Int. J. Advanced Networking and Applications
Volume: 01 Issue: 03 Pages: 175-180 (2009)


# An Analytical Performance Measure for Smooth Handoff in Mobile IPv6

**N. Karpagavalli**
Senior Lecturer *in Computer Science*
Holy Cross College (Autonomous), Tiruchirappalli – 620 002, Tamilnadu, India.
Email: karpagamhccin@yahoo.co.in

**R. Balasubramanian**
Principal, Raja Duraisingam Government Arts College,
Sivagangai. Tamil Nadu. India

**ABSTRACT**

Mobility is the most important feature of a wireless communication system. The mobile device needs to connect multiple points of connection and perhaps multiple networks as it moves from one location to another. Handover management is the way a network uses to maintain connection to a mobile user as it moves and changes its access point to the network. The IETF's mobile IP that uses mobile agents to support seamless handoffs, making it possible for mobile hosts to roam from subnet to subnet without changing IP addresses. To reduce the impact on the performance and the signaling overheads, hierarchical mobility management schemes define protocols that allow movements within a domain to be handled locally, without involvement of the mobile node's home network. To reduce the packet losses during handoff, new schemes have been defined, such as smooth handoff. This paper surveys basic handover mechanisms with an analytical model of mobile Internet protocols and also we have propose a novel performance model to evaluate the packet loss and packet delay for UDP streams that is involved in a handoff. The reason for this loss is identified and solutions to this problem are projected. This paper proposes methodology include mathematical models which is able to predict the handoff latency with empirical study.

**Keywords:** Mobility Management, Mobile IP, IPv4, IPv6, Smooth Handoff.

Date of submission : July 09, 2009 Revised: December 08, 2009 Accepted: December 20, 2009

## 1. INTRODUCTION

Mobile networking technology supports the requirements of today's new class of Internet users as they roam about with sophisticated mobile computers and digital wireless data communication devices. Integrating wireless networks into the global Internet poses a new challenge. The main reason is that the TCP/IP based Internet technologies were designed for wired networks with mostly fixed hosts. Host mobility requires changes in the routing protocol so that packets for a moving host can be delivered to their correct destination. Mobile IP (*home approach*) provides a basic framework to solve this operability problem [1], [2]. A mobile host can communicate with a base station, which is statically connected to the Internet. However, several performance problems in Mobile IP need to be addressed. First, Mobile IP's tunneling scheme creates a triangle routing problem, causing packets to travel through sub-optimal routes. Second, packets in flight during a handoff are often lost because they are tunneled based on out-of-date location information. Third, base stations with small cells result in frequent handoffs, and requiring a registration with a distant home agent for each such local handoff causes higher overhead and further aggravates packet loss. In order to achieve smooth handoff in MIP, numerous handoff mechanisms have been proposed which tend to reduce the handoff delay and packet loss. This paper surveys basic handover mechanisms with an analytical model of mobile Internet protocols and also we have propose a novel performance model to evaluate the packet loss and packet delay for UDP streams that is involved in a handoff Mobile IPv6.

## 2. MOBILITY MANAGEMENT

Mobility management architectures are divided into two main parts, *location management* and *handoff management*. The former entails registering changes in the position of the Mobile Node (MN) and also the localization of an idle MN when an outside client wants to contact it. The other important point is handoff management, which tries to sustain all the connections of the MN despite the frequent changes of its point of attachment to the network. The process by which such change takes place is called *handoff,* during which communication may be interrupted and delay increased. Depending on the type of handoff, the process is more complex, as it may entail changes in the access point, the access router, the access gateway, the access technology and/or the administrative domain.
From the network point of view, *mobility management* is seen from *two* different perspectives. On the one hand,

there is the mobility inside a single administrative domain confined to a localized geographical region, which is called *micromobility*. On the other hand is *macromobility*, which deal with mobility across larger region often comprising various networks, with potentially different access technologies, which themselves may belong to different administrative domains. *Micromobility protocols* try to solve the overhead, packet loss**,** and path reestablishment latency experienced by *macromobility protocols* during handoff. In general, the solutions adopted confine control message exchanges to a reduced area and set up mobility agents representing that area and allowing interoperability with macromobility schemes. The final goal of both solutions is to offer the user a reliable network capable of keeping alive the connections all the time, independently of the actual position of the node, inside a single domain (micromobility) or even inside the whole Internet (macromobility). The following subsections give a brief overview of some of the solutions found in the literature.

