Adaptive Context Transfer Scheme for Fast Handoff in Proxy Mobile IPv6

JaeJong Baek, JooSeok Song
Department of Computer Science
Yonsei University
Shinchon 134, Seodaemungu, Seoul, 120-749, Korea
{jjb27,jssong}@emerald.yonsei.ac.kr

Abstract

In IETF NetLMM WG (Network-Based Localized Mobility Management), Proxy Mobile IPv6 has attracted a lot of attention to support IP mobility for mobile nodes without host involvement. For supporting delay sensitive services like VoIP, various faster handoff schemes have been proposed recently. In this paper, we propose adaptive context transfer schemes for a fast handoff in Proxy Mobile IPv6 which reduces the delay in AAA authentication and specified context transfer scenarios taking into account proactive and reactive handoff. A context transfer protocol will reduce the latency and packet losses by avoiding the reinitiation of signaling to and from the mobile node.

1. Introduction

In recent years, a great deal of research effort has been spent on the issue of the network-based localized mobility. 3GPP, 3GPP2 and WiMAX operators are now showing their strong interests for network-based IP mobility solution. They are even now deploying their non-standardized network-based IP mobility solution. Network-based mobility means no change in Mobile Nodes (MN) protocol stack required. IETF NetLMM WG started to standardize a network-based mobility management protocol and selected Proxy MIPv6 (PMIPv6) as a solution. However, in case of delay sensitive services such as VoIP, PMIPv6 also may have some latency when it attempts to establish and process location update messages. It is considered as beneficial to support transfer of an MN's context between the MN's previous and new access routers in case the MN changes its point of attachment and this change implies a change in the MN's access router. The purpose of this paper is to specify how the context transfer protocol (CXTP) can be achieved in a PMIPv6 enabled network. [1] is referred to as basic and generic protocol operation between access routers to perform context transfer. The associated functional components for context transfer are embedded into the PMIPv6 architecture and protocol operation to support context transfer efficiently by means of reusing Proxy MIPv6 protocol elements and event indications without the requirements to rely on explicit indication from MNs. This paper is organized as follows: in the next section, we investigate the related work, the CXTP and PMIPv6. Then we show basic message flows with the CXTP and present adaptive protocol schemes between the intra and inter domain. Finally, we highlight main conclusions and comment on the future work.

2. Related work

2.1. Context Transfer Protocol

Context Transfer protocols are useful in IP networks. The primary motivation is to quickly re-establish context transfer-candidate services without requiring the mobile host to explicitly perform all protocol flows for those services. Another motivation is to provide an interoperable solution that supports various Layer 2 radio access technologies [1].

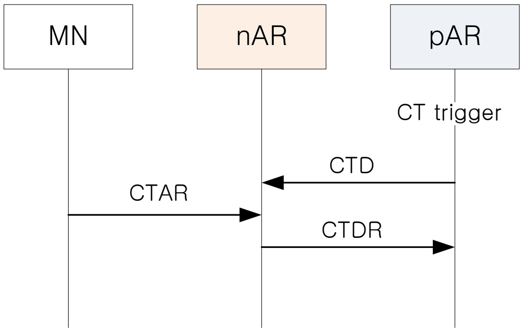

Figure 1. Predictive CTD

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. R01-2006-000-10614-0)

978-0-7695-3333-9 /08 $25.00 © 2008 IEEE
DOI 10.1109/NGMAST.2008.76

Figure 1 shows the network controlled, initiated by previous Access Router (pAR), predictive signaling flows. In response to the context transfer (CT) trigger (eg. link layer trigger), pAR predictively sends a Context Transfer Data (CTD) message. It contains feature contexts such as the MN's previous IP address and parameters for nAR to compute an authorization token to verify the MN's token in the CT Activate Request (CTAR) message [1]. The MN sends the CTAR to its new access router (nAR) immediately prior to handoff. Performing a context transfer in advance of the MN attaching to nAR can increase handoff performance. However, it may have an overhead to predict nAR.

