Handoff Protocol for Bluetooth Public Access

Aman Kansal and UB Desai
Department of Electrical Engineering, Indian Institute of Technology, Bombay
Powai, Mumbai-400076, India
Phone: +91-22-572-0651, Fax: +91-22-572-3707
e-mail: aman@ee.iitb.ac.in, ubdesai@ee.iitb.ac.in

ABSTRACT

A major requirement for providing Internet connectivity to mobile handhelds is the wireless network access for handheld devices. As an alternative to the expensive 3G networks, which share 2 Mbps in several square kilometers, the use of short-range wireless technologies like Bluetooth that shares 1 Mbps among just 7 users, has been proposed. This is much more economical as it works in the unlicensed band and leverages the existing wired broadband infrastructure. In such a Bluetooth network, the mobiles will frequently move out from the range of one access point into that of another, requiring seamless handoff. We discuss a new algorithm to support fast handoff at the wireless layer. Our method exploits the continuity of the user's path and existing connection information at the older access point to reduce the handoff delay. It inter-works with IP micromobility protocols, such as Cellular IP, for managing other mobility related issues at layer 3. Simulations reveal that our proposed method reduces the handoff delay by more than an order of magnitude and significantly enhances the bandwidth utilization.

INTRODUCTION

In this paper we discuss one aspect of the problem of providing network connectivity to mobile handheld devices. For handheld devices, it is advantageous to use low power short-range wireless technologies instead of long-range networks like 3G-UMTS. As discussed in [1], using short-range wireless connectivity in the unlicensed band is significantly more economical than 3G, and it can also preserve the "Internet Culture" marked by simple payment models and openness. Moreover, a large fraction of the network access from handheld devices occurs in indoor areas where wired broadband access is available and wireless access points can be installed to reach out to the handheld devices over short-range wireless links.

We assume the following architecture for providing network connectivity to handheld devices. A wired network exists in the regions where connectivity is required. Access points are distributed such that their wireless ranges cover the entire area in which connectivity is required. This set of access points along with the wired network interconnecting them, is referred to as the access network. Access points accept wireless connections from handheld devices and connect them to the Internet through the wired network.

Bluetooth [2,3] (now part of IEEE 802.15 group of standards [4]) is a short-range low power wireless technology, working in the unlicensed band, designed especially for compact handheld devices and can be used for building the mobile Internet as per the above architecture. Bluetooth however, does not itself provide a fast and seamless handoff. Special measures are thus needed to make the handoff fast enough for acceptable usage experience.

Techniques to handle mobility have been built for the Internet at layer 3. This is advantageous as it makes the mobility mechanisms independent of the wireless layer. The disadvantage is that the handoff of the mobile device from one access point to the next has to wait for the connection to be set up at the wireless layer. This causes excessive delay and packet loss. Thus, fast mechanisms to start the connection with the new access point during a handoff must be provided at the wireless layer.

We present a handoff algorithm optimized for the Bluetooth physical and medium access control (MAC) layers. Mobility management is not shifted from layer 3 to layer 2. A fast handoff protocol is added at the Bluetooth layer that helps the layer 3 mobility mechanisms to reduce the handoff delay, leading to better datarates. The added functionality required for handoff could be implemented using the standard host controller interface (HCI) that is part of all Bluetooth compliant hardware.

The paper is organized as follows. The next section describes some of the existing IP micromobility methods. The specific features of Bluetooth relevant to the design of a handoff protocol are described after that. Then, we discuss our proposed method for fast handoff, namely the mobile Bluetooth Public Access (mBPAC) protocol. A summary of its performance study is presented towards the end.

EXISTING METHODS

Global mobility in the Internet is typically provided thorugh Mobile IP (MIP) [5]. However, as the MIP methods are too slow for micromobility, or mobility within an access network, faster methods have been proposed for such usage. Some of these are:

1. **Hierarchical Mobile IP (HMIP)** [6]: Instead of a single foreign agent for the remote location of the mobile node as in MIP, there is a hierarchy of foreign agents which allow the mobile node to move within the foreign domain. The home agent continues to communicate with only the highest-level foreign agent. Certain improvements to HMIP are given in [7]. The use of layer 2 triggers is also proposed: Fast Handoff HMIP [8] and Proactive HMIP [9].

