# OPTIMIZATION OF HANDOVER PERFORMANCE FOR FMIPV6

Li Jun Zhang[1], Samuel Pierre[1] and Laurent Marchand[2]

[1]Mobile Computing Networking Research Laboratory (LARIM), Department of Computer Engineering, École Polytechnique de Montréal, C.P. 6079, succ. Centre-Ville, Montreal, Que., Canada H3C 3A7; [2]Ericsson Research Canada, 8400, Decarie Blvd, Town of Mount Royal, Que., Canada H4P 2N2

**Abstract:** This paper presents a new protocol, namely Access Routers Tunneling Protocol (ARTP), dedicated to pre-configuring bidirectional secure tunnels among adjacent access routers before handoff. This protocol allows two tunnel endpoints to negotiate quality of service-related parameters, traffic classification aspects, security policies, such as authentication and encryption methods, buffering mechanism, etc. Once the parameters of pre-established tunnels are determined, real-time traffic could be redirected in a cost-efficient way to mobile users using GRE (Generic Routing Encapsulation) tunneling technique. This protocol allows us to optimize handover performance for FMIPv6. An existing analytical model is used to evaluate the performance of the proposed handover procedure. Numerical results show that our new approach has better performance than FMIPv6 in terms of signaling cost, and the buffer size required during handoff.

**Key words:** fast handover; bidirectional secure tunnels; handover latency; performance analysis.

## 1. INTRODUCTION

User mobility and real-time data traffic (e.g. Voice over IP) are two expanding areas within communication systems. On one hand, in order to guarantee user mobility, handover has to be taken into account in mobile networks, where subscribers move around. On the other hand, transporting real-time traffic to the IP-enabled mobile user imposes strict requirements on latency and packet loss. As mobile users roam in the network, they frequently change their point of attachment to the network. Therefore it is

necessary to keep the continuity of communication in progress, and the access network should provide features of minimizing the interruption to ongoing sessions. However, controlling the handover mechanism is quite complicated in mobile networks.

Based on these contexts, we propose a new protocol with the purpose of minimizing handover latency, packet losses and jitter for real-time service. This protocol describes mechanism of pre-configuration of bidirectional secure tunnels among adjacent access routers. With the pre-established tunnels, a mobile node can resume its previous ongoing session immediately after performing L2 handoff at the visited network; moreover, it can initiate a real-time session using its previous care-of-address upon arrival on the new link. By this means, access routers are equipped with the flexibility of offering service with guaranteed quality to their neighbors' subscribers.

The rest of this paper is organized as follows. Section 2 describes the principles of the handover procedures found in recent literature. Section 3 proposes the Access Routers Tunneling Protocol, and the proposed handover procedure for improving handover performance of FMIPv6. Section 4 presents an analytical model to evaluate the performance of our new approach; numerical results are also illustrated and compared with FMIPv6.

## 2. BACKGROUND AND RELATED WORK

Recently, fast and seamless handover procedures for IP-based communication networks have become hot topics in the field of mobility management. Since in the future mobile communication networks, a user is able to conveniently roam between various operators and between fixed and mobile as well as public and private networks independently of the different access technologies used, improving handover performance is quite significant. Furthermore, it is essential to support real-time applications which deal with tight time constraints for offering adequate quality of service and to deploy all-IP networks which are cost efficient comparing with the current network infrastructure in the next generation wireless networks. However, synchronous real-time applications such as Voice over IP and Video Conference over IP place new demands on the quality of IP services: packet loss, delay variation or jitter need careful simultaneous control; these requirements impose strong challenges in mobile environments.

## 2.1 Fast Handover for Mobile IPv6

IETF proposed the approach called Fast Handover for Mobile IPv6 (FMIPv6) with the intention of minimizing the handover latency in MIPv6. FMIPv6 allows a mobile user to pre-configure a new on-link care-of-address before breaking its connection with the previous access router (PAR) [1].

