WIRELESS COMMUNICATIONS AND MOBILE INTERNET MIDTERM EXAM

TEAM-02 5140309065 FENGYU DENG

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. (1) cellular system (2)mobile management (3)mobile IP (4)Wi-Fi (5)WiMAX (6) Self - organizing network (7)Wireless Network Safety (8) Wireless Personal Area Network (9) Sensor network (10)Internet of Things (11)Software defined network

2 Radio Propagation

1. Wiredtransmit by lineThbig bandwidthThlow interferenceThstable environmentWirelesstransmit by airThless bandwidthThhigher interferenceThunstable environment.

2. Licensed :operate within the portion of the radio spectrum designated by the FCC. Unlicensed :set aside by the FCC for industrial, scientific or medical (ISM) applications.

3. space, atmosphere, ionization.

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: many reflection, less diffraction and scattering; Outdoor: Reflected by air and ground, scattered at the edge of building.

6. determined by the expression where is called the path loss exponent. The wireless radio channel puts fundamental limitations to the performance of wireless communications systems.

7. $L_p = L_0 + 10\alpha lgD + X$.

8. The shadow effect caused by the obstruction of the obstruction, the received signal strength decreased, but the field strength with the geographical changes slowly change.

9. $f_{d,n} = f_d + f_m cos\theta = \frac{v}{c} f_c cos\theta$.

10. Macro $L_p P = A + Blg(d)$.

11. multipath/small-scale fading: A propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths.

12. Rayleigh distribution is used for the envelope distribution of multipath fading received signals. Lace distribution is used to describe the envelope attenuation of the received signal.

13. $f_d = \frac{\Delta\varphi}{2\pi\Delta t} = \frac{v}{\lambda} cos\theta$.

14. The signal strength can be calculated by the Rayleigh distribution and the probability distribution function of the Rice distribution.

15. The level of crossing rate: $F(R) = \int_0^\infty rp(R,r)dr$, average fade duration: $\tau_R = \frac{P(r \leq R)}{NR}$.

3-4 Cellular System

1. 3G on the basis of 2G, using CDMA technology, the current development into three kinds of standards, CDMA2000, WCDMA, TD-SCDMA

2. Relationship: The smaller transmitting power, the smaller system capacity. The larger the cell radius, the smaller the capacity.

3. The same frequency band is used by two or more base stations that are located in relative proximity to each other.

4. The entire network coverage area is divided into cells based on the principle of frequency reuse.

5. VLR is a database, is stored in the area of the customer's incoming, outgoing calls required to retrieve the information and the user contracted business and additional business information. HLR is responsible for moving the user-managed database.

6. Handoff management: switching base stations; Location management: location update, call delivery.

7. 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 routing update is the most complex routing update. The MS switches from one SGSN area to another, and then re-connects to the new area.

10. CDMA2000, WCDMA, TD-SCDMA

11. Global roaming. high speed, fast mobility, broadband multimedia service.

12. Transmission rate: 200kb/s or higherbandwidth is biggerfrequency is higher.

13. A channel-access scheme is based on a multiplexing method, that allows several data streams or signals to share the same communication channel or physical medium. In this context. multiplexing is provided by the physical layer.

14. 3G Cellular Network.

5 Future Technologies

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

6 Mobility Management

1. (1)Monitor the signal strength changes.(2)Mobile station begin to recognize the new base station.(3)After several interaction, the new link was established.

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: The mobile station monitors the signal strength and selects the best way. MCHO: Network monitoring signal strength and turn on the switch. MAHO: Mobile station monitor signal strength, network switch.

4. Advantage: soft: the connection to the source cell is broken only when a reliable connection to the target cell has been establishe.hard:at any moment in time one call uses only one channel.disadvantage: soft: require more complex hardware in the phone; hard : ping-ponging effect may occur.

