Abstract— An experimental evaluation of the handover performance in a 802.11b (WiFi) network has been obtained in terms of available bandwidth and handover latency. The network consists of two access points connected to a wired LAN and a measurement setup composed by laptop PCs, equipped with WiFi cards, on which a sniffer is used to capture all the packets transmitted on the radio link. Applications considered are streaming and ftp-like applications. The analysis of the handover delay is performed, showing the dependence on the network configuration parameters and results, both at the MAC and UDP/TCP layer are presented, to show how applications can suffer the handover latencies. It will be shown that these latencies can vary significantly for the same configuration of mobile stations and APs and that the primary source of delay is the scan procedure used to discover the new access point.

Keywords— Wi-Fi, 802.11b, handover.

I. INTRODUCTION

The wireless LAN standard 802.11b, known also as WiFi, is experiencing a great development [1], [2] and many networks are being installed in campuses, airports, stations, etc. In fact, WiFi can provide a wideband wireless access to the Internet by means of the so-called hot-spots.

The IEEE 802.11b specifications define two operating modes, namely ad hoc and infrastructure mode. In the ad hoc mode, two or more stations can recognize each other, establishing a peer-to-peer communication without the need of an access point (AP), while in the infrastructure mode all the mobile stations are associated to an AP that bridges all the traffic.

The AP and the associated mobile stations form a Basic Service Set (BSS), which roughly corresponds to a cell in a cellular network environment. The connection of more APs can extend a BSS into an Extended Service Set (ESS) [3]. Generally the WiFi scenario envisages nomadic stations, moving at pedestrian speed. Hence, a major objective is to provide a seamless handover procedure between different BSS [4]–[6].

II. HANDOVER

A Handover occurs when a mobile station moves out from the radio coverage of an AP, entering a new BSS. During the handover, management frames are exchanged between the mobile station and the AP. During this period the mobile station is not able to send or receive any data traffic. The handover procedure refers to the sequence of actions and messages exchanged by access points and a mobile station, resulting in the transfer of a connection from the origin-AP to the destination-AP. The state information transferred typically consists of the client identification and credentials, which allow the mobile terminal to gain network access and accounting information from the new AP. In a 802.11 network, this transfer can be achieved by an Inter Access Point Protocol (IAPP), or by a proprietary protocol. The complete handover process can be divided into two different logical steps:

1) Discovery
2) Re-authentication

A. Discovery

Due to mobility, the signal to noise ratio perceived by a mobile terminal might degrade. When it drops below a threshold value, it triggers the station to start searching for another AP, in order to remain connected to the LAN, and initiates the handover procedure. The discovery of a new AP is performed by means of the scanning procedure, which consists in monitoring different channels for beacon signals periodically transmitted by APs. The IEEE 802.11 standard defines two methods for scanning:

- Passive scanning: the station sets its frequency to a channel and listens to beacons from access points that use that channel.
- Active scanning: the station issues a so-called Probe Request, on which a Probe Response is expected within a given time frame.

Most of the 802.11 systems implement active scanning as it is found to be faster and more efficient. Performing a series of scans on different channels is called a sweep. To conduct a sweep, the station maintains a channel list. There are two kinds of sweep:

- Full Sweep: all channels in the channel-list are scanned
- Short Sweep: only a subset of the channel-list is scanned to speed up the roaming process.

The subset of the channel-list is dynamically created, and contains channels that have been found to be active during previous scans or where activity is most likely to occur, on the basis of interference criteria.

B. Re-authentication

The station attempts to re-authenticate to an AP according to the priority list. The re-authentication process typically involves an authentication and a re-association to a new AP. The re-authentication phase involves the transfer of credentials and other state information from the old AP. IAPP is a protocol which achieves this task, but also proprietary protocols could be used.

