# Motion-Constraint Based Handoff Protocol for Mobile Internet

Aman Kansal and UB Desai
Department of Electrical Engineering,
Indian Institute of Technology, Bombay

***Abstract*—A major requirement for the mobile Internet is the wireless network access for handheld personal 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 (sharing 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, however, the mobiles will move out from the range of one access point into that of another more frequently, 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.**

***Index Terms*—Handoff, micromobility, Bluetooth, hot-spot communications**

## I. INTRODUCTION

IN this paper we discuss one aspect of the problem of providing network connectivity to mobile handheld devices such as PDA's, security e-tags, electronic museum guides or any information device which may be used while the user is moving. 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. 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.

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. Our algorithm reduces the handoff delay by more than an order of magnitude and also leads to better bandwidth utilization.

It may be noted that 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 in section III. Our proposed method, namely the mobile Bluetooth Public Access (mBPAC) protocol, is discussed in section IV. A summary of its performance study is presented in section V and section VI concludes.

## II. EXISTING METHODS

The problem of supporting mobility in the Internet is typically divided into macromobility and micromobility. Macromobility, referring to support for mobility across the globe, may be handled using Mobile IP (MIP) [5]. For micro-mobility, that is mobility within a local access network, faster methods are available which reduce the delays and packet losses associated with MIP. Some of these are mentioned below:

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 which access point the mobile is sending packets from.
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]. All these methods work at layer 3 and handoff can be affected only after the wireless layer connection has been resumed. Though these methods can work with any wireless MAC/PHY layers, they have limitations:

1. Loss of connection is detected only after the wireless connection is lost, such as through route cache timeout in CIP. It is possible to detect loss of connection much faster at the wireless layer.
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 and then connecting to the access point found.
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 resuming the connection is left to the Bluetooth layer and that results in long handoff delays. Thus there is a need for fast resumption of connection at layer 2, which can exploit the specific features of the wireless layer and achieve handoff in the shortest possible time, as is done in cellular telephony networks [20]. However, layer 2 mechanisms typically rely on power measurement to detect loss of connection and this is not a standard feature of the Bluetooth protocol. Hence an appropriate alternative must be chosen using the standard features available.

## III. BLUETOOTH SPECIFIC ISSUES

### A. Connection Establishment

To re-establish the connection rapidly during handoff, we need to consider the Bluetooth connection establishment mechanism. Connection establishment in Bluetooth consists of two phases:

- **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.
- **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 $-8 \times 1.28s$ to $7 \times 1.28s$, then the page procedure will succeed within $N_{page} \times 16$ slots (one slot is 625 µs 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.

The paging procedure cannot be eliminated from the connection establishment, as the hop sequences have to be synchronized for any communication to take place. The inquiry procedure however may be eliminated if the address information can be known through other means.

### B. Channel Sharing

A single device can page and 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 connected to one master (Figure 1). The master in each piconet controls the channel access. Alternate slots are used for sending and receiving. A slave can transmit only after it receives a packet from the master. 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.

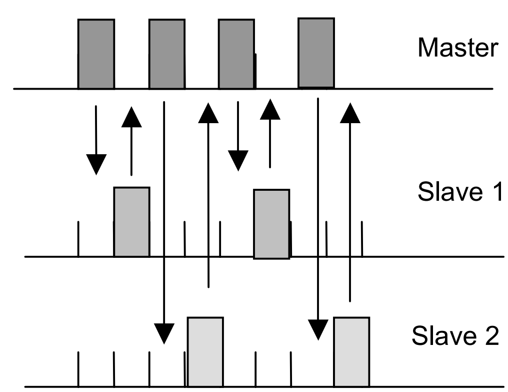


Figure 1. Wireless medium access control within the piconet.

