Wireless Communication and Mobile Internet Midterm Exam

Zhaorun Han 5140309504

Overview of Wireless Networks (Chapter 1)

- Describe the history and development of wireless communication networks.
In ancient times; fireworks and semaphore. 1831: Faraday invented Electromagnetic induction. 1873: Maxwell proposed the theory of electromagnetic field. 1895: Marconi invented radio. 1988: set-up of the first Digital cellular system in Europe. 1997: The first version of the wireless LAN is released. Today: 4G. 5G. Wifi ...
- List the fundational techniques used in Wireless communication networks.
1) Cellular network. 2) Mobile management 3) Mobile IP. 4) Wi-Fi 5) Wi-MAX. 6). Self-organizing network. 7) Wireless network security. 8) Wireless Personal Area Network. 9) Sensor network. 10) IOT. 11). SDN.

Radio Propagation (Chapter 2)

- List the difference between the wired and wireless media.
Wired media: reliable guidance connection. restricted data rate.
Wireless media: propagated through air; unreliable connection. low bandwidth. broadcast, non-boot connection.
- Explain the difference between the licensed and unlicensed band.
Licensed band must be used with license, nobody can use it freely without permission. It includes frequency band used by cellular network, PCS, WLAN. LMDS. IR. Unlicensed band can be used freely, which includes ISM, U-NII and so on.
- List at least three factors that affect radio propagation.
1). distance. 2) frequency attenuation. 3) shadow. 4) reflection at the big obstacle. 5) scattering at small obstacle
- 1) Reflection and transmission: happens when the size of the obstacle is greater than the wavelength of the radio wave; 2) Diffraction: happens when the propagation route between the transmitter and the receiver is blocked by sharpe edge; 3) Scattering: happens when the size of obstacles is smalled than the wavelength and the density is huge.
- 1) Reflection happens on the surface of earth, buildings and walls, and is not the main mechanism on outdoor environments. 2) Diffraction happens on the edge of buildings or walls or shadow, and is weak indoors. 3) Scattering happens on rough surfaces. small objects, so on, e.g. leaves, lamp posts.
- $\frac{P_r}{P_t} = G_t G_r \frac{h_b^2 h_m^2}{d^4}$ (Two-way mode)
- free space modeling: $L_p[dB] = 32.45 + 20\lg f_c[MHz] + 20\lg d[km]$
$10\lg P_r = 10\lg P_0 - 20\lg d$ $\tau = \frac{D}{C} = 3d\,ns$; Two-ray model: $L_p = 10\lg G_t G_r \frac{h_b^2 h_m^2}{d^4}$
$10\lg P_r = 10\lg P_0 - 40\lg d$. $\tau = \frac{D}{C} = 3d\,ns$
- Explain the concept and effect of shadowing/slow fading on pass loss
In mobile communication, the signal strength received from the same distance from the transmitter is different. The change of strength caused by location is called shadowing/slow fading. $L_p = L_0 + 10d\lg D + X$. X is caused by slow fading.
- Compute the fade margin to overcome the shadowing effect.
$$R = \frac{G_A^2 \cdot P_t}{\frac{E_b}{N_0} \cdot F \cdot KT_0 f_b \cdot L_A^2 \cdot L_S}$$
- Compute the pass loss based on different models for marco/micro-cell system.
1) marco-cell: $L_p(d) = \begin{cases} A + B\lg d & \text{city} \\ A + B\lg d - C & \text{suburbs} \\ A + B\lg d - D & \text{open} \end{cases}$
$A = 69.55 + 26.16\lg f_c - 13.82\lg h_b - a(h_m)$
$B = 44.9 - 6.55\lg h_b$ $C = 5.4 + 2\lg[\frac{f_c}{28}]^2$
$D = 40.94 + 4.78(\lg f_c)^2 - 18.33\lg f_c$
2) micro-cell: W-I model: $L = 42.6 + 26\log d + 20\log f$.
- Small-scale fading is the rapid change in the received wireless signal in short time interval of small range. Multipath fading: superposition of signals received from different paths. Doppler: Caused by the mobility of the terminal toward or away from the base station.
- Rayleigh distribution: $f(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}$, $x > 0$.
Ricean distribution, $P(R) = \frac{R}{\sigma^2} \exp(-\frac{R^2+A^2}{2\sigma^2}) I_0(\frac{RA}{\sigma^2})$
- Doppler shift and spectrum: The wavelength of the object radiation changes due to the relative movement of the wave source and the observer. $v(t) = \frac{Vf}{C}\cos\theta(t)$.
- 1) Rayleigh distribution: signaling strength: $f_S(s) = \frac{1}{p}\exp(-\frac{s}{p})$, $s \geq 0$
Ricean distribution: signaling strength: $f_S(s) = \frac{1}{p}\exp(-\frac{p^2+s}{2p}) I_0(\frac{p\sqrt{2s}}{p})$, $s \geq 0$
desired cell radius: $P_R = \frac{r^2}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}}$.
- Compute the level of crossing rate and average fade duration
Rayleigh distribution: $LCR = \sqrt{2\pi} f_d \rho e^{-\rho^2}$ $\rho = \frac{R_{thresh}}{R_{rms}}$
$AFD = \frac{e^{\rho^2}-1}{\rho f_d \sqrt{2\pi}}$

