Seminar: Verteilte und vernetzte Systeme

Mesh Networks Based on IEEE 802.11

Kiran Mathews
(kiranmathews20@gmail.com)

February 26, 2016

Contents

1 Introduction

With the rapid adoption of wireless networks came the need to provide wireless access in places where connecting an Access Point (AP) to a switch was not possible. The idea was to replace the Ethernet cables with wireless links which provide more flexibility in designing the network. Even though there exist several mechanisms to solve the problem, a formal standard solution was not there. In 2003, the IEEE 802.11 working group defined the idea of a *Wireless Distributed System* (WDS) as a mechanism for wireless communication which uses a four address format between access points and extended six address format for communicating between clients connected to the network. It helps the network to expand without the help of any wired backbone infrastructure. But the working group did not describe much more apart from the concept. Since there was not a common mechanism defined by IEEE, several vendors started to design and implement according to their needs. They used different mechanisms for AP discovery, path selection, formation of mesh cloud, link metric etc. This diversity in mechanisms made the inter-vendor comparison very challenging and there were some unanswered questions in the first amendment. Later in 2004 the IEEE 802.11 group created a new group for researching more about these issues and to come up with a clear terminology for the standard. After a long research and discussions, by the end of 2011, IEEE published the 802.11 amendment for mesh networking 802.11s with an idea of flexible, self-forming and self-healing networks. Although the IEEE 802.11s amendment was a draft, it needs a good investigation for specific solutions.
In this seminar, we investigate the IEEE 802.11s standard approach and different networks based on it. Mesh networks need to be designed according to the needs. Section 2, provides a brief overview about existing systems and their limitations. Then section 3 provides details about the architectural overview and other standard features suggested by the draft. Later in section 4, we discuss about the mesh networks, One Laptop Per Child (OLPC) and Seamless Mesh (SMesh). Section 5 concludes our findings.

2 Existing Systems

In this section, we discuss different use cases for WLAN networks including mesh network and earlier attempts to create mesh networks before the publishing of the final draft. First, we discuss about the traditional WLAN accesses such us ad hoc and infrastructure mode and then the extended version combining those modes together [5]. Then we discuss about an infrastructure-mode wireless mesh network (iMesh) [9].

2.1 Traditional approaches

The infrastructure mode in 802.11 is one of the widely used use case. In this mode, there is a single Access Point (AP) where all data and communication between stations moves through this AP, the wireless router. This AP connects the wireless network to a wired Ethernet network. Client stations which want to connect to the network should be configured to the Service Set Identifier (SSID) of the AP. In Fig.1(a) shows a typical example of the infrastructure mode. In the figure, different stations are connected to the AP and all stations will send their packets through that AP.
The main target of the client stations in infrastructure mode is to establish a IP connectivity through the WLAN infrastructure network. When a client enters the coverage of a AP, it will receive the beacon frames send by the AP and associates with the AP. Usually, a Dynamic Host Configuration Protocol (DHCP) server located in the network will provide the client station with an IP address. Once the connection is established with the AP, all packets to other stations or to other networks will pass via this AP. There are certain limitations of this approach. When a station moves from the coverage of one AP to another, it need to be configured with the new SSID and should re-associate with the new AP. It is also necessary to re-configure the communication channel when it moves to new AP, if the

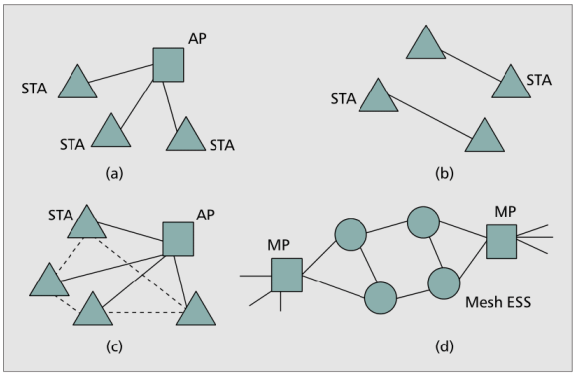

Figure 1: Different modes of WLAN a)infrastructure mode, b)ad hoc mode, c)mixed mode and d) mesh [5]

new AP is operating on a different channel. There is no specific handoff mechanism this purpose and no specific quality of service (QoS) depending on scenario [5].

Ad hoc networks are self-configuring, dynamic networks that are formed without the presence of an AP and independent of pre-existing infrastructure like AP or routers. Establishing IP connectivity using point to point links is the main objective in this case. IP address for station should be statically assigned. Similar to infrastructure mode, when a station wants to join the network, it transmit beacon frames. Beacon frames are expected to be received with in a time limit, if no node receives a beacon frame from an AP, then the station creates a new ad hoc network and sends beacons announcing this network. The main difference from infrastructure mode is that stations can move freely (self-configuring) and there is not AP to control it. Communication between two networks is not possible in this mode. Fig.1(b), shows an example of two ad hoc networks. Security in this mode is provided at higher layer level [5].

The next mode is the mixed mode which is a combination of infrastructure mode and ad hoc mode. The stations can communicate with each other or can communicate through an AP. The stations can move freely inside the network and unlike in ad hoc mode, the stations can communicate with other networks like Internet. Fig.1(c) shows an example of the mixed mode.

Next is the mesh networks, is a combination of stations connected through WLAN network act as Mesh Points (MP) to provide and establish IP connectivity with a station. MP can be either a mesh access points (MAPs) or mesh station (MSTAs). Design and creation of a mesh faced several challenges. A routing mechanism based on layer 2 was necessary, since AP can only communicate in layer 2 and drawbacks of layer 3 mechanism. Another important issue was calculating the link metrics. The concept of "shortest path is the best path" is not suitable in mesh networks. The shortest path might get congested with backbone traffic. So a different link metric calculation is needed. Other issues like providing QoS for real time applications, security and power efficiency remained as a open question. We will discuss more about these issues in the later sections.

