Reducing Handoff Latency in IEEE 802.11b with the Help of Neighbor Graph Using Carrier to Interference Ratio

Debabrata Sarddar[1], Joydeep Banerjee[1], Souvik Kumar Saha[1], Utpal Biswas[2], and M.K. Naskar[1]

[1] Dept. of Electronics and Telecommunication Engg., Jadavpur University, Kolkata – 700032
dsarddar@rediffmail.com, jogs.1989@rediff.com, souviksaha@ymail.com, mrinalnaskar@yahoo.co.in
[2] Dept. of Computer Science and Engg, University of Kalyani, Nadia, West Bengal, Pin –741235
utpal01in@yahoo.com

Abstract. IEEE 802.11 wireless networks have gained ever greater popularity nowadays. Handoff is a critical issue in IEEE 802.11 based wireless networks and latency in the handoff process is a major concern.

In this paper, we propose to reduce handoff latency for IEEE 802.11 wireless networks with Neighbor Graphs (NG) pre-scanning mechanisms. IEEE 802.11 uses 11 channels of which the channels 1, 6 and 11 do not mutually overlap. So these channels are expected to have a lower carrier-to-interference ratio (CI) compared to the other channels present under the same base station, which increases the channel's availability during handoff. Based on the NG pre-scanning mechanism, when handoff criterions have been met, we design an algorithm to first scan the channels 1, 6 and 11, if present under the next Access Point (AP), to reduce the scanning delay. We also introduce pre-authentication mechanism, which will effectively reduce the message processing delay.

Keywords: Handoff, Neighbor Graph, Selective channel scanning mechanism, Carrier-to-Interference (CI) Ratio.

1 Introduction

IEEE 802.11b based wireless and mobile networks [1], also called Wi-Fi commercially, are experiencing a very fast growth upsurge and are being widely deployed for providing variety of services as it is cheap, and allows anytime, anywhere access to network data. However they suffer from limited coverage range of AP, resulting in frequent handoffs, even in moderate mobility scenarios. Handoff, an inherent problem with wireless networks, particularly real time applications, has not been well addressed in IEEE 802.11, which takes a hard handoff approach [2]. Here a mobile host (MH) has to break its connection with its old access point (AP) before connecting to a new AP, resulting in prolonged handoff latency called link switching delay. Now-a-days, soft handoff procedure is in use. Here a mobile node is connected to its old AP

N. Meghanathan et al. (Eds.): NeCoM, WiMoN, and WeST 2010, CCIS 90, pp. 421–430, 2010.

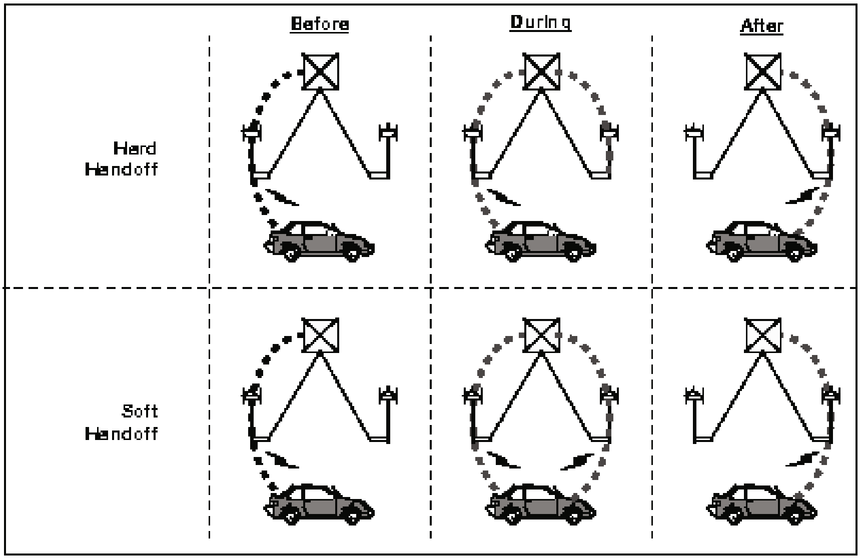


Fig. 1. Diagram showing mechanism of hard and soft handoff

till it makes connection with the new AP. This effectively reduces the packet losses incurred by hard handoff. A schematic diagram showing hard and soft hand off is given in Fig1 taken from [3].