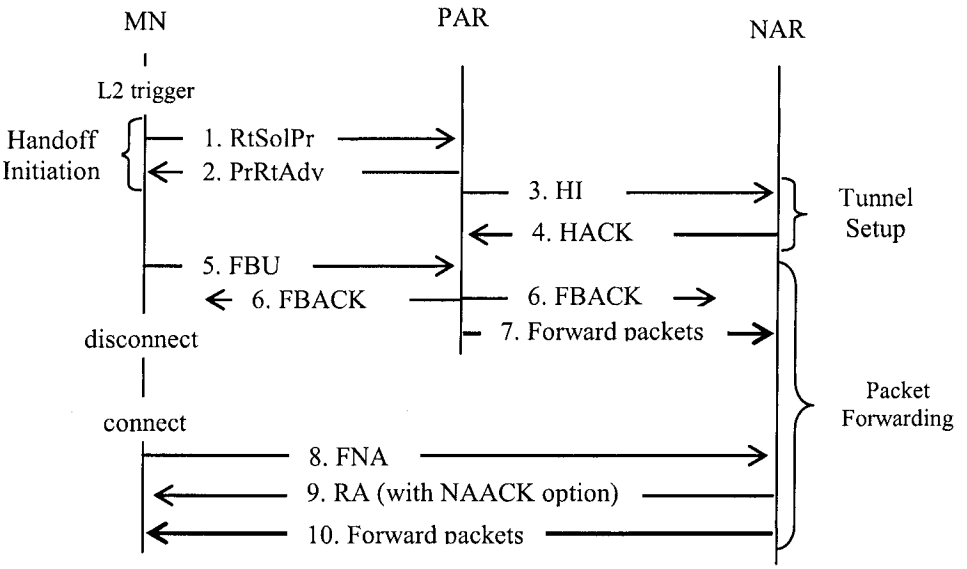


Figure 1. Fast handover with anticipation in FMIPv6

Fast handover is triggered when a mobile node (MN) receives L2 trigger before it moves to the new network. This mobile then sends a *Router Solicitation for Proxy Advertisement* (RtSolPr) message to the PAR asking for resolving the Access Point Identifiers to subnet-specific information. The PAR replies with a *Proxy Router Advertisement* (PrRtAdv) message to the MN. Based on this message, the mobile node generates a new on-link care-of-address, and then sends a *Fast Binding Update* (FBU) to the PAR, including its prospective care-of-address on the new link. During the movement of MN, the PAR sends a *Handover Initiate* (HI) message to the new access router (NAR) to initiate the tunnel setup process. After verifying the uniqueness of the MN's new care-of-address, NAR sends back a *Handover Acknowledgment* (HACK) message to PAR as a reply to the HI message, thus a temporary bidirectional tunnels are established between the two access routers. Consequently, the PAR sends *Fast Binding Acknowledge* (FBACK) to the MN. Once the PAR intercepts packets destined to the mobile node, it tunnels the packets to the NAR. Upon arrival at the new

subnet, the MN sends a *Fast Neighbor Advertisement* (FNA) to the NAR to announce its attachment and also to confirm the validity of new on-link care-of-address in case where MN has not received the FBACK on the previous link. Upon receipt of the FNA, the NAR delivers the packets to the MN. Figure 1 shows the fast handover procedure with anticipation in FMIPv6.

## 2.2 Buffer Management Scheme for Fast Handover

When a mobile user roams from one network to another, there is always an inevitable link down time during handoff which leads to packet loss. This would have bad effect on the quality of communication. To avoid packet drops, a feasible solution is to buffer those in flight packets sent by correspondent nodes. However, the original fast handover protocol, namely FMIPv6, does not support buffering mechanism during a pure link layer handoff [2]. This means that an access router is unable to buffer packets for a mobile user when it is moving between different access points (base stations) within the same subnet, thus the temporary disconnection is unavoidable and results in packet loss. Under this circumstance, an enhanced buffer management scheme is proposed to improve buffer utilization on access routers as well as to support QoS services during handover process [2].

