An Approach to Efficient and Reliable design in Hierarchical Mobile IPv6

Taewan You[1], Seungyun Lee[1], Sangheon Pack[2], and Yanghee Choi[2]

[1]*Protocol Engineering Center, ETRI, 161 Gajoung-dong, Yusong-gu,*
Daejeon 305-350, Korea
{twyou, syl}@etri.re.k
[2]*School of Comupter Science and Engineering, Seoul Nat'l Univ.,*
San 56-1 Shinlim-dong, Kwanak-gu, Seoul 151-742, Korea
{shpack, yhchoi}@mmlab.snu.ac.kr

Abstract

As the demand for wireless mobile devices capable of executing real-time applications increases and as the number of mobility users grows, the Mobile IP has necessitated the development of better handoff techniques, for providing seamless handoff, namely, a packet lossless Quality of Service (QoS) guarantee. The Hierarchical Mobile IPv6 (HMIPv6), is to enhance the Mobile IPv6, is designed to resolve these issues. The MIPv6 protocol handles local and global user mobility equally. Therefore it may lead to some problems like lost data packet and inefficient network bandwidth use when a mobile node is handoff frequently in local area. But the HMIPv6 is planned to reduce the amount of signaling that is required for managing user movement within the mobile network using a new mobility agent, which is called mobile anchor point (MAP). However, since the home agent (HA) and the mobile anchor point (MAP) are main points of failure and performance bottlenecks. In this paper, we propose an approach to efficient and reliable design in Hierarchical Mobile IPv6. In order to remove performance bottlenecks for the MAP, at first, we proposed a load balancing scheme in distributed MAP environment. We are only present appropriated a design adopting load balancing, but we do not present specific methods. And next, we proposed an enhanced Robust Hierarchical Mobile IPv6 (RH-MIPv6). The RH-MIPv6, which is provided by our previous work, supports survivability and fault tolerance with the existing HMIPv6. By these approaches, it is possible to efficient and reliable design for HMIPv6. By simulation, we confirm that our proposed the approach design is efficient and reliable about HMIPv6.

Keywords: QoS, HMIPv6, efficient, reliable, load balancing, fault tolerance

1. Introduction

Recently, a lot of the end hosts are mobile over heterogeneous wireless access networks. And as the demand for this wireless mobile devices capable of executing real-time applications increases, the Mobile IP has necessitated the development of better handoff techniques, for providing seamless handoff, namely, a packet lossless Quality of Service (QoS) guarantee as well as caching and load balancing. In wireless mobile networks, system survivability is also one of the most important issues. It is used to describe the available performance after a failure. 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 proposed to separate mobility into micro-mobility (within one domain) and macro-mobility (between domains) although Mobile IPv6 (MIPv6) [1] considered macro-mobility only. However, in the HMIPv6, HAs and MAPs are two points of failure and potential performance bottlenecks. These problems lead to low availability and reliability. Therefore, when the HMIPv6 is deployed in wireless/mobile networks, fault tolerance and system performance 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] [4] and for performance enhanced in PCS network or mobile network, they are about load balancing schemes and call admission control [5] [6].

In our previous work, we had proposed a new design to support fault tolerance and robustness modifying mobility agent's binding cache and to reduce failure detection time using ICMPv6 messages. This scheme is called Robust Hierarchical Mobile IPv6 (RH-MIPv6) [11]. The key ideas are to allow multiple registrations via primary and secondary regional care-of address (P-RCoA, S-RCoA) by MN and to change the serving MAP from the P-RCoA to the S-RCoA in the case of the MAP failures. In addition for failure detection, when a MN or CN is sending some data packets, it can detect the failure of serving MAP if there no response to the sent packets via Internet Control Message Protocol version 6 (ICMPv6) [7].

