Nomadic Communications Labs

Alessandro Villani
avillani@science.unitn.it

Ad Hoc Networks

Ad Hoc Networks(IBSS)

- The wireless LANs we usually know make use of the mode "infrastructured" which requires one or more Access Points
- The 802.11 standard specifies an additional mode:
  Ad hoc mode
- This mode let the 802.11 network card operate in what the standard defines a network configuration "Independent Basic Service Set (IBSS)"
- In IBSS mode there are no Access Points and the various network cards communicate directly among them in peer-to-peer mode

Ad Hoc Networks(IBSS)

- The Ad Hoc mode allows the users to constitute a wireless LAN autonomously
- Typical applications:
  - Files and resources sharing among laptops
  - application of first aid in emergency situations (disasters, accidents, fires, …)

Ad Hoc Networks(IBSS)

- Advantages/disadvantages:
  - **Reduced costs:** no AP, no cost of infrastructuration
  - **Reduced setup time:** It is enough that users have the wireless network cards
  - **Performance:** In a communication among two clients is better the Ad Hoc mode, otherwise ... it depends
  - **Reduced access to the net:** Generally there is no access to the wired net, in some cases a single client can share its connection to the others clients, however it is not a good solution!
  - **Management of a complex network:** given the fluidity of the network topology and the lack of a centralized device, the security management and the performance analysis is extremely complex

Ad Hoc Networks(IBSS)

- The first station for a particular Ad Hoc network (that is, the first NIC radio) establishes the IBSS determining the BSSID address:
  - In a infrastructured network the BSSID is the address of the wireless interface of the AP
  - In an Ad Hoc network, the BSSID is generated in a random way

Ad Hoc Networks(IBSS)

- A BSSID is reserved, the broadcast BSSID (all the bits to 1):
  - Frames with broadcast BSSID jump all the BSSID filters on the MAC level
  - This address is only used when stations try to identify a net sending a probe request
  - Only the probe request frames can use the BSSID broadcast

Ad Hoc Networks(IBSS)

- Afterwards the first station starts sending beacons, needed to keep the synchronization among the stations
- Note that in infrastrucutured mode, only the Access Point can send beacons

Ad Hoc Networks(IBSS)

- The other stations of the Ad Hoc network will join to the net after receiving a beacon and accepting the parameters of IBSS (in particular the interval of beacon) sent in the beacon frame
- All the stations which join the Ad Hoc network must periodically send a beacon if they do not hear a beacon from another station after a very short random delay from when they presumes that beacon had to be sent

Analysis of Ad Hoc Network packets

Probe Request

- Initially empty frame of *Probe Request* with BSSID FF:FF:FF:FF:FF:FF and with SSID either empty or with default SSID or the SSID of the Ad Hoc network

Probe Request (with ID) – Part 1

```
Frame 3 (51 bytes on wire, 51 bytes captured)
IEEE 802.11
    Type/Subtype: Probe Request (4)
    Frame Control: 0x0040 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 4
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
    From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 1
```

Probe Request (with ID) – Part 2

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (27 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
        Tag interpretation: WNLABTEST
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Probe Request (without ID) – Part 1

```
Frame 4 (42 bytes on wire, 42 bytes captured)
IEEE 802.11
    Type/Subtype: Probe Request (4)
    Frame Control: 0x0040 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 4
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
    From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 2
```

Probe Request (without ID) – Part 2

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (18 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 0
        Tag interpretation:
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Beacon Frame

- Waited for a certain time interval the *Beacon Frame* starts
- In the beacon now there is the BSSID chosen in random way

Beacon Frame – Part 1

```
Frame 32 (82 bytes on wire, 82 bytes captured)
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
    From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 46
```

Beacon Frame – Part 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000000019256
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0022
            .... .... .... ...0 = ESS capabilities: Transmitter is a STA
            .... .... .... ..1. = IBSS status: Transmitter belongs to an IBSS
            .... .... .... 00.. = CFP participation capabilities: Station is not CF-
    Pollable (0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..1. .... = Short Preamble: Short preamble allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
```

Beacon Frame – Part 3