## 2. 1. Macromobility

### Mobile IP

Mobile IP is a network layer protocol conceived to provide macromobility to mobile terminals. Mobile IP is being designed by the Internet Engineering Task Force (IETF) in two versions as Mobile IPv4 and Mobile IPv6. The objective of both protocols is to allow users moving in large areas to maintain their network connections while changing their point of attachment to the network.

### Mobile IPv4 Overview

Mobile IPv4 introduces four functional entities[1]:

- Mobile Node (MN): A mobile device.
- Home Agent (HA): A router of the home network that manages localization of the MN.
- Foreign Agent (FA): A router of the foreign network that cooperates with the HA to provide mobility.
- Correspondent Node (CN): A fixed or mobile node, with which the MN communicates.

The protocol establishes *four phases*. In the *first phase* called *Agent Discovery* the MN has to be able to detect if it is attached to the home network or to a foreign network. For this purpose, HA and FA periodically send Agent Advertisements. When a MN receives this message, it determines in which network it is attached, and if it is on a foreign network, it obtains a Care-of-Address (CoA). The CoA is the IP address temporarily assigned to the MN while in the foreign network. The MN can also request an Agent Advertisement sending an Agent Solicitation to accelerate the process.

In the *second phase*, called *Registration*, the MN registers its CoA in the HA. The MN sends a Registration Request to the FA, which forwards it to the HA. The HA replies a Registration Reply to accept the requests. At this point, the HA knows the localization of the MN and the communication with CN can be initiated, or continued in case of handoff.

In the *third phase*, called *Routing and Tunneling* the CN communicates with the MN (and vice versa). When a CN sends an IP packet to a MN, the destination address is the home address of the MN, i.e. the address assigned to this node when it was in the home network. When this packet arrives at the home network, it is intercepted by the HA. The packet is encapsulated and forwarded to the FA, which decapsulate and delivers it to the MN. On the other hand, when the MN sends a packet to a CN, it is directly sent using the home address as source. This asymmetric routing, which often is not the optimal, is known as *triangle routing*. This generates a series of inefficiencies such as longer packet delivery delays or increased load in the network. Though there are optimizations to solve these problems (route optimization), they require the modification of the CN, which may be any host in the Internet, and thus, their wide deployment is difficult.

In the *fourth phase*, called *Handoff Management* the MN moves from a subnet to another one by changing its point of attachment. The MN must obtain a new CoA and register it in the HA. Once accepted, the MN is able again to communicate with CN. During the *Handoff Management* process the HA is not able to localize the MN, thus some packets may be lost between the CN and the MN.

### Mobile IPv6 Overview

Mobile IPv6 is very similar to Mobile IPv4. However, unlike in IPv4, in which mobility issues were not considered in its initial design, when IPv6 was developed, mobility was taken into account from the outset and is perfectly integrated into the protocol. Mobile IPv6 is more efficient and avoids some problems suffered by Mobile IPv4 [3], [12],[13]. Among others, Mobile IPv6 does not need FAs because IPv6 address autoconfiguration provides the required functions for the *Agent Advertisement phase*. During *Registration* and *Routing and Tunneling*, packets are directly sent from the HA to the CoA of the MN.

Mobile IPv6 also avoids triangle routing because when a CN sends a packet to the home address of a MN, the HA intercepts, encapsulates, and forwards the packet to the MN. However, the MN can also directly send a Binding Update (BU) to the CN. This message includes the CoA of the MN, and it is cached on the CN Binding Cache. At this point, any CN sending a packet first checks its Binding Cache for the IP destination address of the packet. If there is an entry, it will directly send the packet to the MN using the MN's registered CoA. This feature is inherent to IPv6, and no additional modification needs to be done to CNs to make them mobile-aware.

## 2.2 Micromobility

There are many environments where applications running in mobile nodes may become unusable if they frequently change their point of attachment to the network. For example, many real-time applications, like voice-over-IP, experience noticeable degradation of service if handoff is frequent. This problem is especially relevant when very large volumes of wireless subscribers need to be supported.

