An Efficient Approach for Adaptation of MIPv6 in Roaming Environments

*Yoon-su Jeong, Sung-hee Woo, Sang-ho Lee
Dept. of Network Security Laboratory Chungbuk National Univ.
Email : {bukmunro@netsec.cbnu.ac.kr, shwoo@cjnc.ac.kr, shlee@chungbuk.ac.kr }

Abstract: Mobile IPv6(MIPv6) allows a Mobile Node to talk directly to its peers while retaining the ability to move around and change the currently used IP address. One of the major issues regarding the basic Mobile IPv6 protocol is related to the handover management of a mobile node. This paper proposes efficient approach for adaptation of MIPv6 using context information in roaming environments. To investigate on a efficient and secure handover procedure, proposed approach method will give us the following advantages: (1)the intention of context is to reduce latency, packet losses and avoid re-initiation of signaling to and from mobile nodes,(2) FMIPv6 aims to reduce handover latency due to IP protocol operations as small as possible in comparison to the inevitable link switching latency.

Keywords: MIPv6, Authentication, Handover.

1. Introduction

The current version of Internet Protocol (IPv4) and also the newer version (IPv6) assumes that the physical location of the computers do not change during the time the computer is connected to a network. In other words, once a computer is connected to the network using an IPv6 address, throughout the lifetime of the connection, the computer is assigned just one IPv6 address. The location of the computer connected to the network is assumed to be fixed. But all these assumptions seem to disappear once the environment changes to a mobile one. In order to be in a mobile computing environment, the users should have the freedom to connect to the network from different access points through wireless links and the network should be capable to keep the mobile user connected while he/she is on the move.

Therefore mobility management is one of the key issues being researched by the mobile computing research groups all throughout the world. Mobility management deals with maintaining a mobile devices connectivity as it moves from one subnet to another. GSM, one of the most widely used mobility management protocols, deals with maintaining the connectivity of a mobile phone. GSM is still being used by the telecom industry worldwide, which mainly deals with the cellular networks and circuit switching technology. But the Internet, as we know, is a packet switched network and therefore needs its own mobility management protocol. The IETF has proposed the Mobile IP protocol to deal with mobility management across the internet for any mobile device. Mobile IP is an extension to the existing IP protocol and has essentially two versions: Mobile IPv4 and Mobile IPv6, in keeping the old and new versions of IP. This thesis deals with Mobile IPv6.

Mobility management as a whole deals with essentially two major areas: location management and handover management. Although Mobile IPv6 attempts to solve these to some extent, there are still a lot of issues, mainly dealing with the handover management problem. Some researchers[2.4.5.7] have suggested some changes and extensions to the basic Mobile IPv6 protocol aimed at solving the handover management problem. It can decrease the performance of the router and, consume more bandwidth and generate more traffic overhead.

In this paper we present a new method for handover in MIPv6 using context in roaming environments. It is based on Hierarchical Mobile IPv6 (HMIPv6)[2], which is a solution to enhance handovers of MIPv6 clients. To investigate on a efficient and secure handover procedure, the solution in the paper will give us the following advantages: (1)the intention of context is to reduce latency, packet losses and avoid re-initiation of signaling to and from mobile nodes,(2) FMIPv6 aims to reduce handover latency due to IP protocol operations as small as possible in comparison to the inevitable link switching latency. The proposed solution is a way to the problem of handoff induced packet delay that has the potential to surpass the performance of the proposed proposal.

The rest of this paper is organized as follows. Section 2 introduces previous works related to MIPv6. In Section 3, we describe a new method for handover in MIPv6 using Diameter in roaming environments Section 4 concludes the paper.

2. Related Work

1)MIPv6

Each time MN moves to a new link, it would change its IP address[3]. Therefore, packets destined to its previous address would not be able to reach it. In MIPv6, each MN is always identified by its home address(HoA), regardless of its current point of attachment to the Internet. While situated away from its home, a MN is associated with a care-of address (CoA), which provides information about its current location. HA is informed of these addresses binding and IPv6 packets addressed to a MN's HoA are then transparently routed to its CoA by the HA. In this way, MN would be able to maintain transport and higherlayer connections when it changes location. MIPv6 also enables IPv6 nodes corresponding with MN(CNs) to cache the binding of the MN's HoA with its CoA, and to then send any packets destined for the MN directly to it at this CoA.

