Comparison of Survivability & Fault Tolerance of Different MIP Standards

Ayesha Zaman , M.L. Palash , Tanvir Atahary and Shahida Rafique

Abstract— **Mobile IP, the current method of internet connectivity is most often found in WLAN environments where users need to carry their mobile devices across multiple LANs with different IP address. This project work first surveys existing protocols for supporting IP mobility and then proposes an extension to mobile IP architecture, called Robust Hierarchical Mobile IP version6 (RH-MIPv6). This architecture attempts to achieve smaller handoff latency in intra-domain mobile network. In RH-MIPv6 a mobile node (MN) registers primary (P-RCoA) and secondary (S-RCoA) regional care of address to two different MAPs simultaneously. In adaptation to this a “MOVING AREA BASED MAP SELECTION SCHEME” is proposed in this paper. A mechanism is developed to enable the mobile node or correspondent node to detect the failure of primary MAP and change their attachment from primary to secondary MAP. With this recovery procedure, it is possible to reduce the failure recovery time. In this paper it is shown that RH-MIPv6 has faster recovery time than MIPv4 and HMIPv6**

Index Terms— **Intra-domain Mobility, Handoff Latency, Triangular Routing, Transmission Control Protocol Sequence.**

I. Introduction

Mobile IP is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address. A mobile node registers its location at the home agent. The time taken for this registration process combined with the time taken for a mobile node to configure a new network care-of address in the visiting network, amounts to the overall handoff latency.

The less the handoff latency, the shorter the packet failure recovery time within the MIP standard. Again “Survivability” is used to describe the available performance after a failure [1]. MIPv4 does not consider system survivability and fault tolerance due to triangular routing problem. Again in the HMIPv6, HAs and MAPs are two points of failure and potential performance bottlenecks. Since failure of home agent (HA) or mobile anchor point (MAP) causes service interruption, the Hierarchical Mobile IPv6 (HMIPv6) has only weak survivability [2].

In this paper Robust Hierarchical Mobile IPv6 (RH-MIPv6) is proposed which provides survivability and fault tolerance with the existing HMIPv6.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.

II. Architecture of Robust Hierarchical Mobile IPv6 (RH-MIPv6)

Here Figure(1) illustrates the architecture of RH-MIPv6.

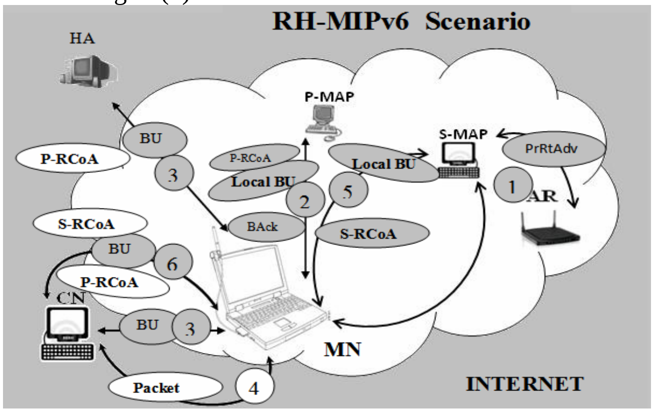


Figure 1. RH-MIPv6 Architecture

Manuscript received Sunday, June 14, 2009. This work was sponsored by the IEEE Computer Society Test Technology Technical Council (TTTC) and financially supported by Cadence, JTAG Technologies, Kaspersky Lab, Synopsis, Mentor Graphics, Tallinn Technical University, Donetsk Institute of Road Transport, Moscow Institute of Electronics and Mathematics, Virage Logic, Echostar, Aldec, Teprocomp, Data Art Lab.

F. A. Ayesha Zaman is a researcher in Dept. of Applied Physics, Electronics and Communication Engineering, University of Dhaka. ph: 01711589484; email: ayeshazaman_gsm@yahoo.com

S. B. M.L. Palash is a lecturer in Department of Electronics and Telecommunication Engineering, Institute of Science & Technology.