2.2 iMesh

iMesh [9] is one of the earlier attempts to create mesh network on IEEE 802.11. iMesh is an infrastructure mode 802.11 based mesh network. The reason behind choosing infrastructure mode above ad hoc mode is due to difficulties to find 'appropriate' AP when the client moves around. It needs extra device configuration in the client side with appropriate software. The main design goal of iMesh was to achieve client transparency. i.e the mobile clients should be unaware about the backbone mesh structure. iMesh network has several *wireless access routers* or APs which are connected wireless links which form the backbone of the network. Clients can move around the network by connecting to nearby

routers in range, so that the client feels like connected to a single network. When a client moves from one wireless access router to another, a layer-2 hand-off occurs which will update the routing informations for that particular client in the mesh network backbone. Hand-off procedure include both layer-2 and layer-3 procedures. Layer-3 handoff process uses a similar solution to mobile IP called *Transparent Mobile IP* and "flat" routing protocol based on link-state routing.
One method to implement mesh network is using bridging technique, a layer-2 alternative to routing. But bridges are unable to handle hierarchies in the network and are unscalable, also the bridging learn route by broadcasting the information which makes the network slow. Apart from that, lack of a centralized mechanism to handle client information, APs were unable to learn about the clients until they receives some message form the client. It makes the hand-off procedure more difficult. Due to these issues layer-3 solution was used in iMesh. APs or wireless access routers were connected with each other through wireless links to form the backbone of the network or to form Wireless Distribution System (WDS). iMesh uses software-based APs which provide provision for layer-3 hand-off process. The hand-off process happens in Link layer and network layer.
Link layer hand-off happens when the node moves from one AP to another. Hand-off condition depends on the configuration. When a client moves from the range of one AP to another, the client will start *probing*. In probing, a client will broadcast a *probe request frame*. After broadcasting, it waits for *probe response frames*. After collecting the response for a certain time, it will switch channel and repeat the process of probing. When it is done on every channel, it select AP with the best Signal-to-Noise ratio (SNR) and re-associate with it by sending necessary information like transmission rate, beacon interval etc to it. For re-association, the AP uses *reassociation request frame* and *reassociation response frames*.
Next hand-off happens in network layer. The APs in the iMesh form a multi-hop network routable at IP layer which make mobility management difficult. iMesh uses two broad approaches to overcome this issue. The first approach is the *Transparent Mobile IP* (TMIP) protocol, which is similar to Mobile IP. Like in mobile IP, every client will have a unique home AP. WDS will keep track of the client and where ever the client is in the network, its the responsibility of the home AP to forward the packet to its clients. Information about the home AP for every client is stored in *Mobile Location Register* (MLR). When a client moves away from its home AP and connects to a foreign AP, foreign AP will find its home AP by searching in MLR and notify the home AP. Thus the messages for the client will tunneled by the home AP to foreign AP. Also it will send ARP message to the client for changing its default gateway address to the MAC of the foreign AP. Thus the IP of client remains unchanged and client will be unaware of the routing behind the scene. But forwarding path for the mobile clients is not optimized due triangle Routing Problem in Mobile IP [8]. iMesh uses the link-state based routing protocol called Optimized Link State Routing (OLSR) [4] using the routing table in APs which contains the IP address of the clients. Clients in the network are unaware about the routing behind the scene and link between the client and AP is considered as an external router to mesh network.
iMesh testbed uses Soekris net4521 boards running in pebble Linux V41 distribution. iMesh was a successful early attempt in obtaining client transparency. The hand-off latency was about 50-100 ms for up to 5-hops with little background traffic. As the network grows the latency increases. Link layer hand-off (probing) delay was major reason for this higher latency. In coming section 3, we will discuss about the final draft by IEEE about the mesh network.

3 IEEE 802.11s

In this section, we discuss about the final draft from IEEE for mesh network (802.11s). According to the draft, a node in the network can be [2]:

- Station (STA), a device that has the capability to use the 802.11 protocol,
- Mesh Station (Mesh STA), a station that gets involved in formation of backbone mesh network and operation of the mesh network,

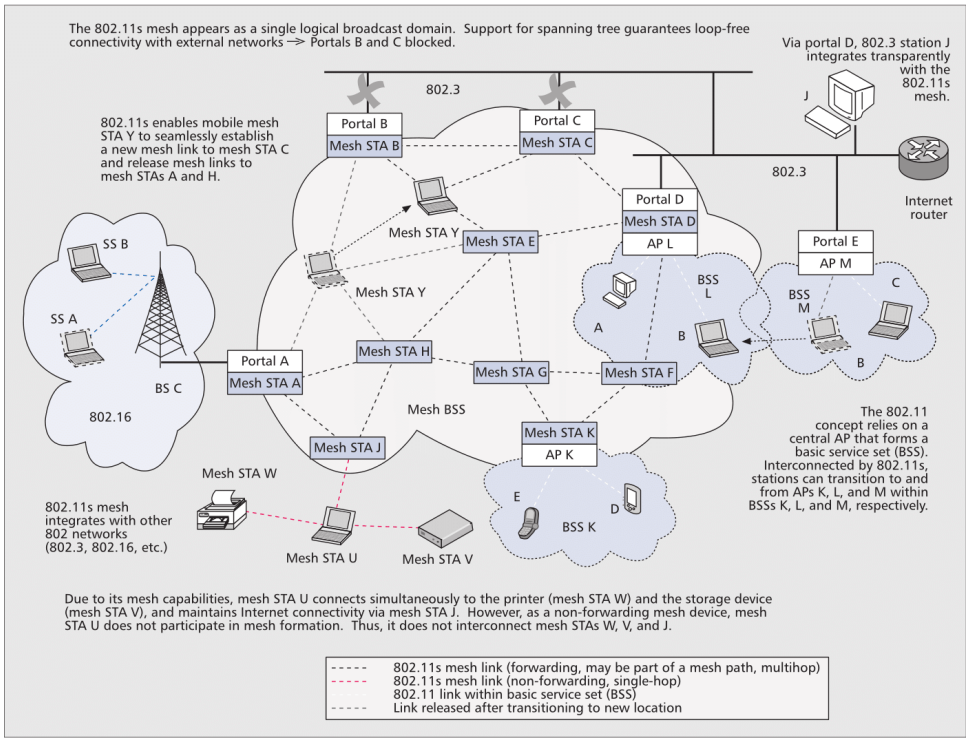

Figure 2: A sample Mesh network [6]

- Mesh Access Point (MAP), a Mesh STA that acts as access point to provide service to other clients which is not the part of the mesh cloud,
- Portal, ia Mesh STA which acts as a gateway or bridge between two mesh network or to some external networks like the Internet.

