CHAPTER 4

HANOVER BETWEEN ACCESS POINTS

4.1 INTRODUCTION TO HANOVER PROCESS

In general handover is defined as the process required to be executed to transfer the physical layer connectivity of a MU from one AP to another AP. In addition to physical connectivity it may also a required transfer of some context or state information with respect to this MU. In terms of 802.11 WLAN this physical connectivity is called the association of an MU with the AP. Sometimes association is also called attachment.

Here we will describe the handover process from the point when a MU operating in infrastructure mode has already associated with a WLAN AP in a Distribution System. When a MU has already associated to a current AP (which we will call a old-AP) and starts moving away from AP, the wireless link quality between MU and this old-AP starts to deteriorate and at some point falls below threshold, which in turn triggers the handover process to start. At this stage the MU starts to search for other APs to attach to by doing a scanning process (which can be either active or passive).

Once the MU finishes scanning it sorts out the scan results and selects an appropriate AP to attach to and then MU authenticates (i.e., 802.11 authentication) and re-associates with the selected AP, by sending appropriate messages/frames to selected AP.
4.1.1 Steps during handover process

To simplify the handover analysis Velayos et al. (2004) proposed splitting the handover process into three phases as shown in Figure 4.1, the first phase is called the detection phase it starts the handover process, actually it seems that this phase is not thus a part of handover process although necessary for analyzing the handover in detail and for optimizing the handover efficiency therefore is included in handover process analysis. The search phase is the second phase during which the MU scans for candidate APs. Third phase is called the execution-phase in which the MU selects the appropriate AP from the scan results obtained in second phase, and tries to attach to the selected AP by sending appropriate management frames to that selected AP.

Mishra et al. (2003) split the handover process into two steps: discovery and reauthentication. The discovery step defined by Mishra et al. (2003) is essentially the combined detection and search phase as described by Velayos et al. (2004). While re-authentication step is the same as the execution-phase in Velayos et al. (2004). We will follow the division of handover process as proposed by Velayos et al. (2004) because it gives greater flexibility in describing and dealing with each step of a handover.

Detection phase: The detection phase in fact is the continues process of checking the quality of the link between MU and AP, and the triggering of the handover process once that quality degrades to a certain pre-defined value which we call here the handover-threshold.

Search phase: The search phase starts by scanning for APs. The MU must wait for prob_delay_time before starting scanning process, which can be either passive or active. Here we will examine the search phase when scanning is done actively.
**Step 1:** Search phase starts, and after start prob delay timer, the current_channel is set to 0.

**Step 2:** MU waits until prob delay timer reaches prob_delay_time.

**Step 3:** MU increments current_channel by 1.

**Step 4:** MU switches channel to current_channel, starts max channel timer, min channel timer, and issues probe request on current_channel.

**Step 5:** MU listens for any probe responses and traffic on current_channel, until min channel timer reaches min_channel_time.

**Step 6:** If no probe responses are received and the MU does not see any traffic, then the current_channel is assumed empty and the MU moves to step 3 to start same process for the next channel, otherwise if a probe response or traffic is seen on the current_channel, then MU listens on this channel until the max channel timer reaches max_channel_time.

**Step 7:** MU processes all received probe responses on current_channel and checks if current_channel = maximum_allowed_channel. If not it then goes back to step 3 to start the same process for next channel.

**Step 8:** Once it has gone through all channels it sorts out the processed scan results and picks the best APs (i.e., the one which may provide the best link quality).

**Step 9:** Search phase ends.

**Execution Phase:** The execution phase utilizes the BSSID (MAC address) of best AP learned during the search phase and tries to connect to that AP as shown in Figure 4.1 by sending first an authentication message to
the selected AP, then once it receives a success message in an authentication response frame from this AP, it sends a re-association frame and expects a re-association response frame from this AP. This indicates that the MU is now associated with this new AP.

Obviously this phase is not executed unless a suitable AP was found during the search phase.

Figure 4.1 shows the normal handover process which is usually inferred from the procedures defined in IEEE 802.11 standard. From this figure we can see that the total handover latency is the sum of delay incurred by execution phase and search phase. However, this is not the case in a real handover. This is show that different kinds of traffic patterns between the MU and AP require that the handover latency be measured in a different way.
Unfortunately there is not standard way to measure handover latency. Previous researchers Mishra et al. (2003), Vatn et al. (2003), Velayos et al. (2004) and Shin et al. (2004) have used different criteria for measuring handover latency. According to our understanding handover latency can be categorized in two types: Raw handover latency and Real handover latency.
**Raw handover latency:** We say that the raw handover latency is the total delay incurred by the search and the execution phase of the handover process. So thus the raw handover latency is measured by measuring the time interval from the first probe request by MU to the re-association response from the new-AP, plus the prob_delay_time.

