Robust Hierarchical Mobile IPv6 (RH-MIPv6)

An Enhancement for Survivability & Fault-Tolerance in Mobile IP Systems

Taewan You, Sangheon Pack, and Yanghee Choi
School of Computer Science & Engineering
Seoul National University
Seoul, Korea
{twyou, shpack}@mmlab.snu.ac.kr and yhchoi@snu.ac.kr

Abstract— **In wireless networks, system survivability is one of the most important issues in providing quality of service (QoS). However, since failure of home agent (HA) or mobile anchor point (MAP) causes service interruption, the Hierarchical Mobile IPv6 (HMIPv6) has only weak survivability. In this paper, we propose Robust Hierarchical Mobile IPv6 (RH-MIPv6), which provides fault tolerance and robustness in mobile networks. In RH-MIPv6, a mobile node (MN) registers primary (P-RCoA) and secondary (S-RCoA) regional care of addresses to two different MAPs (Primary and Secondary) simultaneously. We develop a mechanism to enable the mobile node or correspondent node (CN) to detect the failure of primary MAP and change their attachment from the primary to secondary MAP. By this recovery procedure, it is possible to reduce the failure recovery time. Analytical evaluation indicates that RH-MIPv6 has faster recovery time than HMIPv6 and we also show through simulation as like analytical result. Consequently, RH-MIPv6 shows about 60% faster recovery time compared with HMIPv6.**

Keywords; Hierarchical Mobile IPv6 (HMIPv6), Robust HMIPv6 (RH-MIPv6), Fault-Tolerance, Service Availability.

I. INTRODUCTION

In wireless/mobile networks, system survivability is one of the most important issues in providing quality of service (QoS). Survivability is used to describe the available performance after a failure. To enhance the survivability in cellular networks, many schemes have been proposed in the literature [1]. On the other hand, IP-based mobility management schemes (e.g. Mobile IPv4 and Mobile IPv6) do not consider system survivability and fault tolerance. However, when IP-based mobility management schemes are deployed in wireless/mobile networks, survivability and fault tolerance should be taken into consideration as one of the important performance factors.

The Hierarchical Mobile IPv6 (HMIPv6) [2] is designed to reduce the amount of signaling to the correspondent nodes (CNs) and to the home agent (HA) by allowing the mobile node (MN) to locally register in a domain using mobility anchor point (MAP). In a distributed MAP environment, multiple MAPs can exist on any level in a hierarchy including the access router (AR) and some MAPs can be located within a domain independently of each other. The distributed MAP environment has several advantages in terms of load balancing and scalable service.

In the HMIPv6, HAs and MAPs are two points of failure and potential performance bottlenecks. For example, when the accident attacks such as DoS (Denial of Service) occur in the HA or the MAP, the HA and the MAP will be halted down and the failure leads to the loss of network connectivity to all the MNs, which are currently serviced by these faulty agents. Therefore, when the HMIPv6 is deployed in wireless/mobile networks, fault tolerance and survivability should be considered. Although several protocols have been proposed for the fault tolerance in the Mobile IP, they are based on redundancy-based schemes, which are costly and require a strict synchronization [3].

In this paper, we propose an enhanced HMIPv6 in the distributed MAP environment. The enhanced HMIPv6, called *Robust Hierarchical Mobile IPv6* (RH-MIPv6), provides survivability and fault tolerance with the existing HMIPv6. Unlike other fault-tolerant schemes, RH-MIPv6 does not require any synchronization between mobility agents (e.g., HA and MAP). In the RH-MIPv6, when Router Advertisement messages are received from multiple MAPs, an MN configures two regional care-of addresses (RCoAs): one is primary RCoA (P-RCoA) and the other is secondary RCoA (S-RCoA). Then the MN registers two RCoAs to two MAPs (primary and secondary MAPs). In addition, the MN registers the HA and CNs. To support the registration of multiple RCoAs, Binding Caching should be modified in the RH-MIPv6. However, it can be easily implemented by adding an additional entry to Binding Cache.

In the HMIPv6, when some failures happen in the mobility agents, an MN re-configures a new RCoA after the detection of the failures. Therefore, in this mechanism, a significant amount of time is wasted for the failure detection and the duplicate address detection (DAD). On the other hand, in the RH-MIPv6, multiple RCoAs are configured in advance and are dynamically changed after the failure detection. Thus, it is possible to reduce the failure recovery time compared with the HMIPv6.