With the advent of real time applications, the latency and packet loss caused by mobility became an important issue in Mobile Networks. The most relevant topic of discussion is to reduce the IEEE 802.11 link-layer handoff latency. IEEE 802.11 MAC specification [4] defines two operation modes: *ad hoc* and *infrastructure mode*. In the ad hoc mode, two or more stations (STAs) recognize each other through beacons and hence establish a peer-to-peer relationship. In infrastructure mode**,** an AP provides network connectivity to its associated STAs to form a Basic Service Set (BSS). Multiple APs form an Extended Service Set (ESS) that constructs the same wireless networks.

IEEE 802.11 standards for wireless LAN function on physical and lap layers; as IEEE 802.11b standard is compatible with the 802.11g standard; we focus on the former, since the proposed architecture also holds for 802.11g with slight changes. 802.11b uses 11 of 14 possible channels distributed over the range from 2.402GHz to

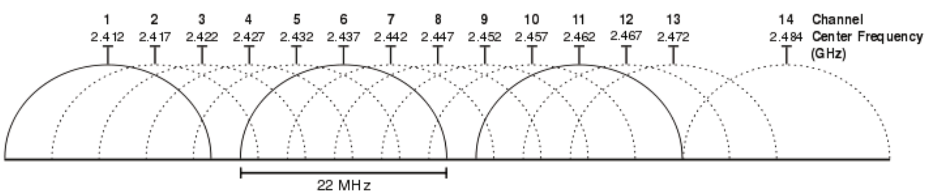


Fig. 2. The channel distribution diagram for IEEE 802.11 standards

2.483 GHz (as in Fig 2) with each channel being 22 MHz wide. Of these channels 1, 6 and 11 do not overlap.

We now describe the handoff procedure with its various phases.

1.1 Handover Process

The complete handoff procedure can be divided into 3 distinct logical parts: scanning, authentication and re-association. In the first phase, an STA scans for AP's by either sending Probe Request messages or by listening for beacon message. After scanning all channels, an AP is selected using the Received Signal Strength Indication (RSSI) and CI ratio, and the selected AP exchanges IEEE 802.11 authentication messages with the STA. Finally, if the AP authenticates the STA, the STA sends Re-association Request message to the new AP.

1.2 Scanning

Scanning can be divided into *active* and *passive* scans. During an active scan, the STA broadcasts a probe request packet asking all APs in those specific channels to impart their existence and capability with a probe response package. In a passive scan, the STA listen passively for the beacons bearing all necessary informations like beacon interval, capability information, supported rate etc. about an AP. The active scans introduce two parameters:

'*Min Channel Time*' represents the arrival time of the first probe response. So a client must listen for this period of time to decide whether there are any APs on this channel. It is recommended to be set as 3-7 ms.

'*Max Channel Time*' is the estimated time to collect all probe responses. It is supposed to be of the magnitude of tens of milliseconds. For all practical implementation, the maximum channel time is set to 30 ms [5].

1.3 Authentication

Authentication is necessary prior to association. Authentication must either immediately proceed to association or must immediately follow a channel scan cycle. In pre-authentication schemes, the MN authenticates with the new AP immediately after the scan cycle finishes. Exchanging null authentication frames takes about 1-2 ms.

1.4 Re-association

Re-association is a process for transferring associations from one AP to another. Once the STA has been authenticated with the new AP, re-association can be started. Previous works has shown re-association delay to be around 1-2 ms.

The overall delay is the summation of scanning delay, authentication delay, and re-association delay. According to [5], 90% of handoff delay comes from scanning delay. The range of scanning delay is given by "$N \times T_{min} \le T_{scan} \le N \times T_{max}$", where N is the total number of channels according to the spectrum released by a country, T_{min} is Min Channel Time, T_{scan} is the total measured scanning delay, and T_{max} is Max Channel Time. Here we focus on reducing the scanning delay.

The total handoff process is shown is Fig 3.