## C. *Who Should Be Master*

When a piconet is being established between the mobile nodes and the access point catering to them, the issue whether the access point should be master or the mobile nodes, needs careful consideration. Typically the device which pages becomes the master and the scanning device becomes the slave. Thus, if the access point only performs scan, which is less time consuming, the mobile will carry out the inquiry, and will become the master initially. The access point should preferably be the master in the piconet to allow better channel sharing among the mobile nodes that are made slaves. If the mobile nodes are masters, the access point will have to involve itself in multiple piconets, reducing its bandwidth capacity. Since there will be no coordination between mobile devices this will also make the implementation of channel sharing and handoff difficult.

# IV. 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 exploits the motion constraints of the mobile node and information from existing connection to an access point for achieving a fast handoff. The method for detecting loss of connection is based on the MAC level channel sharing mechanism of Bluetooth.

The access network uses CIP. The CIP routers and gateway are not changed, as all Bluetooth specific functionality is taken care at the base stations. This takes care of routing at layer 3. The faster handoff at Bluetooth layer helps update the route caches more rapidly and the new route is established in a much shorter time than without mBPAC. The CIP base stations are modified to implement mBPAC, which adapts them to the special features of Bluetooth, and are referred to as mBPAC access points (AP's). The mBPAC AP's present themselves as standard CIP base stations to the CIP network. At the same time mBPAC also makes the CIP implementation transparent to the mobile nodes. Additional mBPAC communication is required between the neighboring AP's. Figure 2 shows the architecture of the mBPAC based access network. The operation of mBPAC is described below.

The mBPAC access network accepts new mobile devices through the standard Bluetooth procedure of inquiry and paging. This may be done by dedicated entry points that carry out inquiry continuously to detect new devices. These entry points then transfer the mobile via mBPAC handoff to the nearest AP. If additional devices are not to be used to act as entry points, the AP's may themselves go into inquiry scan mode R2 (i.e., spend 10ms on scan in every 2.56s). In this case when connection starts, the AP will be slave and a master-slave switch will be required to convert the mobile node into a slave with AP as master.

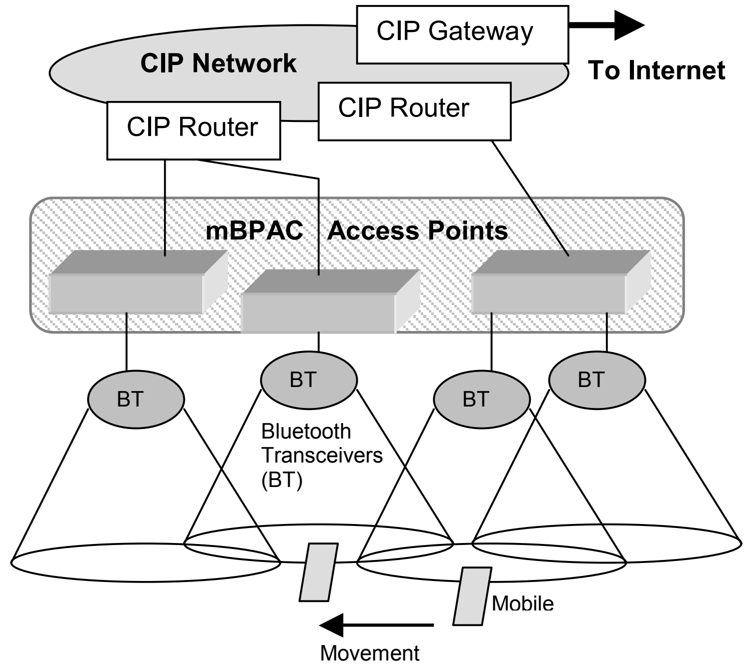


Figure 2. Proposed mBPAC access architecture.