Cellular System (Chapter 3 and 4)

- TDMA → EDGE; GSM → GPRS → EDGE; GSM → GPRS → TD-SCDMA; PDC → WCDMA; cdmaOne → CDMA2000 1X → CDMA2000 3X
2G 2.5G 3G
- $C = MJN$. $P_r = P_0 (\frac{d}{d_0})^{-k}$. As the transmitting power grows, the cell radius also increases, and the system capacity decreases.
- $Q = \sqrt{3N} = (6\cdot\frac{S}{I})^{1/k}$, $C = MJN \Rightarrow \sqrt{\frac{3C}{MJ}} = (6\cdot\frac{S}{I})^{1/k}$, $R = \frac{(6\cdot\frac{S}{I})^{2/k}\cdot\sqrt{MJ}}{\sqrt{3C}}$
- base stations: a land station in the land mobile service; Uplink: the portion of a feeder link used for the transmission of signals from a terminal to the network core; downlink: a connection from terminal data communication equipment to data terminal equipment; Cell: 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, responsible for routing service and SMS as well as other services.
- network structure: base station subsystem, network and switching subsystem, core network. OSS. VLR and HLR locate in NSS. VLR: database of the subscribers who have roamed into the jurisdiction of the MSC which it serves. HLR: a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network.
- Handoff management: Ensuring that a mobile user remains connected while moving from one location to another. Location management: search, update Location info.
- Advantages of 3G over 2G: global multimedia mobile communications 1) can achieve global roaming. 2) can achieve high-speed data transmission and broadband multimedia services.
- purpose: allocating channel resource to users effectively.
Difference: CDMA utilizes the effect of statistical multiplexing without the complex radio channel allocation or reallocation that is required in TDMA.
- SSGN: Detunnel GTP packets from the GGSN; Tunnel IP packets toward the GGSN; GGSN: converting the packets coming from SGSN into appropriate packet data protocol format; subscriber screening. MSC: routing voice calls and SMS as well as other services. GMSC: obtaining the current roaming number of the called MS from the HLR query and routing based on this information. HLR: store details of every SIM card issued by the mobile phone operator.
- List three standards for 3G wireless system: TD-SCDMA, WCDMA, CDMA2000.
- key features: 1). Can achieve global roaming 2) can achieve high-speed data transmission and broadband multimedia services.
- GPRS: transmission rate: 172 Kbps. bandwidth: 200KHz. GSM-850: 824-849 MHz (uplink). 869-894 MHz (downlink) 3G (WCDMA): 3.8Mcps bandwidth: 5MHz. 1940~1955MHz (uplink). 2130~2145MHz (downlink)
- Application scenarios: Broadband Internet access. Video call. Mobile business
- Explain a possible architecture of All-IP wireless networks
IntServ-based architecture./Diffserv-based architecture/Integrated

Future Technologies (Chapter 5)

- List at least three techniques that will be used in future mobile communication: mobile cloud computing. mobile web page. mobile access

Mobility Management (Chapter 6).

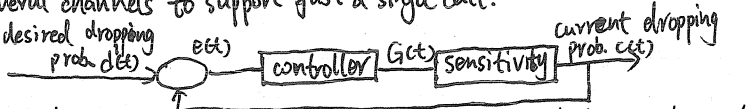
- Explain the different phases of handoff operation.

Handoff initiation: detecting the signal strength to decide whether the handoff is happening. Handoff decision: making decisions according to different handoff scheme / matrices.

- Explain intra- and inter-switch handoff.

intra-switch handoff: handoff happens from one cell to another under the same MSC. inter-switch handoff: handoff happens from one cell to another under different MSC.