A STA can be any device which contains the 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless network. In Fig.2, devices A, B and C are STAs. A Mesh STA should contain all function to support the mesh network such as frame formats, access rules etc. In Fig.2 Mesh STA J provides these functionalities and is part of the back bone mesh network while the Mesh STA K also acts as MAP by providing connectivity to E and D. Portals act as a gateways to different layer-3 subnet, thus help to extend the network by connecting it other networks. Next we discuss the extended frame format used for routing in mesh networks.

3.1 Frame Structure

One of the open questions regarding mesh networks was layer-2 routing mechanism. For multihop functioning at the MAC layer, IEEE 802.11s extends the frame format of original 802.11. It extends data and management frames in the original version. It introduces an additional mesh control field as shown in Fig.3. The extended version supports four or six MAC addresses for routing and other subtypes. The four address frame format is used when two Mesh STAs are communicating. The four addresses are:

- Source Address (SA), MAC address of the STA which created the message,
- Destination Address (DA), MAC address of the STA where the message is to be received,
- Transmitter Address (TA), MAC address of the Mesh STA that is transmitting the message (may or may not be the source Mesh STA) ,

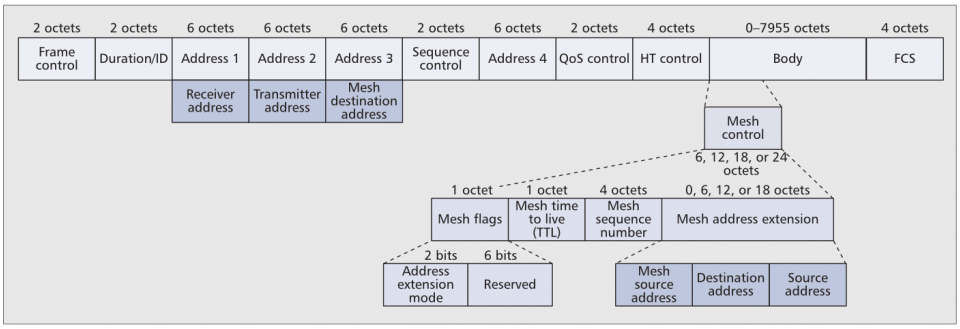

Figure 3: Extended frame format [6]

- Receiver Address (RA), MAC address of the Mesh STA that is receiving the message (may or may not be the final destination Mesh STA).

The six address frame format is used when two stations which are not part of the mesh network is communicating. The two additional addresses are:

- Mesh SA, MAC address of the Mesh STA which introduce the message from a STA into the mesh network,
- Mesh DA, MAC address of the Mesh STA in the mesh network which handles target STA.

For example, consider the routing from node E to B through Mesh STAs K→F→D in Fig.2. When node E sends a messages destined to node B, the value for SA will be MAC address node E and DA will be the MAC address node B. Node E is connected to the mesh network via MAP K. So the value for Mesh SA will be MAC address of Mesh STA K and Mesh DA will be MAC address of Mesh STA D since the node B is connected to mesh network via Mesh STA D. The value for TA in the first phase will be Mesh STA K and RA will be Mesh STA F. When the message is received by Mesh STA F, it retransmits the message by changing the value of TA to the MAC address of Mesh STA F and RA to the MAC address of Mesh STA D. TA and RA are mainly the address's of the intermediate Mesh STAs in the routing.
Apart from the new address format (mesh address extension fields), the extended version has additional mesh control fields such as Time to Live (TTL), a mesh sequence number and a mesh flags field. TTL and mesh sequence fields are used to avoid infinite looping of the frames inside the mesh network and help to detect the duplicates. TTL is decremented by each intermediate node in routing to the limit number of hops a frame can travel inside the mesh network. Next we discuss about the formation of a mesh network.

3.2 Mesh Formation

IEEE draft proposes Mesh Identifier (Mesh ID) similar to SSID in infrastructure mode to distinguish set of Mesh APs. Similar to 802.11, special beacon frames are used to announce a Mesh ID by setting SSID value to a wildcard value. This helps to differentiate other STAs from connecting the mesh network. Mesh ID along with path selection protocol and path selection metric forms a profile. A Mesh STA may support different profiles but at a moment a mesh cloud should work in same profile, i.e all Mesh STAs in a mesh cloud should use the same path selection protocol and path selection metric for routing. We discuss the default path selection protocol and link metric according to the draft in later sections.
Mesh formations is started either by active (probe frames) or passive (beacon frame) scanning similar

to 802.11. Mesh STAs broadcast beacon frames to find neighbors with the same profile. Thus, Mesh STAs with similar profile form a mesh network. Beacon frames and probe frame used by Mesh STAs include mesh related fields in order to distinguish them from normal 802.11 beacon and probe request fames. Once a Mesh STA finds a suitable neighbor, it establishs a peer link between its neighboring Mesh STAs using the Mesh Peer Link Management Protocol. Peer links use MAC address of the device and a pair of link identifiers to establish the connection. For example, If Mesh STA A wants to establish a peer link with Mesh STA B, A will send a *Peer Link Open* frame to B. Then B will reply with a *Peer Link Confirm* frame to confirm the connection from A→B. If B wants to establish connection with A, the same procedure needs to be done. A peer link connection can be closed by sending a *Peer Link Close* frame. Even if the link breaks, Mesh STAs keep the peer link status to improve minimize re-connection speed.