2. **TeleMIP:** This method [10] introduces load balancing and instead of a single foreign agent, multiple foreign agents take the responsibility of a single foreign agent in HMIP. Only two levels are maintained in the hierarchy.
3. **Cellular IP (CIP):** This protocol [11,12] also uses MIP for global mobility but maintains routes within the access network from the foreign agent (or gateway connecting the access network to the Internet) to the mobile nodes. It updates these routes as the mobile device moves from one access point to the other, by observing from which access point the mobile is sending packets.
4. **Hawaii:** Hawaii [13,14], like CIP, maintains routes within the access network, but it works above the IP layer and provides support for RSVP.
5. **Edge Mobility architecture (EMA):** In this method [15], the mobile node is allotted a local sub-net based address and IP like routing can be used.
6. **Intra-domain Mobility Management Protocol (IDMP):** In this method [16], the foreign network maintains a local care-off address for the mobile node, which it updates as the mobile moves within the foreign network.

A comparison of some of these methods has been made in [17]. However, as these methods all work at layer 3, they have the following limitations:

1. Loss of connection is detected only after the wireless connection is lost, such as through route cache timeout in CIP. The wireless layer can detect the loss of connection faster.
2. The mobile has to search and connect to the next access point on its own. In Bluetooth, this involves carrying out the time consuming inquiry procedure.
3. The mobility methods are limited to devices using IP. In compact dedicated devices, the application may directly access Bluetooth and it will be an added advantage to have handoff at that layer itself.

CIP has been used with Bluetooth in [18,19], where no special measures are taken to resume connection at the Bluetooth layer and long handoff delays are reported. Thus there is a need to exploit the specific features of the wireless layer and affect handoff in the shortest possible time, as is done in cellular telephony networks [20]. Most layer 2 mechanisms rely on power measurement, which is not a standard feature of Bluetooth. Hence appropriate alternatives must be chosen.

BLUETOOTH SPECIFIC ISSUES

Connection Establishment

Each handoff requires a new connection to be established with the access point that has come into the range of the mobile handheld. Connection establishment in Bluetooth consists of two phases:

1. **Inquiry:** This phase is required to discover the address of the device to which a connection is required. This may take upto 10.24s in an error free environment.
2. **Paging:** This phase is required to synchronize the frequency-hop sequences of the devices among which the connection is being set up. If the clocks of the two devices are synchronized to within –8 x 1.28*s* to 7 x 1.28*s*, then the page procedure will succeed within N_{page} x 16 slots (one slot is 625 ?s in the Bluetooth standard). N_{page} is 1 for page scan mode R0 and 128 for mode R1, leading to paging times upto 0.01s for R0 and 1.28s for R1. When the synchronization is worse than mentioned above, it may take double the times mentioned above.

A good handoff should exploit the address information known to the current access point in the access network to eliminate time consuming inquiry.

Channel Sharing

A single device can connect upto 7 active devices to itself. The device to whose hop sequence all other devices are synchronized after connection establishment is called the master. The group of the synchronized devices is called a piconet. The wireless channel is time division duplex and further time shared among devices in one piconet (Figure 1). The master controls the channel access. The master sends out packets in alternate slots and uses the intermediate slot to listen for a packet from the slave to which it transmitted. A slave can transmit only after it receives a packet from the master. A good handoff scheme should inter-work with the channel sharing mechanism without wasting extra slots for handoff.

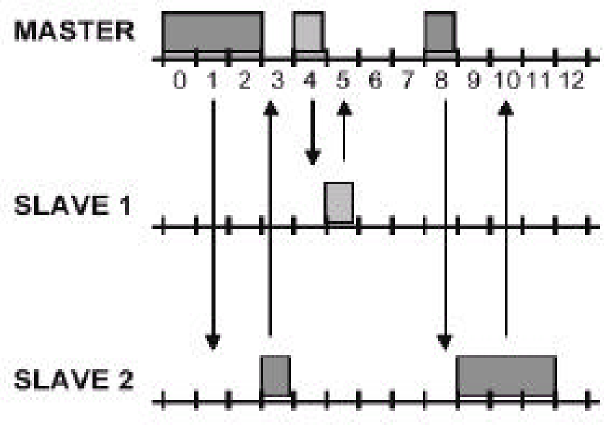

Figure 1. Wireless medium access control within the piconet.

MBPAC HANDOFF PROTOCOL

The mobile Bluetooth Public Access (mBPAC) protocol enables fast handoff of a mobile moving from the range of one access point to that of another. It has better performance than direct application of Layer 3 methods as it exploits the address information known to the access network before handoff and uses wireless layer specific methods to detect loss of connection.

