Notes on
802.11-WLAN: ENTS 689F course material

Surya Teja Paruchuri,
email: surya@terpmail.umd.edu

August 19, 2017

1 Slides

1.1 Lecture-1

1. *NOTE: This list is from wikipedia, not from lecture slides!!*
   802.3 Ethernet.
   802.15 - WPAN.
   802.15.1- Bluetooth.
   802.15.2 - 802.11 and 802.15 co-existence.
   802.15.4 - Low-Rate PAN like ZigBee, MiWi etc.
   802.15.5 - Mesh networking for WPAN.
   802.15.6 - Body Area Network (BAN).
   802.16 - WiMAX.
   802.16.1 - Local Multi-point Distribution Service.
   802.21 - Media Independent Handoff (MIH). Vertical Handover across heterogeneous networks including 802.11 and 3GPP networks.
   802.22 - Super WIFI or using Wireless regional area network in TV white Spaces.
   802.24 - Smart Grid TAG.

2. 802.11ac supports upto 1500 Mbps, 802.11ad works in 60 GHz.

1.2 Lecture-2

1.3 Lecture-3

1. WLAN is half-duplex (Both APs and client/work stations), while wired LAN's are full duplex.

2. Two types of Access points:

   (a) Autonomous AP: Half-Duplex, with switch/MAC addresses based traffic directing capabilities, i.e, either to wired back bone or back into wireless network.

   (b) Light weight AP- a simple repeater to boost the RF power.

3. Hierarchical Architecture:

   (a) Access: deliver traffic directly to end user. (APs are deployed at this layer.

   (b) Distribution: Does route the traffic.

   (c) c)Core: High Speed Switching, fast and reliable delivery of packets, does NOT route traffic.

4. Standard Topologies defined by 802.11 standard:

   (a) BSS: Basic Service Set: Basic toplogy consisting of few clients and an AP, which has a BSSID-Basic Service Set Identifier (based on

APs MAC address). BSSID $\neq$ SSID: Service Set ID, which is configured by admin. Connected Clients are called associated with layer 2 connection.

(b) IBSS: Independent Basic Service Set: A stand alone topology for forming an ad-hoc WLAN network. Here the communication initiator will generate a random MAC like number to be used as BSSID. Communicate through peer connections.

(c) EBSS: Extended Basic Service Set: group of BSS, that communication among themselves to forward packets from

5. Modes of Operation in 802.11:

   (a) Infrastructure mode (Default mode):

      i. Infrastructure with ESS is typically used to cover multi-building campuses or larger areas. Inside ESS, DS determines and routes the packets to either same BSS, or other BSS or outside network. Terminals mobility is shielded outside ESS, as they appear to be on a single MAC-layer network. Additionally, ESSś coverage may be non-overlapping, "Nomadic roaming" or 100% overlapping,"co-location".

   (b) Ad-hoc mode:

6. Rayleigh Fading: Downfade- if phase difference is between 120 deg to179 deg, and upfade- if phase difference is between 0 deg to120 deg.

7. Beam Divergence: Phenomenon of natural divergence of a waves from an Antenna.

1.4 Lecture-4

1. IEEE 802.11 standard defines RSSI as a relative metric. RSSI is used for Layer-2 ReTX decision, Roaming decisions, and Dynamic Rate Switching decision.

1.5 Lecture-5

1. 802.11 only defines PHY and MAC (of Data Link's Logic and MAC sub layers). FHSS and DSSS are two PHY methods currently used (Infrared is obsolete).

2. In ISM band: 2.4 GHz to 2.4835GHz, FHSS uses 1MHz sub-carriers, while DSSS uses the entire spectrum by dividing it into multiple channels. ***NOTE:*** *FHSS and DSSS devices are incompatible with each other. Vendors may manufacture either clause 14 (FHSS) or clause 15 (DSSS) radio cards.*

3. UNII-Unlicensed National Information Infrastructure Bands/ 5GHz Bands: from 5.150GHz to 5.825GHz. Has following bands as of today:

