Wireless Communications & Mobile Internet

Midterm Exam 张[illegible], 5140309508

Chapter 1 Overview of Wireless Network.

1. Describe the history & development of wireless comm net.

1837, Morse invented telegram. Bell invented telephone in 1876. Marconi invented radio telegraph in 1895. Comm satellite SCORE was launched in 1958. NMT was established in 1981. GSM was established in 1988.

2. List the foundational techs used in wireless comm net.

① cellular system ② mobile management ③ mobile IP ④ WiFi ⑤ WiMAX ⑥ AdHoc ⑦ security of wireless net ⑧ WPAN ⑨ sensor net ⑩ IoT ⑪ SDN

Chapter 2 Radio Propagation

1. ① wire medium includes twisted-pair, coaxial-cable and optical cable; wireless medium is air, three main techs are microwave, laser and infrared ray. ② WM is more reliable than wireless medium.

2. Authorized spectrum: ① cellular system 1GHz ② PCS & WLAN 2GHz ③ WLAN 5GHz ④ LMDS 28-60GHz Unauthorized spectrum: ① ISM ② U-NII ③ PCS. ITU-R helps manage this.

3. ① topography (indoor/outdoor) ② frequency (low/high) ③ v of MT

4. ① Reflection: obstacle size > λ ② Diffraction: the path between transmitter & receiver is blocked by sharp edges. ③ Scattering: obstacle size ≤ λ, obstacle num is large.

5. ① reflection happens on the surface of earth/building/wall ② scattering happens on surface of small/irregular objects ③ diffraction happens at shadowing area.

6. Path loss is $L_P = \frac{P_t}{P_r}$, $P_r = \frac{G_t G_r P_t}{L}$, $L = L_P L_S L_F$.

$L_P[dB] = 32.45 + 20 \lg f_c[MHz] + 20 \lg d[km]$. height of bs ↑ P_r ↑

7. ① Free Space $L_P[dB] = 32.45 + 20\lg f_c + 20 \lg d$, $z = D/C = 3d$ ns

② Two-Ray $L_P[dB] = 40 \log_{10}(d) - 10 \lg_{10}(G h_t^2 h_r^2)$

8. Slow fading can be caused by events such as shadowing, where a large obstruction such as a hill or large building obscures the main signal path between the transmitter & receiver.

9. Fade margin is an expression for how much margin - in dB - there is between the received signal strength level & the receiver sensitivity of the radio.

Log-normal shadowing $P_R = d^2 10^{\frac{x}{10}} g(d) P_T G_T G_R$ $x \sim N(0, \sigma^2)$

so, fade margin = $P_R - rs$.

10. Macro-cell

$$L_P(d) = \begin{cases} A + B\lg d & \text{city} \\ A + B\lg d - C & \text{suburban} \\ A + B\lg d - D & \text{open area} \end{cases}$$

$A = 69.55 + 26.16 \lg f_c - 13.82 \lg h_b - a(h_m)$

$B = 44.9 - 6.55 \lg h_b$ $a(h_m) = (1.1 \lg f_c - 0.7) h_m - (1.56 \lg f_c - 0.8)$ small city

$C = 5.4 + 2[\lg(f_c/28)]^2$ $a(h_m) = \begin{cases} 8.29[\lg(1.54 h_m)]^2 - 1.1 & f_c \le 200MHz \\ 3.2[\lg(11.75 h_m)]^2 - 4.97 & f_c > 200MHz \end{cases}$ large city

$D = 40.94 + 4.78(\lg f_c)^2 - 18.33 \lg f_c$

11. small-scale fading is the rapid variation of the received wireless signal in short time/distance, including multipath fading (due to multipath prop) & Doppler Effect (MT movement).