T.C. Tanvir Atahary is a lecturer in Department of Electronics and Telecommunication Engineering, University of Liberal Arts Bangladesh, Dhaka Bangladesh. email: tanoy_ece@yahoo.com

Fo. C. Prof. Dr. Shahida Rafique is a Professor in Dept. of Applied Physics, Electronics and Communication Engineering, University of Dhaka. She is also the Dean of Engineering faculty of the same university, email: Shahida.rafique@hotmail.com

III. Primary and Secondary MAP Selection Scheme

A MAP periodically broadcasts a RA message with a MAP option, in order to inform MNs of its presence. The MAP option, which is an IPv6 neighbor discovery extension, is used to disseminate the MAP information throughout a foreign network. For the purpose of MAP selection, the MAP option contains two fields: Distance and Preference fields. The Distance field records the hop distance from the MAP to the MN whereas the Preference field indicates the willingness of the MAP to offer a local registration service. In the furthest MAP selection algorithm, the furthest MAP may be overloaded if all MNs register to the furthest MAP. In addition, if an MN's movement is bounded to the limited area, a nearer MAP can reduce registration delay and signaling overhead than the furthest MAP. For the preference selection, it is difficult to determine how to assign preference values for each MAP. For this a new MAP selection scheme has been proposed which is the "MOVING AREA-BASED MAP SELECTION".

IV. Moving Area-Based MAP Selection

The proposed scheme is called Moving Area-Based MAP selection, in which the MH keeps track of its moving area to determine the best MAP. Figure (2) illustrates the basic idea of the proposed scheme, in which each mobile host selects the closest MAP that covers its moving area. The mechanism for a MH to keep track of its moving area is based on the MAP option periodically transmitted downward by each MAP in the hierarchy. The MH records the total number of MAP options issued by each MAP in its MAP Option Table. When the MH moves to a new subnet, it invokes the MAP selection algorithm to select the MAP with most MAP options received by the MH over a predefined period of time. If there are two or more MAP candidates with the same most MAP options, the MH selects the lowest MAP.

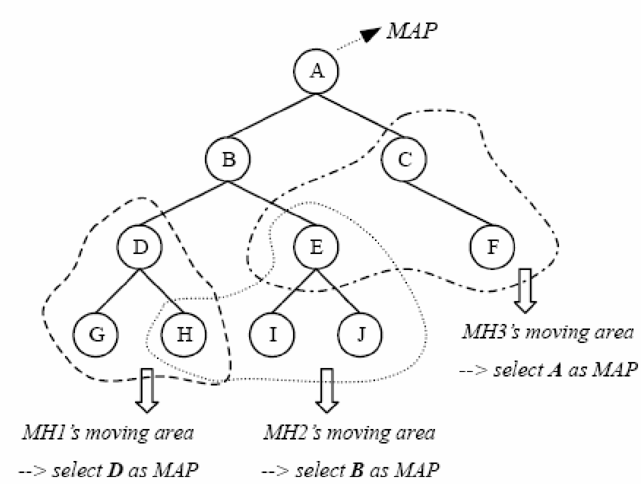
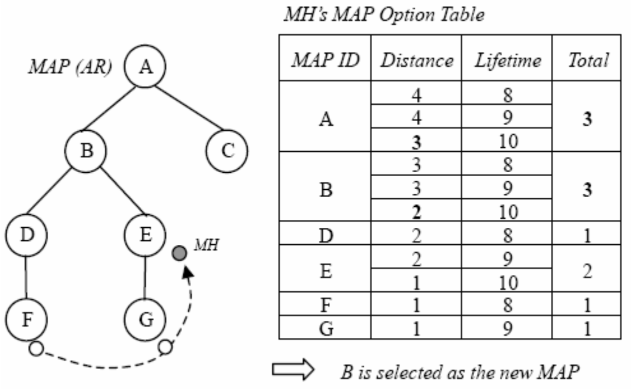


Figure 2. Moving area based MAP selection

For example, the MH in Figure (3) moves from MAP F (the initial position) to MAP G, and then to MAP E. It is assumed that the MH receives only one RA (sent out by MAP A) while it is on each MAP and the lifetime for a new MAP option is set to 10. The MAP Option Table maintained by the MH is shown in figure (3). According to the proposed scheme, MAP B is selected as the new MAP by the MH since it is the closest MAP from which the MH has received the most MAP options. So an MN, receiving multiple RA messages from multiple MAPs, can select two MAPs: the most suitable MAP and the next one. The most suitable MAP is called a primary MAP (P-MAP) and the next one a secondary MAP (S-MAP). In addition, the MN configures a primary RCoA (P-RCoA) and a secondary RCoA (SRCoA) in the P-MAP and S-MAP domains, respectively. After that, the MN registers its (Local Care of Address)L-CoA to the P-MAP/S-MAP.