- MCHO: handoff decisions are made by the network based on the measurements of the MSs at a number of BSs. NCHO: the MS makes measurements and the network makes the decision. MAHO: each MS is completely in control of the handoff process.
- 1) Hard handoffs: Advantages: at any moment in time one call uses only one channel; it is cheaper and simpler for hardwares. Disadvantages: if a handoff fails the call may be temporarily disrupted. 2) Soft Handoffs: Advantages: during handoff execution mobile does not lose contact with the system; Ping Ponging is eliminated; More control may be given. Dis: it uses several channels to support just a single call.



feed-back-based handoff makes use of information fed back from the mobile. Feedback interval is the inverse of data rate.

- straight-line: moving at a random speed v along the straight line from a random starting point S to a random destination point D. fluid flow: mobile travels in direction uniformly distributed over [0, 2π).
- Compute the handoff rate based on different mobility nodes.

$$H_{kj}(v) = \begin{cases} \frac{2}{\pi} M_1(T_{kj}^{(v)})\, v & \text{if } k \neq j \\ \frac{2}{\pi} M_1(T_{kj}^{(v)})\, v & \text{if } k = j. \end{cases}$$

- Compute intra-cluster and inter-cluster handoff rate.

$H_{total} = N \cdot M_{cell} \cdot \beta 2\lambda$. $H_{inter\text{-}cluster} = M_{cluster} \cdot \beta 2\lambda$

$H_{intra\text{-}cluster} = (N \times M_{cell} - M_{cluster}) \times \beta 2\lambda$

- Evaluate the effect of cell splitting on handoff rate.

Cell splitting increases the handoff rate because the cells are smaller and a mobile is likely to cross cell boundaries more often.

- Describe the two-tier network architecture.

Two-tier network is composed of core network and access network.

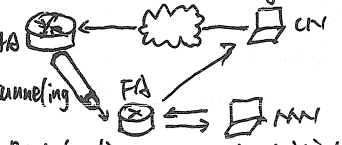
- Location update: Mobile continously detect the coding of the routing area. Once it detects changes on code, it will send Location update request to the network. Service delivery: monitor for strongest signal, request for connection, paging, call accepted, ongoing call, handoff.
- time-based: advantage: not dependant on Location Areas, and lower paging cost. disadvantage: if the user is stationary, unnecessary updates would be performed. Movement-based: advantage: simplicity. disadvantage: when user travels around the boundary, unnecessary updates may happen. Distance-based: simplicity, disadvantage: if user crosses the boundary very frequently, unnecessary location updates occur.
- 1) Sending a location update message to gateways to inform gateways to update location database (2). With pointer forwarding, Location handoff only involves setting up a forwarding pointer between two neighboring MRs without trigger Location update event.

Mobile IP (Chapter 7)

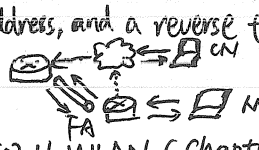
- Explain why would you want to have a permanet IP address.

Because it's convenient to share resources and get access to.

- MN: nodes where the position changes frequently. HA: a router on MN's home network which stores info about the MN. FA: a router on foreign link which stores info about the MN. CoA: An IP adress associated with the MN when it switches to a foreign link. CN: the communication object of the MN.
- with reverse tunneling: CN sends IP packets to HA, HA encapsulates the packet and sends it to FA through tunnel; then MN get it from FA; MN sends packets to CN through standard IP routing. Without: MN send packets to FA, FA encapsulates them and send to HA through reverse tunneling.



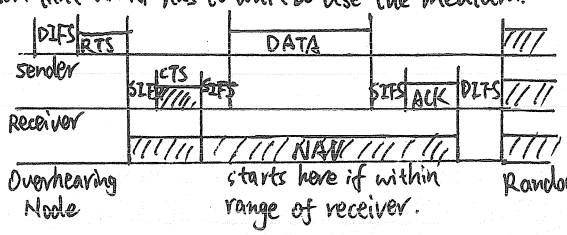
- Registration process is initiated by MN. MN sends registration request to FA. FA processes with the request and send it to HA. HA sends response to FA. FA then sends it back to MN.
- Because the MN may move to a new place and the MN needs to know whether it should connect to a new link.
- Type: indicating that this is the Mobility Agent Advertisement Extension; Length: the length in octets of the extension; Sequence number: the number of Agent Advertisement messages; Reg Lifetime the longest time that this agent is willing to accept for requests.
- Type: indicating whether this is a registration request or reply. Lifetime: the number of seconds remaining before the registration is considered expired. Home address: home address. Home agent: IP of HA. Care-of address: the mobile's CoA.
- If the HA judges the IP is invalid or the FA doesn't have enough resources, the registration may fail.
- IP in IP: encapsulates one IP packet in another IP packet. Chosen when simplicity is required. Minimal Encapsulation: new IP header is inserted into the packect and inner IP header is removed. Chosen when shorter packet is required. GRE: encapsulates one protocol packet into another protocol packet. Chosen when different protocols are used.
- A traverse reverse tunnel is a tunnel that starts at the care-of address and terminates at the home agent.
- Because intermediate routers might check for a topologically correct source address, and a reverse tunnel is needed then.