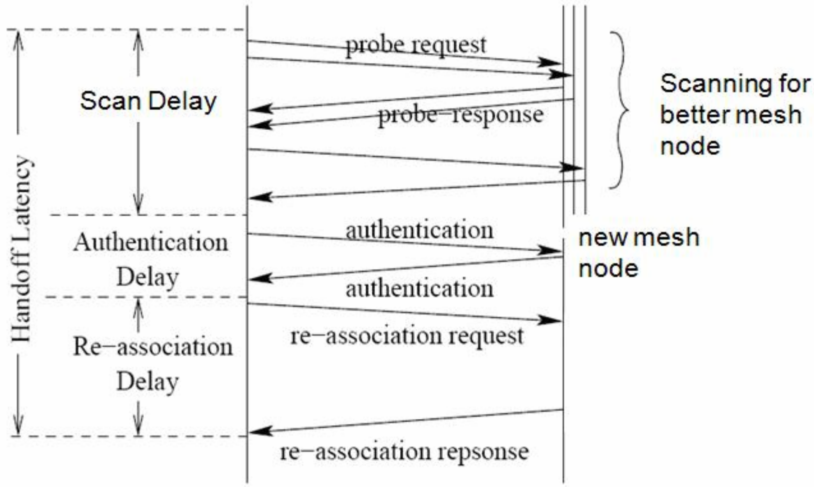


Fig. 3. The total handoff process in brief

We divide our paper into the following sections: Section-2 discusses the related works in this field; the proposed method is explained in Section-3. Section-4 discusses our simulations and experimental results, followed by conclusions and future works, and finally the references.

2 Related Works

Most of the related works focus on reducing this delay in the scan phase, as delay in the potential phase is hardware dependent and in the authentication phase is negligible in an open wireless environment. The process of AP scan and reconnection is intolerably slow, of the order of 200-300 ms or even longer, of which 80-90% delay is attributed to *probe delay* [4]. In real scenario, it is seen that maximum handoff latency for Voice over IP (VoIP) applications is 50 ms [5]. To reduce handoff latency in wireless LAN using IAPP [7], an algorithm on context transfer mechanism using 'Neighbor Graph' (NG) [4] was suggested in [7]. However, IAPP was only reactive in nature and creates an additional delay in a handoff. One approach on Physical layer (PHY) is the method using two trans-receivers, where a wireless mobile node (MN) has two Wireless Network Interface Cards (WNICs) [4], one for keeping connection to current AP and the other for scanning channels to search for alternate APs [8].

In this paper, we propose a selective scanning mechanism using NG to solve the problem of handoff latency. CI ratio forms an essential part in channel selection process during handoff, though traffic plays a more dominant role. IEEE 802.11b uses 11 channels out of 14 possible channels, of which only channels 1,6,11 do not mutually overlap. So these channels will have a very low interference with other frequency. It may have a noticeable interference only if the same channel is used by any other APs within its frequency re-use range. Thus it is quite evident that these channels will have a high probability of having a greater CI ratio as compared to the other channels within the same AP. So based on this fact, when the MN responds to handoff, according to the pre-scanning mechanism of NG, it first looks for the potential AP and then first scans the channels 1, 6 and 11, if present. If this fails, it will start scanning the other channels. In addition, we propose to reduce the authentication delay by pre-authentication method, where the authentication process is performed during the scan phase.

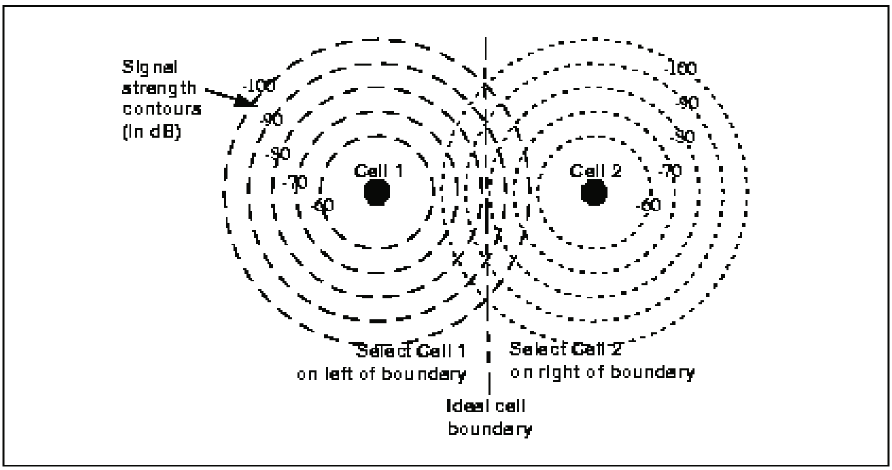
3 Proposed Method

The maximum range up to which the signal can be transmitted is determined by the height of the antenna and the power of the signal is inversely proportional to the square of the distance from the AP. But due to fading, the signal strength is never equally spread in all direction even for an omni-directional antenna. There are mainly two types of fading responsible for the uneven distribution of the signal strength from the AP. They are namely *fast fading* (fading due to scattering of the signal by object near transmitter) and *slow fading* (fading due to long term spatial and temporal variations). Ideally without fading, the cell's coverage area would be circular, but due to fading it becomes an undefined contour. Signal strength contours for two APs operating in ideal condition without fading is given in Fig 4 (a) and operating in real condition with fading is given in Fig 4 (b) both of which are taken from [3] . Here we define the coverage area of each AP to be concentrated within a hexagon of certain edge length, which is the best approximation so far considering uneven distribution of signal.