Frequency Range	Bandwidth	Amendment	No of channels
UNII-1/Lower (5.150-5.250 GHz)	100 MHz	802.11a	4
UNII-2/Middle (5.250-5.350 GHz)	100 MHz	802.11a	4
UNII-3/Upper (5.725-5.825 GHz)	100 MHz	802.11a	4
UNII-2/Extended (5.47 - 5.725 GHz)	255 MHz	8011.h	11

4. Few Important 802.11 standards:

amendment	Details
802.11	Original standard defined in 2.4 GHz for 1Mbps & 2Mbps
802.11b	11Mbps standard in 2.4 GHz Band.
802.11a	54Mbps standard in 5 GHz Band. (**NOTE**:both 802.11b and a are both defined in 1999)
802.11g	54Mbps standard on 2.4GHz
802.11n	To explore smart antenna techniques.
802.11f*	Supports Inter-AP roaming.
802.11i*	for enhanced security.
802.11h*	support for European requirements.
802.11j*	support Japanese requirements.
802.11v*	support Wireless Network Management standard.

* some other standards.

5. 802.11 uses HR-DSSS and supports 1,2,5.5,11 Mbps Data rates, while 802.11a supports 6,12,24, and 54 Mbps (Additional data rates 9, 18, 36, 48 Mbps are also supported).

6. 802.11g uses ER-OFDM as PHY later, and HR-DSSS and DSSS for backward compatibility with 802.11b and 802.11. Three modes of operation for 802.11g: 802.11b only, 802.11g only, 802.11b/g mode. In the 802.11b/g mode, AP send a message to 802.11g clients when it identifies any DSSS clients to protect 802.11g clients- (Protection Mechanism).

7. 802.11 n- supports MIMO, upto 100 Mbps Data rates, backward compatible. Devices can be either only 2 GHz or only 5 GHz or Dual Band devices.

8. ***PHY-FHSS:*** In ISM band-2.4GHz, FHSS divides the band into 75 1 MHz sub-channels (FCC's regulation limits sub-channel bandwidth ¡1MHz); Tx and Rx agree on a hopping pattern to minimize the interference from others. The hop time (time to shift from CHx to CHy) deters achievable rates, along with Dwell time (time on a single sub CHx). Simpler and cheaper than DSSS, but not as reliant as DSSS. Maximum Dwell time of 400ms on any given CH or carrier frequency during any 30s period. (75 channels $\times$ 400ms = 30s).Typical Dwell time: 100-200ms and hop time: 200-300ms. AP decides the pattern and then informed to client through "Beacon Management Frame".

9. ***PHY-DSSS:*** divides ISM into 14 overlapping 22MHz sub Channels, each at a distance of 5MHz from each other. IEEE requires that two channels can be called non-overlapping in ISM band only if their center frequencies are 25 MHz apart.

1.6 Lecture-6

1. Transmit mask: First side band i.e, from -11 to -22 MHZ on the lower side and +11 to +22 MHz on the higher side should be atleast 30dB lower than the current lobe.

1.7 Lecture-7

1. 5GHz Band-UNII- 4 channels in each UNII 1,2,3 and 11 in the extended bandwidth, each with 20MHz wide. Different sub bands inn 5GHz have different Tx power limits and restrictions on the center frequency location of outermost channels (for UNII 1,2 : 30 MHz from band's edge, and UNII 3: 20 MHz from Band Edge.

2. OFDM sub-carrier symbols in 802 family are 312.5 KHhz wide.

3. code rate for FEC:

$$(No.of Databits)/(No.of Total Codebits)$$

4. ***MAC in 802.11:*** CSMA/CD suffices in 802.3 because of full-duplex communication, but CSMA/CA is required for 802.11, as it is a half-duplex communication.

5. 3 Modes of operation of MAC: Distributed Coordination Function (DCF), Point Coordination Function (PCF), and Hybrid Coordination Function (HCF). DCF has not central controller, where as PCF, AP is the controller, thus enabling the QoS guarantees for voice and video applications - AP polls the clients in PCF and Ad-hoc networks cannot use PCF mode, as there is no AP.