The remainder of this paper is organized as follows. Section II introduces previous works related to fault-tolerance. In Section III, we describe the basic operation and failure recovery mechanism in RH-MIPv6. Section IV analyzes failure recovery time in RH-MIPv6. Also, several simulation results using ns-2 simulator [7] are given in Section V. At last, Section VI concludes this paper.

This work was supported in part by the Brain Korea 21 project of Ministry of Education, and in part by the National Research Laboratory project of Ministry of Science and Technology, 2003, Korea.

II. PREVIOUS WORK

In Mobile IP, mobility agents such as HA/FA (MIPv4) or MAP (HMIPv6) are single points of failure. Many researches related to fault-tolerance and failure recovery have been studied in the literature. The works can be classified into two categories: redundancy-based scheme and refresh-based scheme.

A. Redundancy-based Schemes

In the redundancy-based schemes, multiple mobility agents are available and these agents should be synchronized. If a mobility agent (primary) makes no response, another mobility agent (backup) takes a role of the failed mobility agent. In [4], multiple mobility agents (i.e. HA) are deployed and they are synchronized using periodical message exchanges. Therefore, it can reduce the recovery time by replacing primary HA with backup HA. In [5], Hot Standby Router Protocol (HSRP) was developed by Cisco. It provides network redundancy to ensure that user traffic will immediately and transparently recover from "first hop" failures in network edge devices and access circuits. In addition, the Internet Engineering Task Force (IETF) had standardized redundancy among HAs [6].

B. Refresh-based Schemes

Unlike halt down of mobility agents, it is possible to miss mobility-related information stored in mobility database. These fails can be recovered by refresh-based schemes. In other words, when the database, which is located in HA or FA was crashed or lost, this problem is resolved using periodically binding update [8] proposed an optimal refresh time interval to minimize recovery time in the case of cellular networks. This scheme synthetically considers the point of times that last Binding Update and call arrival.

III. ROBUST HIERARCHICAL MOBILE IPV6 (RH-MIPV6)

A. Architecture

In HMIPv6 draft, a MAP can exist on any level in a hierarchy including the AR or several MAPs can be located within a hierarchy independently of each other. In this paper, we consider a distributed HMIPv6 environment, where there exist multiple independent MAPs, shown in Fig. 1. In Fig. 1, MAPs act as a kind of local HAs. In this environment, an MN receives Route Advertisement messages with MAP option from all MAPs located in a domain. In addition, each MAP domain may be overlapped.

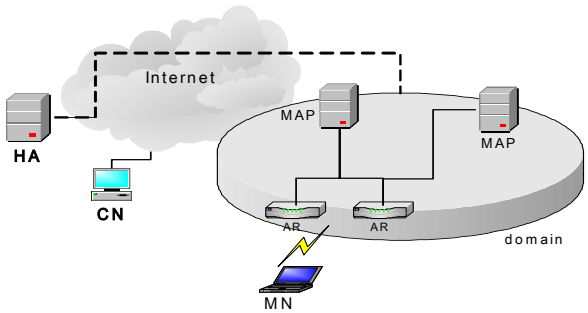


Figure 1. Distributed HMIPv6 Architecture.

B. Operations in RH-MIPv6

The RH-MIPv6 allows MNs and CNs to maintain two binding entries. In other words, MAPs keep binding information related to MN's regional care-of address with on-link care-of address (LCoA), Also, MNs and CNs keep binding information of MNs' primary and secondary RCoA.

The first operation of RH-MIPv6 is a binding update invoked by an MN. Fig. 2 shows the binding update procedures.