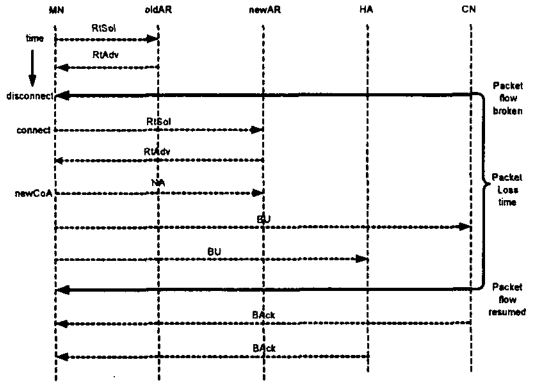

Figure 1. MIPv6 signaling diagram

The signaling diagram is shown in figure 1. Note that only after the MN has been disconnected and then connected to a new link does the MIPv6 process realize that HO has occurred due to the detection of a new Router Advertisement(RtAdv).

Packet flow is disrupted when the L2 link between the MN and older is broken. The MN must receive an RtAdv from the newAR to calculate a newCoA. When this newCoA has been accepted, it must be registered with the newAR using a Neighbor Advertisement(NA). Finally, a BU containing the newCoA must be registered with the CN before the packet flow can be resumed

2) HMIPv6

The Hierarchical Mobile IPv6 protocol (HMIPv6)[2] is also a recently proposed protocol aimed at making the handover process in a Mobile IPv6 environment more efficient. This protocol also extends the basic Mobile IPv6 protocol and suggests some new functions which make the handover process a seamless one. The Hierarchical Mobile IPv6 protocol proposes the introduction of a new entity known as a Mobility Anchor Point (MAP). Figure 2 depicts the use of a MAP as specified in the protocol [2].

The newly introduced entity known as the MAP acts as a local Home Agent (HA) for the moving mobile node. In the above figure the MAP domain is shown to contain three subnets, each of them having their own access router (AR). Whenever the mobile node changes position from one subnet to another subnet in the same MAP domain, then a Binding Update only needs to be sent to the MAP, instead of sending it all the way to the HA, thus reducing handover latency. Like in the case of a HA, the MAP will receive all packets on behalf of the MN it is serving and will encapsulate and forward them directly to the MN's current address. If the MN changes its current address within a local MAP domain, it only needs to register the new address with the MAP. This new care-of address will only be a local care-of address. Hence, the global CoA which the mobile node registered with Correspondent Nodes (CNs) and the HA does not change. This makes the MN's mobility transparent to the CNs it is communicating with. The Hierarchical Mobile IPv6 protocol is not dependant on the Layer 2 protocol used. The boundary of a MAPs domain is defined by the access routers advertising the MAP information in the form of Router Advertisements to the mobile node. When a mobile node arrives in a foreign network, the mobile node discovers the address of the MAP, by receiving the Router Advertisements sent by the access routers.

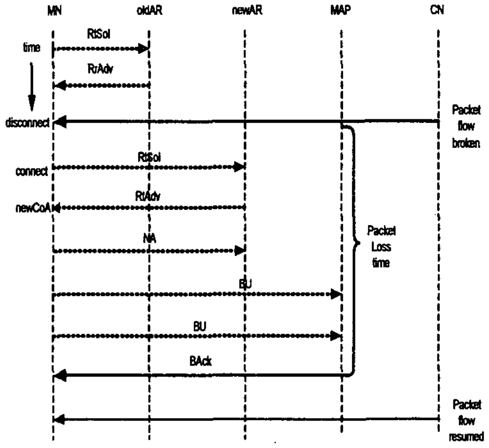

Figure 2. Hierarchical MIPv6 signaling diagram

The signaling diagram is very similar to that of the basic model. As long as the MN remains within the MAP domain, the BU only has to be registered with the MAP. This is because the HA has a tunnel to the MAP. The tunnel from the MAP to the CN is broken during the HO process just as the packet flow is broken in the basic model. The MAP, however, is fewer router-hops away from the MN than the HA, resulting in a shorter period of packet loss.

3) FMIPv6

The fast handover protocol[6] is one of the proposed new protocols for handover management in MIPv6. As mentioned previously in section 2.4, the handover latency resulting due to the standard Mobile IPv6 handover could be greater than the acceptable delay in real-time or delaysensitive traffic. The fast handover protocol attempts to reduce this delay, by suggesting some changes to the standard Mobile IPv6 protocol[7].