The principal ideas are: buffering implemented both in PAR and in NAR, and three types of services, namely real-time traffic, high priority and best effort traffic, are defined so that packets can be treated differently based on their traffic characteristics. Handover procedure is triggered by specific link layer events or policy [2]. Upon receipt of this trigger, the mobile node sends a request of B*uffer Iinitiation* (BI) message piggybacked in the *Router Solicitation for Proxy Advertisement* (RtSolPr) to the PAR for requesting the buffer space. While the establishment of a bidirectional tunnel between PAR and NAR, the allocation of buffer space for the MN is also negotiated via the *Buffer Request* (BR) and *Buffer Acknowledge* (BA) messages. Subsequently, the PAR sends a *Proxy Router Advertisement* (PrRtAdv) message to the MN indicating the success of allocation of buffer space, and informing it of the new subnet prefix. With this message, MN generates a new on-link care-of-address (NLCoA) and includes this address in a *Fast Binding Update* (FBU) sent to PAR. Upon receipt of the FBU, the PAR starts buffering packets and/or forwards them to NAR. While connecting to NAR, the mobile node sends a *Buffer Forward* (BF) message to both the PAR (via the NAR) and the NAR. Thereafter, the two access routers forward packets in their buffers to the MN. Figure 2 shows the handover procedure with buffer scheme.

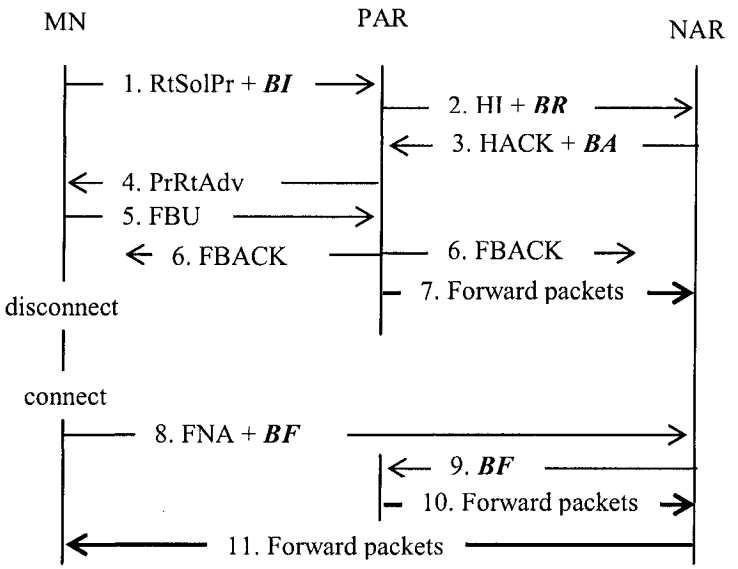


Figure 2. Handover procedure with buffering scheme

Recent work has been directed at improving handover performance to support real-time traffic. However, in order to provide successful real-time services, it is necessary to minimize the traffic redirection in mobile environments. Whether a mobile user has the right to obtain specific routing treatment depends on whether it negotiated a successful Authentication, Authorization and Accounting (AAA) exchange with a network access server at some point of the past [3, 4]. Furthermore, the mobile node for which the context transfer protocol operations are undertaken is always identified by its previous care-of-address [4]. Therefore, we propose a new protocol dedicated to pre-establishing bidirectional secure tunnel before actual handoff so that mobile nodes could use their previous care-of-address in a visited network. By this means, packet losses and handover latency could be reduced. Furthermore, since the pre-configured tunnels support quality-of-service (QoS) by traffic classification mechanism, local resource reservation as well as admission control, the disruption for real-time ongoing session can be minimized significantly.

## 3. ACCESS ROUTERS TUNNELING PROTOCOL

The Access Routers Tunneling Protocol (ARTP) is a new signaling protocol to setup tunnel parameters between two access routers. ICMP-type messages are defined and used to carry information of QoS-related

parameters, authentication method, encryption method, service class, etc. so as to facilitate the negotiation between two tunnel endpoints. Concerning the security aspects, two mechanisms are deployed to secure the traffic: session key generated by access router and tunnel token formulated by mobile node.