12. Rayleigh Pdf $f_{ray}(r) = \frac{r}{\sigma^2} \exp(-\frac{r^2}{2\sigma^2})$

Ricean Pdf $f_{ric}(r) = \frac{r}{\sigma^2} \exp(\frac{-(r^2+\alpha^2)}{2\sigma^2}) I_0(\frac{\alpha r}{\sigma^2})$, $r \ge 0$, $\alpha \ge 0$

13. Doppler shift $v(t) = \frac{Vf}{c} \cos\theta(t)$

Doppler shift Spectrum $S(f) = \frac{A}{4\pi f_m} \frac{1}{\sqrt{1 - (\frac{f - f_c}{f_m})^2}}$, $|f - f_c| \le f_m$

14. Rayleigh fading $P_R = \alpha^2 10^{\frac{x}{10}} g(d) P_T G_T G_R$, $P_R = \frac{\alpha}{\sigma^2} e^{-\alpha^2/2\sigma^2}$

Ricean fading $P_r(x) = \frac{x}{\sigma^2} e^{-\frac{(x^2+s^2)^2}{2\sigma^2}} I_0(\frac{xs}{\sigma^2})$, $x \ge 0$, $s^2 = m_I^2(t) + m_Q^2(t)$

15. $LCR = \sqrt{2\pi} f_d \rho e^{-\rho^2}$, f_d Doppler shift, $\rho = \frac{R_{thresh}}{R_{rms}}$

$AFD = \frac{e^{\rho^2} - 1}{\rho f_d \sqrt{2\pi}}$, $AFD \times LCR = 1 - e^{-\rho^2}$ (for Rayleigh fading)

Chapter 3 & 4 Cellular System

1. 2G is digital network, it emerged in 1990s. 2.5G used GPRS, 2.75G used EDGE. 3G is high speed IP data network. It used WCDMA/CDMA, TD-SCDMA.

2. P_t ↑ ⇒ CCI ↑ ⇒ System Capacity ↓, R ↓ ⇒ num of clusters ↑ ⇒ Cap ↑

3. $S/I = S / \sum_{i=1}^{N_I} I_i$, $S/I = \frac{(D/R)^k}{N_I}$, worst case: $S/I = \frac{1}{2(Q-1)^{-4} + 2Q^{-4} + 2(Q+1)^{-4}}$

Q ↑ ⇒ S/I ↑, Q ↑ ⇒ N ↑ ⇒ C ↓ (C = MJN, JN = k)

4. BS: a land station in the land mobile service; UPL: transmission path from MT → BS; DNL: path from BS → MT; cell: network distributed over land areas; location area: a set of BS; MSC: interconnect between subscribers.

5. MSC setup/release end-to-end connection. HLR central database contains mobile phone subscribers' detail; VLR database of subscribers who roamed ano MSC.

6. handoff: transition from one BS to ano BS; location management: to achieve location update & call delivery.

7. Advantages: higher speed, relieve overcrowding, more secure/reliable

Disadvantages: higher power consumption, expensive infrastructure

8. CAC in 2G is developed for a single service environment, in 3G it should consider the QoS of both voice & data. (Topology based)

9. GGSN/SGSN Gateway/Serving GPRS support Node. GGSN: internetwork between GPRS & external packet switched net. SGSN: serve MS/UE.

MSC: route voice calls & SMS GMSC: determine which VMSC the subscriber who is being called is located at. HLR⇒5.

10. WCDMA, CDMA2000, TD-SCDMA

11. ① support greater voice & data capacity & high data transmission at low-cost ② security ③ provide localized service

12. GPRS download 85.6/64.2 kbps upload 21.4/42.8 kbps operating frequency 850, 900, 1800, 1900 MHz bandwidth 25~75MHz

WCDMA 384kbps HSDPA 3.6/7.2 Mbps, 850MHz, 1800~2100MHz

13. FDMA (1G), TDMA (2G), CDMA (3G), SDMA, PDMA

14. wireless IntServ & wireless DiffServ.

Chapter 5 Future Technologies

1. ① virtualization SDN & NFV ② IoT & IoE ③ cognitive network

Chapter 6 Mobility Management

1. ① create neighbor list ② signal detection ③ handover

2. In terrestrial networks the source and the target cells may be served from two different cells sites or from one and the same cell site. Such a handover is called inter-cell handover. If the source and the target are one and the same cell ⇒ intra-cell

3. MCHO ⇒ Mobile controlled handover, NCHO ⇒ network controlled handover, MAHO ⇒ mobile phone assisted handover.

4. Advantages for hard handover: ① at any moment in time one call used only one channel ② hardware is simpler & cheaper

Disadvantages for hard handover: If a handover fails that the call may be terminated abnormally.