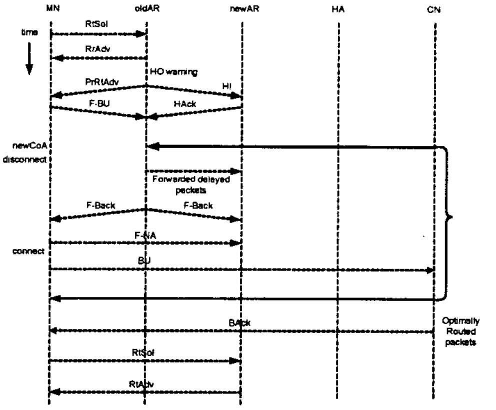

Figure 3. Fast-HO MIPv6 signaling diagram

A major difference between this model and the basic and hierarchical models is L2 assistance in performing an HO. The assumption here is that L2 assistance is provided in the network(older), not in the end-node(MN).

When an HO-warning occurs, the older calculates the newCoA, relieving the MN of this task. The newCoA is sent to both the MN and newAR(PrRtAdv and HI messages, respectfully). Their responses (F-BU and Hack) verify the validity of the newCoA. A forwarding tunnel can now be constructed from the older to the newAR. This prevents packet loss but packets from the CN are not optimally routed to the MN and must take a "side-trip" through the older. At a later time, the new link is established and the MN sends an NA to start the flow of packets from the newAR. These packets have experienced delay due to buffering in the older and NewAR and the sub-optimal route they have taken. Once the CN is informed of the newCoA in a BU, it can send optimally routed packets directly to the MN.

3. Proposed Handover Mechanism

1) Assumption

The following basic restrictions have been assumed in our MIPv6 scenario. In scenarios outside of these restrictions where the proposed mode is not able to assist in performing a handover, the handover mechanisms of the basic MIPv6 model can take over.

We assume that 1) L2 is able to signal L3 in advance that a handover event will occur. 2) L2 is able to supply information about the mapping of access-point identifiers to the IPv6 addresses of the ARs to which they are linked. 3) The single-link assumption is used in that the MN has, at most, one active L2 link to an access-point at any given time.

Under the above assumptions, when an MN moves across the boundary between two suppliers of MIPv6 services, the suppliers will have to provide each other with the mapping information (in assumption 2 above) where their neighboring access-points(e.g. base stations) are concerned.

2) The fundamental mechanism

Based on the proposal of the integration of CT and FMIPv6 in [5], our model to solve the identified issues in CT and integrate CT and FMIPv6 is shown in Figure 1. The main difference between the proposed model and the FMIPv6 model is the BU which sent from the oldAR to the CN immediately after the HO-warning from the data-link (L2). Although Packets are still tunneled from the oldAR to the newAR, they are fewer in number when compared to the MIPv6 model. The total time during which packets are delayed is shorter than when compared to the FMIPv6 model.

The goal of the proposed-model is to inform the CN of a newCoA immediately after HO. This is accomplished by allowing the AR to send out BUs on behalf of the MN. The BU list in the MN is copied to the AR. This copy must be managed by the AR-proxy in the same way that the original is managed in the MN. The copy is periodically sychronized with the original. As soon as an HO-event is detected and the newCoA has been generated by the AR, the copy of the BU list is used to inform all active CNs of the NewCoA.

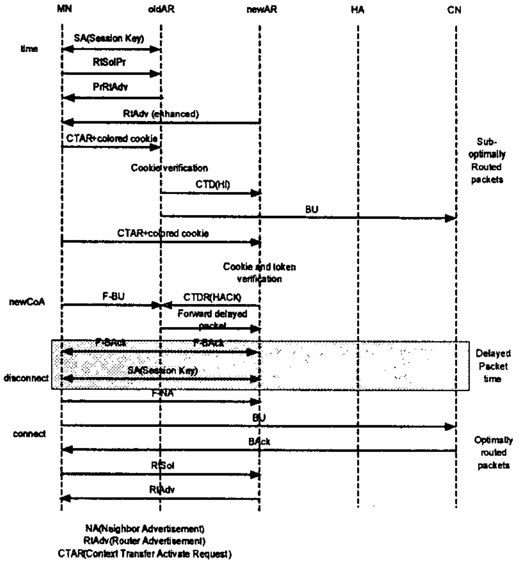

Figure 4. procedure scheme

Before MN initiates a handover procedure, it is assumed that MN has a SA with oldAR sharing a session key and MN is granted a colored cookie, which contains its authorization information.

To investigate on a efficient and secure handover procedure, the above procedure will give us the following advantages: (1)the intention of Ct is to reduce latency, packet losses and avoid re-initiation of signaling to and from mobile nodes,(2) FMIPv6 aims to reduce handover latency due to IP protocol operations as small as possible in comparison to the inevitable link switching latency.

An each processing step of proposed model is as follows:

Step 1: MN sends RtSolPr message or it receives an enhanced advertisement from NewAR. It makes a handover decision based on the information in the enhanced advertisement.