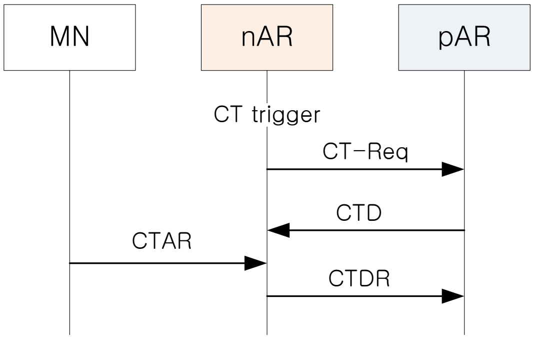

Figure 2. Reactive CTD

As shown in Figure 2, pAR receives a Context Transfer Request (CT-Req) message from nAR. The nAR itself generates the CT-Req message after receiving a context transfer trigger (eg. IP layer indication [2]). In the CT-Req message, nAR supplies the MN's previous IP address, the FPT (Feature Profile Types)s for the feature contexts to be transferred, the sequence number from the CTAR, and the authorization token from the CTAR. In response to a CT-Req message, pAR sends a Context Transfer Data (CTD) message that includes the MN's previous IP address and feature contexts. When it receives a corresponding CTD message, nAR may generate a CTD Reply (CTDR) message to report the status of processing the received contexts. The nAR installs the contexts once it has received them from the pAR [1].

2.2. PMIPv6

Figure 3 shows the signaling call flow when the MN enters the PMIPv6 domain. Once a MN attaches to an access link MAG obtains MN's ID and profile information by the MN_ATTACH API. MN's profile information which contains MN-ID, LMA Address, IP address configuration mode and home network address of MN can get from such like a policy server. (eg. AAA) This policy contents could be included in the context data. For updating the local mobility anchor (LMA) about the current location of the MN, the mobile access gateway (MAG) sends a Proxy Binding Update (PBU) message to the MN's LMA. Upon accepting this PBU message, the LMA sends a Proxy Binding Acknowledgement (PBA) message including the MN's home network prefix (HNP). It also creates the Binding Cache Entry (BCE) and sets up its endpoint of the bi-directional tunnel to the MAG [3].

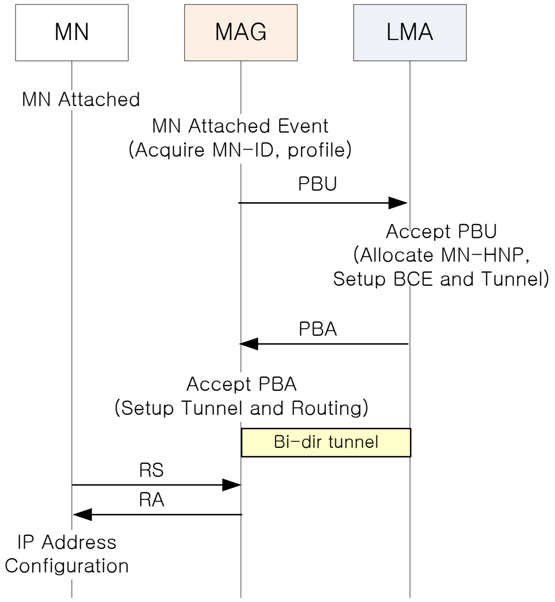

Figure 3. MN Attachment - Signaling Flow

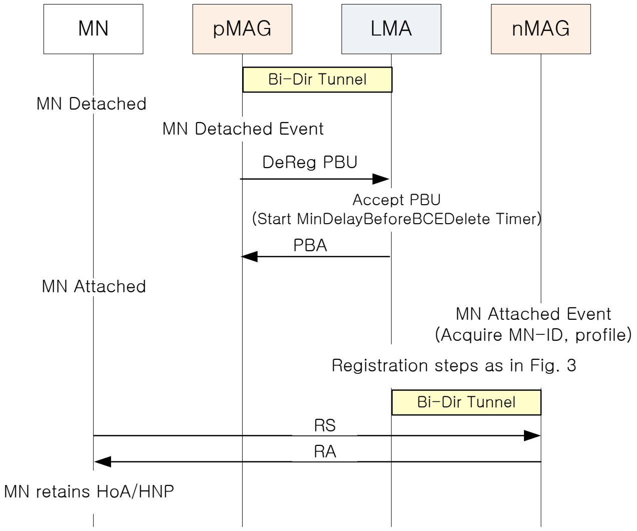

Figure 4. MN Handoff - Signaling Flow

Figure 4 shows the signaling call flow for the MN's handoff from previously attached MAG (pMAG) to the newly attached MAG (nMAG). If the MN changes its point of attachment, the pMAG will detect the MN's detachment by the MN_DETACH API will signal (PBU message) the LMA with deregistration. The LMA upon receiving this request will remove the binding and routing state for that MN. Router Advertisement (RA) should be unicasted to an MN by nMAG. It will contain MN's Home Network Prefix (MN-HNP). Hence the MN will obtain the same home address which used in pMAG [3].