The basic mobile IP protocol based on *tunneling mechanism* introduces network overhead in terms of

Volume: 01 Issue: 03 Pages: 175-180 (2009)

increasing delay, packet loss and signaling. The establishment of new tunnels can introduce additional delays in the handoff process, causing packet loss and delayed delivery of data to applications. This delay is inherent in the round-trip introduced by Mobile IP as the registration request is sent to the home agent and the response sent back to the mobile node (or sometimes to the foreign agent).

Micromobility protocols [3] aim to handle movement within a domain of MNs with minimum or zero packet loss, minimum signaling, reduced power consumption and by just interacting with Mobile IP in the Access Network Gateway (ANG), i.e. the node through which the domain connects to the Internet. This has the benefit of reducing delay and packet loss during handoff, eliminating registration between MNs and, possibly, distant home agents when MNs remain inside their local coverage areas. All IP micromobility protocols share the same operational principles related to fast handoff, e.g. reduced location updates, fast security or even the quality of service.

Support for fast handoff is an important characteristic of micromobility protocols. Handoff is influenced by handoff management, buffering and forwarding techniques, radio behaviour, movement detection and prediction and coupling and synchronization between the IP and radio layers. Micromobility protocols try to guarantee the arrival of packets and reduce signaling by hiding local migrations from home agents. Hierarchical mobility protocols do it by registering in the HA the address of the ANG instead of the CoA assigned to the MN in the visited domain. In this way, when a MN moves from one access point to another one (which is reachable through the same gateway) the HA need not be informed. The role of micromobility protocols is to ensure that packets arriving at the ANG are forwarded to the appropriate access point. In order to route packets to the MN's actual point of attachment, protocols maintain a location database that maps host identifiers to location information.

There are two styles of micromobility: hierarchical tunneling and mobile-specific routing [14], [15].

- In hierarchical tunneling, the location database is maintained in a distributed way by a set of mobility agents. Each agent reads the incoming packet's original destination address and searches its list of visitors for a corresponding entry. The entry contains the address of the next lower level agent. Entries are created and maintained by registration messages transmitted by MNs. Some proposals rely on a tree-like structure of mobility agents but, in the HMIP (Hierarchical Mobile IP), one of the main hierarchical tunneling proposals, mobility agents directly interact with MNs without the need for such a structure [4].

- Mobile-specific routing approaches avoid the overhead introduced by decapsulation and reencapsulation schemes of tunneling approaches. These schemes typically introduce implicit or explicit signaling to update host-specific routes. In the case of Cellular IP [5] MNs attached to an access network use the IP address of the gateway as their Mobile IP care-of address. The gateway decapsulates packets and forwards them towards the access point. Inside the access network, MNs are identified by their home address and data packets are directly routed without tunneling or address conversion. The routing protocol ensures that packets are delivered to the MN's actual location.

***HAWAII*** - Handoff-Aware Wireless Access Internet Infrastructure protocol

Hawaii is a domain-based structure. In a domain, mobility related works are done by gateways which are called as domain root router. The coming packets are routed by IP routing, when the MN is in its own domain. But if the MN is in a foreign domain then the coming packets are firstly taken by the HA. Then they are sent to the domain root router which forwards the packets by the host-based-routing entries to the MN[10].

## 3. THE ANALYTICAL MODEL

The analytical model [6], [7] for the smooth handoff scheme [8] - [15] based on a queuing network.

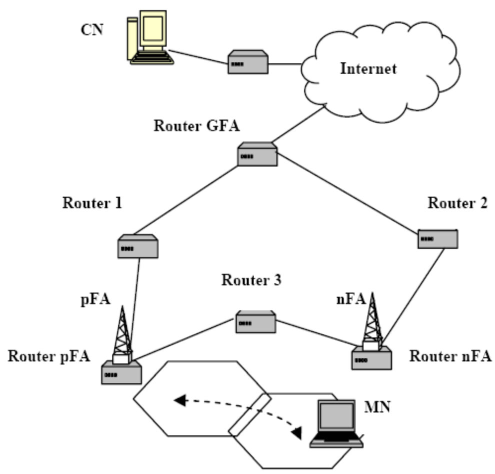


Fig. 1: Network architecture

We assume the network architecture as depicted in Fig.1. The following assumption is essential for computational tractability reasons and all routers are modeled as simple M/M/1 queues[11]. The exponentially distributed service time of a packet includes both the processing time and the transmission time.

