless media is relatively unstable); Bandwidth; Broadcast Nature
2) Differences between the licensed band and unlicensed band: Licensed bands use Cellular system around 1GHz, 2GHz-PCS/WLAN，5GHz-WLAN，28-60GHz-LMDS，IR while unlicensed band uses ISM，U-NII，PCS
3) Three factors: Interference between different signals, operating frequency and obstacle in the path.
4) Reflection: The size of obstacle is large than wavelength.

   Diffraction: The path is blocked by something sharp.

   Scattering: The size of obstacles is smaller than wavelength and there are huge numbers of the obstacles.
5) Indoor: Diffraction, scattering; Outdoor: Reflection, diffraction
6) Large distance between transmitters and receivers result large pass loss, smaller antenna gains,

   The heights of mobile stations and base stations is small result in that the receiving power is small at the certain transmitting power
7) Free space modeling: L_p[dB]=32.45+20lgf_c[MHz]+20lgd[km]

   Two-ray modeling: $10\lg P_r = 10\lg P_0 - 10\alpha \lg(d)$
8) shadowing/slow fading，long-term changes in average level and its effect will cause the strength of the signal changes in terms of location change.
9) $L_p = L_0 + 10\alpha \lg D + X$
10) Macro-cell: $L_p = A + B\lg(d)$ -C/-D; Micro-cell: $L(dB) = L_{os}(d_a, h_t) + L_B$
11) multipath/small-scale fading: A propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths.

    The Doppler effect: the change in frequency or wavelength of a wave for an observer moving relative to its source.
12) Rayleigh distributions: It is used to detect the envelope caused by multipath fading.

    Ricean distributions: It is used to describe the fading changes in received envelope.
13) Doppler shift: V(t) = Vf/c*cosΘ(t). It is caused by high-speed object and relative motion.
14) Ricean: $K(dB) = 10\lg(A^2/2\sigma^2)$ Rayleigh: $r_{mean} = 1.2533\sigma$
15) crossing rate $F(R) = \int_0^\infty \dot{r} p(R, \dot{r}) d\dot{r}$, Average fade duration: $\tau_R = \frac{P(r \le R)}{N_R}$

Chapter 3 and 4 Cellular System

1) 3G has been used in TD-SCDMA，WCDMA，CDMA2000 by adopting CDMA and packet switching technology since 2008, while 2G only use the TDMA and circuit switching technology.
2) Relationship: The smaller transmitting power, the smaller system capacity. The larger the cell radius, the smaller the capacity.
3) We determine the value of k layers using N, and then determine the radius D. Thus, we can determine the cluster size.
4) Base stations: A land station in the land mobile service.

   Uplink: A link used for the transmission of signals from an earth station to a space radio station

   Downlink: A link used for the transmission of signals from a space radio station to an earth station.

   Cells: Area of radio coverage in a cellular network

   Location areas: A set of base stations that are grouped together to optimise signalling.

   Mobile switching centers: The primary service delivery node for GSM/CDMA.
5) Architecture: HLR is used for obtaining data about the SIM and mobile services ISDN number; VLR provides subscriber information when the subscriber is outside its home network. The base station subsystem and The UMTS terrestrial radio access network and other things.
6) handoff management: switching base stations;

   location management: location update, call delivery.
7) Advantages: The speed of transmitting signals and pictures is improved. Multimedia, website and roaming can be supported through 3G system.
8) Call Admission Control prevents oversubscription of VoIP networks and often used in the call set-up phase and applies to real-time media traffic as opposed to data traffic.

   Difference: In TDMA we allow only one user to connect, however CDMA allows more than one users to connect.
9) SGSN/GGSN: They use the port of UDP2123 to listen the replies of GTP-C and listen the replies of GTP-U through the port of UDP2152.