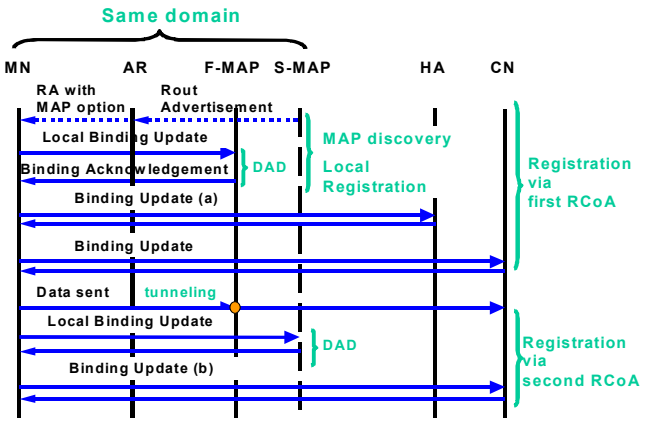


Figure 2. Binding Update Procedure in RH-MIPv6.

In Fig 2, when an MN moves into a new MAP domain, it receives Router Advertisement messages containing information on locally available MAPs. Binding update in the RH-MIPv6 is similar to that of the HMIPv6. However, RH-MIPv6 registers two RCoAs to the CNs to provide service survivability in mobile networks. To support this function, we added a new flag to the Binding Update message. The new flag, the *P flag*, indicates whether the specified RCoA is primary RCoA or secondary RCoA. Fig.3 depicts the modified Binding Update message. When an MN registers its primary RCoA to the HA and CNs, P flag is set to 1 (refer to (a) in Fig. 2). After the first binding update procedure is completed, the second binding update procedure is performed using the Binding Update message with secondary RCoA and the unset P flag (refer to (b) in Fig. 2). In the case of second binding update, the MN needs not to send Binding Update message to the HA.

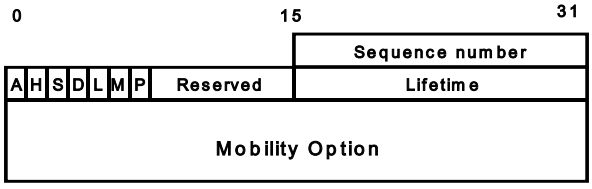


Figure 3. Extensions to the Binding Update.

C. *Failure Recovery Mechanism*

In the HMIPv6, the failure of the MAP can be detected using a MAP option containing a valid lifetime. However, it takes too much time for an MN to detect the failure because the interval of Router Advertisements messages is set to a few seconds.[1] Thus, the failure recovery mechanism of the HMIPv6 results in high packet loss, especially when the MN is communicating with several CNs. On the other hand, compared with HMIPv6 the failure recovery mechanism of RH-MIPv6 reduces the packet loss rate in the case of MAP failure using more active failure detection methods. We divided the failure detection into two cases: failure detection by the MN, and by the CN.

1) *CN dectects MAP failure*

When a CN is sending some data packets to an MN via a MAP, which is a serving MAP containing binding information between the MN's primary RCoA and LCoA, the CN can detect the failure of MAP if there is no response to the sent packets via Internet Control Message Protocol version 6 (ICMPv6) [9]. IPv6 nodes to report errors encountered in processing packets use the ICMPv6. The ICMPv6 error messages include destination unreachable, packet too big, time exceeded, and parameter problem.

The RH-MIPv6 uses ICMPv6 in order to detect MAP failure, especially destination unreachable message. A destination unreachable message should be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. The message handles following error of four cases such as no route to destination, communication with destination administratively prohibited, address unreachable, and port unreachable. Therefore, if a MAP fails, the source MN considers that the MAP breaks down after receiving destination unreachable messages in terms of RH-MIPv6.

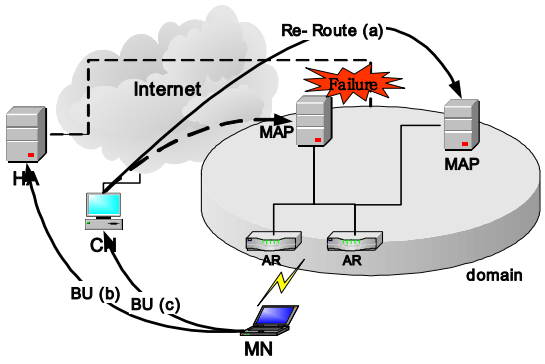


Figure 4. Failure Detection and Failure Recovery Procedure.

Fig. 4 shows the failure detection and recovery procedure. Detailed operations are as follows:

(a) When the CN detects a failure of the MAP, it searches for second binding entry from the Binding Cache, which is updated by the previous Binding Update message with P flag. Then, the CN sends data packets through secondary RCoA to destination nodes.