Step 2: MN sends a message to OldAR including CTAR and the colored cookie which is encrypted with the session key. OldAR verifies the colored cookie. If the verification passes, OldAR authenticates MN and authorizes the MN's QoS request successfully. Then it sends CTD to NewAR. This message can be regarded as HI as in FMIPv6. The CTD contains the parameters for NewAR to verify the colored cookie and the authorization token, including the session key etc.

Step 3: MN sends a message to NewAR also including CTAR and the colored cookie which is transmitted in plain text. NewAR verifies both the colored cookie and authorization token. If the verifications are successfuly, NewAR assures that MN claims its own context. Then NewAR sends a CTDR, which is regarded as HACK in FMIPv6, to OldAR. So far, NewAR and MN have set up a SA also by sharing the session key.

Step 4: Even though MN has to disconnect OldAR, OldAR forwards packets to NewAR to avoid a great degree of packet loss. Then NewAR initiates the BU and QoS establishment processes by means of e.g. CASP-QoS client or RSVP protocol.

Step 5: When the processes succeed, NewAR acknowledges MN to use the NewCoa and grants MN a new colored cookie. NewAR starts to deliver packets to MN.

4. Analysis

In this section, it will show that the proposed mechanism performance is superior than MIPv6 and FMIPv6 comparing those performance.

[Figure 5] is for analysis which is concentrated on handoff delay time, L3, which is happening during communicating when MN was handoff.

The L3 handover latency time in MIPv6 consist of MD, DAD, and BU latency time. But FMIPv6 or proposed protocol does not follow this.

Right after MN is handoff in FMIPv6 or proposed protocol, it sends FNA message to NAR for let oneself know. It can communicate with NCoA generated before handoff after NAR recognizes the existence of MN.

L3 handoff delay time in FMIPv6 or the proposed protocol defines the time as it is from after finishing L2 handoff delay time to receiving packet for the first time.

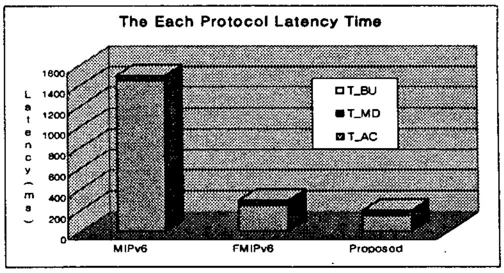

Figure 5. The Each Protocol Latency Time

As [Figure 3], FMIPv6 and the proposed protocol can reduce DAD delay time because they testify NCoA before doing handoff. Also, because it holds communication again as soon as it is handoff, L3 handoff delay time could be reduced. The delay time in the proposed protocol decreases 12% more than FMIPv6 because it supports security but not FMIPv6.

5. Conclusions

This paper suggests a proposal for reducing that the impact of handover induced packet delay on wireless real-time multimedia applications. Our model builds upon the fundamental concepts of the integration of CT and FMIPv6. It allows the routing algorithms in the router-subnet to quickly find the optimal route between the CN and MN. Packet-delay caused by the forwarding of packets from the old-AR to the newAR is minimized. Future work includes a more profound analysis of the execution of simulations with varying topologies, number of hosts, user moving patterns and active sessions regarding their QoS needs in order to evaluate the protocol's performance from both user and network perspectives.

References

[1] Stefano M. F, Franck L, Basavaraj P, Charles E. P., "Diameter Mobile IPv6 Application", *IETF Internet-Draft, draft-le-aaa-diameter-mobileipv6-03.txt.*

[2] Hesham S, Claude C., Karim E. M. and Ludovic B., "Hierarchical Mobile IPv6 mobility management(HMIPv6)", *Internet Draft, draft-ietf-mipshop-hmipv6-01.txt*, February 2004.

[3] Johnson. D, and Perkins, C. E., "Mobility Support in IPv6", *draft-ietf-mobileip-ipv6-18.txt, IETF, Work In Progress.*

[4] Perkins. C.E. (ed.), "IP Mobility Support", *RFC 2002*, IETF, October 1996.

[5] Thomas. M, "Analysis of Mobile IP and RSVP Interactions", October 2002.

[6] Koodli R., "Fast Handovers for Mobile IPv6", *Internet Draft, draft-ietf-mipshop-fast-mipv6-01.txt*, January 2004.

[7] Song, L., Kotz, D., Jain, R., He, X., "Evaluating location predictors with extensive Wi-Fi mobility data", *Proceedings of the 23rd Joint Conference of the IEEE Comp. and Comm. Societies (INFOCOM).* Volume 2. (2004) 1414-1424.