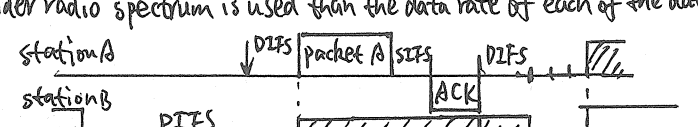
→ with reverse tunneling

IEEE 802.11 WLAN (Chapter 8)

- DCF: a MAC technique which employs a CSMA/CA algorithm. PCF: a Media Access Control technique used in IEEE 802.11. DIFS: the time duration that a medium is idle before it can be used. SIFS: the time duration that medium is idle before it gets ACK. PIFS: the time duration that an AP has to wait to use the medium.



- 802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of QoS enhancements for WLAN applications through modifications to the MAC layer. EDCA: high-priority traffic has a higher chance of being sent than low-priority traffic. HCF: enhances the DCF and the PCF through a new hybrid coordination function.
- Wi-Fi networks in infrastructure mode are generally created by Wi-Fi routers, while ad-hoc networks are usually short-lived networks created by a laptop or other device.
- Infrastructure mode: Access points connect mobiles into wired network. handoff: mobile changes AP providing connection into wired network. Ad-hoc mode: no APs. nodes can only transmit to other nodes within link coverage. nodes organize themselves into a network.
- 802.11 standard locates in the link layer in the TCP/IP(OSI) stack.
- LLC: provides multiplexing mechanisms, flow control and ARQ error management mechanisms. MAC: manages communications between 802.11 stations (RNC/AP). PLCP: prepares MAC protocol data units for transmission and minimizes the dependence of MAC on PMD. PMD: provides transmission and reception of Physical layer data units between two stations.
- Infrared: uses IR diodes, diffuse light, multiple reflections. Advantages: simple, cheap, available in many mobile devices. no license needed. simple shielding possible. disadvantage: interference by light, heat sources. low BW. Radio: use the license-free ISM band at 2.4GHz. Advantages: experience from wireless WAN and mobile phones can be used. coverage of lager areas. Disadvantages: very limited license-free frequency bands. shielding more difficult.
- 802.11: FHSS. DSSS. 802.11a: OFDM. 802.11b: data rate extension of 802.11 DSSS. 802.11g: OFDM in the 2.4GHz band (like 802.11b)
- ACK packets have priority over RTS or data ones. This is done by affecting to each packet type a certain Inter Frame Spacing before which a packet cannot be transmitted, once the channel becomes idle.
- FDMA: provides different frequency bands to different data-streams. TDMA: provides different time-slots to different data-streams. CDMA: wider radio spectrum is used than the data rate of each of the data-stream