   MSC/GMSC/HLR: They are used to set up and releases the end-to-end connection, handles mobility and hand-over requirements during the call and takes care of charging and real time pre-paid account monitoring.
10) WCDMA, CDMA2000, TD-SCDMA
11) Global roaming. high speed, fast mobility, broadband multimedia service.
12) GPRS: 114 Kbps,1800MHz, 1710~1785MHz(uplink), 890~915MHz(downlink)

    WCDMA:3.84Mcps, 5MHz, 1940~1955MHz(uplink), 2130~2145MHz(downlink)

    CDMA2000: 1.2288Mcps, 1.25MHz, 1920~1935MHz(uplink), 2110~2125MHz(downlink)
13) broadband internet、phone business、Video Calling Services and so on.
14) 3G Cellular Network

Chapter 5 Future Technologies

1) Mobile Cloud Computing; Mobile Web; Pervasive Computing.

Chapter 6 Mobility Management

1) A handover, in which the cell is not changed, is called intra-cell handover. Monitor the signal strength changes. Once it exceeds the threshold, switch begins; Mobile station begin to recognize the new base station. Then by undergoing some interactions, we establish a new link.
2) Intra-switch handoff: Switch between the mobile units which is controlled by different MTSO; Inter-switch handoff: Switch between the mobile units which is

controlled by same MTSO.

3) MCHO: Mobile station monitor the signal strength and choose the best choice.

NCHO: Network monitor the signal strength and launch the switch.

MAHO: Mobile station monitor the signal strength and network make the switch choice.

4) Hard handoffs: Advantages: One call uses only one channel at any moment. Disadvantages: Ping-ponging effect may occur.

Soft handoffs: Advantages: The connection to the source cell is broken only when a reliable connection to the target cell has been established and therefore the chances that the call will be terminated abnormally due to failed handovers are lower; Disadvantages: Require more complex hardware.

5) Feedback-based handoff: When we find the signal strength change between base unit and mobile unit, we are supposed to execute handoff.

6) Straight-line: The sequence of user's behavior is linear and straight

Fluid flow model: It is used for intra-cell and inter-cell movements of mobile nodes. The behavior of the users is executed by randomly determined periods.

7) Handoff rate: $\mathrm{f}(d_0, d_{av}) = a(d_0)[d_{av}]^{d(d_0)}$, $\mathrm{g}(d_0, d_{av}) = b(d_0)[d_{av}]^{c(d_0)}$

8) Intra-switch: When a mobile signal becomes weak in a given cell and MTSO finds other cell within its system to which it can transfer the call then it uses Intra system handoff.

Inter-switch: When a mobile signal becomes weak in a given cell and MTSO cannot find other cell within its system to which it can transfer the call then it uses Inter system handoff.

9) Intra-cluster handoff rate: $f(t)_0 = \frac{\beta^{\gamma} * t^{\gamma-1}}{\Gamma(\gamma)} e^{-\beta t}$; Inter-cluster handoff rate: $f(s)^* = (\frac{\beta}{\beta+s})^{\gamma}, \beta = \gamma\eta$

10) The effect of cell splitting: It may be performed to provide additional capacity within the region of the original cell site.

11) Two-tier network: A two-tier network architecture is a network architecture in two separate networks govern a channel.

12) Location update: The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next.

Service delivery: Cellular network search for the available access interface for called user. If succeed, caller will send a feedback to end this service delivery.

13) Time-based: Advantages: easy to manage because each base station requires maintaining its internal clock only. Disadvantages: sometimes if the user is stationary at that time unnecessary updates would be performed.

Movement-based: Advantages: High efficiency; Disadvantages: when user travels around the boundary at that time unnecessary updates may happen.

Distance-based: Advantages: Cost would be low; Disadvantages: when the user crosses the boundary very frequently, unnecessary location updates would occur

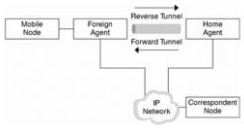
14) Static Location Update: One scheme involves the user updating its location upon every inter-cell movement, and is named always-update. This will incur significant energy and computational costs to both the network and the user, especially to the most mobile users. This may be particularly wasteful, as if a user makes frequent, quick movements within an LA, beginning and ending at the same location, many LUs will occur that might be unnecessary, especially if few or no calls are incoming. However, the network will always be able to quickly locate a user upon an incoming call, and extensive paging will not be necessary.