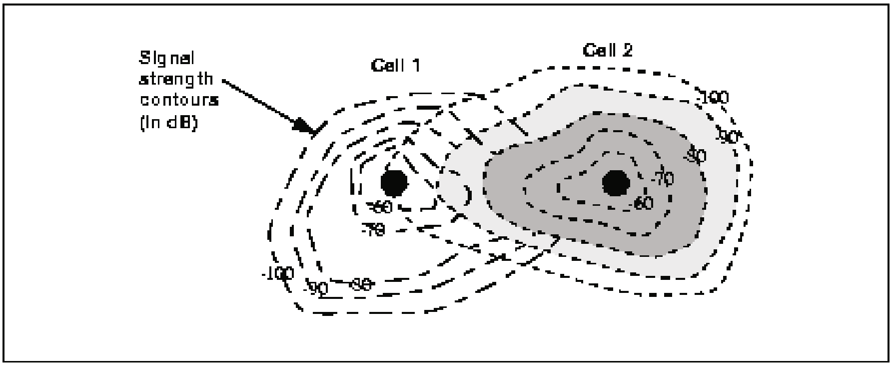
The same frequency band or channel used in a cell can be reused by another cell as long as the cells are far apart and the signal strength does not interfere with each other (this mechanism is shown in Fig 5 where the three yellow marked cells can use the same frequency channel to avoid frequency interference). Thus frequency channels are allocated in such a way that the interference due to any two neighboring APs, i.e., the co-channel interference is minimum. But within a cell, the channels used may be mutually overlapped and this may lead to interference within the same AP. We cannot reduce both the types of interference simultaneously. But for optimizing it to a minimum value, the channel allocation protocol is designed in such a way so that at least one of channels 1, 6 and 11 are made available to each AP. This is due to the fact that the channels 1, 6 and 11 are mutually non-overlapping. Due to increasing traffic, the need of greater frequency range is realized. Hence, by implementing the above procedure, we can thus use a maximum number of channels in one AP with at least one channel having minimum interference even in regions where signal strength is very low, thereby increasing the net *signal to noise ratio* (SNR).

Now handoff is primarily dependent upon signal strength received and the CI ratio. The term CI ratio is the ratio between the frequency band allocated to the MN and the interference associated with this frequency band. Thus as per our theory, channels 1, 6 and 11 are expected to have a greater CI ratio than the others. So, during handoff, if we scan channels 1, 6 and 11, if present, first, then there will be a greater probability that the call is transferred to any of these channels of the next AP. So based on CI ratio, it is seen that scanning non over-lapping channels is better for reducing the latency due to scanning delay.

Second generation wireless systems and most of the research works follow Frequency Division Multiple Access (FDMA) or Time Division Multiple Access (TDMA) for multiple access of a single channel frequency band. In TDMA, one channel is used by several users, with AP assigning time slots for different users, and each user is served in a round-robin method. In FDMA, the allocated frequency band for one channel is subdivided into many sub-bands and each sub-band is allocated by the AP to each user. Thus, in FDMA, it may be seen that a particular sub-band is allocated to a user which falls between the interference zones of channels within the same AP. Thus, protocols using FDMA techniques have a certain probability that during handoff, even when the channel is free, the user is allocated such a sub-band within the above mentioned region. Thus, it will encounter a very low CI ratio and the MN ceases to operate on that channel and scans for the next channel. During scanning of the non over-lapping channels, this problem will not be faced. So our method works even better in cases where FDMA is used for multiple access of a single channel.