3.3 Routing in 802.11s

According to the draft, IEEE proposes a mandatory path selection protocol called Hybrid Wireless Mesh Protocol (HWMP) which is supported by all vendors. As the name suggests, HWMP is a hybrid protocol which provides proactive and reactive path selection. The draft does not force to use this protocol, it also allows to use modified versions according to the scenario and also other vendor specific protocols. HWMP depends on Ad hoc On-Demand Distance Vector Routing (AODV) and a tree based routing approach. Configuration parameter of a mesh STA is exchanged as *Mesh Configuration Element*. *Mesh Configuration Element* contains identifiers to determine the path selection protocol and the path selection metric used by the mesh cloud. It is exchanged along with beacon frames, *Peer Link Open Frames* and *Peer Link Confirm Frames*. As mentioned HWMP operates in two modes :

- On-demand reactive mode,
- tree-based proactive mode which can be further subdivided into Proactive PREQ mechanism and RANN mechanism.

In on-demand reactive mode, the Mesh STAs search for routes to a particular target using HWMP management frames. Once a route is determined, it stores or updates the routing table for future use. On the other hand, proactive mode is a tree based approach and a Mesh STA is pre-configured as the root or elected as root for managing the routing. HWMP path selection is carried out by four HWMP management frames namely [2]:

- Path Request (PREQ), frames sent by the source Mesh STA that wants to discover the path to the destination Mesh STA.
- Path Reply (PREP), are reply frames sent by the destination Mesh STA to the source confirming the PREQ frame. Depending on the flags in the frames, PREP frames are also used by the intermediate node to confirm PREQ.
- Path Error (PERR), used to report a broken path.
- Root Announcement (RANN), used in proactive mode to flood the routing information.

Mesh STAs will use those management frames along with DO (Destination Only) and RF (Replay and Forward) flags to find the route in on-demand reactive mode. If DO flag is set to 1, then intermediate node are not allowed to reply PREP frames for PREQ request, i.e. only destination will send the PREP for a PREQ frame. RF flags are used to limit the PREP reply frames for a PREQ frame by the source. If RF flag is set to 1 and DO set to 0, then intermediate nodes may respond to the PREQ, also broadcast the PREQ frame from the source and if the RF flag is set to 0, then the intermediates will not forward the PREQ frame. When a destination Mesh STA receives a PREQ frame passed through different path, it considers the metric values to evaluate the best path from source. We discuss the link metric calculation later. Link metric values are transferred along with PREQ and PREP frames.

Lets consider the scenario to find route from Mesh STA K to Mesh STA D in Fig.2. Mesh STA K sends the PREQ frame from K requesting the route path to Mesh STA D. Mesh STA F and G receive this frames from K. Depending on DO and RF flag Mesh STA F and G processes the PREQ frames. Suppose the RF and DO is set to 0, then the search for a route will fail since it doesn't reach the destination. Now lets assume that the RF and DO flags are set 1, then Mesh STA G and F reply with PREP frame to K and they broadcast the PREQ frame from K. Broadcast from Mesh STA G is received by Mesh STA E and H, also the broadcast from Mesh STA F reachs Mesh STA D which is the final destination. Depending on the TTL flags set by source K, broadcast PREQ message via Mesh STA G will reach Mesh STA D if there is enough time to live. Upon receiving PREQ message from different paths Mesh STA D will calculate the link metric for finding the best path. It unicasts the PREP frame through the path it chosen to communicate with the source. So if the K→F→D is the best path according the metric, the Mesh STA D unicasts PREP frames via D→F→K. Apart from TTL, HWMP use a *HWMP Sequence Number* to uniquely identify the HWMP route request frames from a source.

Apart from on-demand path discovery mechanism, HWMP provides two different reactive approaches based on the forwarding table created by the reactive approach. The first approach is the proactive PREQ mechanism based on PREQ frames. It can used be when a large amount of data is targeted to pass through a particular node. In such case node is assigned as the root node and this root node will constantly propagate PREQ routing messages that maintain the paths to all node in the mesh cloud. The root sends PREQ messages by setting the DO and RF flag to 1. Upon receiving a PREQ frame from the node the Mesh STAs updates the value of TTL and path metric for PREQ message and broadcast it to its neighbors. When PREQ frame is received by a Mesh STA, depending on *Proactive PREP* flag Mesh STA decides to reply for PREQ or not. Also if Mesh STA wants to establish a bi-directional link with the root node, it sends a PREP message to the root. Consider a mesh network where the Mesh STAs are backbone for providing Internet in a university. The majority of mobile STAs connected to the mesh network want to connect to Internet. In such case, most of the traffic will be passing through the portal nodes which will be the root node in pro-active routing. Also, Mesh STAs are almost stationary in this case, so the peer links will be stable. In this proactive PREQ mechanism, will congest the network with unwanted traffic through mesh backbone. Proactive PREQ mechanism will be a chatty mechanism if PREP is activated for all reception of PREQ frames. An alternative for this is RANN mechanism. Instead of sending PREQ message by the root node, the root will send RANN message notifying the Mesh STAs the presence of root node. Mesh STAs which want to establish a connection between the root will send a PREQ message to root through the Mesh STA where the RANN message is received. Once the root node receives this PREQ message from Mesh STA, it replies with PREP. RANN is advantageous only if there are few Mesh STAs, that want to establish communication between the root. Also when a path is broken the node reports it to the root with PERR message.
According to the draft, IEEE 802.11s uses the Airtime Link metric to calculate the quality of the path. This metric calculates the amount of resources used by the frame for traveling through a path. It considers the time taken by the frame depending on the bit rate at which the frames can be transmitted, the overhead posed by the PHY implementation and the probability for retransmission [2]. The draft does not mention about the method for calculating the loss probability. The Airtime Link metric can be calculated by the formula,

$$c_a = [O + \frac{B_t}{r}]\frac{1}{1 - e_f}$$

where O is a constant overhead latency, B_t is the test frame size, r is the data rate Mb/s, e_f test frame error rate. Other link metric were also proposed by different researchers and NMH (New Metric for Hybrid Wireless Mesh Protocol) [3] is metric based on two hop channel diversity and hop delay.