Chapter 7 Mobile IP

1) Reason: Once the location of the user has been changed, we need a new address. However, the process of switching may cause the loss of the data or the interruption of the applications

2) MN: mobile node; HA: Home Agent; FA: foreign agent; COA: care-of address; CN: communication node.

3) MH sends to FA ; FA tunnels packets to HA by encapsulation; HA forwards the packet to the receiver

4) 

5) Registration process: Initiate: The MN sends a registration request to the FA. Then FA switches registration to the HA. HA will send reply to FA in order to check. Finally, the FA uses its registration and relay it to MN.

6) A limited lifetime allows a mobile node registers with its home agent using a registration request message so that its home agent can create or modify a mobility binding for that mobile node.

7) Functions:

8) Functions:

9) The registration may fail in that a FA or HA receives a request with the "T" bit set while it does not support a reverse tunnel.

10) IP in IP: It is an IP tunneling protocol that encapsulates one IP packet in another IP packet. To encapsulate an IP packet in another IP packet, an outer header is added with Source IP, the entry point of the tunnel and the Destination point, the exit point of the tunnel. Present by RFC2003.

Minimal Encapsulation: An IP datagram is encapsulated with an outer minimal forwarding IP header. Present by RFC 2004.

Generic Routing Encapsulation: It is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

To avoid extra bits, minimal encapsulation is needed.

11) When MN reaches foreign network, it will sense proxy advertisements and select a FA which supports reverse tunneling, it begins from the care of address of the MH, and ends in that of the HA.

12) A reverse tunnel allows a MN located on a foreign network to establish a topology-oriented packet to ensure that it establishes a communication connection on the foreign network where the ingress filter router is set up.

13) The mobile IP nodes are with the reverse tunneling and firewalls. Then we can send through the reversed tunneling and avoid firewalls to obtain the link between MN and FA.

Chapter 8 IEEE 802.11 WLAN

1) DCF: A fundamental MAC technique of the IEEE 802.11 based WLAN standard; PCF: A Media Access Control (MAC) technique used in IEEE 802.11 based WLANs; DIFS: DCF Interframe Space; SIFS: The shortest Interframe spacing. It is considered as shortest among above mention networking terminology; PIFS: one of the interframe space used in IEEE 802.11 based Wireless LANs.

2) DCF has an optional virtual carrier sense mechanism that exchanges short Request-to-send (RTS) and Clear-to-send (CTS) frames between source and destination stations during the intervals between the data frame transmissions.

3) IEEE 802.11e: 802.11 is an IEEE standard that allows devices such as laptop computers or cellular phones to join a wireless LAN widely used in the home, office and some commercial establishments.

EDCA: Enhanced distributed channel access

HCF: The hybrid coordination function

4) Differences: An Infrastructure mode network requires the use of an Access Point., however there is no central Access Point controlling device communication in Ad-hoc network.

5) AP: receive wireless signal and send it to wired net; STA: wireless network devices in WLAN.

6) MAC layer and PHY layer

7) LLC: The logical link control data communication protocol layer is the upper sublayer of the data link layer of the seven-layer OSI model;

MAC: The MAC layer emulates a full-duplex logical communication channel in a multi-point network.

PLCP: carrier sensing assessment, forming packets for PHYs.

PMD: modulation and coding.

8) Differences: Mainly in working frequency;

Infrared wireless networks: simple, portable, safe, cheap but short range.

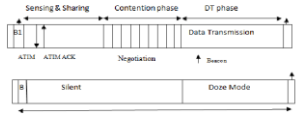
radio wireless networks: simple, high speed, large coverage but unsafe, limited spectrum of frequency.

9) DSSS FHSS OFDM DSSS STBC

10) There are five different priorities for data packets ready to be sent

11) the IEEE 802.11 Distributed Coordination Function (DCF), Point coordination function (PCF), the hybrid coordination function (HCF).

12) The timing diagram:



13) Differences: Unicast is more reliable than multicast.

14) NAV is a logical abstraction which limits the need for physical carrier-sensing at the air interface in order to save power.

15) QoS is not supported in 802.11 but supported in 802.11e and is not supported in infrastructure mode. And also Qos is not supported in ad-hoc mode.