(b) If an MN received packets from the secondary MAP, the MN considers that primary MAP does not work anymore. Then, the MN sends Binding Update messages with the secondary RCoA, which is configured in the MAP discovery procedure in advance, to HA as soon as possible. In addition, the MN has to send Binding Update messages to the CN to update the binding cache in the CN.

After re-Binding Update procedure, the MN can communicate with CNs via the secondary RCoA.

2) *MN dectects MAP's fauilure*

In HMIPv6, an MN can detect MAP failures from the lifetime value, which is contained in the MAP option of Router Advertisement message. As mentioned above, since the interval for Router Advertisement is too coarse grained, an MN, which is actively communicating with CNs, can detect MAP failures when there is no response from the primary MAP via ICMPv6 destination unreachable message. In this case, an MN performs similar procedures to that of the detection by CN.

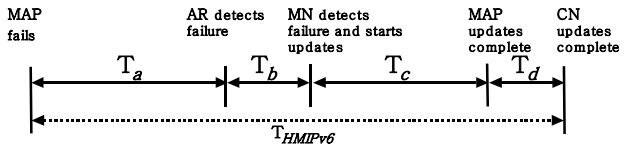
3) *HA detects MAP's failure*

When a MAP fails and a new CN tries to communicate with a MN, a HA can detect failure of the MAP. Because there is no response to data that the CN sent to MN and that is delivered to a MN through the serving MAP, which is containing binding information.

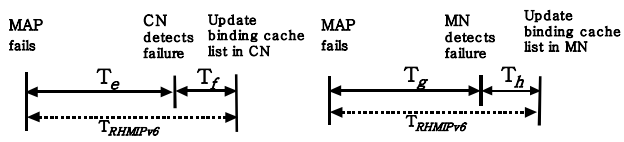
In this paper, we don't consider any cases that the HA detects MAP's failure. Because it doesn't affected any of ongoing session's quality of service.

IV. PERFORMANCE ANALYSIS

To investigate the effectiveness of our proposed mechanism, we analyze the failure recovery time in the HMIPv6 and in the RH-MIPv6.



(a) HMIPv6's recovery time



(b) RH-MIPv6's recovery time

Figure 5. The timing diagram for recovery process

[1] Recently, Router Advertisement interval is set to about 50ms for fast movement detection. However, a few seconds is more reasonable value because Router Advertisement from MAP is not related with movement detection.

(a) As shown in Fig 5(a), we divide the total recovery time of HMIPv6 into following components.

T_a: the time taken by an AR to detect MAP's failure.

T_b: the time required for the propagation of message from the AR to the MN.

T_c: the time taken by an MN to perform local Binding Update with secondary MAP

T_d: the additional time required by an MN to perform binding update with the HA and CN.

Let T_{HMIPv6} be the recovery time in the HMIPv6. Then, the recovery time can be

$$T_{HMIPv6} = T_a + T_b + T_c + T_d$$

The Neighbor Discovery protocol specification [10] limits routers to a minimum interval of 3 seconds between sending unsolicited multicast Router Advertisement messages from any given network interface. But this limitation, however, is not suitable to providing timely movement detection for mobile nodes. In latest MIPv6 draft [11], routers supporting mobility should be able to be configured with a smaller interval value to allow sending of unsolicited multicast Router Advertisements more often. As a consequence the mean time between unsolicited multicast router advertisements is 50ms.

However, the RH-MIP adapts above two case of interval of Router Advertisement messages; in wired region that is between MAP and AR, the interval is 3 seconds and in wireless region that is between AR and MN, the interval is 50ms.

As we consider above that, T_a is associated with wired region, the average T_a is about 1.5 seconds. T_c also includes the time for DAD process performed in the binding update procedure. In general, the mobility agent waits for a response for at least one second in order to perform DAD, and DAD takes a few seconds [12]. Therefore, the recovery time, T_{HMIPv6}, is in the order of a few seconds, although T_b and T_d are small. This recovery time has adverse impact on the service availability.

(b) We define following additional times related to the RH-MIPv6, as shown in Fig 5(b).

T_e: the time taken by a CN to detect MAP's failure.