3.4 Internetworking

Internetworking in mesh network is done with help of gateways node called Portals. Portals are Mesh STAs which interconnect a mesh cloud to another mesh cloud, i.e a mesh cloud with different profile or it interconnects the mesh network to other LAN network or the Internet. Once a Mesh STA is assigned to work as Portal, it should notify other Mesh STAs in the network. Portals uses Portal Announcement (PANN) frame for this purpose. When Mesh STA receives a PANN message from a Portal, it stores the Portal MAC address and the associated path metric value and broadcast it again. Every Mesh STAs in the mesh cloud will have the list of Portals in the mesh cloud and path metric to that Portal. Depending on the path metric value, a Mesh STA will use a Portal to communicate with external network.

3.5 Medium Access Control

For medium access control, mesh stations implement Mesh Coordination Function (MCF). MCF is a combination of contention-based (mandatory) and scheduled access methods (optional). MCF also uses the medium access mechanism in 802.11, the Enhanced Distributed Channel Access (EDCA). The optional part of MCF to improve the QoS is the Mesh Coordination Channel Access (MCCA). The difference of EDCA from the implementation in 802.11 is that a Mesh STA can send multiple frames in alloted time period [7]. This transmission duration is called Transmission Opportunity (TXOP). The optional part MCCA is a distributed protocol where the Mesh STA reserves the medium to sending frames in the future called MCCA opportunities (MCCAOP). If a Mesh STA A wants to send some frame to Mesh STA B in the future, Mesh STA A sends a MCCAOP setup request message to the Mesh STA B. Once the Mesh STA A gets a time slot in the future, it will advertise this information by broadcasting it to other Mesh STAs and when the reserved time arrives, Mesh STA A will access medium by using standard EDCA. The issue with this approach is that Mesh STA A does not have priority over STAs in the network that do not support MCCA. Once MCCA transmission is done, the Mesh STAs will use EDCA for further contention if does not a have MACCOPs left for the future. [6]

3.6 Other features

Synchronization: According to the draft, synchronization is optional for the IEEE 802.11s. It extends standard beacon frames used in 802.11 with additional Information Element (IE) for 802.11s. Similar to 802.11, Mesh STA send their local timestamp which is the copy of Timing Synchronization Function (TSF) when the beacon is to sent. Beacon frames are sent at Target Beacon Transmission Time (TBTT) [7]. In 802.11s Mesh STAs will use the Mesh Beacon Collision Avoidance (MBCA) mechanism to avoid the collision of beacon frames by the idea of giving different TSF for each Mesh STAs. Initially, Mesh STAs will choose a random value to TBTT (SelfTBTT) and broadcast it. Upon receiving a SelfTBTT from a Mesh STA the receiver will calculate the common Mesh TSF and it will adapt its own local Mesh TSF. In such way, a Mesh STA can determine the TBTT of its neighbors and adjust its sending to avoid collisions. The special IE frame is used by Mesh STA to propagate the information of TBTT to other Mesh STAs along the mesh cloud. This will adjust the TBTT of each Mesh STA and reduce the chance for collision.

Power Management: An important aspect is the power management of the nodes in a mesh cloud. Mesh STAs can be either battery powered or not. IEEE 802.11s draft proposes two new power management modes. It is important to reduce the power utilization by the nodes without compromising the performance of the mesh cloud i.e less packet loss. For this, three modes (one from 802.11) can be used:

- **Active Mode:**In this mode, Mesh STAs operates in the 802.11 standard Awake mode and Mesh STAs are always active by participating in data forwarding, path discovery and other mesh activities. Since the Mesh STAs are always awake, the power consumption will be high. Normally Mesh STAs which are connected to direct power are set to active mode.
- **Light Sleep Mode:** As the name suggest, the Mesh STAs will wake up to full power whenever the Mesh STA want to send some frames or when it is expected to receive some frame from its neighbors. Turning on and going back to sleep will consume a lot of energy, so it is wise to use this mode if the node is not handling high backbone traffic.
- **Deep Sleep Mode:** In this mode, the Mesh STAs will wake up only when the Mesh STA wants to send the beacon frames. During this awake time, Mesh STA will send its buffered traffic. Since messages are only sent during its awake period, messages can expect a delay up to the interval between two beacon frames.

Security: Mesh networks are vulnerable to all attacks in 802.11 like signal jamming, wormhole attack etc. Apart from that, mesh networks may face attacks based on their constraints such as limited battery power, bandwidth, low computation power and mobility [10]. There are reported attacks based on these constraints, like giving enormous computation to a node and reducing its performance, battery exhaustion (sleep deprivation attack) etc. In 802.11s Mesh STAs perform the dictionary attack-proof Simultaneous Authentication of Equals (SAE) algorithm. SAE provides authentication between two Mesh STAs with a pairwise master key (PMK) [6]. It encrypts the communication between peer links and each peer links in the mesh cloud is independently secure. If a Mesh STA wants to broadcast a frame, it must use its broadcast traffic key to encrypt the message and it must also notify others with its new key for every new peering. Due to this independent pairwise authentication, 802.11s does not provide end to end encryption. Authentication is another important aspect. When a Mesh STA joins the network, it should authenticate with a centralized system to prove its authenticity. Approaches like Secure Transient Association or Imprinting can used for this purpose [10].