Advantages for soft handover: chance of call terminated abnormally is much lower. Disadvantages: expensive cost/hardware.

5. It's a lossless & fast handoff scheme that can handle relatively frequent handoffs & satisfies QoS requirements.

6. Fluid flow model $\frac{dX(t)}{dt} = \begin{cases} r_i & \text{if } X(t) > 0 \\ \max(r_i, 0) & \text{if } X(t) = 0 \end{cases}$.

7. If user moves quickly, his handoff rate should be relatively high. If a user is stable, handoff rate is low.

8. The purpose of inter-cell handover is to maintain the cell as the subscriber is moving out of the area covered by the source cell and entering the area of the target cell. The purpose of intra-cell handover is to change one channel, which may be interferred or fading with a new clearer or less fading channel.

9. $D_{inter} = \left(\frac{\sum_{i=1}^{N_1} \sum_{j=N_1+1}^{N_1+N_2} (\vec{x}_i - \vec{x}_j)^2}{N_1 N_2}\right)^{1/2}$ $D_{intra} = \left(\frac{\sum_{i=1}^{N_1+N_2} \sum_{j=1}^{N_1+N_2} (\vec{x}_i - \vec{x}_j)^2}{(N_1+N_2)(N_1+N_2-1)}\right)^{1/2}$

10. After splitting a cell to several smaller cells, the handoff rate should increase.

11. A presentation layer/interface runs on client, and a data layer runs on server.

12. ① distance $C_{R} = M = 1 + \frac{1}{2}(k^2 - k)$, $C_{u,av} \le \frac{V_{av}}{k}$ ② time $C_{u,av} = 1/t = \frac{V_{max}}{k}$ ③ movement $C_{u,av} = \frac{V_{av}}{k} \le \frac{V_{max}}{k}$

$C_{dist} \le C_{mov} \le C_{time}$

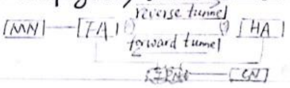
13. Forward Pointer-Based Routing Scheme ① tree formation ② mobility management ③ routing

Chapter 7 Mobile IP

1. If my computer is hosting a server, its IP should stay the same over time. In this example, I need a permanent IP.

2. MN = mobile node, HA = home agent, FA = foreign agent, CN = corresponding node, CoA = care-of address.

3. A reverse tunnel is a tunnel that starts at the MN's CoA and terminates at HA. It takes place when an intermediate router checks for a topologically correct source address.

4. 

5. MN initiates registration. When a mn find outs that its access point changes, it needs to register. UDP TTL.

6. To save resource when the UDP packet including release message is not transmitted to former FA correctly.

7. MT uses agent advertisements to determine their current point of attachment to the Internet or to an organization network.

8. Request forwarding services when visiting a foreign network. Inform their home agent of their current care-of address.

9. UDP packet loss, run out of resource.

10. Transport layer TCP/UDP; Network layer IP; Link layer: Ethernet header & trailer, frame.

11. When an intermediate router might want to check for a topologically correct source address.

12. set up a reverse tunnel from MN's CoA to HA.

13. With reverse tunneling, we can ensure a topologically correct source address for the IP data packet.

Chapter 8 IEEE 802.11 WLAN

1. DCF = distributed coordination function, PCF = point coordination function. DIFS = DCF interframe space, SIFS = Short interframe space, PIFS = PCF interframe space

2. DCF has a carriersense mechanism that exchanges for RTS & CTS frames between source & destination stations during the intervals.

3. IEEE802.11e is an approved amendment to IEEE802.11.
EDCA = enhanced distributed channel access, with EDCA, high-priority traffic has a higher chance of being sent than low-priority.
HCF = hybrid coordination function.