- A unicast transmission sends IP packets to a single recipient on a network. A multicast transmission sends IP packets to a group of hosts.
- Sender needs to tell other nodes in the network how long it will use the medium. Receiver needs to tell other nodes the transmitting is still going on while sending ACK or processing the packets.
- QoS is not supported in 802.11, but is supported in 802.11e, and only applies to network in infrastructure mode, by using a PCF in which a coordinator polls the connected nodes, giving them an opportunity to transmit.
- Sychronization is needed for frequency hopping and power saving.
- Time ~~Sych~~ Synchronization in 802.11 is achieved by stations periodically exchanging timing information through beacon frames. In (infra) BSS, the AP sends the TSF information in the beacons. In IBSS (ad-hoc), each station competes to send the beacon.
- Because the synchronization in PLCP preamble is used for one particular transmission. Beacons are used for time sychronization in hopping.
- 802.11's synchronization mechanism can work in a multi-hop environment but not well, because nodes with faster clocks cannot always successfully send out beacon frames.
- 1) Mobile devices are battery powered 2) Enhancement of battery life enhances network life 3) Idle receive state dominates LAN adapter power consumption over time.
- Infra-mode: allow idle station to go to sleep. AP buffers packets for sleeping nodes. Power saving stations wake up periodically, etc. Ad hoc mode: Before a station goes to sleep has to complete a frame-handshake with "any" other station with power management bit set, etc.
- DTIM: time when multicast frames are to be delivered by AP and is determined by AP. ATIM is the time when other stations announce if they have buffered packets for a sleeping station.
- The mobile device is entirely in charge of deciding when to hand off and to which access point it wished to hand off.
- Larger packets are more susceptible to corruption by radio interference than smaller ones, so a node may increase fragmentation to reduce retransmissions in conditions of heavy interference.
- Protocol version. Type. Subtype. ToDs. FromDS. Retry. More fragments. power management. More Data. WEP. Order.
- Host ↔ Host. 2 addresses. Station ↔ AP ↔ Host. 3 addresses Station 1 ↔ AP1 ↔ AP2 ↔ Station 2. 4 addresses (Two APs locate in different wireless networks).
- 802.11a is an amendment to 802.11 WLAN that defined requirements for an OFDM communication system. 802.11b is an amendment to 802.11 that extends throughput up to 11 Mbs using the same 2.4GHz band.
- WEP's intention was to provide data confidentiality comparable to that of a traditional wired network.
- WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity.
- Modification: when decryption, check CRC code before XOR keystream with encrypted data to check integrity. It will cause some errors because the CRC checksum is also encrypted in the encryption.
- 1) Authentication request sent to AP. 2) AP sends challenge text 3) clients encrypts challenge text and send it back AP. 4) AP decrypts and if correct, authenticates client. 5) Client connects to network
- WEP: Attacker can get encrypted challeng text and hence get WEP shared keys, which is the main weakness. MAC filtering: authentication is based on MAC address, more safe. captive portal: MAC address and IP are required. which can be spoofed by other machines.
- In Passive Scanning, WLAN station moves to each channel as per channel list and waits for beacon frames. In active scanning, stations find out network rather than waiting for network to announce its availability
- 802.11e uses WMM to ensure that high-priority packets have priority to send, so as to ensure that voice, video and other applications in the wireless network have better quality.
- Throughput can be obtained by: $S = \frac{P_s P_{tr} E[P]}{(1-P_{tr})\sigma + P_{tr}P_s T_s + P_{tr}(1-P_s)T_c}$

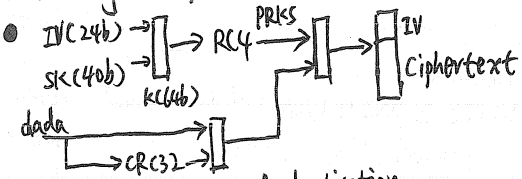
WiMAX (Chapter 9)

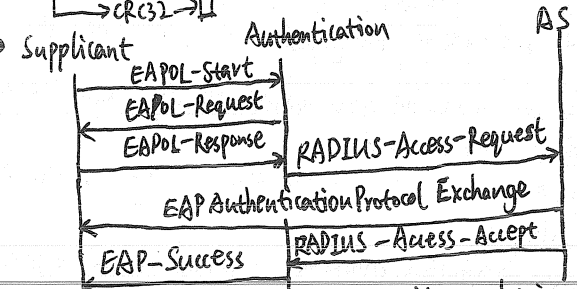
- WiMAX provides carrier-class multimedia communications services with better scalability and stability.
- IEEE 802.16 standard physical layer defines the duplex mode, frame length, modulation and coding technology. 4 PHY implementations, OFDM, etc.
- In permissible band, OFDM supports time division duplex and frequency division duplex, BPSK, QPSK, 16QAM, 64QAM; In licence-free band, only supports time division duplex, BPSK, QPSK, 16QAM; 64QAM optional

Ad Hoc Networks (Chapter 10).

- In frastructure networks, every wireless device on the network links up with a central AP. In Ad-hoc network, wireless devices can connect directly with each other.
- In protocol Interference model, if a node falls in the interference range of a ~~non-trans~~ non-intended transmitter, then this node is considered to be interfered and thus cannot receive correctly from its intended transmitter.
- An exclusion region is a region around each receiver such that no interferers exist inside this region.
- For the protocol model, both upper bound and lower bound of the transport capacity is $\Theta(W\sqrt{n})$, which is ~~related to~~ W and n.
- Hidden terminal: a node is visible from a AP, but not from other nodes communicating with that AP. Exposed terminal: a node is prevented from sending packets to other nodes because of a neighboring transmitter.