The CIP access architecture is preserved for routing within the access network and managing mobility at layer 3. However, when a handheld moves, the connection is resumed at the wireless layer using mBPAC. This is achieved by adding mBPAC functionality to CIP base stations. These mBPAC aware base stations, referred to as mBPAC access points (AP's), appear as standard CIP base stations to the CIP network and other wireless technologies may work at non-mBPAC aware base stations in the same network. At the same time mBPAC also makes the CIP implementation transparent to the mobile nodes. Additional mBPAC communication is required between neighboring AP's. Figure 2 shows the architecture of the mBPAC based access network. The operation of mBPAC is described below.

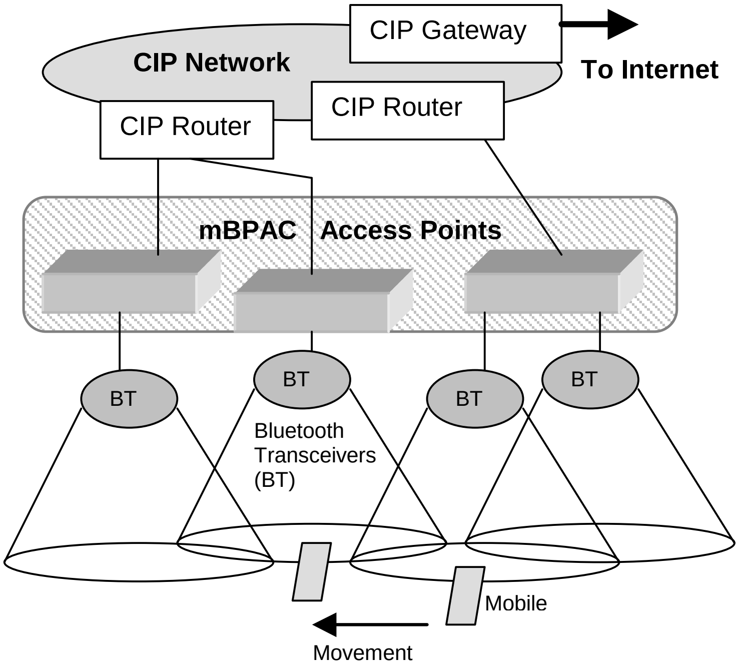

Figure 2. Proposed mBPAC access architecture.

The mBPAC access network accepts new mobile devices through the standard Bluetooth procedure of inquiry and paging. This may be carried out by having dedicated entry points that carry out inquiry continuously to detect new devices. Alternatively, the AP's may themselves carry out inquiry scan as per scan mode R2 (which amounts to spending 10ms on inquiry scan in every 2.56s) and then affect a master-slave switch to make the mobile node slave to the AP.

Once a device has entered, as long as the device stays connected, its handoff from one AP to another is handled as follows:

1. **Detecting loss of connection:** The AP is the master in the piconet and the mobile handhelds connected to it are slaves. The AP polls each device in round robin fashion. The poll packet would typically be the data packet to be sent to the slave unless there is no data to be sent. The slaves have to acknowledge every packet from the master. The AP assumes a loss of connection if a slave does not acknowledge a packet for the timeout period, $T_{pollreplytimeout}$. At the mobile, too a similar procedure is followed to detect loss of connection. At both the AP (master) and the mobiles (slaves) the timeout value, $T_{pollreplytimeout}$, is specified to be equal to the maximum number of slots that may pass between two successive poll turns. $T_{pollreplytimeout}$ depends on the number of slaves in the piconet and whether the AP is involved in paging. When no paging is taking place, $T_{pollreplytimeout}$ may be a maximum of 80 slots (50ms) for seven slaves with multislot packets of length 5. When the master is involved in paging, for processing a "handoff message" (described later) from a neighbor, the timeout is increased both at the master and the mobiles. A HOLD packet is sent to the mobiles, which suspend their timers for duration equal to $T_{AP\ Page}$. The timer is resumed either on expiry of the $T_{AP\ Page}$ duration or if the master sends a regular poll message before that. $T_{AP\ Page}$ is the maximum time an AP spends on paging on receiving a handoff message. It is 128 slots (80ms) in mBPAC. The AP also sends CIP route cache updates on behalf of the mobile if there is no data from a mobile. This makes the AP appear as a standard CIP base station to the CIP network.
2. **Resuming connection with next AP:** We define the *Neighborhood set* of an AP *A* as the set of all AP's into whose range a mobile node may have ventured after having been known to be present in the range of AP *A*, $T_{pollreplytimeout}$ time units ago. As soon as loss of connection is detected, the current AP sends a handoff message, consisting of the clock and address of the lost mobile, to all the AP's contained in its *Neighborhood set*. These messages wait in the handoff message queue at the AP's to which they are sent until those AP's process them. Each AP receiving the handoff message finishes its poll round and checks if the handoff message queue has any pending messages. If it has, the AP sends a HOLD message to all its connected slaves to suspend their connection loss detection timers for duration of $T_{AP\ Page}$. It then pages the mobile node using the clock and address received from the neighbor. Since the page scan mode used at the mobile is R0, each page train needs to be attempted only once, which means both trains can be tried out in 32 slots. Four page attempts are made for robustness, leading to $T_{AP\ Page}$ equal to 128 slots, which is 80 milliseconds. As a very recent clock record is used, paging will succeed in the first attempt.