T_f: the time taken by a CN to update its binding cache list.

T_g: the time taken by an MN to detect MAP's failure.

T_h: the time taken by an MN to update its binding cache list.

The failure recovery times the RH-MIPv6 are

$$T_{HMIPv6} = T_e + T_f \text{ (\textit{when CN detects MAP's failure})}$$

$$T_{RH\text{-}MIPv6} = T_g + T_h \text{ (\textit{when MN detects MAP's failure})}$$

As explained earlier, the MN or CN can easily detect the MAP's failure using ICMPv6 when these agents are in active communication. Therefore, in most cases, T_e (or T_g) is just a few milliseconds. In addition, T_f and T_h, which are required for binding cache update operations, are negligible

Therefore, the recovery time in the RH-MIPv6 is far less than that of the HMIPv6. In later section, we present simulation results to confirm the analytical evaluations.

V. SIMULATIOIN

In this section, we present our simulation model and show simulation results that compared RH-MIPv6's recovery time with HMIPv6's one in case that serving MAP failed.

A. Simulation Model

For the simulation, we use Hierarchical Mobile IP (HMIP) implementation, which was implemented in Columbia IP Micro-mobility Software (CIMS) [13]. It supports micro-mobility protocols such as Hawaii, Cellular IP, and HMIP extension for the ns-2 network simulator based on version 2.1b6. We added the MAP functionality to provide regional registration with the existing CIMS implementations. In addition, we implemented the multiple registrations, which register simultaneously P-RCoA and S-RCoA to CNs.

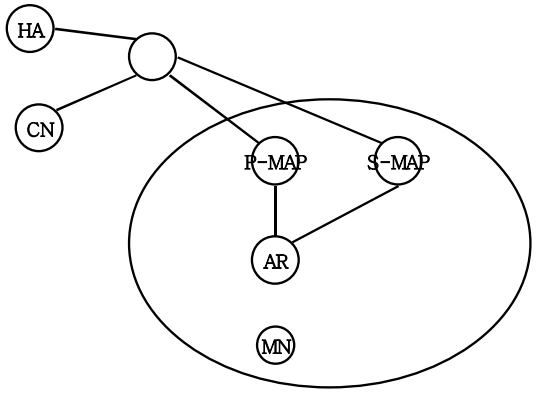


Figure 6. Simulation Network Topology

The simulation is performed using the network topology shown in Figure 6. In this network topology, an MN can detect the presence of primary MAP and secondary MAP. We did not consider MN's mobility. Because the goal of our simulation is to evaluate and compare recovery time in RH-MIPv6 and HMIPv6 for ongoing sessions.

We performed two simulations: one if for HMIPv6 and the other is for RH-MIPv6. In the simulation, we used a TCP connection and a FTP application. FTP service begins at time 0 sec and the primary MAP is failed at time 22 sec. When the MAP failure occurs, the recovery mechanism of the standard HMIPv6, which is explained in the previous section, is performed. Simulation scenario for RH-MIPv6 is same as that of HMIPv6. However, in case of RH-MIPv6, the proposed failure detection and recovery mechanisms are performed when P-MAP is failed at time 22 sec.