3. Proposed Schemes

We propose a general signaling scheme through proactive/reactive handoff-based AAA authentication server by use of EAP-TLS. The AAA context can be established by a number of different protocols, for example RADIUS protocol[4]. The AAA context includes authentication information (e.g. MN-ID, shared secret key), authorization information (e.g. a list of authorized services), and accounting information. (e.g. usage record of resources and services) When MNs attempt to handoff inter/intra domain, the AAA context information stored in LMAs and MAGs will be used to support the handoff without visiting the AAA server. Therefore, handoff latency will be reduced drastically [5]. On this authentication infrastructure, we specified two scenario as proactive and reactive cases.

3.1. Proactive Handoff scheme

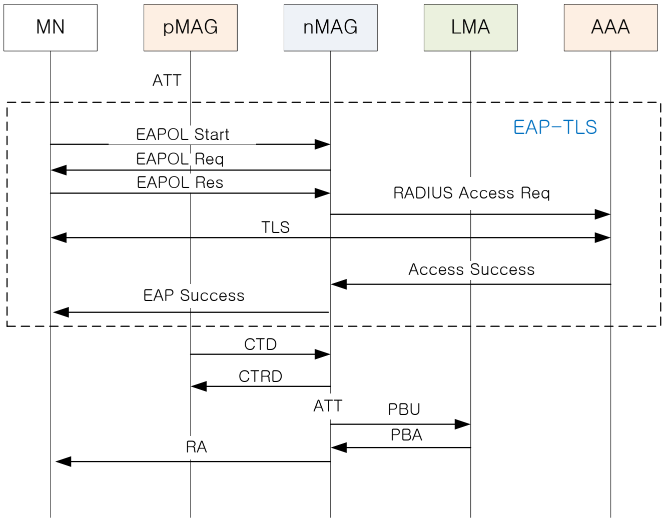

Figure 5. Proactive Handoff Signaling Flow

Figure 5 shows proactive handoff signaling call flow, where the pMAG can push an MN's context data to its nMAG even before the MN attaches (ATT) to the pMAG. The pMAG receives information about the nMAG through a local indication. (eg. predictive handoff trigger) MAGs that may exchange contexts have preconfigured security associations. When a local indication occurs at nMAG, nMAG retrieves information about the MN's pMAG through CT-Req (CT-Request) message.

3.2. Reactive Handoff scheme

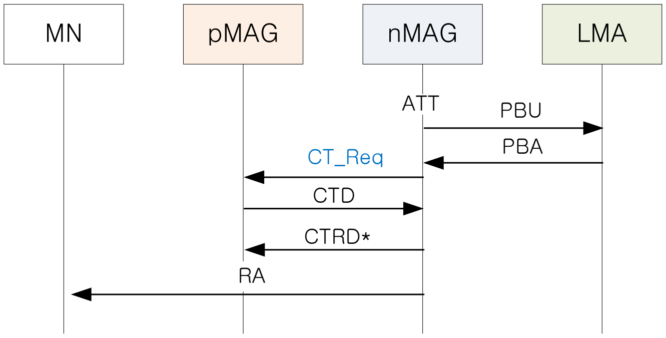

Figure 6. Reactive Handoff Signaling Flow

Figure 6 shows reactive handoff signaling call flow, where the nMAG can initiate CT only after the required information about the pMAG has been retrieved from the MN's LMA. When the MN attaches to the nMAG and the LMA is aware of the MN's pMAG, the LMA can inform the nMAG about the pMAG's IP address. This information can be conveyed in a Mobility Option of the PBA (Proxy Binding Acknowledge) message. Additionally, the nMAG retrieves information about the MN's pMAG through CT-Req (CT-Request) message.