- Denote the service rate of Router *i* (*i*= 1, 2, 3, MAP, pFA and nFA) by μ, and the load by ρ, then its response time random variable *Ri* is exponentially distributed with rate μ *(1*-ρ*)*.

Time instants for the handoff procedure[7], [8]:

- *t0*: the time instant the MN leaves sub-network A (and hence has no layer 2 connection any longer with it) and enters sub-network B.
- *t1*: the time instant the binding update message containing the new CoA of the MN, sent by the new FA, reaches the previous FA;
- *t2*: the time instant the regional registration request reaches the MAP and is processed by the MAP
- *t3*: the time instant the regional registration reply, originating from the MAP, reaches the new FA.

The instances *t1*, *t2* and *t3* are random variables distributed as sums of exponentially distributed random variables and constants (conditioned on a fixed value of $\Delta FA$ ):

- $t1 = t0 + \Delta FA + RnFA + R3 + RpFA$ + fixed link delays
- $t2 = t0 + \Delta FA + RnFA + R2 + RMAP$ + fixed link delays
- $t3 = t2 + RMAP + R2 + RnFA$ + fixed link delays

Each packet of a stream belongs to exactly one of the following classes or subclasses:

- Class 0: packets routed via the previous FA and directly forwarded to the MN.
- Class 1: packets routed via the previous FA and buffered before being forwarded to the new FA.
  - Subclass (a): packets forwarded but lost because they arrive at the new FA before the Registration Reply.
  - Subclass (b): packets forwarded and arriving at the new FA after the Registration Reply.
  - Subclass (c): packets that are lost due to buffer overflow at the previous FA.
- Class 2: packets routed via the previous FA and directly forwarded to the new FA.
  - Subclass (a): packets lost because they arrive at the new FA before the Registration Reply.
  - Subclass (b): packets arriving at the new FA after the Registration Reply.
- Class 3: packets routed via the new FA. Remark that subclasses can be empty.

Now consider a UDP stream originating from a CN destined to the MN. The handoff does not affect the path of the stream until it reaches the MAP, therefore we take up the point of view of packets arriving at the MAP.

We assume that every *T*ms a packet arrives at the MAP (the jitter introduced by the network between CN and MAP is not taken into account). Let us denote the time of arrival in the MAP by *tMAP*.

Packets are lost if they belong to subclasses 1(a), 1(c) or 2(a). So, the probability that a packet will be lost equals *P*[packet lost] = *P*[1(a)] + *P*[1(c)] + *P* [2(a)]

The different probabilities of the right hand side are obtained as follows.

- $P[1(a)] = P[(t_{MAP} + c < t_2)$ and $(t_0 < X < t_1)$ and $(X' > t_1)$ and $(t_1 + Y' < t_3)]$
  $+ P[(t_{MAP} < t_2 < t_{MAP} + c)$ and $(t_0 < X < t_1)$ and $(t_1 + Y' < t_3)]$
- $P[1(c)] = P[(t_{MAP} + c < t_2)$ and $(t_0 < X < t_1)$ and $(X' < t_1)]$
- $P[2(a)] = P[(t_{MAP} < t_2)$ and $(X > t_1)$ and $(X + Y < t_3)]$

where, the random variables *X*, *X'*, *Y*, Y', and *c* are given by

$X = \{tMAP + RMAP + R1 + RpFA$ + fixed delays$\}$

$X' = \{tMAP + c + RMAP + R1 + RpFA$ + fixed delays$\}$

$Y = \{RpFA + R3 + RnFA$ + fixed delays$\}$

$Y' = \{$burst delay $+ RpFA + R3 + RnFA$ + fixed delays$\}$

$c = BS \times T$ , where *BS* denotes the size of the forwarding buffer.

The burst delay is determined as the expected number of packets in the queue in front of the current packet, and counting one extra service time per packet per router.