As soon as connection is resumed, the new AP sends a route cache update for CIP routers to update the location of the mobile and hence the route update in the network can happen as soon as the Bluetooth layer has established the new connection. As will be seen from simulations on handoff delay, in the following section, CIP should use a short cache timeout of 250ms. The cardinality of the neighbourhood set can be a maximum of 6 if AP's are installed in a hexagonal arrangement but it will be lower for most indoor deployment scenarios due to such constraints on the movement as walls and building structure.

Implementation Issues

The mBPAC protocol is based completely on the mandatory features of the Bluetooth protocol and does not use power measurements or any of the optional features. The complete handoff mechanism can be implemented using the HCI interface that all Bluetooth compliant hardware has to provide. The HCI commands used for mBPAC implementation are listed in Table 1.

TABLE 1. HCI commands required for mBPAC.

Hex Code	Command	Description
0x0001	Create_Connection	Inquiry for specified duration
0x0005	Write_Page_Timeout	Page, connect and set page scan mode
0x0019	Read_Scan_Enable	Get scan mode config.
0x001A	Write_Scan_Enable	Set periodic page, inquiry scan modes
0x001B	Read_Page_Scan_Activity	Check page scanning parameters
0x001C	Write_Page_Scan_Activity	Set page scanning parameters

SIMULATION RESULTS

A simulator has been built to evaluate the behavior of the access network with different numbers of stationary and mobile nodes [21]. The simulator is designed to capture all the relevant features of the Bluetooth data-link layer, which affect the performance of mBPAC. It implements the complete frequency-hopping scheme, addressing and timing to study the effect of paging and inquiry procedures on connection establishment and the handoff protocol.

Handoff Delay

Simulations are performed for cases with varying number of mobile nodes, fixed nodes, and with different numbers of neighbor handoff messages waiting due to simultaneous handoffs.

Let the number of devices already connected to the AP when the mobile arrives be s and the number of neighbor messages to be processed before the paging attempt for the mobile can be made be k. When there is no neighbor message in queue the paging can start after one poll round. The handoff delays obtained for varying k and s have been plotted in Figure 3. Each value plotted is obtained by averaging over 100 runs of the simulation.

Datarates

To study the datarate performance it is assumed that s stationary devices are connected to an AP and s_m mobile devices move in and out of its range. Also, the cardinality of the *Neighborhood set* is assumed to be N. This means that each handoff would produce N-1 false neighbor messages leading to waste paging attempts. As the maximum number of mobiles that may connect to an AP is 7, s and s_m vary between 1 and 7 under the constraint that $s + s_m$? 7. These ranges cover various possible load conditions and number of mobiles that may be present in the access network. In the simulations, we record the number of slots allotted to each device for data in the presence of handoff under varying load conditions. These measurements in terms of slots may be converted to actual datarate achieved based on which packet type is used for data transfer by the mobiles and AP's. The maximum datarate is achieved when multislot packets of length 5 are used without any forward error correction, that is, DH5 packets provided by the Bluetooth standard. The datarate achieved by one mobile device for the case N = 4 is plotted in Figure 4.