B. Simulation Results

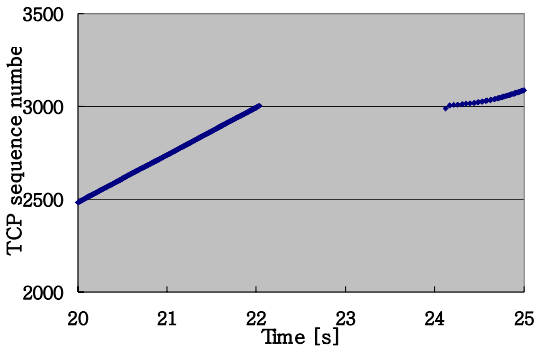


Figure 7. TCP sequence numbers in case of HMIP

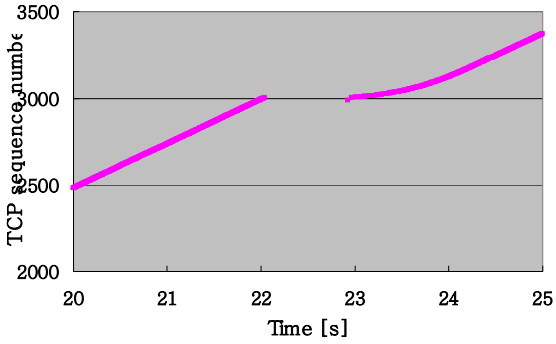


Figure 8. TCP sequence numbers in case of RH-MIP

Figure 7 and Figure 8 show the performance evaluation result to compare HMIPv6 with RH-MIPv6. As shown Figure 7, at time 22.0 sec into the simulation the serving MAP's failure occurs. The data is not transmitted during re-register other MAP and performance of the TCP connection is seriously degraded. The MN sends binding update to other MAP at time 22.9 sec. However the TCP connection is not recovery immediately. Because the CN does not know that a MN's RCoA is changed. The CN continuously retransmits using TCP timer until receiving a binding update message from the MN. Although the binding cache list of CN is updated, the CN waits an acknowledgement in order to know the sequence number that should be used in the next packet. By these procedures, the packets can be started to transmit only after time 24.1 sec. Consequently, the packet loss time of HMIP is about 2.2 seconds.

In Figure 8, the serving MAP fails at time 20 sec same as the previous case. The CN can detect MAP's failure using ICMPv6 in several milliseconds during the CN waiting acknowledgement. At time 22.4 sec, the CN receives ICMPv6 and retransmits immediately data packets using S-RCoA in its binding cache. Hence, the packet loss time of RH-MIPv6 is about 0.9 seconds.

We confirm that the RH-MIPv6 outperforms HMIPv6 in terms of the packet loss time. In other words, RH-MIPv6 has faster recovery time about 60% than HMIPv6 so that RH-MIPv6 is of benefit to guarantee a certain quality of service to mobile users.

VI. CONCLUSION

Fault-tolerance and reliability are critical issues for successful deployment and operation of mobile systems. In this paper, we propose an enhanced HMIPv6 in the distributed MAP environment. The enhanced HMIPv6, called *Robust Hierarchical Mobile IPv6* (RH-MIPv6). The key ideas are to allow multiple registrations via primary and secondary regional CoAs by the MN and to change the serving MAP from the primary RCoA to the secondary RCoA in the case of the MAP failures. By this mechanism, it is possible to reduce the failure detection time and the failure recovery time. In the performance analysis, RH-MIPv6 shows a shorter recovery time than HMIPv6. And we present simulation results by ns-2 simulator that confirms the analytical evaluations under different environments. Consequently, we should say that RH-MIPv6, which we are proposed has faster recovery time about 60% compared with the HMIPv6.

REFERENCES

[1] D.Tipper et al., "Providing Fault Tolerance in Wireless Access Networks," *IEEE Communications Magazine*, January 2002.

[2] H. Soliman, C. Castelluccia et al, "Hierarchical Mobile IPv6 managemenet (HMIPv6)," *IETF draft,* draft-ietf-mobileip-hmipv6-07.txt

[3] H. Omar et al., "Supportinf for Falt Tolerance in Local Registration Mobile IP Systems," *MILCOM, 1998*.

[4] Rajib Ghosh, George Varghese, "Fault-Tolerant Mobile IP," *Washington University Technical Report WUCS-98-11, 1998*.

[5] Cisco Co.Ltd, "Mobile IP Home Agent Redundancy," http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t2/haredun.htm.

[6] S. Knight, D. Weaver et al.," Virtual Router Redundancy Protocol," *IETF RFC 2338*.

[7] ns-2 simulator: www.isi.edu/nsnam/ns/

[8] Yuguang Fang et al, "Analytical Results for Optimal Choice of Location Update Interval for Mobility Database Failure Restoration in PCS Networks," IEEE Transactions on Parallel and Distributed Systems, 2000.

[9] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," *IETF RFC 2463*

[10] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," *IETF RFC 2461*

[11] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," *IETF draft, draft-ietf-mobileip-ipv6-23.txt.*

[12] N. Montavont et al., "Handover Management for Mobile Nodes in IPv6 Network," *IEEE Communications Magazine, August 2002.*

[13] Columbia IP Micro-mobility Software (CIMS), http://comet.columbia.edu/micromobility