In this paper, we propose an approach to efficient and reliable design in Hierarchical Mobile IPv6. In order to remove performance bottlenecks for the MAP, at first, we proposed a load balancing scheme in distributed MAP environment. 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. In this environment where several MAPs are discovered by the MN in a domain, the MN may need some sophisticated algorithms to be able to select the appropriate MAP. These algorithms would have characteristic of the MN combined with the preference field in the MAP option. To adopt load balancing, the MAP should set the preference value according to shared load table, which is keep by MAP. After the MN receives MAP option, it select serving MAP to load balancing. We are only present appropriated a design adopting load balancing, but we do not present specific methods or algorithms. And next, we proposed an enhanced RH-MIPv6. The case of the RH-MIPv6, when the serving MAP is failed, the MN or CN can detect during communicate with each others via ICMPv6 error message. In this time, the MN or CN only send data packets using secondary RCoA to destination node. As a result, other nodes that serviced by failed MAP and that do not communication currently need much time to detect serving MAP failure. Therefore, we enhance RH-MIPv6 to other nodes to inform serving MAP failure as soon as known the fact. By these approaches, it is possible to reduce failure detection time and recovery time.

The remainder of this paper is organized as follows. In Section 2, we describe the efficient and reliable design modifying mobility agents in HMIPv6 based on RH-MIPv6. Section 3 explains load balancing scheme. In section 4, we also explain failure detection, and recovery mechanism. Several simulation results using ns-2 simulator [8] are given in Section 5. At last, Section 6 concludes this paper.

2. Efficient and Reliable design for HMIPv6

2.1 Architecture

In this paper, we consider a distributed MAP environment, where there exist multiple independent MAPs, shown in Fig. 1. In Fig.1, MAPs act as a kind of local HAs. This environment has several advantages in terms of load balancing and scalable service. Therefore we recommend distributed MAP environment to efficient and reliable design of HMIPv6.

In HMIPv6, when the MN moves into a new MAP domain, it needs to configure two CoAs: an RCoA on the MAP's link and an on-link CoA (LCoA) and sends local binding update (BU) to MAP to bind LCoA to its LCoA. After registering with the MAP, the MN must register its new RCoA with its HA and CN. But we proposed design allows multiple registrations via primary RCoA (P-RCoA) and secondary RCoA (S-RCoA). Therefore, the binding cache in CNs and the mapping table in MAPs should be modified and a new management scheme for them should be introduced by [11].

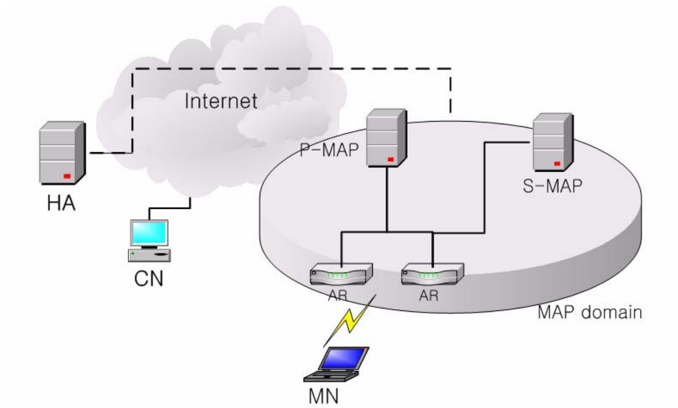

Figure 1. Distributed MAP environment

2.2 Mobility Agents Design

The MN and CN are modified binding cache to maintain two binding entries: MN's P-RCoA and S-RCoA. We proposed binding cache structure, shown in Fig. 2. The only different point from general binding update cache is P field. P filed is set 1 means that MN's RCoA is primary. When a CN receives a BU messages with RCoA, P field is set 1 whether or not using P flag within BU messages. Later, we explain BU operation in section 2.3.