16) We need to separate the time slot signals correctly.

17) In 802.11: preamble and ranging. Infrastructure: AP controls timing. Ad hoc mode: timing divided

18) Because we are supposed to deal with the situations that cannot be solved by the synchronization field.

19) Yes. Automatic self-time correcting procedure (ASP), was proposed to synchronize a multi-hop MANET. It is used to let the faster nodes send out beacon more often and self-correction of the clocks.

20) Because mobile hosts are supported by battery power, it is important that we need power management.

21) In Ad-hoc mode: CSMA/CA is used to access the channel. RTS, CTS, ASK, PS-Poll are used to overcome hidden terminal.

In infrastructure mode: CSMA/CA is used to access the channel. RTS, CTS, ACK, PS-Poll are used to overcome hidden terminal.

22) ATIM: It is used to be transmitted in ATIM-Window by stations who want to send buffered packets;

DTIM: It is used for sending buffered broadcast packets.

23) Handover is performed in the sequence of scanning, authenticating and reconnecting.

24) Through fragmenting packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size.

25) Frame Control (2 Bytes); Duration/ID (2 Bytes); Address 1 – 4 (6 Bytes each); Sequence Control (2 Byte); QoS control (2 Bytes); HT Control (4 Bytes, only for 802.11n frames)

26) For identifying.

27) 802.11a was an amendment to the IEEE 802.11 wireless local network specifications that defined requirements for an orthogonal frequency division multiplexing (OFDM) communication system. It transmits data faster than 802.11.802.11b uses DSSS,802.11a use OFDM.

28) The goal of WEP is to make wireless networks as secure as wired network.

29) WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity.

30) I cannot solve

31) In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication.

In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake

32) WEP: They can be shared between users while they do not tell us who is connected

MAC filtering: it doesn't identify a person

Captive portal: flexible, easy to implement but it is not transparent and standardized.

33) Differences: In an active scan, the client radio transmits a probe request and listens for a probe response from an AP while in a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time.

34) High priority: SIFS; Medium priority: PCF IFS; Low priority: DCF, Distributed Coordinate Function IFS.

35) The combination can be discussed in a particular form and AP and stations establish a continuous link.

Chapter 9 WiMAX

1) Fast rate, stable, long distance, mobility.

2) The original version of the standard on which WiMAX is based (IEEE 802.16) specified a physical layer operating in the 10 to 66 GHz range.

3) OFDM is a method of encoding digital data on multiple carrier frequencies. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels. Each sub-carrier is modulated with a conventional modulation scheme at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

Chapter 10 Ad Hoc Networks

1) Comparison: In Ad-hoc mode we do not have Aps while in infrastructure networks we do have.

2) Transmitter's perspective: When a node is visible from a wireless AP, hidden terminal problem occur.

3) Receiver's perspective: When receiving, it will be interfered by others and exposed node problem may occur.

4) IEEE 802.11MAC has asked that all user share one channel. When interference

happens, one of the approach of the decision is to set exclusion region.

5) Upper bound: $Th^{upper} = \frac{E[P]}{\min(4, H_s) \times T}$, Lower bound: $Th^{lower} = \frac{E[P]}{\min(H_s, 6) \times T + \max(H_s - 6, 0) \times T_{max}^{wait}}$

6) Hidden terminal problem occurs when a node is visible from a wireless AP, but not from other nodes communicating with that AP.

Exposed node problem occurs when a node is prevented from sending packets to other nodes because of a neighboring transmitter.

Chapter 11 Security

1) WEP: The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

2) 1. Initialization On detection of a new supplicant, the port on the switch (authenticator) is enabled and set to the "unauthorized" state. 2. Initiation, initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. 3. Negotiation The authentication server sends a reply to the authenticator, containing an EAP Request specifying the EAP Method 4. Authentication If the authentication server and supplicant agree on an EAP Method.

3) WEP is optional and has security vulnerabilities. WAPI has WAI for authentication and it is safer. IEEE802.11i adds TKIP and CCMP.

Chapter 12 Bluetooth and RFID

1) Less power consumption, more transmission distance.