III. PHYSICAL LAYER PARAMETERS IN THE HANDOVER PROCEDURE

The basic measure that determines a roaming station to switch from one AP to another is the SNR value obtained from the beacon signals. Beacons are issued by all APs at a rate of 10 beacons per second. As soon as the value of the SNR drops below the so-called Cell Search Threshold, the scanning procedure is initiated. The SNR values obtained from each channel are compared with that measured on the active connection: re-authentication and re-association process is initiated when the difference between the two values exceeds a threshold ΔSNR. The roaming station will remain in the “cell search” state until the SNR has passed the Cell Search Threshold again.
A. Handover latency

From measurements we have found that the power loss \( PL \) along the wireless link obeys a log-distance model of the form

\[
PL(d) = 40 + \alpha \log (d) \quad [\text{dB}]
\]

(1)

where \( d \) denotes the distance, expressed in meters, and the attenuation coefficient has been estimated to be \( \alpha = 35 \).

From this model we can estimate the handover time as a function of the main parameters and of the speed \( v \) of the mobile terminal. Let us consider a model where the mobile terminal (MT) is moving from AP1 to AP2 and let \( d_1 \) denote the distances from AP1, \( d_{th} \) the separation between the APs, and \( d_{th} \) the distance from AP1 where the cell search procedure is initiated, as depicted in Fig. 1. Then

\[
T_{HG} = \frac{d_1 - d_{th}}{v}
\]

(2)

where the distance \( d_1 \) from AP1, considered as the origin AP, must satisfy

\[
\begin{align*}
  & d - d_1 < d_{th} \\
  & \alpha \log \frac{d}{d_1} > \Delta SNR
\end{align*}
\]

(3)

The first condition represents the possibility to connect to AP2 and the second represents the actual decision to change AP, on the basis of a better link quality. The value of the Cell Search Threshold \( SNR_{th} \) for the wireless cards has been estimated equal to 10 dB, 23 dB, and 26 dB, depending on the setting of the parameter sensitivity to 1, 2, and 3, respectively. Assuming a constant noise level \( N_0 \) of -95 dBm, the handover time increases linearly with \( d \) after a threshold value, as shown in Fig. 2 for a mobile speed \( v = 1 \text{ m/s} \), a transmitted power \( P_0 = 15 \text{ dBm} \), and \( \Delta SNR = 6 \text{ dB} \).

Note that the actual latency is in general dependent also on the scanning strategy used, in particular when the overlapping between the coverage areas of the APs is wide. In this case, in fact, as soon as the cell search begins, the beacon level from the new AP is high enough to satisfy the conditions on the SNR.

IV. EXPERIMENTAL SETUP

The 802.11 network consists of two access points (AP) located into an office environment as outlined in the map of Fig. 3. Two scenarios for the location of the APs are considered: in a first scenario the APs are located at the limits of each other coverage, while the second location is chosen to have a sufficient overlapping of the coverage areas, to reduce the handover latency. The position of AP1 is left unchanged, while the position of AP2 is denoted in Fig. 3 by AP2 and AP2’ for the first and the second case considered, respectively.

The APs are configured as root, that is, each AP is connected to a wired network and provides wired network access to the mobile terminals. We used two APs Compaq WL410 11 Mbps Wi-Fi, 10Base-T and PCMCIA interfaces. The APs are controlled via a web-based network management software (AP Manager) to set their parameters. A proprietary inter-access point communications between APs is implemented. Therefore, no control is applied on the authentication phase.

The measurement setup consists of a sniffer (Ethereal) installed on a laptop, able to capture and display packets from any interface, or display packets captured under a number of other capture programs (i.e. tcpdump), save captures to a number of formats, filter packets on many criteria and search for packets using filters and examine packets. all the packets transmitted on the radio channel, so that power levels and delays can be estimated, moving together with another laptop, where the application is running, as depicted in Fig. 4. The mobile terminals are notebook PC,
nearly an Acer TravelMate 527 TXV (CPU Pentium III 800 MHz, 128MB RAM, 256 MB cache, PCMCIA interface, OS Linux Red-Hat 9, Kernel 2.4.20-8) and a Dell Latitude (CPU Pentium IV 1700 MHz, 256 MB RAM, 256 KB cache, PCMCIA interface, OS Linux Red-Hat 7.3, Kernel 2.4.18-18.7.x), equipped with Compaq WL110 11 Mbps Wi-Fi PCMCIA cards realizing the radio interface according to the 802.11b standard. The application considered is a streaming using TCP or UDP at the transport level.