MH's MAP Option Table

MAP ID	*Distance*	*Lifetime*	*Total*
A	4	8	**3**
	4	9	
	3	10	
B	3	8	**3**
	3	9	
	2	10	
D	2	8	1
E	2	9	2
	1	10	
F	1	8	1
G	1	9	1

⇨ *B is selected as the new MAP*

Figure 3. An example of MAP option table

V. Failure detection and recovery mechanisms

In the HMIPv6 specification, a MAP failure event can be detected by checking a MAP option, which contains an invalid lifetime in the broadcasted RA message. However, it takes too much time for an MN to detect the failure by this passive method because the RA interval is set to a few seconds. Thus, the passive failure recovery mechanism of HMIPv6 results in high packet losses, especially when the MN is communicating with multiple CNs. On the other hand, an MN in the RH-MIPv6 specification detects a MAP failure during packet transmission by utilizing ICMP. Therefore, faster failure detection can be achieved in the presence of active sessions without waiting for any RA message with a coarse grained RA interval. In this section, the failure detection and recovery mechanisms are divided into two cases: those detected by the MN and those by the CN.

A. Failure Detection and Recovery by MN

RH-MIPv6 provides a more active failure detection method than HMIPv6. If an MN is actively sending packets to CN, the MN can detect the MAP failure by receiving ICMP error messages from a router adjacent to the failed P-MAP. Or, when the MN is receiving packets from CN, the MN will receive the encapsulated packets from the S-MAP instead of the P-MAP. This indicates that a P-MAP failure happens. After detection of the P-MAP failure, the MN changes its serving MAP from the P-MAP to the S-MAP. Then, the MN can resume data transmission, if the MN was sending packets to a CN. In this case, the CN receives packets from the MN, which has registered a binding entry of a reset P field during secondary BU(Binding Update) procedure. Then, the CN eliminates primary binding information (i.e. the P field is set) and sets the P field of the secondary binding entry to 1. At the same time, the MN sends BU messages with S-RCoA to the HA and S-MAP as soon as possible. When the BU message arrives at the HA,the HA updates CoA of the MN from the P-RCoA to the S-RCoA. In addition, the S-MAP moves the binding entry of the MN from the backup mapping table to the serving mapping table.

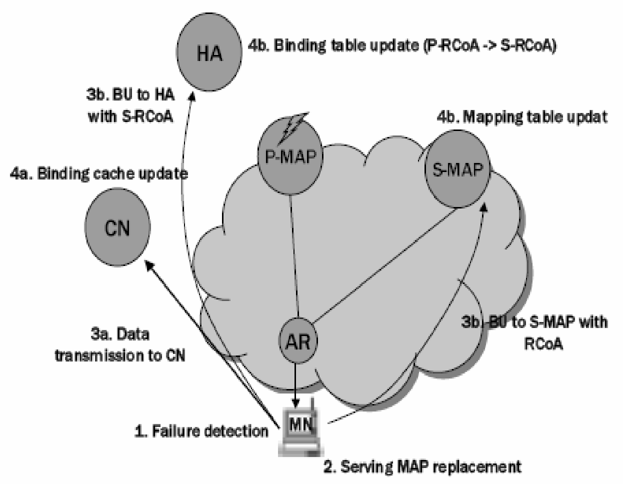

HA
4b. Binding table update (P-RCoA -> S-RCoA)
3b. BU to HA with S-RCoA
P-MAP
4b. Mapping table updat
S-MAP
4a. Binding cache update
CN
3a. Data transmission to CN
AR
3b. BU to S-MAP with RCoA
1. Failure detection
MN
2. Serving MAP replacement

Figure 4.Failure recovery procedure by the MN

B. *Failure Detection and Recovery by CN*

It is assumed that a CN is currently sending data packets to an MN via P-MAP. If the P-MAP fails, the CN receives ICMP error messages (i.e., Host Unreachable) for the sent packets. Then, the CN decides that the P-MAP has failed and rerouting through the S-MAP is then required. Typically, the link loss rate in a wired link is extremely low. Therefore, if the CN determines the MAP failure after receiving a few successive ICMP error messages, a wrong decision can be minimized [7].