```
    Tagged parameters (46 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
        Tag interpretation: WNLABTEST
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 9
        Tag Number: 6 (IBSS Parameter set)
        Tag length: 2
        Tag interpretation: ATIM window 0x0
        Tag Number: 221 (Vendor Specific)
        Tag length: 7
        Tag interpretation: WME IE: type 2, subtype 0, version 1, parameter set 0
        Tag Number: 42 (ERP Information)
        Tag length: 1
        Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use protection, long
    preambles)
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Probe Response

- When a new station ask to join the network, it starts sending the frame *Probe Request*
- The first station answers with a frame Probe Response destined to the new station

Probe Response – Part 1

```
Frame 147 (82 bytes on wire, 82 bytes captured)
IEEE 802.11
    Type/Subtype: Probe Response (5)
    Frame Control: 0x0050 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 5
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
    From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:0b:cd:8d:30:3b (10.0.0.10)
    Source address: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 143
```

Probe Response – Part 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000000920D3E
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0022
            .... .... .... ...0 = ESS capabilities: Transmitter is a STA
            .... .... .... ..1. = IBSS status: Transmitter belongs to an IBSS
            .... .... .... 00.. = CFP participation capabilities: Station is not CF-
    Pollable (0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..1. .... = Short Preamble: Short preamble allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
```

Probe Response – Part 3

```
    Tagged parameters (46 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
        Tag interpretation: WNLABTEST
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 9
        Tag Number: 6 (IBSS Parameter set)
        Tag length: 2
        Tag interpretation: ATIM window 0x0
        Tag Number: 221 (Vendor Specific)
        Tag length: 7
        Tag interpretation: WME IE: type 2, subtype 0, version 1, parameter set 0
        Tag Number: 42 (ERP Information)
        Tag length: 1
        Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use protection, long
    preambles)
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Data Frame

- Substantially identical to those of an infrastructured wireless network
- Note as the BSSID is always the one transmitted in the *Beacon Frames*

Data Frame – Part 1

```
Frame 361 (92 bytes on wire, 92 bytes captured)
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0008 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
    From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 258
    Destination address: 00:0e:35:6e:20:39 (10.0.0.11)
    Source address: 00:0b:cd:8d:30:3b (10.0.0.10)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 111
Logical-Link Control
Internet Protocol, Src Addr: 10.0.0.10 (10.0.0.10), Dst Addr: 10.0.0.11 (10.0.0.11)
```

Data Frame – Part 2

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x495c (correct)
    Identifier: 0x0200
    Sequence number: 0x0200
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Ad Hoc Network: the task

- Analysis of Ad Hoc network frames:
  - Start an Ad Hoc Network with a laptop
  - Join the previous Ad Hoc Network with a second laptop
  - Use a third one to acquire the packets, using wireshark, analyzing all the possible situations (like the first station leaves, the second asks for all the available network, ...)

Ad Hoc Network: the task

- Play with MTU:
  - Start an Ad Hoc network using two laptops
  - Run iperf server (suggestion: use UDP) on one laptop and client on the second
  - Modify the MTU parameters on the wireless card (like: 1500 on both, 250 on both, 2500 and 250, 2500 and 512, ...)

Ad Hoc Network: the task

- Performance Analysis:
  - Start an Ad Hoc network using two, three, four laptops
  - Run iperf server (suggestion: use UDP) on one laptop and in client mode on the others, starting the clients in a "synchronized" way
  - Evaluate the performance, using one client, then two, three, four
  - How the throughput decrease? Remember to run iperf N times (with N > 20)

Ad Hoc Network: the task

- Interferences between channels:
  - Take 4 laptops and start 2 different Ad Hoc network on 2 different channels (i.e.: 1 and 7)
  - Run 2 iperf server (suggestion: use UDP) on one laptop for both Ad Hoc Network, and in client mode on the others two, starting the clients in a "synchronized" way
  - Evaluate the performance, remember to run iperf N times (with N > 20)
  - Change the channels of one of the Ad Hoc network choosing a channel closer to the other (i.e.: 1 and 6), and repeat the evaluation