5. Monitor the signal strength changes, once exceeded the threshold, to switch.

6. Straight-line: The sequence of userfis 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. Intra: 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 :when a mobile signal becomes weak in a given cell and MTSO can not find other cell within its system to which it can transfer the call then it uses Inter system handoff.

8. Intra-switch: When the mobile signal in the given hive becomes very weak, the MTSO discovers that the other cells in the system can transmit the signal, and the MTSO uses the intra-switch; Inter-switch: MTSO can not find other replaceable cells in the system to transmit signals, so use inter-switch.

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

10. The smaller area of the cell is, the handoff frequency is higher.

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

12. Ocation update: When the mobile device is restarted or shut down, the mobile network asks for the reporting location and interrupts the time to send the location information. Service delivery: The mobile network is looking for a viable channel for the called person. If successful, the caller will send a feedback signal to terminate the 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.

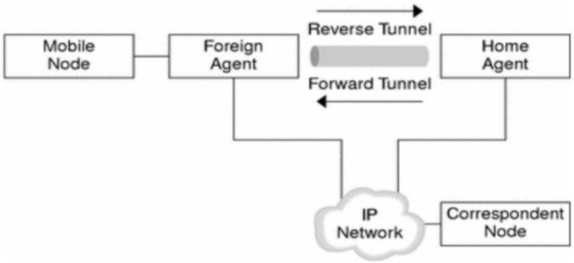
7 Mobile IP

1. Once the user's location changes, a new address is required, but most of the network data is transmitted over TCP. Changing the IP address will create a new connection accordingly, resulting in application interruption and loss of data.

2. MN:the location always change.HA:the servers of moving nodes are always for keep the location of moving nodes.FA:the servers are used to transmit the information of moving.COA:not using transmit location as the destination.CN:a object of moving nodes.

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. The limited lifetime allows the mobile node to register with its home agent using the registration request message so that its home agent can create or modify the mobility binding of the mobile node.

7. The only change to the Mobility Agent Advertisement Extension is the additional 'T' bit. A foreign agent that sets the 'T' bit MUST support the two delivery.

8. If the 'T' bit is set, the mobile node asks its home agent to accept a reverse tunnel from the care-of address. Mobile nodes using a foreign agent care-of address ask the foreign agent to reverse-tunnel its packets.

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

10. IP in IP:the data bag of IP will be baged as the payload of a new IP,the outside part of IPhead is the whole information of IP.Mixmum:the new IPhead is insert in the original IP head and the payload of original IPhead,it can decrease the quatity of extra bytes.unite server:be transport before the IP moving.

11. Every tube has a beginning and an end. The big tube, your SSH connection, started with your SSH client and ends up at the SSH server you connected to. All the smaller tubes have the same endpoints.

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.

8 IEEE 802.11 WLAN

1. PCF: a MAC technique used in WLANs. It resides in a point coordinator also known as Access Point (AP), to coordinate the communication within the network. The AP waits for PIFS duration rather than DIFS duration to grasp the channel. PIFS is less than DIFS duration and hence the point coordinator always has the priority to access the channel.

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-2005 or 802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of quality of service (QoS) enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer. With EDCA, high-priority traffic has a higher chance of being sent than low-priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic. Within the HCF, there are two methods of channel access, similar to those defined in the legacy 802.11 MAC.

4. Ad-hos:allows each device to communicate directly with each other. Infrastructure mode network:requires the use of an Access Point.

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

6. Responsible for reliable link-to-link data transfer. Including Channel access, Addressing, Frame Validation, Error Detection and Security Mechanisms.

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.