4. Ad-hoc networking refers to a system of network elements that combine to form a networking requiring little or no planning.

5. Infrastructure STA & AP. ESS. Ad-hoc STA IBSS.

6. L1 & L2 physical layer & data link layer.

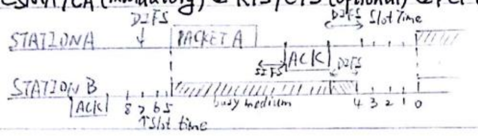
7. LLC = logical link control, MAC = media access control, PLCP = physical layer convergence protocal, PMD = physical media dependent

8. IR is more private than RF wireless but cannot pass through walls. It's not suitable for transmission between rooms.

9. 802.11 DSSS & FHSS, 802.11a OFDM, 802.11b DSSS
802.11g DSSS & OFDM 802.11n/ac MIMO-OFDM

10. 802.11e modify MAC layer to implement QoS enhancement. EDCA

11. ① CSMA/CA (mandatory) ② RTS/CTS (optional) ③ PCF (opt)

12. 

13. A 802.11 client starts a multicast by sending multicast packets in 802.11 unicast frames directed to only the access point. Then AP broadcasts this frame as a multicast frame.

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

15. There's no QoS guarantee in 802.11 DCF and part of it in PCF. In 802.11e, EDCA, HCF enhanced DCF & PCF. (HCCA)

16. ATSF keeps the timers for all stations in the same BSS synced.

17. Timing sync is achieved by stations periodically exchanging timing info. BSS: Ap sends; IBSS: competes to send.

18. Each station maintains a TSF timer. Adopt receiving if later than self.

19. No Some previous work based on asynchronous clock. MASP/MTSP.

20. MT has limited power resource so we need power management.

21. Infra ① Allow idle station to sleep ② AP buffer packets for sleeping nodes ③ Wake up periodically AdHoc ① complete frame-handshake before sleep ② wake up for every Beacon transmission

22. During ATIM window, clients with no incoming/outgoing frames can reenter sleep mode during data-transmission window. DTIM: delivery Traffic Indication Message.

23. in 802.11. mobile device is entirely in charge of when to handoff and which AP to handoff with four messages.

24. When the size of a message is larger than MTU.

25. Frame control; Duration/ID; Address 1-4; Sequence Control; QoS Control; HT control.

26. src MT, src router, dst router, dst MT.

27. 802.11a uses OFDM, 5GHz, faster. 802.11(b) DSSS, 2.4GHz.

28. WEP = wired equivalent privacy. provide data confidentiality.

29. stream cipher RC4 for confidentiality; CRC-32 checksum for integrity. Open system / Shared key authentication.

30. 64-bit WEP key ⇒ 128/156/258-bit WEP key (4x26+24 IV)

31. Open Sys: client need not provide credentials, authentic with AP & associate; Shared key: ① client sends request ② AP replies clear-text challenge ③ client encrypts sends ④ AP decrypts match reply.

32. WEP. 24-bit IV, 50% prob the same IV will repeat after 5000 packets. Captive portal merely require user pass an SSL encrpted page which is exploitable.

33. Active scanning: client transmits a probe & listen for probe response; passive scanning: client listens for beacons.

34. in 802.11e with HCF & EDCA.

35. Throughput $\leq \frac{RWIN}{RTT}$, RWIN ⇒ TCP receive window

Chapter 9 WiMAX

1. WiMAX base on IEEE 802.16, provides multiple physical layer (PHY) and media access control (MAC)

2. IEEE 802.16 10~66GHz, 802.16a 2~11 GHz; orthogonal frequency-division multiple access (SOFDMA) 802.16e; OFDM 802.16d. MIMO in 802.16e.

3. OFDM is a FDM scheme used a digital multi-carrier modulation method. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data stream

Chapter 10 Ad Hoc Networks

1. Ad-hoc combine network elements to form requiring little/no planning

2. A successful transmission occurs when a node falls inside the transmission range of its intended transmitter and falls outside the interference ranges of other non-intended transmitters.

3. exclusion region quantizes the amount of spacial resources occupied by a link.