No	Home Address	Care-of Address	Lifetime	P	…
1	2001:4ef::1:2:3	2001:230e::3:2:1	2000	1	…
2	2001:3201::2:4:f	2001:390f::3:f:e	1500	1	…
3	3ffe:e3f1::6:4:3	3ffe:270e::2:4:4	700	1	…
4	2001:4ef::1:2:3	2001:230e::5:3:1	3000	0	…
…	…	…	…	…	…

Figure 2 Modified binding cache structure

For primary and secondary BU procedures, the MAP maintains two types of mapping tables: primary mapping table and backup mapping table and shared Load tables to give reference to decide preference field within MAP option. The primary mapping table contains a number of (Home Address, LCoA) pairs for MNs having performed a primary BU procedure. Another hand, the backup mapping table contains (Home Address, LCoA) pairs obtained by means of the secondary BU procedure. At last, the shared load table indicates the capacity of accommodating about registered MNs. A MAP is kept each other MAPs' loaded value within a MAP domain. This value is categorized three classes by two level thresholds: high, middle, low. A MAP formulates two of thresholds value about traffic load considering MAP's buffer size and system performance. When a MAP has number of registered MN over Upper threshold, this MAP set Load field to high. It means that the MAP has high overhead to register MNs. A specific MAP's operation is explained in section 3.1

2.3 Registration with P-RCoA and S-RCoA

When an MN moves into a new MAP domain, it receives Router Advertisement messages containing information on locally available MAPs. The MN collects all RA messages from MAPs can be reachable from the MN in a foreign network. Then, the MN selects a P-MAP and a S-MAP using an MAP selection algorithm as follows in section 3. After selecting P-MAP and configuring P-RCoA, the MN should perform a local binding update (BU) procedure to the selected P-MAP. These Binding update mechanism is similar to that of the HMIPv6. However, the MN needs to register another RCoA, which is called S-RCoA. In our proposed scheme, the MN registers both P-RCoA and S-RCoA 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.

3. Load balancing mechanism

3.1 MAP Operation

As a mentioned before, multiple MAPs share the load table among a MAP domain to help decision serving MAP by a MN. At first, the MAP should monitor its buffer size and system performance. And the MAP formulates two of thresholds value. When the number of registered MNs is under Upper threshold value and over Lower threshold value, the MAP set middle to load field. Each MAP periodically broadcasts its traffic load message to all the other MAPs in a MAP domain. Upon receiving the traffic load message from other MAPs, the MAP make a Load Table, shown in Fig. 3. This shared load table is updated whenever it is received periodically.

MAP IP	Load value
2001:230e::1	High
2001:230e::2	Low
2001:230e::3	Low
…	…

Figure 3. Shared Load Table

At last, the MAP decides a preference value referencing shared load table. And the preference value is set to MAP option, which is sent with router advertisement (RA) to all of AR in a MAP domain. In this paper, we are only present appropriated a design adopting load balancing, but we do not present specific methods or algorithms.

3.2 MAP Selection Scheme

A MAP periodically broadcasts RA messages with MAP options, in order to inform MNs of its presence. The MAP option, which is an IPv6 neighbor discovery extension, is defined in [2] to dissemination MAP information throughout a foreign network. For 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 and the Preference field indicates the willingness of the MAP to offer a local registration service. In our proposed load balancing scheme, the MAP already decide preference value and send RA with MAP option to MNs. When a MN receive RA with MAP option, the MN select P-MAP and S-MAP to load balancing referencing Preference field in MAP option. Other selection algorithm is published [9].

4. Failure Detection and Recovery Mechanisms: Enhanced RH-MIPv6

In the HMIPv6, the failure of the MAP can be detected using a MAP option containing a valid lifetime. These detect failure and recovery mechanism takes too much time for an MN to detect the failure because the interval of Router Advertisements messages is set to a few seconds [10]. 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 our proposed failure recovery mechanism reduces the packet loss rate in the case of MAP failure using more active failure detection methods by utilizing Internet Control Management Protocol version 6(ICMPv6) [7] as shown in Fig.4.