6. DCF accesses channel using time slots. Senses for RF energy, and channel should be idle for (DIFS = SIFS + 2× time slit) + Random Back-off period of time, and only transmit if the channel is still free. DCF uses the following to avoid multiple transmissions at a given point:

   (a) Frame Spaces (IFS)- time separation between two frames. Types:
   a). Short IFS(SIFS)
   b). PCF IFS(PIFS)
   c). DCF IFS (DIFS)
   d). Arbitration IFS(AIFS)- for QoS applications and
   e). Extended IFS (EIFS) -for ReTX.
   The time duration in increasing order is SIFS < PIFS < DIFS < AIFS < EIFS. ***NOTE:*** IFS is a feasible solution because all terminal, weather APs or clients are time synchronized. Restriction is laid on which IFS may follow the previous IFS. As an Eg: only an ACK (using SIFS) are allowed to be Tx after a Data Frame (using either PIFS or DIFS).

   (b) Carrier sensing (physical and virtual). Physical Sensing includes, sensing through sampling of RF signal. Virtual Sensing uses Network Allocation Vector (NAV)- always indicated in μs, which is present in every header- this describes the amount of time the bandwidth is allocated for a client. Sensing should be done after this period.

   (c) Random Back-off counter.

1.8 Lecture -11

1. ***Contention Process using DFS:***

   (a) Check if the CH is idle.

   (b) if it is idle for DIFS, then start contention process (described in the next point), else wait until CH is idle for DIFS amount of time.

   (c) if CH was idle for DIFS, begin contention process: Back-Off(BO) = Random(0,CW)× timeslot, that is CH should be idle for BO period, where CW is Max. Contention Window size.

   (d) if CH is not idle occupied during contention period, then pause the contention period until NAV in the present header, and then resume contention process with stored values, at the end of the NAV time.

   (e) if CH idle at end of contention process, Tx your data.

2. RTS (Request to Send) and CTS (Clear to Send): A hand shake mechanism to solve hidden node problem. Each RTS and CTS frames have their own NAV within their frames.

3. ***802.11 Frames:*** 3 Types of Frames are there in 802.11 (802.3 has only one Frame structure).

(a) Management Frames : to join and leave BSS. (Association requests, Association responses, Probe Requests, Beacon Management, Authentication).

(b) Control Frames : help with delivery of frames (ACK, RTS, CTS).

(c) Data Frames: 2 Types - Basic Data Frame (which contains MSDU-MAC Service Data Unit, max size of MSDU 2312 Bytes), and Null Data Frame (Contains no Data, used for update changes in power control settings). Also it contains, a 32-bit FCS or Frame Correction Sequence. The MAC header, MSDU and FCS together form the MAC Protocol Data Unit. (MPDU).

4. PSDU - Physical Service Data Unit; PPDU - Physical Protocol Data Unit, are the packets at Physical layer.

5. Ref* slides for MAC header and Frame Structure and details. lecture-11 slides, slides 42 to 48, for more details about frame structure and it's fields.

6. MAC Frame has 4 Addresses: one for sender, one for final receiver, one for the currently transmitting AP's MAC and the last one for the current receiving AP's MAC.

1.9 Lecture-12

1. Max. Frame Size is 2346 Bytes.

2. When multiple frames are present, the first frame contends for resources and then sets the NAV for a time to transmit first DATA, get first ACK, transmit DATA and get it's ACK, with SIFS in between each. Additionally, the more fragments in Frame control to 1.

3. Beacons, apart from broadcasting the WLAN information, helping in synchronizing, informing the supported Data rates and physical layer signaling method (FHSS or DSSS or OFDM), also does support the power saving mode operation, using Traffic Indication Map (TIM) -which uses the clients Association ID (AID) to inform that the client has data queued at AP.

4. ***802.11 Authentication:*** Two methods:

5. 802.11 defines 2 types of scanning: Passive and Active.

6. Beacon interval selection: Trade-off between level of over head and fastness in roaming.

7. There is no priority for Beacon frames. So Beacons frames have to follow same process to sense medium as any other frame, and thus may experience delays.

8. In adhoc networks, one of the clients assumes the responsibility of sending beacons.

9. ***802.11 Authentication:***

   (a) Open System Architecture: Null Authentication, where all requested gets approved. WEP can be used with Open Authentication.