Congestion Control: Congestion control is optional according to the draft. The congestion normally occurs in the nodes which are central to the network than peripheral nodes. When a Mesh STA is congested it can use the management frames to indicate others about the high traffic in the node and expected duration for congestion. Then neighbor nodes can slow down the messages expected to travel through congested node. The congestion control messages are flooded across the network so that all Mesh STAs can be aware of the high traffic in a node.

4 Case Study

In this section we discuss the mesh networks One Laptop Per Child (OLPC) [2] and Seamless Mesh (SMesh) [1]. Each of these networks were designed for specific objectives.

4.1 OLPC

One Laptop Per Child (OLPC) was an educational project with the goal to develop distributed education devices. For this purpose, they used a special laptop called OLPC XO, a low-cost and low power device. The idea was to connect those device together as a mesh cloud. It is the first device to implement almost the complete draft apart from peer link encryption, access control, synchronization and power saving methods. The implementation of HWMP routing protocol and airtime metrics has its own features and was different from the standard draft proposal. The first difference was the path asymmetry, i.e. in IEEE 802.11s HWMP, the path or route found by on-demand path selection were considered as bi-directional paths i.e. if on-demand path selection algorithm finds a path S→D, then it is assumed that there is also a path from D→S. But in OLPC, it is considered as uni-directional. In

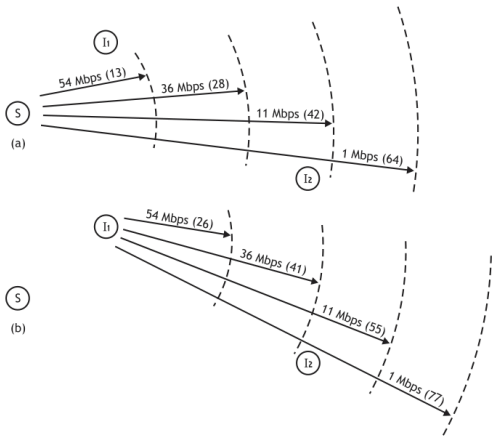

Figure 4: Path discovery process in OLPC (PREQ clusters) [2]

order to have a bi-directional path, same method of path selection is need to be performed from D→S. The second difference was in metrics. The cost for a given link was calculated on the basis of PREQ frames that successfully reached at destination and also there is no account for error probability other than the reception of PREQ frames [2]. Next, we discuss the path discovery mechanism in OLPC.

The on-demand path discovery mechanism in OLPC is modified from the standard techniques. XO devices broadcast PREQ frames at different data rates (54 Mbps, 36 Mbps, 11Mbps and 1 Mbps) with a fixed link cost of 13, 28, 42 and 64 (higher the cost lower the data rate) respectively as seen in the Fig.4. This PREQ frames will from a PREQ cluster by transmitting at different rate. As shown in Fig.4, the node S transmits the frame at different rate to intermediate nodes. When an intermediate node receives a PREQ from a node, it checks the frame rate at which it was sent and re-broadcast it after a short delay. Nodes will wait for a certain amount of time after a PREQ frame are received for further re-broadcasting and this delay is know as *rreqdelay*. During this delay nodes may receive different PREQ frames from the same sender with different data rate or from different sender. Then it will re-broadcast the PREQ frame along with link cost of the best received data rat. This process is called Network Wide Broadcast (NWB) and continues until it reaches the destination. In Fig.4, intermediate node I1 will broadcast the PREQ from S with data rate of 54 Mbps (link cost 13) to its neighbors. The intermediate node I2 receives PREQ frame with data rate 11 Mbps (link cost 55) and I2 will re-broadcast it after a certain rreqdelay. During the process of re-broadcast, nodes will make a new PREQ frame with updated link cost and broadcast it. The DO and RF flags for path discovery is not considered on OLPC path discovery process. Because it is necessary that intermediate node must forward the PREQ frame with link update in this path discovery mechanism and the response for PREQ frame is to re-broadcast the PREQ frame, not to acknowledge with PREP frames.

As mentioned OLPC project did not implement several features in the draft. OLPC nodes have no idea of links being established. Security features were established in the higher layer and absolutely no security features in the link layer. Even though the XO were low power device, OLPC project did not consider the power saving mechanisms in the draft. Apart from these drawbacks, OLPC tried implementing a successful mesh network with these devices.

4.2 SMesh

Seamless Mesh or SMesh is a project which was mainly targeted to design a mesh network for supporting real time application to communicate with external networks. For achieving that goal, it should offer a seamless and fast handoff between Mesh APs. In SMesh, the entire network is seen as a single AP to the mobile client. So when a mobile client moves from one AP to another AP, the handoff should be quick, in order to reduce the packet loss in between. Real time applications like VoIP