If an MN is actively sending packets to CNs, the MN can detect MAP failures by receiving ICMP error messages from failed P-MAP (1). Or, if the MN is receiving some packet from CNs, the MN will receive the encapsulated packets from the S-MAP instead of the P-MAP. Then, the MN considers the fact that the P-MAP has failed. The MN changes its serving MAP from P-MAP to S-MAP. Then the MN notice fact of P-MAP failure to announce all of MN, which is serviced by P-MAP (2.a). After AR receives announce message from the MN, AR set life time to zero. Therefore AR reduces failure recovery time to eliminate procedure, that the AR is triggered to advertise a MAP option by sending echo request messages. As a result, the MNs, which receive MAP option containing zero lifetime, can know serving MAP failure. And then other MNs begin to work to search S-MAP in Binding Cache list as soon as possible. Next step, the data transmission is resumed (2.b). With data transmission, the MN also sends BU message to the HA and the CN with S-RCoA as soon as possible (2.c-2.d). When the BU message arrives at the CN, the CN updates a RCoA of the MN from P-RCoA to S-RCoA. The other case, the CN performs similar procedures to that of the detection and recovery by MN

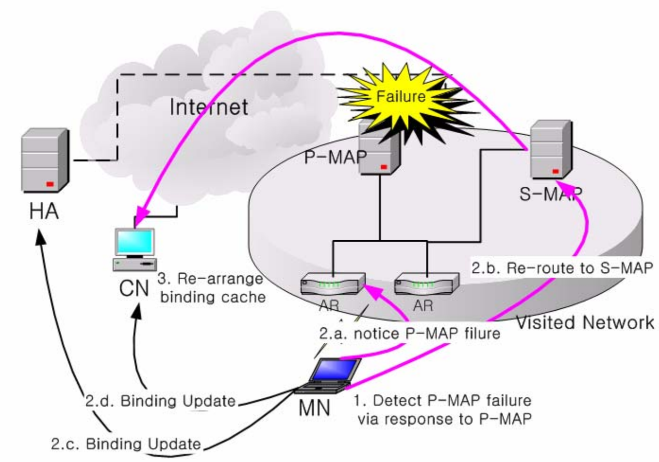

Figure 4 Failure detection and recovery procedure in MN

5. Simulation Study

In this section, we present our simulation environment and show simulation results that compared our proposed scheme's recovery time with HMIPv6's one in case that serving MAP failed. For the simulation, we use network simulator (ns-2) [8]. We performed two simulations: one if for HMIPv6 and the other is for our proposed scheme. In the simulation, we used a TCP connection and a FTP application. FTP service begins at time 3 sec and the primary MAP is failed at time 10 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 new scheme is same as that of HMIPv6. However, in case of new scheme, the proposed failure detection and recovery mechanisms are performed when P-MAP is failed at time 10 sec.

Fig. 5 shows the performance evaluation result to compare HMIPv6 with new scheme. As shown Fig. 5's left side, at time 10.0 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 10.9 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 (refer to 0.6 sec in case of this simulation) until receiving a binding update message from the MN. Timeout occurs at the time of 10.60sec, 11.80sec, and 14.20sec. By these procedures, the packets can be started to transmit only after time 14.34 sec. Consequently, the packet loss time of HMIP is about 4.34 secs. In TCP, a congestion window size is set to one and a slow start threshold value is changed to the half of the congestion window size after timeout. Therefore, if a number of timeouts occurs as shown in Fig. 5's right side, TCP throughput decreases drastically.

In contrast, right side shows TCP sequences as time increases. In new scheme, since the faulty time is smaller than that of HMIPv6, only one timeout occurs. Therefore, a slow start can be begun earlier than in the case of HMIPv6 and this enables it to reach the network capacity faster. In more detail, the serving MAP fails at time 10 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 10.4 sec, the CN receives ICMPv6 and retransmits immediately data packets using S-RCoA in its binding cache. Hence, the packet loss time of new scheme is about 1.9 seconds.