## 3.1 Tunnels Setup Algorithm

The algorithm for setup the tunnels is described as follows:

```
1)  request = 0;    request_MAX = 4;            neighbor_indice=0;
2)  Tunnel brokers at access routers create their neighbor tables.
3)  AR_1 selects one entry from its Neighbor Table.
4)  /*verify the reachability of the neighbor*/
    if(the selected neighbor: AR_2 is reachable) {
5)      request=request+1;
6)      if(request < request_MAX) {
7)          AR_1 sends a tunnel Request message to AR_2;
            AR_2 verifies its capability;
            AR_2 proposes parameters with Tunnel Reply message;
            AR_2 sends this Tunnel Reply to AR_1;
8)          if(AR_1 accepts the condition) {
                AR_1 sends a Tunnel_ACK to AR_2;
9)              if(tunnels is symmetric) /*symmetric tunnel*/ {
                    with the negotiation results,
                    AR_1&AR_2 add an entry in Forward Tunnel table;
                    AR_1&AR_2 add en entry in Reverse Tunnel table;
                    go to END; }
10)             else /* in case of asymmetric tunnel*/ {
                     AR_1 adds an entry in its Forward Tunnel table;
                     AR_2 adds an entry in its Reverse Tunnel table;
                     /* reverse tunnel setup procedure*/
                     AR_1 sends AR_2 a Reverse Tunnel Request message;
                     AR_2 sends a Tunnel Request to AR_1;
                     AR1 responses with a Tunnel Reply;
11)                  if(AR_2 accepts the proposed parameters of AR_1) {
                       negotiation = true;
                       AR_2 adds an entry to its Forward Tunnel table;
                       AR_1 adds an entry to its Reverse Tunnel table;
                       go to END; }
                     else { negotiation = false; go to END; }
                  }/* end of reverse tunnel*/
              }
              else /* another negotiation*/ { go to step 5; }
          }
          else /*request > request_MAX*/ { go to END; }
      }
      else /* in case neighbor is unreachable*/ {
          go to step 3 ;
          neighbor_indice ++ ;  /* select another neighbor*/ }
  END;
```

## 3.2 The Proposed Handoff Scheme

The proposed handover algorithm allows a mobile node to resume its real-time ongoing session with its correspondent as soon as it attaches to the new link. With the preconfigured bidirectional tunnels, traffic will be redirected to the new network using the MN's previous care-of-address. By this means, the service disruption for an on-going real-time session could be minimized. Figure 3 shows the overall handover procedure.

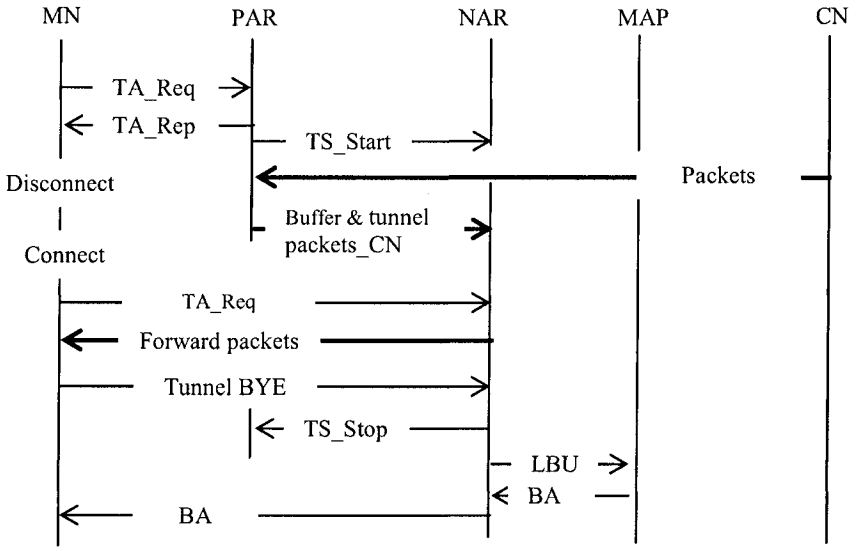


Figure 3. Proposed handover procedure

Before actual handover, adjacent access routers have established business relationships so that bidirectional secure tunnels have already been created. Handover is triggered by specific link layer event. A mobile user roams with a real-time session in course. Before the MN breaks the connection with the PAR, it sends a Tunnel Activate Request (TA_Req) message to the PAR. Upon receipt of this message, the PAR performs local resource reservation for the mobile and sends a Tunnel Activate Reply (TA_Rep) to the MN; meanwhile, it sends a Tunnel Session Start indication to the new access router (NAR) with the bearer context of the mobile. When the correspondent node (CN) sends packets to the MN, the PAR intercepts the packets, buffers them and tunnels to the NAR. Upon receipt of the TS_Start indication, the NAR performs admission control and also reserve the required bandwidth for the imminent MN. As the mobile arrives on the new link, after the L2 handover, it may initiate a new real-time session or just send a TA_Req to the NAR using its previous care-of-address. The NAR