Once a device has entered into the mBPAC access network, each time it moves from one AP to the next, handoff takes place in two steps:

1. **Loss of Connection is detected.** The method for detecting loss of connection is based on the polling scheme followed by the AP in its piconet. Polling scheme in mBPAC is round robin, in which the master (AP) polls each slave (mobile) one after the other. Data requirements may differ for different slaves -- the packet duration may be adjusted for this, using single slot packets for slaves with low datarate requirements and multislot packets (of 3 or 5 slots) for higher datarates. Data packets themselves act as poll packets. A slave is required to acknowledge every packet it receives from the master as per Bluetooth specification. If no reply occurs for the timeout period, $T_{pollreplytimeout}$, connection is assumed broken. At the mobile too a similar procedure is followed to detect loss of connection. At both the AP and the mobiles 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 for each slave. 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 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 loss of connection will be detected at the first unsuccessful poll attempt. Even if there is no data to send to a particular mobile node, the AP still polls each mobile and also sends the route cache update message to the CIP routers on behalf of the mobiles.

2. **Connection is restored with new 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 *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 usually succeed in the first attempt.

The *Neighborhood set* will depend upon the space in which the access network is deployed. Figure 3 shows a sample floor plan. Consider the AP *A* marked in the figure. It is clear that a mobile node that was in the range of A $T_{pollreplytimeout}$ ago could have moved to only the AP's marked *P* now. The maximum cardinality of the *Neighborhood set* may be 6 but is expected

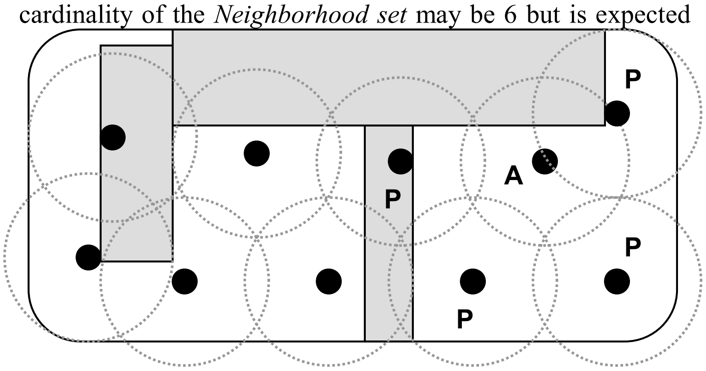


Figure 3. Sample arrangement of access points and entry points in a Bluetooth access network running mBPAC

to be lower than that in most practical deployment scenarios. Each AP needs to be made aware of its Neighborhood set. Unless the AP's have some location service available, this needs to be done manually during installation.

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. CIP should use a short cache timeout of 250ms.

### A. 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_Ac tivity | Check page scanning parameters |
| 0x001C | Write_Page_Scan_A ctivity | Set page scanning parameters |

### B. Robustness

The access network is fairly robust to mobile devices not following the mBPAC protocol:

1. **Intruding Devices:** As soon as a mobile device enters the access network, it becomes a slave in the piconet of its AP and cannot damage the operation of other devices in the same piconet.
2. **Malicious Devices:** After the device has been accepted into the network, it may stop following the mBPAC protocol. When the device is in connection state, the protocol requires it to either continue data communication, be in HOLD state (suspend its connection timeout timer), or to enter page scan on detecting loss of connection. In case it does not follow the protocol, all what happens is that the mobile device loses connection and is unable to connect again. The only effect on the network will be that some false page attempts will take place. They will stay limited to one *Neighborhood set.*

## V. 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 to study the effect of paging and inquiry procedures on connection establishment and the handoff protocol. The simulator implements the correct Bluetooth addressing and timing as per the standard. This section summarizes the simulations carried out to evaluate the performance of the proposed mBPAC access schemes.

### *A. Handoff Delay*

The handoff delay consists of two components:

1. The time to detect loss of connection, which depends on:
   - The number of devices connected to the AP as this affects the duration of a poll round in each piconet.
   - Whether the AP is in connection state or page state when the mobile leaves.
2. The time to resume a new connection at the new AP into whose range the mobile has moved in after loss of connection. This consists of:
   - The paging delay for starting the connection
   - The number of neighbor messages waiting in the queue, before paging takes place.