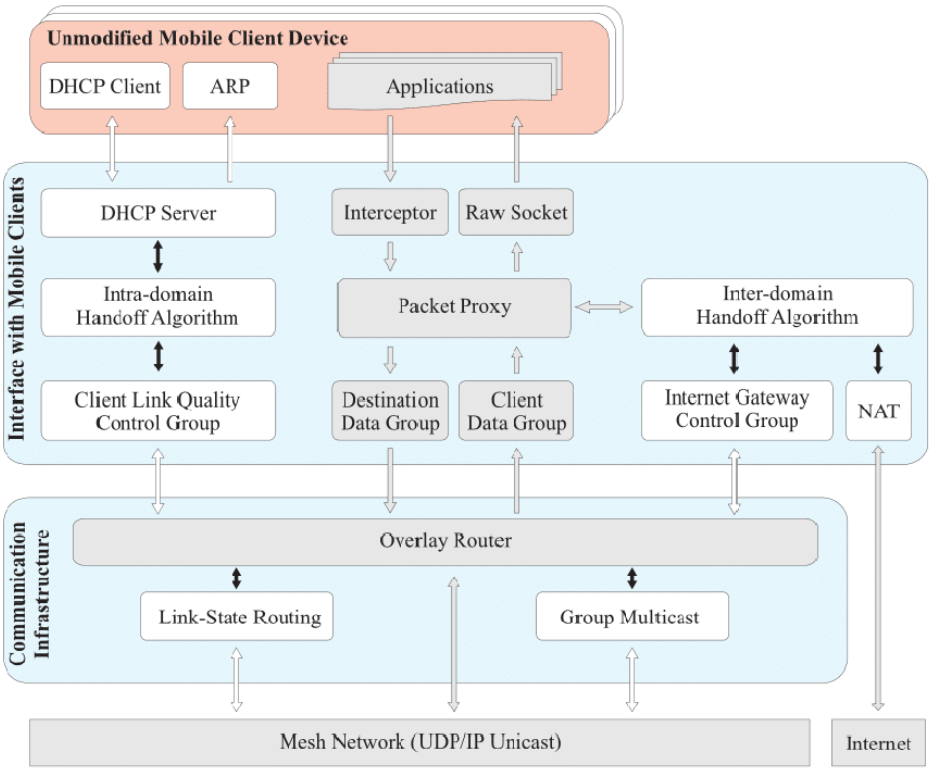

Figure 5: Architecture of the SMesh [1]

need a handoff latency less than 100 ms for maintaining the quality. In SMesh, handoff procedure can be divided into intra-domain and inter-domain handoff. Intra-domain protocol of the SMesh was designed to handle mobility of the mobile clients inside the network. Inter-domain protocol is designed to provide free flow Internet connectivity with reduced packet loss while switching the access points. SMesh also provides a hybrid routing protocol that optimizes the routes of wireless and wired links in a multi-homed environment. SMesh was developed above Spines messaging system for forwarding and coordinating between APs. Spines messaging system was developed by the Distributed Systems and Networks Lab at Johns Hopkins University and at Spread Concepts, LLC which provide unicast and multicast communication in an overlay network environment. Next, we discuss the architecture of SMesh, Intra-domain and Inter-domain handoff protocols used by the network.

4.2.1 Architecture

In order to provide interruption free Internet connectivity to the mobile clients inside the mesh network, the connections opened by a mobile client through AP should remain connected through out the mesh coverage area. Mobile clients are not considered to be the part of SMesh topology (The word node refers to the Mesh STA which are part of the SMesh). Fig.5 shows the SMesh architecture to achieve above goal. It has two main components, 1) Communication Infrastructure and 2) Interface with Mobile Clients.

Communication Infrastructure: The Communication Infrastructure of the SMesh relies on the Spines messaging system. SMesh instantiates a Spines daemon in every Mesh STAs and periodically sends hello message to its direct neighbors for tracking the links. This link information along with sequence number of the link (to identify update information) is flooded in the network using a link-state protocol. The Mesh STAs in SMesh form a group which will used by the Spines messaging system to

multicast the routing information. Each node in the network will be a member of a multicast group. For example, the node which Portals or Internet gateways will join a multicast group called *Internet Gateway Multicast Group* (IGMP). So whenever a Mesh STA joins or leaves the group, the Spines daemon will notify other node through a reliable flood similar to the link-state protocol. The information is saved as a tuple (*mesh_ node_ address, group_ address*)in Spines. Based on the group membership, Spines will build a multicast trees for sending the routing information.
When a node is turned on, the node broadcasts some message to notify its presence to its neighbors. When such a message is received by a node, depending on the Received Signal Strength (RSS), it establishs a link between the nodes and advertise this link information to other nodes. Other important aspect in SMesh is that, the nodes which are in IGMP (Internet gateway) group will establish a wired overlay link. In such a way the gateways forms a fully connected graph using their wired infrastructure. So SMesh will have both wired and wireless links. The cost of sending message through wired link is less than wireless links, so SMesh uses a different link metric than 802.11s draft suggested.

Interface with Mobile Clients: SMesh provides the illusion of single distributed access point to the mobile clients by always providing same connectivity information i.e. same IP address, Netmask and Default Gateway through DHCP. For this purpose, every node runs a DHCP server, it is the responsibility of DHCP servers to provide same IP to client through out the network. For this it calculate IP using a hash function on clients MAC address. In such a way, clients will have the same IP address through out the network.
Each mobile client belongs to a unique multicast group in the mesh called *Client Data Group*. A mesh node in the vicinity of the client will join a group so that there will be at least one node every group. i.e. the mobile client will be connected to this node or AP. It is one of key differences in SMesh that the APs decides about the nodes that can connect with it rather than clients connecting to a AP. So if AP finds that it can provide a client better connectivity then that AP, it joins the respective Client Data Group. If a client, internet gateway or a node wants to send a message to another client which is inside the SMesh then the data is send to node which handles thats client's Data group. Its the responsibility of the node that handles the Data group to forward the message to the client. It is done with the help of interceptor, to grab a message from a client and a raw socket to send a message to the client. Packets which are sent by the client destined to Internet are sent to Internet Gateway by forwarding it to anycast group (IGMP). When a reply is received, the Network Address Translator (NAT) will send the packet to the appropriate Client Data Group and then to the client. So if the node moves to a different SMesh node, then the node which handles the client will join the Client Data Group and will forward the data to the client. So if there is two or more mesh nodes in a Client Data Group, the client will receive duplicate IP packets. Next, we will discuss about the Intra-domain and Inter-domain handoff protocols.