then forwards packets to the MN. Once the session in course is complete, the MN sends a Tunnel BYE message to the NAR to deactivate the tunnel. The NAR releases the reserved resource and sends a Tunnel Session Stop message to the PAR requesting the PAR to deactivate the session; meanwhile, the NAR assigns a new care-of-address to the MN and sends a local binding update (LBU) to the MAP on behalf of the MN. Accordingly, the MAP modifies its binding cache, and reply with a *Binding Acknowledgement* (BA) to the NAR which then forwards the BA to the MN.

## 4. PERFORMANCE ANALYSIS

We use an existing analytical model and the reference values found in the literature [5] to evaluate the performance of our new approach. Table 1 and Table 2 illustrate the parameters used to get numerical results. With the same principle as the analytical model [5], we obtain Figure 4 and Figure 5.

**Table 1.** System parameters for signaling cost

| $\alpha$ | $\beta$ | $\gamma$ | $C_{transmit\_MP}$ | $C_{transmit\_PN}$ | $C_{process\_PAR}$ | $C_{process\_NAR}$ | $C_{signal\_MIPv6}$ |
|---|---|---|---|---|---|---|---|
| 0.2 | 0.8 | 1.0 | 10 | 2 | 5 | 5 | 100 |

**Table 2.** System parameters for packet delivery cost

| $\delta$ | $\varepsilon$ | $\lambda$ | $t_L + t_I$ | $t_R$ | $t_{PAR\_NAR}$ | $t_{BU}$ | $t_{New}$ | $t_{CN\_PAR}$ | $t_{MN\_NAR}$ |
|---|---|---|---|---|---|---|---|---|---|
| 0.2 | 0.8 | 1.0 | 165 | 10 | 5 | 160 | 160 | 150 | 10 |

Figure 4 shows the signaling cost comparison as L2 trigger time changes in case where the decreasing factor equals to 0.5. As shown in Figure 4, the ARTP-based handover scheme has better performance than FMIPv6 in terms of signaling cost because bidirectional secure tunnels are established before actual handoff. The average signaling cost of ARTP-based handover is 118.9, compared to 129.1 for FMIPv6, the gain is 7.90%; compared to 129.4 for buffer-based Handover, the average gain is 8.11%. As L2 trigger time elapses, the signaling cost of FMIPv6 and buffer-based HO converges to certain value. However, FMIPv6, buffer-based HO and ARTP-based HO have more important signaling cost than MIPv6 because ARTP-based HO aims to improve the performance of FMIPv6 without intention to minimize the signaling overhead of MIPv6.