We observe that all these random variables are the sums of three independent exponential variables with rate $\mu\ (1-\rho)$ and some constants, hence the computation of *P*[1(a)], *P*[1(c)] and *P*[2(a)] is fairly straightforward. As for the delay distribution we have that,

$$P[\text{delay}>t] = P[\text{packet lost}] + \sum_{\text{class} \in A} [\text{class and delay} > t$$

where, A ={0, 1(b), 2(b), 3}.

Here we have that,

$P[0$ and delay $> t] = P[(T_{MAP} < t_2)$ and $(X < t_0)$ and (delay $> t)]$

$P[1(b)$ and delay $> t] = P[(T_{MAP} + c < t_2)$ and $(t_0 < X < t_1$ and $(X' > t_1)$ and $(t_1 + Y') > t3]$ and (delay $> t)] + P[(t_{MAP} < t_2 < t_{MAP} + c)$ and $(t_0 < X < t_1)$ and $(t_1 + Y' > t_3)$ and (delay $> t)]$

$P[2(b)$ and delay $> t] = P[(T_{MAP} < t_2)$ and $(X > t_1$ and $(X + Y > t_3)$ and (delay $> t)]$

$P[3$ and delay $> t] = P[(T_{MAP} > t_2)$ and (delay $> t)]$

The delay is a random variable that takes on different forms according to the class:

- 0: delay $= X - t_{MAP}$
- 1(b): delay $= t_1 + Y' - t_{MAP}$
- 2(b): delay $= X + Y - t_{MAP}$
- 3: delay $= Z - t_{MAP}$

where $Z = \{t_{MAP} + R_{MAP} + R_2 + R_{nFA}$ + fixed delays$\}$ and the other variables are defined as before. Thus the delay is the time of arrival in the current FA minus the departure time $t_{MAP}$. For the total end-to-end delay CN-MN, we approximate this by adding the expected end-to-end delay $CN_{MAP}$, which is the same for every packet.

The M/M/1 assumption allows us to compute each of these probabilities in a fairly straightforward way. In order to compute the expected number of lost packets due to the handoff, we can proceed as follows. If we set the instance of handoff *t0* = 0, then we can compute the loss probability for a number of *N* consecutive packets, starting sufficiently before the handoff, say $t_{MAP} = -100$, and ending sufficiently after the handoff.

The expected number of lost packets for such a stream is then given by the sum of the individual probabilities:

$$E[\text{number of lost packets}] = \sum_{k=1}^{N} P[\text{lost}, t_{MAP} = -100 + (k-1) \times T]$$

First we study the loss probability of packets in the forwarding buffer of the previous FA and the loss probability of forwarded packets in the new FA.

Consider the network depicted in Fig.1, with the following system parameters. Each router is loaded up to 0.8, the propagation delay between routers is $\tau = 5$ ms, the average processing time of a packet in a router is 1ms. In Fig.2, the expected number of lost packets is shown as a function of the buffer size at the previous FA. The expected packet loss due to buffer overflow is given by the dashed line, while the solid line represents the additional loss at the new FA, due to early arrival. The results for link delays equal to 5ms on every link.

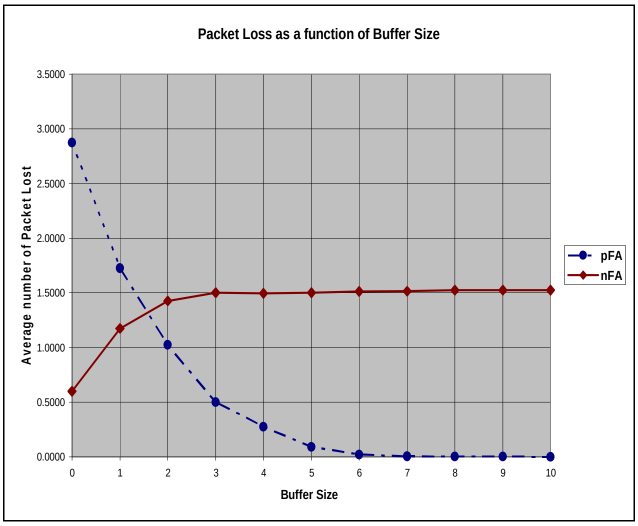


Fig. 2: Average Packet Loss as a function of Buffer Size

The result does not depend on the length of the stream that is considered here, as long as the first and last packet considered have negligible loss probabilities.