Security (Chapter 11)

- 

- 

- In view of the weakness of WEP security mechanism, WAP1 uses WA1 to implement user's authentication. IEEE802.11i introduces 802.1X into WLAN security mechanism, TKIP and CCMP as well.

Bluetooth and RFID (Chapter 12)

- Bluetooth 4.0: transmission rate unchanged, but enhance the transmission distance, reduce energy consumption by 90%.
- List the working state in Bluetooth: Connection / Intermediate / idle state.
- List hardware devices of RFID and describe their functions.

Reader: perform two-way communication with electronic tag, while receiving control commands from the host system. (Radio Interface, Cabl, antenna)

Electronic tag: data carrier of RFID system, communicate with reader

- List some key techniques in RFID.

Chip technique. Packaging technique. Tag application technique.

- Three applications of RFID in IOT: Logistics field. Retail field. asset management.

Wireless Sensor Networks (Chapter 13).

- base station: gateway between sensor nodes and the end user. Monitoring station: manage on and control sensor nodes. Sensor network: data collector. aggregation nodes: reduce the amount of nw traffic.
- Sensor node: Controller: perform tasks, process data and control the functionality of other components. Transceiver: transmitter and receiver. External memory: store data and processing program. Power source: provide electricity. Sensors: capture data from their environment.
- Smart dust. Remote health testing. Environment inspection system.
- some node deployment algorithm: Incremental NDA. Artificial-potencial-Field-based NDA. Grid-Partitioning-based NDA.
- data rate: 10/kbs - 1Mbs. range: 10 ~ 500 meters range.
- Energy-accuracy tradeoff. Communication-computation Trade-off Energy-Latency trade-off. Energy-throughput trade-off. Utility-Lifetime Tradeoff.
- Electricity (batteries). heat. solar energy. Radioactive power sources. chemical energy.

Internet of Things (Chapter 14)

- List three key techniques in IOT: Ultra wideband wireless transmission technology. Software. radio. RFID. Cognitive Radio.
- Features of ultra Wideband: safety. High processing gain. Multipath resolution ability. high transmission rate. large system capacity. Anti-interference ability. Low power consumption. Accurate positioning. low cost
- Differences between BLE and Bluetooth: simplified protocol stack. high transfer rate. Low power consumption.
- 1) CR cognitive ability: capture information from the wireless environment in which it operates to select the most appropriate spectrum and parameters. 2) Reconstruction ability: allows the CR to be dynamically programmed according to the wireless environment to transmit and receive data using different wireless transmission technologies.
- Body area network: A human-centered network consisting of nw elements related to the human body. Application: medical care. wireless access. Navigation positioning. Personal multimedia entertainment

Software-Defined Networking (Chapter 15)

- SDN is a programmable network architecture.
- Working principles of SDN: Decoupling of controller and data planes. Logically centralized control. Exposure of abstract network resources and state to external applications.
- Applications: SDWAN. SD-WAN. SD-LAN. Security using the SDN paradigm.
- 1) Seperate the network control and physical network topologically, which get rid of hardware restrictions on the network architecture. 2) SDN makes the network data control and management more efficient and stable.

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

- motion system. sensor system. processing system. communication system.
- Applications: Autopilot · Environment monitoring. unmanned search.

MIMO (chapter 19)

- Differences: There is only one transmission path between the transmitter and the receiver of the SISO system, while there are multiple paths in MIMO system.
- Channel model of MIMO system: $y = Hx + n$. $x = [x_1\ x_2 \cdots x_{N_T}]^T$. $y = [y_1\ y_2 \cdots y_{N_R}]^T$. $n = [n_1\ n_2 \cdots n_{N_R}]^T$. $H = \begin{bmatrix} h_{11} & \cdots & h_{1N_T} \\ h_{21} & \cdots & h_{2N_T} \\ h_{N_R1} & \cdots & h_{N_RN_T} \end{bmatrix}$
- Space-diversity: multiple antennas transmit the same info but in different encoding manners, to decrease error rate. Space-multiplexing: The data stream is divided into multiple sub-streams.
- Distributed MIMO. Virtual MIMO. Multi-user MIMO

Bitcoin and Graphic code (Chapter 21 and 22)

- It's relatively safe to use bitcoins in transaction.
- Components of QR code: coding area and function graphics.