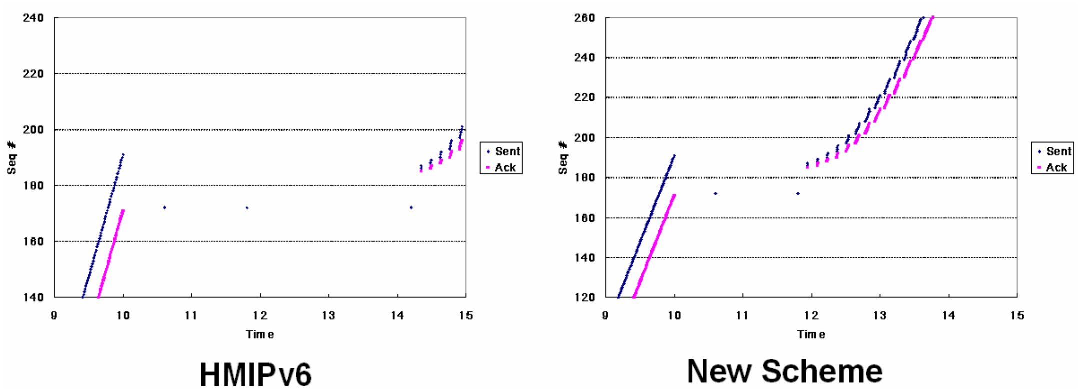

Figure 5 Simulation Results

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

6. Conclusion

Recently, as the demand for the wireless mobile devices capable of executing real-time applications increases, the Mobile IP has necessitated the development of better handoff techniques, for providing seamless handoff, namely, a packet lossless Quality of Service (QoS) guarantee as well as caching and load balancing. In this paper, we propose approaches for efficient and reliable design in Hierarchical Mobile IPv6. In order to remove performance bottlenecks for the MAP. 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. And to adopt load balancing, the MAP should set the preference value according to shared load table, which is keep by MAP. By this proposed mechanism, it is possible to reduce the failure detection time and the failure recovery time and to eliminate performance bottleneck using load balancing scheme at the MAP. We present simulation results by ns-2 simulator to confirm that our proposed design is the efficient and reliable. Consequently, we should say that the approach design is efficient and reliable compared with the origin HMIPv6.

7. References

[1] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6,”IETF draft, draft-ietf-mobileip-ipv6-24.txt.

[2] H. Soliman, C. Castelluccia et al, “Hierarchical Mobile IPv6 management (HMIPv6),” IETF draft, draft-ietf-mipshop-hmipv6-01.txt.

[3] J. H. Ahn, S. G. Min, and C. S. Hwang, “Scalable and Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP-based Systems,” Future Generation Computer Systems, vol. 18, no. 5, pp. 613-625, Apr. 2002.

[4] J. Lin and J. Arul, “An Efficient Fault-Tolerant Approach for Mobile IP in Wireless Systems,” IEEE Trans. on Mobile Computing, Vol. 2, Vo. 3, July-Sep. 2003.

[5] S. B. ZahirAzami, G. Yekrangian, M. Spencer, “Load Balancing and Call Admission Control in UMTS-RNC, using Fuzzy Logic,” Proceedings of ICCT2003, vol. 2, 9-11, Aprill 2003.

[6] H. Deng, X. Huang, K. Zhang, Z. Niu, M. Ojima, “A Hybrid Load Balance Mechanism for Distributed Home Agent in Mobile IPv6,” IEEE 2003 International Symposium on Personal, vol. 3, Sept. 7-10 2003.

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

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

[9] Y. Xu, H. C. Lee, V. L. L. Thing, “A Local Mobility Agent Selection Algorithm for Mobile Networks,” Proc.IEEE ICC 2003, May 2003.

[10] T. Narten, E. Nordmark, W. Simson, “Neighbor Discovery for IP version 6 (IPv6),” IETF RFC 2461.

[11] T.W.You, S.H.Pack, Y.H.Choi, “Robust Hierarchical Mobile IPv6 (RH-MIPv6),” Proc. IEEE VTC 2003-fall, Oct. 2003.