4. Hidden terminal: when a node is visible from a AP, but not from other nodes communicating with that AP.
Exposed terminal: when a node is prevented from sending packets to other nodes because of a neighboring transmitter.

Chapter 11 Security

1. WEP encryption/authentication. Shared key authentication: ① client send authentication request ② AP replies clear-text challenge ③ client encrypts text with WEP key, reply. ④ AP decrypt response, match, reply.
2. ① initialization, only 802.1x traffic is allowed. ② Initiation, EAP-request ③ Negotiation (EAP), EAP method ④ Authentication EAP-Success/failure message.
3. WEP can not satisfy users' security requirement. WAPI consists WAI & WPI, ASU, STA. WPI uses symmetric cryptography to encrypt MSDU on MAC layer.
IEEE802.11i, RSN, TKIP, CCMP, WRAP.

Chapter 12 Bluetooth and RFID

1. Bluetooth 4.0 includes Classic Bluetooth, high speed & low energy.
2. ① active ② sniff ③ hold ④ park
3. ① reader, bidirectional communication between tag & reader. receive control commands from host sys.
② tag, contains an integrated circuit & an antenna, can be passive, active or battery assisted passive.
4. ① integrated circuit ② antenna design ③ encapsulation technology ④ tag application ⑤ standardization.
5. ① real-time location ② mobile payment (NFC) ③ anti-counterfeit

Chapter 13 Wireless Sensor Networks

1. BS is a component of WSN with much more computational, energy and communication resources. It acts like a gateway between sensor & end users. Star network / multi-hop wireless mesh net.
2. controller & external memory & power source & sensors
3. smart dust; a line in the sand; remote health monitoring; environmental
4. manual deployment; random deployment (health/environmental)
5. ZigBee based on IEEE802.15.4 250 kbps, 10m range.
6. battery life & bandwidth & broad in scale
7 solar cell, fuel cell

Chapter 14 Internet of Things

1. ① ultra wideband ② software defined radio ③ RFID
2. ① more secure ② high processing gain ③ high multi-path resolving power
3. bluetooth: handle lots of data, high power consumption; BLE: low power consumption
4. A CR monitors its own performance continuously to determine RF environment and then sets to deliver required QoS subjects to a use's req.
5. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer-assisted rehabilition or nearly dectection of medical condition. Healthcare

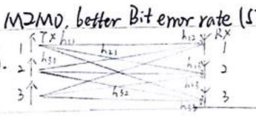
Chapter 15 Software-Defined Networking.

1. An architecture purporting to be dynamic, manageable for today's application seeking to be suitable
2. Decouple network control and forwarding functions, enable network control programmable abstract underlying to application
3. SDMN, SD-WAN, SD-LAN, security using SDN paradigm
4. ① change traffic pattern dynamically ② offer better cloud service

Chapter 16.17 & 18 Intelligent Robots, Cars and Quadrotors

1. CPU, memory, electromotor, camera, sensors (gravity), network module
2. ① real-time indoor mapping ② cooperative estimation & control
③ Autopilot (Tesla, Google, Baidu) Tesla autopilot requires operators to monitor the vehicle at all times. It achieves adaptive cruise control, autopark/summon and autosteer. It uses reward looking side camera, wide forward camera, main forward camera, narrow forward camera, radar, forward looking side camera, ultrasonics, and rear view camera to sensor the environment.

Chapter 19 MIMO

1. SISO: only one antenna as transmitter/receiver. MIMO: multiple MIMO, better Bit error rate (STBC), higher data rate.
2. 

3. Space diversity: same data different path; space multiplexing: different data different antennas.
4. MIMO-OFDM (802.11n) MU-MIMO (2ST-MASCOT) MIMO (3GPP)

Chapter 21 & 22 Bitcoin and Graphic Code

1. bitcoin protocol's features protect it against unauthorized spending, double spending, race attack, history modification and deanonymisation of clients
2. Consits of black squares arranged in a square grid on white bg. can be processed by Reed-Solomon error correction until appropriately interpreted.