   (b) Shared Key Authentication: WEP authentication challenge is given to client, and AP verifies authenticity using the response and shared key.

10. WEP: Wired Equivalent Privacy, only used to encrypt the sessions.

11. During association, AP reserves memory space and allocates Association ID (AID), once it receives an association request.

1.10 Lecture-13

1. Three possible authentication and association states for client:

   (a) Unauthenticated and Unassociated.

   (b) Authenticated and Unassociated.

   (c) Authenticated and Associated.

2. ***Roaming may be within Layer-2 Network:*** A client may still be able to communicate with Layer-3 or above, while roaming, either if it is moving across APs in same subnet or if there is support for IP Tunneling at L-3, such as implementation of MobileIP.

   (a) If moving across AP's within the same subnet, client will decide when to roam; AP has no control over this. In this case, Client issues a ReAssociation request to the new AP, which ACKs this. New AP contacts old AP for any buffered packets via Distribution System (Not Specified by standard). Then a ReAssociation response is issued by new AP. Client may/not Tx disassociation request to old AP.

1. ***802.11n or High Throughput (HT) WIFI:*** improved throughput and range, fully backward compatible, and flexible configurations. Key features : MIMO (MIMO-radio chains, Spatial Multiplexing, Diversity and Beam forming), PHY layer enhancements (20 and 40 MHz Channels, higher order QAM such as 16, 64, and increased sub-carriers), and MAC layer (reduced IFS, Frame Aggregation).

2. Radio chain: A single radio, along with all the required components such as mixers, attenuators, amplifiers, ADC/DAcs etc.

3. The standard supports upto 4 independent streams of data.

4. Channel Bonding: combining two adjacent 20MHz channels into a single 40MHz channel. As typically, in a 2.4GHz band, multi-carrier architecture (non-overlapping design- with CHs 1,6,11) is deployed, WIFI alliance does support 40MHz only in 5GHz band.

5. unlike in 802.11a/g where a 20MHz CH is sub divided into 52 sub-carriers, 802.11n divides 20MHz CH into 56 sub-carriers.

6. MAC Improvements/Frame Aggregation: Introduced Aggregated MAC Protocol Data Unit (AMPDU)- where client can send 64 frames in one shot. AP could avoid overhead from 64 headers and ACKs, by simply replying with a Block ACK,which tells exactly which frames needs to be reTx.

7. Some other improvements are: 40MHz channels, Short Guard Intervals, more efficient modulation and coding, Block ACKs.

8.

1.11 Lecture-14 & 15

1. Manual Channel is not a feasible option for large networks. So a Dynamic Channel Assignments (DCA) algorithm is used for this purpose. It is important to note that DCA might perform badly if there is too much interference in the channel, as DCA algorithm constantly tries to switch channels. (*NOTE: when switching the CH, an AP issues disassociation frame to all the clients, and then switches to a new channel, as there is no established mechanism to indicate such a CH switch*).

2. ***802.11ac or Very High Throughput (VHT) under 6GHz:***

   (a) 802.11ac -mainly meant to support video services, is a set of Physical layer improvements based off 802.11n, like higher spatial multiplexing, modulation, and wider RF Channels.

   (b) 802.11ac has wider channels-a mandatory 80MHz channels and an optional 160MHz channel.

   (c) 802.11ac doubles the spatial streams from 4 in 902.11n to 8. Although currently typically only 3×3 is used.

   (d) 802.11ac supports 256 QAM, with a maximum code rate of 5/6.

   (e) MU-MIMO (only in Downlink): enables using different spatial streams for clients physically separated by distance. As all 802.11¡x¿ technologies allow only a single user Tx till now, allowing multi-user transmission on the same CH is a major leap (accomplished using beam forming on multiple physically separated users). ***NOTE: Although parallel streams of data are allowed, ACKs are done serially only***. Additionally, the co-channel interference in MU-MIMO stymes the SNR ratio to a certain extent. Lastly, link adaptation is challenging.

(f) In Uplink, all the clients operate only in half-duplex mode.

3. ***This Notes doesn't include the 802.11's security section of the last lecture***.