(a)



(b)

Fig. 4. (a) It shows the distribution of signal strength of APs in ideal condition ; (b) It shows the distribution of signal strength of APs in real condition

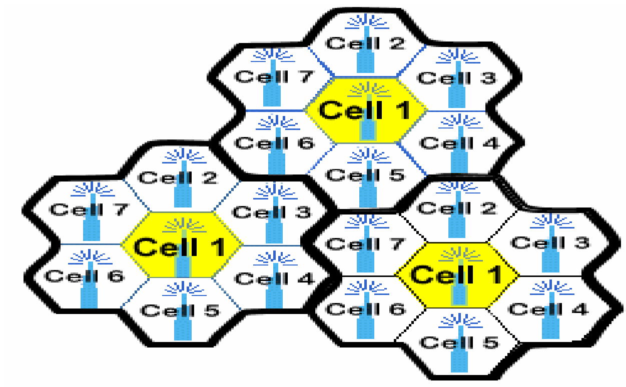


Fig. 5. Diagram representing cells that can use the same frequency channels

With these assumptions, we propose (i) a selective channel scan, as in [4], and (ii) pre-authentication scheme with the help of neighbor graph for reducing the total handoff delay.

3.1 Selective Channel Scanning

As in [3], the MN downloads from the server the data which not only contains the neighbor of the AP on which it is presently operating, but also the channels used by the neighboring APs. However the MN must wait for min channel time or max channel time as the MN does not know how many APs would respond to the probe request. So here we use unicast instead of broadcast which selects the potential APs to which the call may be handed off and scans only the channels associated with those APs. Selective channel probing with the help of unicast instead of broadcast brilliantly reduces the handoff delay by a massive percentage when compared with selective scanning or basic active scanning. Moreover, it was also stated that the MN has to wait for only the *'round trip time'* (rtt) for scanning each channel instead of the min channel time or the max channel time. We know that IEEE uses 11 out of the 14 possible channels, out of which 1, 6 and 11 are mutually non-overlapping. When the MN responds to handoff, according to the pre-scanning mechanism of NG, it first looks for the potential AP and then first scans the channels 1, 6 and 11 if present. If this fails, it will start scanning the other channels. As proposed in [4], the expected scanning delay using selective scanning is $t = N' \times \tau + \alpha$, where 't' is the scanning delay, N' is the number of channels scanned, 'τ' is the round trip time and α is the message processing time. 'τ' is the summation of the time taken for the Probe Request to be sent to the selected AP's and for the Probe Response to be received, which, in our case, is nothing but the Min Channel Time, which has been estimated to be around 3-7 ms.

3.2 Pre Authentication

To reduce the message processing delay, authentication is done during scanning phase. By this method, the authentication delay vanishes and the message processing delay, α, is composed only of the re-association time. Thus the parameter 'α' is reduced by at least half of its initial value and hence the net time delay, t, as proposed in [3], is greatly reduced. This can be implemented as proposed in [9] and [10].

Thus, the authentication time, which was very minute in proportion as compared to scanning phase delay of previous methods, would now command a greater percent of time delay, because, in our case, the scanning phase delay has been much reduced. However, by the process of pre-authentication, even this delay is nullified. So our method reduces the net handoff latency by a great extent as compared to the previous proposed methods. The experimental results are given in the forthcoming section. It gives a brief overview of the simulation process and the results obtained conform to our theory.

4 Experimental Results

For the simulation part, we used a 2D-plane with APs on centre of hexagons packed together. The heights of each antenna were considered to be the same and the topology distribution was also considered to be similar. We used hexagons for specifying the range of the APs as hexagons can fit side by side like honey combs and is mainly used by all research workers for this category of simulations. The frequency was allocated as per the protocols that are generally followed in frequency allocation in IEEE 802.11 standards. Calls originate on a memory less basis, that is, they follow Poisson distribution function and use the channel within the AP on whose range the call is created. The channel allocated to it is determined by the AP. The channel allocation is considered to be static and FDMA was used for multiple accesses. The CI ratio was calculated for each channel within each AP which is an important parameter for our method. Moreover, separate CI ratios were calculated for all the sub bands when a single channel was used by multiple users. The sub bands' CI ratio takes into account the CI ratio of the channel on which the multiple access is carried on. Now, we considered various instances of time where there is a case where a randomly generated MN has a need for handoff. The different parameters, like the number of existing MNs in the two APs, the CI ratios etc. at that instance of time were taken into consideration. Then we applied our method, i.e, the MN first looks for the potential AP and then first scans the channels 1, 6 and 11 if present. If this fails, it will start scanning the other channels. We also neglect the authentication delay as pre-authentication was done during the scan phase. We considered the round trip time to be 3 ms and the message processing time which comprises of only the re-association time was neglected to carry out our calculations.