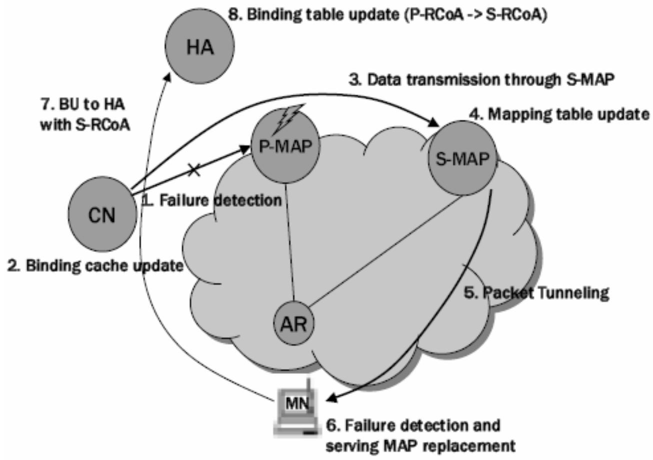


Figure 5. Failure recovery procedure by the CN

Fig.(5) illustrates the failure recovery procedure when a MAP failure is detected by a CN. As mentioned before, the CN regards multiple receptions of ICMP error messages as the indication of a MAP failure. Then, the CN looks for a binding entry with a reset P field in its binding cache, which is updated by the secondary BU procedure.After updating the binding cache, the CN resumes data transmission through the S-MAP and the S-MAP updates its mapping tables. After completion of the mapping table update, the S-MAP tunnels the received packets to the destination MN. If the MN detects a MAP failure, the MN sends a BU message with the S-RCoA, which is configured in the MAP selection procedure in advance, to the HA. After re-BU procedure, the MN can communicate with new CNs, which tries to connect the MN using binding information at the HA, through the S-MAP.

VI. Simulation Based Performance

In this paper IP packet recovery time of three Mobile IP standards has been compared. Here NCTUns-4.0 has been used as the simulator.

A. *TCP sequence number in case if MIPv4*

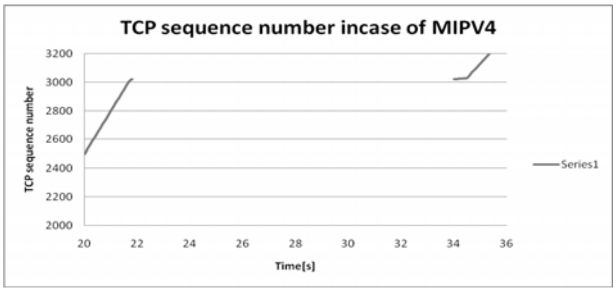


Figure 6. Time vs TCP sequence number for MIPv4

Analysis: When the MN travels from one subnet to another, in between the traversal process handover is halt for sometimes. Then packet transmission from the CN to the MN also halts for a few seconds. Again when the MN registers with a new point of attachment with the n FA, packet transmission continues. The registration process takes some non-zero time to complete as the registration requests propagate through the network. During this period of time the MN is unable to send or receive (IPv4) packets. Here the handover latency is larger due to the requirement of several registrations with different FAs. This is why the packet recovery time is of considerable amount which is shown here about 12 seconds.