## 4. PERFORMANCE MESAURES OF MODEL

We consider network with N packets. The average packet loss for different buffer sizes were analytically examined using the following formula:

$$E(q) = (1- \rho/k)^k$$

$$E(Loss) = \rho -1+(1- \rho/k)^k$$

Here we have that, $\rho$ buffer utilization factor and k buffer size of the packets. The buffer size is taken as k=10 and k=50 and the Fig.3 and Fig.4 depicts the E(q) and E(loss). The results have been shows while the $\rho$ increases, the expected queue length decreased and the packet loss increases.

Our approximation scheme is iterative and is described for the following Algorithm.

P(0) = P
FOR I = 1 TO N DO
BEGIN
  set P = P(i-1)
  calculate $X_{k,0}, X_{k,1}, \dots, X_{k,k}$
  evaluate Po, i, Pl, i, . . . , Pb,i
  evaluate E(q), E(lost) for packet i
P(i) = 1 -Po, i
END

In order to avoid packet loss at the previous FA, the forwarding buffer need to be dimensioned such that it can store packets of the order of the product bit rate of the stream times delay (MN –new FA – previous FA). The loss at the new FA on the other hand depends on the difference between the distance (new FA – GFA) and (new FA – previous FA). If the latter is smaller than the former, then packets may get lost. A possible solution would be to provide the new FA with a buffer to store temporarily unauthorized traffic until the registration reply from the GFA arrives at the new FA.

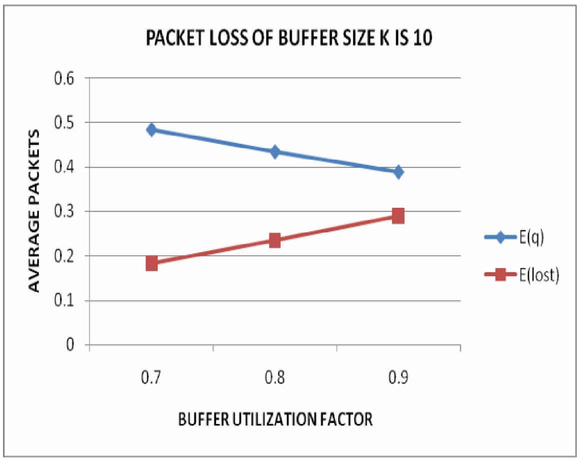


Fig. 3:Packet Loss as a function of Buffer size is 10

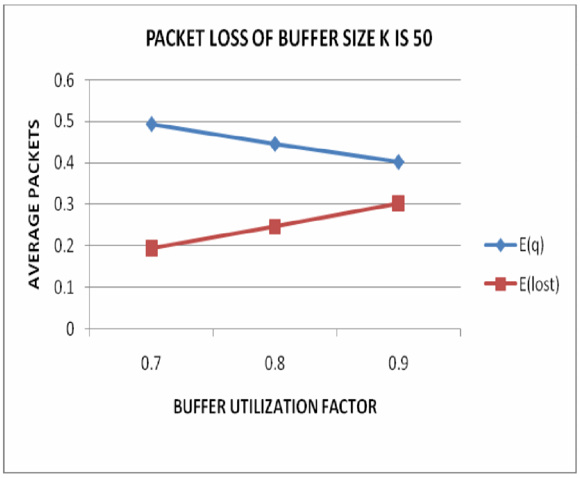


Fig. 4:Packet Loss as a function of Buffer size is 50

## 5. CONCLUSIONS

This paper surveys basic handover mechanisms with an analytical model of mobile Internet protocols and also we have propose a novel performance model to evaluate the packet loss and packet delay for UDP streams that is involved in a handoff. We have seen that the origin of packet loss is two-fold: first, packets may get lost in the previous FA when the forwarding buffer overflows and secondly, they may get lost in the new FA when upon their arrival the registration reply from the MAP has not arrived yet in the new FA. The first reason for loss may be avoided by appropriately dimensioning the forwarding buffer. This buffer should be able to store arriving packets at least during a time equal to the delay on the new FA – previous FA path. The second loss is more difficult to deal with. It is determined by the difference between the delays of the paths previous FA – new FA and new FA – MAP. A number of solutions are possible to solve this problem. Similar to the Multiple Stream Forwarding scheme of the HAWAII protocol, the binding update message sent by the new FA to the previous FA could be routed via the MAP in order to allow the registration reply message to arrive before the first forwarded packets. This however would increase the handoff latency. A second solution consists of storing the forwarded packets temporarily in a buffer at the new FA, until the new registration reply has arrived. This buffer could be dimensioned based on the distance between the FA and its neighboring FAs.