So the formula for measuring raw handover latency is,

\[ Rhl = \text{ProbeDelay} + (\text{ReAssResponse} – \text{FirstProbeReq}) \]

where

- **Rhl** = Raw handover latency
- **ReAssResponse** = Time stamp of Re-Association response frame from new-AP
- **FirstProbeReq** = Time stamp of First Probe Request sent by MU
- **ProbeDelay** = Fixed time [Total Association Time – Search Phase(prob_delay_time)]

Also note that either there is no layer 3 traffic or it is not accounted for when measuring raw handover latency.

**Real handover latency:** However when there is layer 3 traffic in WLAN when measuring the Real handover latency; its measurement consists of same two phases of handover process (search phase and execution phase), but the detection phase must also be included when studying packet loss and handover decision techniques. The most difficult phase to analyze is the detection phase because it is a nearly continuous phase; thus we must chose the correct moment in the detection phase to mark as the start of the handover process. Real handover can be further divided into three types: Upstream Real handover latency, Downstream Real handover latency, and Two-way Real handover latency.
4.1.3 Cross Layer Issues

Many networks, especially WLAN, need information from across layers. As we will see below this is more importantly from the lower layers to enable maximum throughput for different application usage. Thus there must be some standard defined for measurements and how to pass that information from lower to upper layers and vice versa. Even though IEEE 802 based networks can take advantage of the ways defined in IEEE 802 for passing information across layers, 802.11 which is also based on 802 does not take full advantage of this standard communication technique and does not share wireless medium knowledge from physical and MAC layer with the logical link layer and upper layers. Also there is no any standard method defined for wireless link quality measurement, so different WLAN interface cards implement link quality measurement in different ways.

This cross layer communication is usually referred to as cross layer signaling becomes more important when WLAN network access is used for different purposes. For example when a WLAN MU use, the WLAN for data access, interruptions due to handover are not usually noticeable to MUs. But when same MU uses the WLAN for real time or delay sensitive communication, then even the very small interruptions caused by handover may be noticeable, hence requiring special handling by upper layers, unfortunately the lower layers in WLAN did not give any information about these handovers to upper layers, therefore the upper layers can't optimize accordingly. Similarly WLAN networks don't pass signal strength and noise information to upper layers, which again often results in degradation of services at the higher layers.
4.2 HANDOVER BETWEEN ACCESS POINTS

In WLAN networks that use the Infrastructure Mode of the IEEE 802.11 standard, each MU is associated with an AP that provides access to the fixed network infrastructure. When the current AP workload is going to beyond the threshold, it is needed to change the AP. The most of the WLAN networks are used in telephony and multimedia applications the more important such handovers are becoming. In particular, there is a need to speed up the handover process such that it does not interrupt application level sessions.

The handover process is composed of three main phases:

**Phase 1:** Detecting the possible set of next APs, which is holding minimum no of APs among the APs.

**Phase 2:** Associating with that target AP, and finally

**Phase 3:** (re-)authenticating the MU to the network.

In this algorithm, we focus on the problem of speeding up the third, authentication phase.

Authentication of the MUs is an important security requirement in WLAN networks. In particular, due to the lack of a physical connection between the MU and the AP, authentication becomes indispensable for controlling access to the network. However, the authentication mechanisms used in WLAN were not designed to be exceptionally fast, and they are unable to guarantee low handover latencies needed by today's real-time applications.

Moreover, HOAP shortens the time delay for authentication during handover by pre-authorization and authorization dependency technologies,
with which mutual authentication between the AP is fulfilled before handover and the authorization granted by certain an AP can be extended to other reliable APs. Second, the MU initiating handover takes no account of traffic of the target AP, which is more possible to cause frequent handovers among several APs and results in low handover efficiency.

The HOAP enables an AP to make handover decision according to its load strategy and distribution of traffic load in the ESS. This greatly improves the handover success rate, and avoids frequent handover. Third, the MU initiating handover has no security guarantee scheme for handover.

Though the IAPP supports safe handover based on Remote Authentication Dial In User Service (RADIUS), the handover process with low efficiency is possibly threatened by Denial of Service (DoS) attacks.

The HOAP, however, may use the security strategies of wired networks to guarantee mutual authentication and authorization between the AP, and ensure the handover security of the MU by handover control at the AP.

4.2.1 Process of HOAP in Access Point

HOAP can be fulfilled at the AP with the following process, is also shown in Figure 4.2.
Figure 4.2 Implementation process of HOAP
**Step 1:** The MU establishes a connection and transfers the data with the current AP.

**Step 2:** The current AP makes handover decision according to the workload of current AP; the AP checks the validity of the target AP.

**Step 3:** The current AP sends the information about the MU to the target AP.

**Step 4:** The target AP changes the MU into a handover status.

**Step 5:** The target AP replies to the current AP with a successful transfer response.

**Step 6:** The current AP updates the local Layer 2 forward table, modifies the MU route in DS, and then deletes the local MU information.

**Step 7:** The current AP sends update of the Layer 2 forward table in DS.

**Step 8:** The target AP renews the local Layer 2 forward table and changes the MU into a status of completed handover.

**Step 9:** After receiving the acknowledgement, the current AP gives the MU a handover indication or a permission response to the handover request to inform it to be switched to the target AP.

**Step 10:** The MU sends reconnection request to access the target AP.