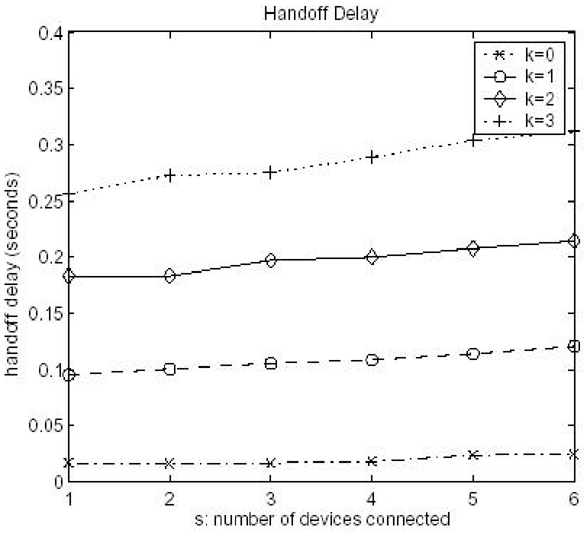

Figure 3. Aggregate handoff delay for varying s and k.

All datarates shown in the plots are symmetric datarates, that is, same datarate is available from the AP to mobile and from the mobile to the AP. The maximum datarate achieved is 215.43 kbps with one mobile and one stationary node. The minimum datarates are above 61 kbps with the AP loaded to full 7 devices. In comparison, if the devices are stationary, then the maximum datarate that Bluetooth can provide is 217 kbps for 2 devices and 69 kbps for 7 devices. Thus mBPAC is able to extract most of the available bandwidth while supporting handoff. In the simulations, we assume that dedicated entry points carry out the entry procedure. If however, the AP's themselves are used for entry, it will waste only 10 ms in 2.56s on inquiry scan and a few slots on exchanging responses, which means that the results will hold

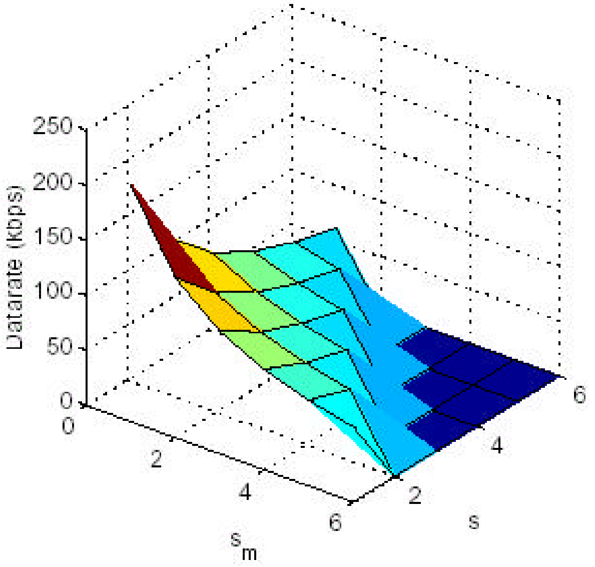

Figure 4. Datarate achieved with DH5 packet type at a mobile terminal for varying s and s_m (N=4).

for that case to a close approximation.

Comparison with pure CIP

CIP performance without the mBPAC modifications has been reported in [18] for handoff purposes. The handoff delays for mBPAC are better by more than an order of magnitude. The total time to resume connection after the mobile once moves out of range is found to range from 8 to 25 seconds in [18] of which an average of 20s was to detect loss of connection and an average of 5s to resume connection. With mBPAC the total delay is less than 0.25s. If the common Bluetooth class 3 devices having a range of 10m are used, then the range of one AP can be traversed in 20s at an average walking speed of 1m/s. A handoff taking 25s is unacceptable. Hence, the use of a special method such as mBPAC is essential. Due to large handoff delay, the datarate achieved and number of mobiles supported at an AP would be much lower in pure CIP.

CONCLUSION

This paper described why layer 2 optimizations are required for handoff and presented our new handoff protocol that promises rapid handoff, achieving efficient utilization of the bandwidth at the MAC layer. Only the standard features of Bluetooth are used and our method inter-works with the layer 3 micro-mobility protocols.

Future work may include reducing the cardinality of the *Neighborhood set* by using mobility tracking algorithms such as those proposed for cellular networks [22]. Further, the *Neighborhood set* could be partitioned and paging could be carried out progressively in partitions with reducing probability of containing the mobile [23].

The proposed schemes improve the performance of existing methods significantly in terms of handoff delay, datarates available to mobile nodes and the number of mobiles supported at an AP. Thus, they can significantly enhance the performance of any CIP network into which they are incorporated.

REFERENCES

[1] D Schefstrom, "Designing a Mobile Internet," *Proc. Fifteenth International Conference on Computer Communication,* vol. II pp. 750-767, August 2002.