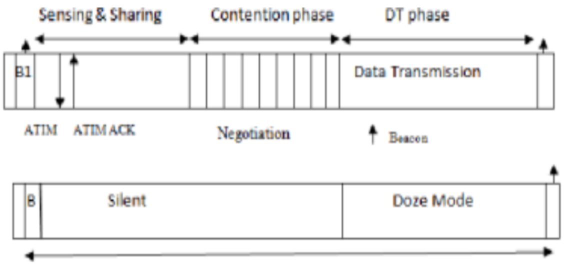
8. Infrared is used in devices for short-range communication. Radio wireless networks is used in longer range. Advantages: Simple Circuit, Low Power Consumption, Higher Security, Simple Shielding and Portable. Disadvantages: Works ONLY on Line-of-Sight (LOS) Mode, Short Range, Blocked by common materials: people, walls, etc. Low bandwidth, Speed is comparatively slow.

9. DSSS FHSS OFDM DSSS STBC

10. The802.11 defines the signal character and modulation ways.

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

12. The timing diagram:



13. Multicast is group communication where information is addressed to a group of destination computers simultaneously. Unicast transmission is the sending of messages to a single network destination identified by a unique address

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 supported in 802.11 in both modes by measuring quality of service like bit rate.

16. Timing synchronization is achieved by stations periodically exchanging timing information through beacon frames. In (infra) BSS, the AP sends the TSF information in the beacons. In Independent Basic Service Set, each station competes to send the beacon.

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

18. Frames are transmitted periodically to announce the presence of a wireless LAN not PLCP.

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. The power cannot be inefficient to the mobile devices, so 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 is a management frame with no frame body. When a SEA receives ATIM, the formally dozing station must begin the process of retrieving buffered frame from the stations that transmit the ATIM. DTIM beacon is identical to the ordinary beacon.

23. Mobility Management offers seamless handovers when moving from one network to another.

24. IP fragmentation is an IP process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller MTU than the original datagram size.

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

26. The distinction to understand is that while an 802.11 device is transmitting to a receiving device, either one (or both) of these devices may not be the actual source or destination of the L2 traffic.

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. The WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently, WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys.

31. In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently, WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys. In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake (1). The client sends an authentication request to the Access Point. (2). The Access Point replies with a clear-text challenge. (3). The client encrypts the challenge-text using the configured WEP key and sends it back in another authentication request. (4). The Access Point decrypts the response. If this matches the challenge text, the Access Point sends back a positive reply.

32. Active scanning occurs when the client changes its IEEE 802.11 radio to the channel being scanned, broadcasts a probe request. Passive scanning is performed by simply changing the clients IEEE 802.11 radio to the channel being scanned and waiting for a periodic beacon from any APs on that channel.

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.

9 WiMAX

1. WiMAX technology to provide high-speed connection for the Internet, the data transmission distance up to 50km, with high transmission rate, business diversity. Using OFDM / OFDMA, AAS, MIMO, and other advanced technology to achieve the broadband business mobile.

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 will channel into several orthogonal sub channels, high-speed data signal into parallel low-speed data streams, modulation to transmit in each sub channel. Orthogonal signal can be separated by the relevant technology at the receiver.

10 Ad Hoc Networks

1. Infrastructure: is the traditional ap mode, opening only one center, and the other nodes access the center point through the center of the data exchange. Ad-hoc: is ad hoc network mode, each point is equal, any point can communicate with other nodes, do not need the center point.

2. The definition of the number of nodes for NfiffRt indicates that the node can transmit distance, Rl represents interference distance,following two conditions:1)IJ = Rt2) meet any node node K DKJ = Rl are not for data transmission

3. Receiverfis perspective: When receiving, it will be interfered by others and exposed node problem may occur.

4. In order to achieve optimal throughput, the sending rate of each node must be strictly controlled and carefully scheduled. In order to calculate the end-to-end throughput limit, it is necessary to find out how many hops the nodes are spaced enough to ensure that they can transmit data at the same time. Throughput decreases with data schedules.

5. It will cause the contention and waste of the resources in the ad hoc network, increase the probability of data collision, and seriously affect the network throughput.