2) Active, Sniff, Hold, Park

3) Reader: responsible for two-way communication between electronic tags and also receive command control from host.

Electronic tags: communicate with readers.

4) Chip technology, Antenna Design Technology, Packaging technology, Tag application technology, Anti-collision technology.

5) Student ID card, Traffic tracking, Asset management.

Chapter 13 Wireless Sensor Networks

1) The WSN is built of "nodes" and each node is connected to one sensors. The process of data transfer is transmitted back to the base station through the transmission of adjacent nodes, and then transmitted by the base station to the final user through satellite.

2) Power module: offering the reliable power needed for the system; Sensor: obtaining the environmental and equipment status. Microcontroller: receiving the data from the sensor; Wireless Transceiver: transferring the data

3) Smart dust, A line in the Sand, C4ISRT.

4) Firstly, the sensor network nodes broadcast their status to the surroundings and receive status from other nodes to detect each other. Secondly, the sensor network nodes are organized into a connected network according to a certain topology (linear, star, tree, mesh, etc.). Finally, suitable paths are computed on the constructed network for transmitting the sensing data.

5) Self-organization, Multi-hop, Low power consumption, small range, dynamic, low data rates.

6) The transmission rate, delivery reliability and network lifetime. The smaller the transmission rate, the higher the delivery reliability and the longer network lifetime will be.

7) solar energy, nuclear energy.

Chapter 14

1) UBW, SDR, RFID.

2) High transfer rate, Multi-path resolution ability, High processing gain, Good security, large system capacity.

3) Bluetooth Low Energy is a simplified Bluetooth which has a lower power consumption and high data transmission.

4) A cognitive radio monitors its own performance continuously and then uses this information to determine the RF environment, channel conditions, link performance and then adjusts its quality.

5) Features: Short distance, Low transmit power, high transmission speed. Application: Localization, Navigation positioning, Health care, Wireless identification system.

Chapter 15 Software-Defined Networking

1) SDN is an approach to computer networking that allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality.

2) Directly programmable, Agile, Programmatically configured, Open standards-based.

3) OpenDaylight, Protocol Oblivious Forwarding POF, Open Computing Project OCP

4) Reasons: Traditional devices are intended to rely on hardware, However, we can change the situation by using SDN in order to apply software devices. It can be easily updated and revised. This could make it more flexible and cheaper than traditional ones.

Chapter 16,17,18 Intelligent Robots, Cars and Quadrotors

1) Camera, Microphone, Sensors, Motors.

2) Autonomous car, Environment monitoring, Fully Distributed Scalable Smoothing and Mapping

Autonomous car: An autonomous car (also known as a driverless car, self-driving car, robotic car) is a vehicle that is capable of sensing its environment and navigating without human input.. They all require a human driver at the wheel who is ready at a moment's notice to take control of the vehicle.

Chapter 19 MIMO

1) Differences: MIMO has more than one transmission path, while SISO has only one.

2) MIMO mode can be found in the textbook: $\mathbf{x} = [x_1\ x_2 \dots x_{N_T}]^T$, x_m represent the signal the m_{th} line sends. $\mathbf{y} = [y_1\ y_2 \dots y_{N_R}]^T$, y_n represents the signal it receives. Chanel : $\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} \dots \\ h_{21} & h_{22} \dots \end{bmatrix}$. Then we can obtain the equation of y=Hx+n.

3) Differences: Space-multiplexing transmits signals in the same frequency band while Space-diversity in different band.

4) Networked MIMO, Non-wireless communications systems, DAS

Networked MIMO: A multiple-input, multiple-output (MIMO) communication system comprising a master base station and a slave base station. The master base station has a plurality of transmit antennas and transmits a first set of data to a mobile station in a first transmission. The slave base station has a plurality of transmit antennas and transmits a second set of data to the mobile station in the first transmission

Chapter 21 and 22

1) Security: It has large variance in value; The wallet cannot be found once it has been lost, therefore it has some problems in keeping. The exchanging cannot be ensured. The privacy that keeps exchangers anonymous.

2) Version information, Format information, Coding area, Checking bits, flag symbos and function graphics.