[2] Bluetooth SIG, “Bluetooth specification version 1.1: Core,” http://www.bluetooth.com.

[3] C Bisdikian, “An overview of the Bluetooth wireless technology,” *IEEE Communications magazine*, vol. 39(12) December 2001, pp. 86-94.

[4] IEEE 802.15 Working Group for WPAN, http://grouper.ieee.org/groups/802/15/

[5] C Perkins, “IP mobility support,” Internet RFC 2002, 1996.

[6] E Gustafsson, A Jonsson, and C Perkins, “Mobile IP Regional Registration,” Internet draft, draft-ietf-mobileip-reg-tunnel-04.txt, March 2001.

[7] H Haverinen and J Malinen, “Mobile IP regional paging,” Internet draft, drafthaverinen-mobileip-reg-paging-00.txt, June 2000.

[8] K El-Malki and H Soliman, “Fast handoffs in mobile IPv4,” Internet draft, draftelmalki-mobileip-fast-handoffs-03.txt, September 2000.

[9] P Calhoun, T Hiller, J Kempf, P McCann, C Pairla, A Singh, and S Thalanany, “Foreign agent assisted hand-off,” Internet draft, draft-ietf-mobileip-proactive-fa-03.txt, November 2000.

[10] Subir Das et al., “TeleMIP: Telecommunication-enhanced mobile IP architecture for fast intradomain mobility,” *IEEE Personal Communications*, vol. 7(4), August 2000, pp. 50–58.

[11] A Campbell, J Gomez, C-Y Wan, and S Kim, “Cellular IP,” Internet draft, draft-ietf-mobileipcellularip-00.txt, January 2000, http://comet.ctr.columbia.edu/cellularip/pub/draft-ietf-mobileip-cellularip-00.txt.

[12] AT Campbell, J Gomez, S Kim, AG Valko, C-Y Wan, and Z Turanyi, “Design, implementation, and evaluation of cellular IP,” *IEEE Personal Communications*, vol. 7(4), August 2000, pp. 42–49.

[13] R Ramjee, T La Porta, S Thuel, and K Varadhan, “IP Micro-Mobility support through HAWAII,” Internet draft, draft-ramjee-micro-mobility-hawaii-00.txt, March 1999.

[14] R Ramjee, T La Porta, S Thuel, K Varadhan, and L Salgarelli, “IP micromobility support using HAWAII,” Internet draft, draft-ietf-mobileip-hawaii-01.txt, July 2000.

[15] A O’Neill, G Tsirtsis, and S Corson. Edge Mobility Architecture. Internet draft, draft-oneill-ema-01.txt, March 2000.

[16] S Das, A McAuley, A Dutta, A Misra, K Chakraborty, and SK Das, “IDMP: An intradomain mobility management protocol for next-generation wireless networks,” *IEEE Wireless Communications*, vol. 9(3), June 2002.

[17] P Reinbold and O Bonaventure, “A comparison of IP mobility protocols,” Technical Report, Infonet group, University of Namur, Belgium, http://www.infonet.fundp.ac.be.

[18] S Baatz, M Frank, R Gopffarth, D Kassatkine, P Martini, M Scetelig, and A Vilavaara, “Handoff support for mobility with IP over bluetooth,” *Proc. 25th Annual Conference on Local Computer Networks (LCN’00)*, Tampa, FL, USA, November 2000.

[19] M Albretch, M Frank, P Martini, M Scetelig, A Vilavaara, and A Wenzel, “IP over Bluetooth: Leading the way to a new mobility,” in *Proc. 24th Annual Conference on Local Computer Networks 2000*, Lowell, USA, October 1999, pp. 2–11.

[20] GL Stubor, *Principles of Mobile Communication*, Chapter 10, Kluwer Academic Publishers, 1996.

[21] A Kansal, “A handoff protocol for mobility in Bluetooth public access,” *Masters Thesis*, Indian Institute of Technology Bombay, 2002.

[22] A Chandra, D Bansal, R Shorey, A Kulshreshtha, and M Gupta, “Characterization of mobility patterns based on cell topography in a cellular radio system,” *Proc. IEEE International Conference on Personal Wireless Communications (ICPWC)*, Jaipur, India, February 1999.

[23] W Wang, IF Akyildiz, GL Stubor, and B-Y Chung, “Effective paging schemes with delay bounds as QoS constraint in wireless systems,” *Wireless Networks*, vol. 7, no. 5, September 2001, pp. 455-466.