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. In this state, only 802.1X traffic is allowed; other traffic, such as the Internet Protocol (and with that TCP and UDP), is dropped. 2. Initiation To initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. 3. Negotiation (Technically EAP negotiation) The authentication server sends a reply (encapsulated in a RADIUS Access-Challenge packet) to the authenticator, containing an EAP Request specifying the EAP Method (The type of EAP based authentication it wishes the supplicant to perform). 4. Authentication If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet),

or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the 'authorized' state and normal traffic is allowed, if it is unsuccessful the port remains in the 'unauthorized' state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the 'unauthorized' state, once again blocking all non-EAP traffic.

3. WEP: Authentication status is unidirectional, resulting in potentially impoverished AP. WAPI: add a certification infrastructure WAI used to achieve the user's identity authentication. IEEE 802.11i: the IEEE802.1X protocol into the WLAN security mechanism to enhance the WLAN identity authentication and access control capabilities.

12 Bluetooth and RFID

1. Low power consumption, very low running and standby power consumption. Low cost, support two deployment methods: dual mode and single mode. Strengthen the compatibility between different OEM manufacturers equipment. Reduce the delay. Effective coverage expanded to more than 60 meters.

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. Providing of power,data transmition beween tag and read,security of data transmition.multiple destinationsfi identity.

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

13 Wireless Sensor Networks

1. The WSN is built of 'nodes' and each node is connected to one (or sometimes several) 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 or wired network connection.

2. The power supply module provides a reliable power supply for the system. The sensor is a binding of WSN nodes that can get the environment and the state of the device. The microcontroller receives data from the sensor and processes the data accordingly. The wireless transceiver will transmit data to achieve the physical implementation of the communication.

3. (1)WSN application in the smart grid which is a online monitoring system for transmission lines. (2)WSN application in smart homes,WSNs are key for improving the energy efficient performances of existing buildings.

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. The communication distance of the nodes in the network is generally short. The node can communicate with nodes outside the coverage area, you need to route through the intermediate node.

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. Ambient energy harvesting from external sources are used to power small autonomous sensors such as those based on MEMS technology.

14 Internet of Things

1. Ultra-wideband wireless communication,Software Defined Radio,Radio Frequency Identification.

2. Good security,High processing gain, Multi-path resolution ability,High transfer rate,System capacity is large,Anti-jamming performance,Accurate positioning,low cost.

3. Bluetooth Low Energy is based on Bluetooth, at the same time simplify the Bluetooth. The single-mode Bluetooth chip using a separate Bluetooth Low Energy Protocol, which is the simplification of the classic Bluetooth protocol.

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.

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. The data forwarding mechanism based on the flow; the routing mechanism based on the central control;the application oriented programming mechanism.

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.

16-18 Intelligent Robots, Cars and Quadrotors

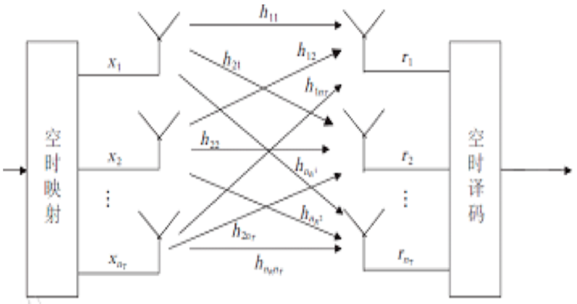
1. Ethernet support,motor,camera,microphone,inertial navigator,infared receiver and so on.

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.

19 MIMO

1. MIMO: The system transmitter and receiver are equipped with multiple antennas for simultaneous transmission. SISO: only one transmission path between the transmitter and the receiver.

2.



3. Space-multiplexing: At the transmitter, high-rate data streams are partitioned into multiple lower-rate sub-data streams, and different sub-streams are transmitted on different transmit antennas on the same frequency band. Space diversity: Use the multiple transmission paths provided by multiple antennas on the transmitting or receiving side to send the same data to enhance the transmission quality of the data.

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

21-22 Bitcoin and Graphic Code

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.