B. *TCP sequence number in case of HMIPv6*

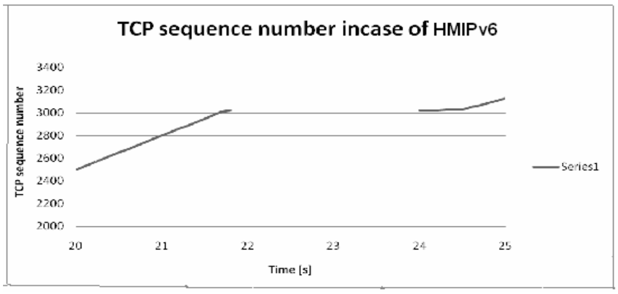


Figure 7. Time vs TCP sequence number for MIPv4

Analysis: In terms of failure recovery, in the case of HMIPv6 , when a failure happens at the MAP, an MN re-configures a new R-CoA after failure detection and the MN registers the new R-CoA to the HA and CNs . Only after the completion of these processes, the MN can resume the suspended sessions. Therefore a significant amount of time which may not be acceptable in real-time applications is wasted for failure detection and recovery in HMIPv6 networks. In this case the failure recovery time is about 2 seconds which is less than that of MIPv4 recovery mechanism.

C. *TCP sequence number in case of RH-MIPv6*

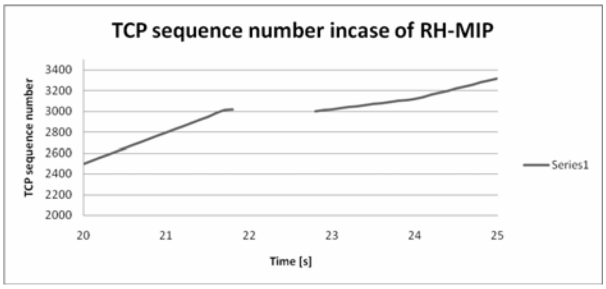


Figure 8. Time vs TCP sequence number for RH-MIPv6

Analysis: In RH-MIPv6, multiple R-CoAs are configured in advance and are dynamically changed after failure detection. Hence it is possible to reduce the failure recovery time than HMIPv6, which is about 1 second as shown in figure above.

VII. Conclusion

One of the most important criteria that affects the scalability property of a mobility management scheme is its signaling load i.e. the bandwidth used by the control messages, such as the Binding Updates to support mobility. In this project MOVING AREA BASED MAP SELECTION SCHEME is proposed where the most suitable MAP had the maximum MAP OPTIONs with minimum number of hop count. This scheme is proposed because in the conventional furthest MAP selection scheme there is a problem of signaling overload. Our future work will be to propose an appropriate load balancing mechanism for the MAPs within a domain in RH-MIPv6 standard.

Acknowledgment

The authors thank Prof. S.Y. Wang of Harvard University for the availability of software package NCTUns 4.0 Network Simulator and Emulator which has high-fidelity of simulating various protocols used in both wired and wireless IP networks.

References

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

[2] H. Omar et al., “Supporting for Fault Tolerance in Local Registration Mobile IP Systems,” MIlcom,1998

[3] C. Caetelluccia and L. Bellier, “ Hierarchical Mobile IPv6 Mobility Management (HMIPv6)”, Internet Draft, draft-ietf-mobile ip-hmipv6-08.txt, Work in Progess , Jun, 2003.

[4] K. Kawano, K. Kinoshita, K. Murakami, “ A Mobility –Based Terminal Management in IPv6 Networks”, *ICICE Trans. Commun*. Vol. E85-B, No. 10, Oct, 2002.

[5] S.Pack, T. Kwon, Y. Choi, “ A Comparative Study of Mobility Anchor Point Selection Schemes in Hierarchical Mobile IPv6 Networks”, *ACM MobiWac 2004*, October 2004.

[6] Sangheon Pack, “Robust Hierarchical Mobile IPv6: An Enhancement for Fault-Tolerant Mobile Networks”.

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

First A. Ayesha Zaman was born in Dhaka, Bangladesh on 20th October, 1984. She completed her BSc. Engineering in 2007 and MSc. in 2009 from the department of Applied Physics, Electronics & Communication Engineering, University of Dhaka. She stood 1st class 2nd in BSc. and 1st class 1st in MSc. examination from the same department.

At present she is a research worker at University of Dhaka. She has also worked with neuro-image processing. She has keen interest in Biomedical Engineering also. She has a conference paper in this field; World Academy of Science, Engineering & Technology 57,2009: ISSN 2070-3724, p-p: 230-235; Amsterdam, The Netherlands. She intends to do her further research in the field of communication engineering especially high speed networking.