We made a sample run of our simulation and calculated the time required for handoff at regular intervals of time. We calculated 100 such instances and calculated the total time required for the handoff to take place. From a particular sample run we got the average time delay for all 100 instances as 6.1129 ms. The graph of this simulation is plotted in Fig 6, which shows the various handoff delay times in the 'Y' axis in milliseconds, for each instance, which is shown in the 'X' axis. The variation of results obtained from other simulation was negligible. So we can consider that our method reduces the net handoff delay to a minimum of around 6 ms in the best case which is much lower than the previous results.

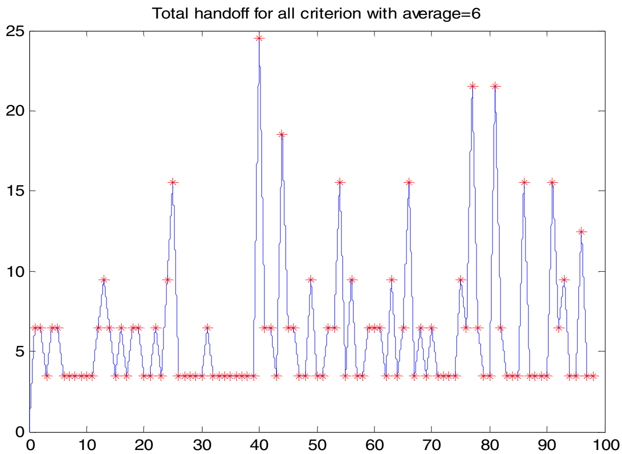


Fig. 6. Graph showing the handoff delays at various instances

5 Conclusion and Future Work

In this paper, we claim our contributions as discussed. Firstly, we have discussed a pre-scanning procedure using channels 1, 6 and 11, which greatly reduces the scanning time. Here, we have set a best scenario time of about 6 ms, which is an improvement on the best scenario time of 18 ms previously set [9]. Secondly, we have used pre-authentication in which the STA authenticates the new AP just after the scanning phase, thus minimizing the message processing delay.

Our discussion is based on IEEE 802.11b standard, even though the proposed setup is also valid for IEEE 802.11g with minor adjustments.

As is evident, the discovery phase is still the most time consuming phase of the handoff process. Future simulations may be done using different topologies with modifications regarding selective scanning and pre-authentication using IAPP.

Moreover, our method works best in networks where FDMA is used for multiple accesses. Though networks using TDMA has also reduced handoff latency by this method, but still in the best case scenario, the net time delay is a bit more than that of networks using FDMA. So, further research work can be done in this field.

We have considered link layer handoff delay only. For intra-system handoff, a bit more time will be required due to increase in message processing delay. Though we have nullified the authentication delay, yet the re-association delay cannot be neglected while doing the simulations. But for this case, as the re-association delay is very small as compared to the handoff delay, so we can neglect it for our experimental results.

References

1. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards (1999)
2. Puangkor, W., Pongpaibool, P.: A Survey of Techniques for Reducing Handover Latency and Packet Loss in Mobile IPv6

3. Taylor, M.S., Waung, W., Banan, M.: Internetwork Mobility The CDPD Approach. Pearson Education, Inc., London
4. Kim, H.-S., Park, S.H., Park, C.-S., Kim, J.W., Ko, S.-J.: Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph (July 2004)
5. Teng, J., Xu, C., Jia, W., Xuan, D.: D-scan: Enabling Fast and Smooth Handoffs in AP-dense 802.11 Wireless Networks
6. Zhai, H., Chen, X., Fang, Y.: How well can the IEEE 802.11 wireless lan support quality of service? IEEE Transactions on Wireless Communications 4(6), 3084–3094 (2005)
7. Huang, P.-J., Tseng, Y.-C.: A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks
8. Ohta, M.: Smooth Handover over IEEE 802.11 Wireless LAN, Internet Draft: draft-ohta-smooth-handover-wlan-00.txt (June 2002)
9. Powar, Y.A., Apte, V.: Improving the IEEE 802.11 MAC Layer Handoff Latency to Support Multimedia Traffic
10. Kim, E.-D., Ahn, D.-K., Kim, S.-Y., Cho, S.-J.: Improvement of Pre-authentication with Neighbor Graph for Fast Handoff in WLANs
11. Mishra, A., Shin, M., Arbaugh, W.: An Empirical Analysis of the IEEE 802.11 Mac Layer Handoff Process. In: ACM SIGCOM 2003 (April 2003)
12. IEEE, part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. IEEE Standard 802.11 (1999)