3.3. Inter Domain mobility support Handoff scheme

Figure 7 shows inter domain mobility support handoff signaling call flow. As the MN attaches to domain A to B, it requests the user authentication to nMAG. The nMAG also requests the RADIUS Access to the AAA server. However, If the AAA context is applied to this mechanism, it can skip the RADIUS Access request message. The authentication service will be provided by the context transfer protocol. Instead of skipping the RADIUS Access Request message, the nMAG will send CTAR (CT Activation Request) message which contains MN's authentication token to the nLMA. After the context transfer, nLMA sends user's AAA success message to the nMAG. After registering the MN, the nMAG sends Router Advertisements (RA) contained MN's home network prefix. Consequently, the context transfer protocol with an AAA context reduces the overall handoff latency dramatically. Figure 7 is reactive CT handoff case.

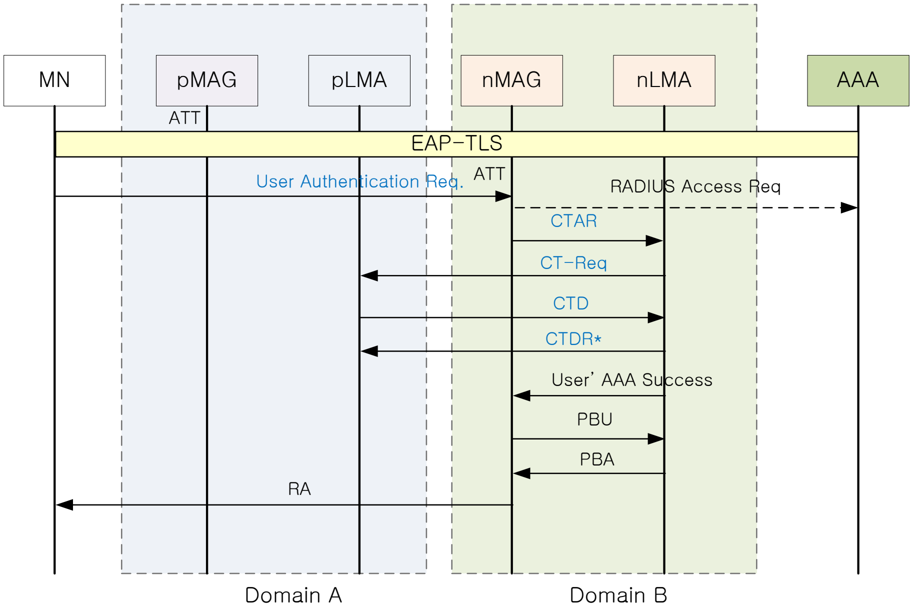

Figure 7. Inter Domain mobility support Handoff scheme

4. Conclusion and Future Work

In this paper, we specified some scenarios for the network-based localized mobility management as proactive and reactive schemes. In addition, adaptive context transfer schemes are proposed for a fast handoff in Proxy Mobile IPv6. As a result, the Context transfer protocol reduces the inter and intra handoff latency by avoiding the re-initiation of signaling to and from the MN. In the future, we will focus on the detail message structure like how it will be implemented without modifications on the current PMIPv6 architecture and present performance results to assess the effectiveness of this scheme.

References

[1] J. Lougney, M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol (CXTP)," RFC 4067, IETF, July 2005, Tech. Rep.

[2] P. De Silva and H. Sirisena, "A mobility management protocol for IP-based cellular networks," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 9, no. 3, 2002.

[3] S. Gundavelli and K. Leung, "Localized mobility management using proxy mobile IPv6: draft-gundavelli-netlmmmip6-proxy-11. txt," *IETF draft, February*, 2008.

[4] J. Kempf *et al.*, "Goals for Network-based Localized Mobility Management (NETLMM)," *RFC 4831, April*, 2007.

[5] H. Duong and S. Dadej, A.and Gordon, "A General Framework for Context Transfer in Mobile IP Networks," *Vehicular Technology Conference, VTC 2006-Spring. IEEE 63rd*, vol. 2, pp. 1017–102 176–88, 2006.

[6] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *RFC 3775, June*, 2004.

[7] C. Politis, K. Chew, N. Akhtar, M. Georgiades, R. Tafazolli, and T. Dagiuklas, "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 11, no. 4, pp. 76–88, 2004.

[8] M. Georgiades, N. Akhtar, C. Politis, and R. Tafazolli, "Enhancing mobility management protocols to minimise AAA impact on handoff performance," *Computer Communications*, vol. 30, no. 3, pp. 608–618, 2007.