To evaluate the effect of the above factors, simulations are performed for cases with varying numbers of mobile and fixed nodes, and with different numbers of neighbor messages waiting in queue that have to be processed before the new mobile can be handled.

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*. The handoff delay depends on when exactly the paging starts after the neighbor message is received. When there is no neighbor message in queue the paging can start after one poll round. The time to detect loss of connection also depends on where in the poll round the turn for polling the moved device comes. Due to this, the detection of connection loss may not always take longer when more devices are connected. The handoff delays obtained for varying *k* and *s* have been plotted in Figure 4. Each value plotted is obtained by averaging 100 runs of the simulation.

### *B. 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 $s + s_m \leq 7$. 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 5.

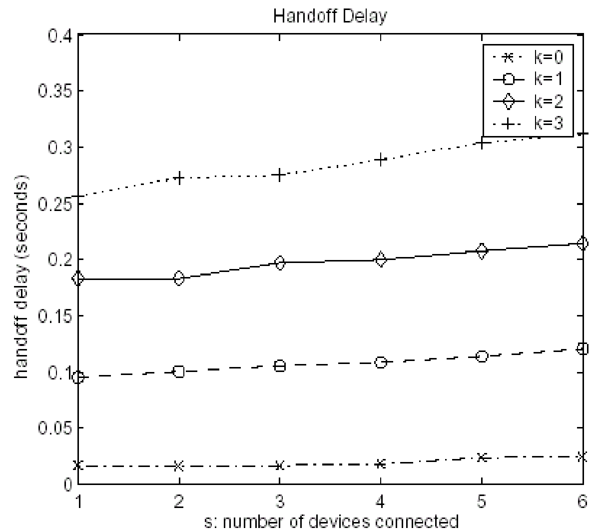


Figure 4. Aggregate handoff delay for varying *s* and *k*.

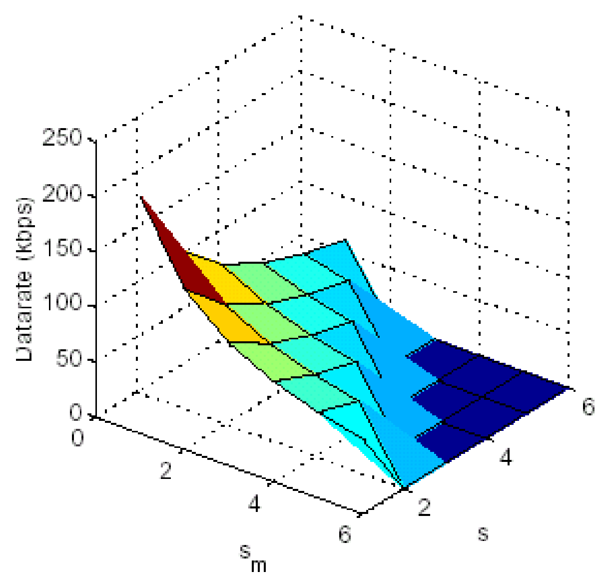


Figure 5. Datarate achieved with DH5 packet type at a mobile terminal for varying *s* and $s_m$ (*N=4*).

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 for that case to a close approximation.

### C. 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]. It took upto 20s to detect loss of connection and on the average 5s to resume connection. With mBPAC the delays are 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. If it takes 25s for the handoff the mobile will never be able to communicate. Hence, the use of a special method like mBPAC is essential to reduce the handoff delay to an insignificant fraction of the time duration between two handoffs. The datarate achieved in pure CIP would be much lower as much more time would be wasted in connection re-establishment. This would also reduce the number of mobile nodes the access network can support.

## VI. CONCLUSION

Providing wireless connectivity through short-range technologies such as Bluetooth has generated a need for supporting frequent handoffs. This paper discussed the various available options for providing mobility, 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 layer 3 micromobility mechanisms are preserved.

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]. Schemes for the AP's to automatically learn the Neighborhood set are also required.

The proposed schemes improve the 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.