## REFERENCES

[1] C. Perkins, ed. "IP Mobility Support for IPv4." IETF RFC 3344, August 2002.

[2] D. Johnson, C. Perkins, J. Arkko. “Mobility Support in IPv6.” Internet Draft, draft-ietf-mobileip-ipv6-24, June 2003.

[3] A. T. Campbell, J. Gomez, S. Kim, A. Valko, C.-Y Wan, and Z. Turanyi. “Comparison of IP Micromobility Protocols.” IEEE Wireless Communications Magazine, 9(1): 72–82, February 2002.

[4] H. Soliman, C. Castelluccia, K. Malki, L. Bellier. “Hierarchical Mobile IPv6”, Internet Draft, draft-ietf-mipshop-hmipv6-00, October 2003.

[5] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, C.-Y. Wan, and A. Valkó. “Design, Implementation and Evaluation of Cellular IP.” IEEE Personal Communications 7 (4): 42–49, August 2000.

[6] C. Blondia, O. Casals, P. De Cleyn and G.Willems, “Performance analysis of IP Micro-Mobility Handoff Protocols”, Proceedings of Protocols for High Speed Networks 2002 (PfHSN 2002), Berlin 2002.

[7] C. Blondia, O. Casals, L. Cerda and G.Willems, “Performance analysis of a forwarding scheme for handoff in HAWAII”, Proceedings of Networking 2002, Pisa 2002.

[8] Wang Ting, Wang Yu. Survey on a Queue Theory Based Handover Scheme for UAVS Communication Network. Chinese Journal of Sensors and Actuators, 2007, 04.

[9] Li Da-Qi, Shen Jun-Yi. Queuing Theory Supervising K-Means Clustering Algorithm and ITS Application in Optimized Design of TTC Network .Journal of Astronautics, 2007, 03.

[10] I.F. Akyildiz, J. Xie, S. Mohanty, “A survey of mobility management in next-generation all-IP-based wireless systems”, IEEE Wireless Com. Mag., vol. 11, issue 4, pp. 16-28, Aug. 2004.

[11] K. S. Trivedi, “Probability, Statistics with Reliability, Queueing and Computer Science Applications,” Second Edition, Wiley, 2002, ISBN 0-471-33341-7.

[12] Hee Young Jung, Jun Seob Lee, Seok Joo Koh, Hesham Soliman, Karim El-Malki.Fast Handover for Hierarchical MIPv6 (F-HMIPv6) .IETF Draft, May,2003.

[13] M.Torrent-Moreno. A Performance Study of Fast Handovers for Mobile IPv6. IEEE International Conference on Local Computer Networks, 2003.

[14] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, Hierarchical Mobile IPv6 Mobility Management (HMIPv6),RFC 4140, August 2005.

[15] Sapna Gambhir, M.N.Doja, Moinuudin and Mohit Gambhir. “Impact of SHM Attributes of Mobile Node on QoS forHMIPv6 Mobile Networks”, Advances in Wireless and Mobile Communications. ISSN 0973-6972 Volume 1, Number 1-3 (2008), pp. 25–35.

### Authors Biography

**N. Karpagavalli,** is a Senior Lecturer at the Department of Computer Science, Holy Cross College (Autonomous), Tiruchirappalli, Tamil Nadu, India. She received her M.C.A., and M.Phil., in Computer Science from the Bharathidasan University in 2002 and 2005 respectively. She is currently pursuing her Ph. D. degree in Computer Science at Mother Teresa Women’s University, Kodaikanal, India. Her research interests include Wireless Mobile Adhoc Networks, IPv6 based Networks and Applications.