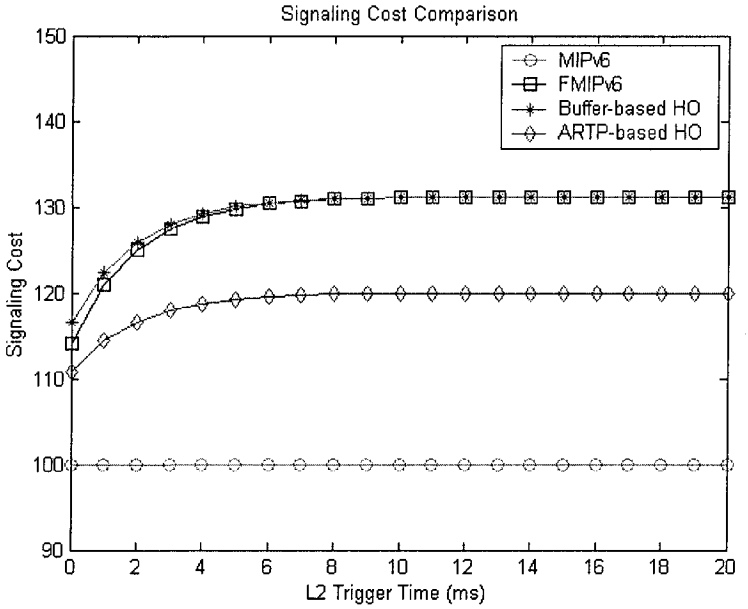


Figure 4. Signaling cost comparison as L2 trigger time changes

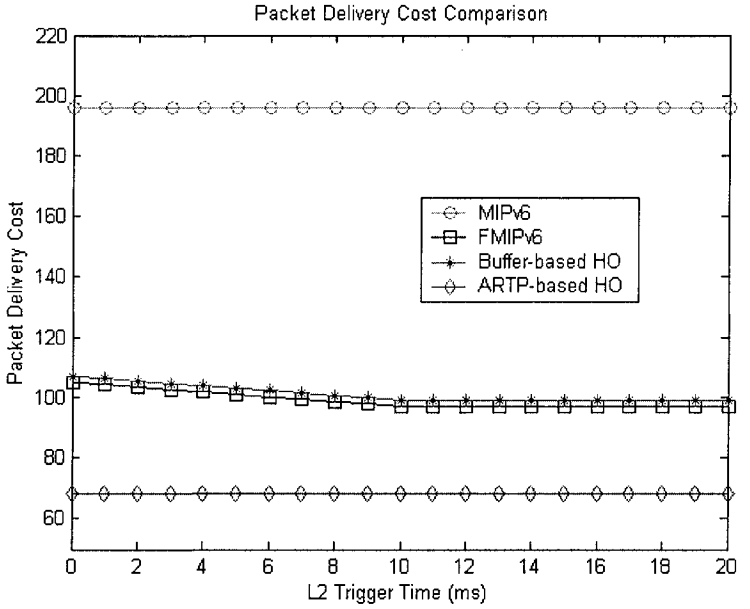


Figure 5. Packet delivery cost comparison as L2 trigger time changes

From Figure 5, we find that ARTP-based handover has better performance than FMIPv6 in terms of number of buffered packets during

handoff. The average packet delivery cost of ARTP-based handover is 68.0, compared to 99.1 for FMIPv6, the gain is 31.38%; compared to 101.1 for buffer-based Handover, the average gain is 32.74%; compared to 196.0 for MIPv6, the average gain is 65.31%. As shown in Figure 5, L2 trigger time has less influence on packet delivery cost. Since the cost is defined as the number of packets buffered during handoff, it is proportional to the packet arrival rate and the handover latency. In our example, the handover latency in MIPv6 is more important than FMIPv6, more buffer space is required in MIPv6. In addition, we can find that the handover latency in the ARTP-based HO scheme is much shorter than in FMIPv6.

## 5. CONCLUSION

In this paper, we proposed a new protocol for pre-establishing bidirectional secure tunnels among adjacent access routers. Using the preconfigured tunnels, handover latency and the required buffer during handoff can be reduced significantly. Numerical results show that the ARTP-based handover scheme has better performance than pure FMIPv6 and the buffering-based handover scheme in terms of signaling cost and the number of buffered packets during handover. In addition, service disruption for real-time ongoing session could also be minimized. This protocol also allows access routers to provide certain quality of service to their neighbors' clients as the QoS-related parameters are negotiated on the basis of service class prior to handoff process. Further performance comparison will be done with realistic workloads through implementation and simulation.

## REFERENCES

1. R. Koodli, "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fast-mipv6-03.txt, October 2004.
2. W.M. Yao, Y.C. Chen, "An enhanced buffer management scheme for fast handover protocol", the 24th International Conference on Distributed Computing Systems Workshops Proceedings, Mar. 2004, pp. 896 – 902.
3. J. Kempf, "Problem Description: Reasons for Performing Context Transfers Between Nodes in an IP Access Network", RFC-3374, September 2002.
4. J. Loughney, M. Nakhjiri, C. Perkins, "Context Transfer Protocol", draft-ietf-seamoby-ctp-11.txt, August 2004.
5. S. Pack, Y. Choi, "Performance Analysis of Fast Handover in Mobile IPv6 Networks", IFIP PWC 2003, Venice, Italy, September 2003.