4.2.2 Fast Intra-Domain Protocol

As mentioned, the handoff procedure depends on the Mesh APs of the SMesh network. When a client moves from one position to another, SMesh tracks the client and mesh node which can provide better connectivity to the client forces the client for connecting to its AP. To achieve this, SMesh uses gratuitous ARP message to change the default gateway without changing the IP address in the client side. In such a way, a client feels like it is connected to a single AP. In order to monitor the clients, SMesh relies on heartbeat using DHCP and ARP messages. DHCP server instructs the clients to renew IP every 2 seconds which serves as a heartbeat to keep track of the client. It can be done by sending ARP requests and monitoring the APR responses. Both DHCP and ARP replies are broadcasted by the client so that other mesh nodes can check its link quality with the client.
So when mesh node believes that it has better connectivity with the client, it will join the client's Client Data Group. Apart Client Data Group, SMesh has another multicast group called *Client Control Group* which is used to share other mesh nodes in the client's vicinity about the link quality

metric for a client and to decide which AP is best to serve that client. Both groups work together to handle the intra handoff process of the client. To initiate the client handoff, the mesh node will send a gratuitous ARP message which will update the local ARP table of client with the value it received. So if a mesh node wants to forcefully change the AP of a client, it sends a unicast ARP message to the client for changing the MAC address of the default gateway. In such a way the default gateway IP address of the client will remain same and client will feel like its connected to a single AP.

4.2.3 Fast Inter-Domain Protocol

Apart from intra-domain handoff, it is necessary to provide continuous inter-domain handoff. When mobile clients move with in the network, it should maintain its connection with the Internet. In SMesh the TCP and UDP connection are handled separately. For a TCP connection the source IP, destination IP and the port remains constant during the life of connection. The Internet destination regards source as the connection coming from a Internet gateway of the SMesh network. When a client moves from one AP to another, it might change its Internet gateway too which results in connection loss. To handle this, Internet gateways of SMesh monitor the packets its receiving. If an Internet gateway receives a TCP packet which is not SYN packet and it does not have an entry for that connection in its NAT table, then the it forwards the packet to IGMG group to notify the original owner of the connection. The original owner notifies the IGMG that this connection belong to him and it tunnel the reply for TCP packet back the Internet gateway to the node that handling the client. There might be a situation like the original gateway is crashed and Internet gateway did not get any response from the IGMG. In such a case, the Internet gateway will send RST packet to the client requesting for closing the existing connection (but connection remains open from internet gateway to the internet).
UDP connections are generally connection-less, but many real time applications build their own protocol above UDP to meet latency requirement. In SMesh, UDP is classified as connection-less and connection oriented based on the port number. Connection-less are easy to handle because when a new UDP packet arrives at a Internet gateway, it will consider as new request. For connection-oriented, the Internet gateways use the similar mechanism as in TCP. Internet gateway which receives the UDP message from the client forwards the packet to IGMG and will also sent packet to the destination. If there is owner for that particular UDP, it will also do the same procedure as in TCP handoff. The end-host in the Internet may see duplicate UDP packets. Internet gateway which is connected to the client too, will wait for replies from IGMG to check whether if there any other Internet gateway hold the ownership for the UDP packet. If not it claims the ownership for of the UDP connection.
SMesh is a complex mesh network but it satisfies the constraints of real time applications. The testing of the network founds that the management overhead of the network grows linearly with the number of clients connected to the network but it is independent is of the amount of data that clients send or receive.

5 Conclusion

The IEEE 802.11s draft helped to solve a lot of issues and answered a lot of open questions. In this seminar we investigate the technical side of 802.11s draft and compared different networks based on it. The final draft has a flexible design and also helps user to solve inter-vendor compactability issues. For example, the routing protocol HWMP, provides flexibility to use between pro-active and reactive protocols which can be tuned according to the scenario. Even though it was able to answers a lot of open questions, still there are lot of questions to be answered. The management overhead of mesh networks is the biggest question. Management overhead increases according to the number of users in networks. Apart from that, the security side of Mesh network is still an open question where patches for lots of attacks need to be found. In SMesh network, intra domain handoff protocol uses ARP gratuitous messages to update the ARP table which is a threat to the network. If an attacker find

the format of that special ARP message (since links are not encrypted), he can attack the clients by redirecting them to a different AP. Overall 802.11s was able to solve most of the open issues.

References

[1] Yair Amir, Claudiu Danilov, Raluca Musuăloiu-Elefteri, and Nilo Rivera. The SMesh wireless mesh network. *ACM Transactions on Computer Systems (TOCS)*, 28(3):6, 2010.

[2] Ricardo C Carrano, Luiz Magalhaes, Débora C Muchaluat Saade, and Célio VN Albuquerque. IEEE 802.11 s multihop MAC: A tutorial. *Communications Surveys & Tutorials, IEEE*, 13(1):52–67, 2011.

[3] Sidi Ould Cheikh, Malik Mubashir Hassan, and Abdelhak Geuroui. New metric for HWMP protocol (NMH). *International Journal of Computer Networks & Communications*, 5(2):49, 2013.

[4] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, and Laurent Viennot. Optimized link state routing protocol (OLSR). 2003.

[5] Stefano M Faccin, Carl Wijting, Jarkko Kenckt, and Ameya Damle. Mesh WLAN networks: concept and system design. *Wireless Communications, IEEE*, 13(2):10–17, 2006.

[6] Guido R Hiertz, Dee Denteneer, Sebastian Max, Rakesh Taori, Javier Cardona, Lars Berlemann, and Bernhard Walke. IEEE 802.11 s: the WLAN mesh standard. *Wireless Communications, IEEE*, 17(1):104–111, 2010.

[7] Guido R Hiertz, Sebastian Max, Rui Zhao, Dee Denteneer, and Lars Berlemann. Principles of IEEE 802.11 s. In *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 1002–1007. IEEE, 2007.

[8] Eng Sherif Kamel Hussein and Khaled Mohamed ALmustafa. Triangle routing problem in mobile ip. *Journal of Communication and Computer*, 10:1554–1565, 2013.

[9] Vishnu Navda, Anand Kashyap, and Samir R Das. Design and evaluation of imesh: an infrastructure-mode wireless mesh network. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 164–170. IEEE, 2005.

[10] Muhammad Shoaib Siddiqui and Choong Seon Hong. Security issues in wireless mesh networks. In *Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on*, pages 717–722. IEEE, 2007.