The system parameters that can be set in the network are the receiver sensitivity, the so-called distance between APs and obviously the position of the APs. Note that the sensitivity affects only SNRth according the values already mentioned while ΔSNR remains unchanged. The parameter distance between APs determines the rate at which the beacon signal is transmitted, thus giving different coverage areas for the reception of the beacon. Nevertheless, this parameter does not affect the value of SNRth.

V. RESULTS

In the first configuration, the two APs are positioned at a relatively large distance, so that the handover delay includes also a certain amount of time needed to move from the area of one AP to the other and the latency can be rather large. Due to the large distance the value of sensitivity should be reduced to the minimum, thus triggering the scanning to perform the handover only when the mobile is rather far away from the origin access. In Fig. 5 the histogram of the handover latency is presented for this configuration. It can be seen that the delay values are quite large, of the order of seconds, hence not compliant with delay sensitive applications. The mean value has been derived for the three possible values that can be taken by the parameter distance between APs, namely small, medium and large. The corresponding average delay is 2.76 s, 2.62 s and 2.53 s respectively, thus showing a certain amount of time needed to move from the area of one AP to the other and the latency can be rather large. Due to the in the reverse direction. Indeed, AP1 operates on channel 1 while AP2 on channel 6 and the scanning sequence is 1, 9, 6, 10, 11. This effect can be reduced dynamically adapting the channel list with a Short Sweep.

In the second configuration, the two APs are positioned close to each other with an overlapping region large enough to reduce the handover delay to a fast scan time. In this situation, in fact, it is very probable that the power received by the new AP on the transmission of the first Probe Response is high enough to switch to the new AP. In this scenario, the handover delay is presented in Fig. 7 for a sensitivity 2.

What can be seen clearly from these results are values of delay which are order of magnitude smaller than those obtained in the first scenario. To analyze the contributions of the different components on the overall delay, the delay of each phase is considered separately and presented in Fig. 8, where the histogram of the delay in the discovery phase is shown, and in Fig. 9, where the re-association delay is shown.

It can be seen clearly that the variability is mainly due to the scan phase, while the re-association phase introduces a delay which...
is almost constant.

Fig. 10 shows the histogram of the number of UDP packets lost during the handover, considering a streaming at 2 Mbit/s. Note that a UDP packet is lost if the MAC layer, employing automatic retransmission request (ARQ), does not succeed to transmit correctly the packet for three times.

A. Example of application: VoIP

As an example of application, we can consider the effect of the handover on a Voice over IP (VoIP)-like connection. In this case, the Round Trip Time (RTT) plays a fundamental role, since the delay encountered by the packets along the link must lie within strict limits, both in terms of absolute delay and of jitter. In particular the absolute delay should be kept below 100 ms. We assume a source emitting packets of 40 bytes at the rate of one packet every 20 ms, corresponding to a constant bit-rate of 16 kbit/s suitable to support the coded voice. RTT is measured by means of the ping command in a series of experiments where the mobile terminal moves from one AP to the other, thus performing at least one handover in its path. The histogram of the maximum RTT is presented in Fig. 11. It can be seen that the values of RTT are well below the maximum allowed for this kind of applications. Note that the mean RTT would be much smaller in the absence of handover, but the wireless link does not represent a bottle-neck so narrow to prevent this kind of applications.

VI. CONCLUSIONS

The performance of the handover procedure in a WiFi network has been investigated, relating the delay introduced by this procedure to the main network parameters and configuration. The handover latency can be ascribed primarily to the discovery phase in which the mobile terminal scans the set of RF channels and waits for the conditions on the power received from the APs to be satisfied. The delay, thus, can be reduced by a proper choice of the positions of the APs and a suitable definition of the sweep phase. It can be seen that the system can support applications rather sensitive to the delay and to its jitter, like VoIP or similar.

REFERENCES


Proceedings of WPMC04, 12-15 sept. 2004 Abano Terme (Padova), Italy