[5A-16]

MIPv6 네트워크 접속을 위한 인증 제공 방안

이준원, 민상원
광운대학교, 전자통신공학과, 통신프로토콜 연구실
junwonlee@empal.com min@kw.ac.kr

A Novel Authentication Procedure in MIPv6 Networks

Junwon Lee, Sangwon Min
Kwangwoon University, Department of Electronics and Communications, CPE Lab.

요 약

현재 데이터 서비스를 위하여 다양한 유무선 기술이 혼재 되어 있으며 이러한 서로 다른 네트워크간의 로밍과 네트워크 접속시 보안에 대한 문제점이 이슈가 되고 있다. MIPv6 (Mobile IP) 기술은 IP 망에서의 이동성을 제공하며 핵심망이 All-IP 망으로 발전했을 때 서로 다른 네트워크간의 이동성을 제공해 줄 수 있다. 하지만 MIP는 서로 다른 도메인간의 로밍에서 네트워크 접속을 위한 MN (Mobile Node)의 인증과 서비스에 대한 권한을 부여 받기 위해 추가적인 메커니즘이 필요하다. 이것은 기존의 AAA (Authentication, Authorization, Accounting) 인프라를 이용하여 해결될 수 있으며 MIPv4 와 AAA가 결합된 구조가 이미 제안되어 있다. 본 논문에서는 기존의 MIPv4-AAA 연동 구조 기반으로 MIPv6-AAA 연동 구조를 설계하였으며 inter-domain 간의 핸드오프시 seamless한 핸드오프를 위한 인증 메커니즘에 대해 연구하였다.

I. 서론

기존의 음성 위주의 네트워크는 현재 데이터 및 다양한 멀티미디어 서비스를 위한 데이터 중심의 네트워크로 빠르게 발전하고 있으며, 현재 이러한 멀티미디어 서비스를 위한 다양한 네트워크들이 혼재 되어 발전해 나가고 있다. 최근 이러한 서로 다른 네트워크간의 연동에 대한 연구가 활발히 이루어지고 있으며 그림 1 에서와 같이 IP망에서 이동성을 제공하는 MIP가 서로 다른 이종 네트워크간의 연동을 위한 기술로써 대두되고 있다. MIP는 MN의 이동시 seamless하고 투명한 이동성을 제공하지만 서로 다른 도메인간의 로밍시 사용자의 인증과 서비스 권한 부여를 위해 추가적인 메커니즘이 요구된다. AAA 프로토콜은 MIP의 이러한 문제점을 해결해 줄 수 있으며 MIPv4 와 AAA간의 연동에 대한 구조와 메커니즘이 연구되고 있다[1][2].

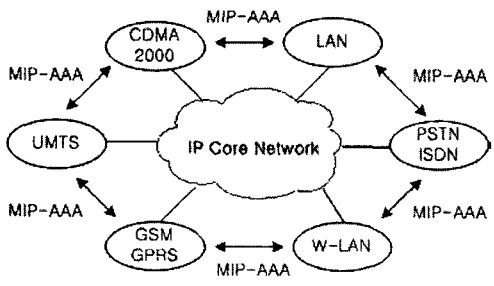

그림 1. 이종 망간의 이동성

IETF (Internet Engineering Task Force)에서는 WG (Working Group)을 통해 MIPv6 와 AAA 연동을 위한 구조를 연구하고 있으며 현재 MIPv6-AAA 연동 구조에 대한 요구 사항을 draft 문서를 통해 제시하였다. 본 논문에서는 기존의 MIPv4-AAA 구조에 대한 연구와 IETF 의 요구 사항을 통해 MIPv6-AAA 연동 구조를 설계하고 inter-domain간의 핸드오프시 seamless한 핸드오프 제공을 위한 인증 메커니즘에 대해 연구하였다. 관련 연구에서 기존의 MIPv4-AAA 연동 구조와 MIPv6-AAA 연동 구조에 대한 요구사항을 살펴보고 이를 바탕으로 한 MIPv6-AAA 연동 구조에 살펴본 후 제안된 인증 메커니즘에 대해 설명한다.

II. 관련 연구

2.1 MIPv4-AAA 연동 구조

그림 2 에서 보는 바와 같이 MIPv4-AAA 연동 구조는 기존의 AAA 인프라를 사용하며 MIPv4 의 구성 요소들이 결합되어 있는 구조로 되어 있다. MIPv4 의 FA (Foreign Agent)와 HA (Home Agent)는 AAA 서버와 인증 메커니즘을 수행하는 AAA 클라이언트의 역할 수행하게 된다. AAAF 서버는 MN의 인증 정보를 홈 도메인의 AAAH 서버로 전달하는 역할을 하며 MN이 AAAH에 의해 인증을 받게 되면 이에 대한 인증 정보를 저장하고 서비스를 제공한다. AAAH는 MN에 대한 인증을 수행하고 MN의 BU (Binding Update)에 대한 정보를 HA로 전달하며, 각 구성요소들간의 SA (Security Association)을 위한 키를 생성하고 분배하는 기능을 수행한다. AAA 인프라에 대한 SA는 long-term 키를 통해 이루어지며, HA, FA, MN 의 SA는 MN이 이동할 때 마다 동적으로 구성된다[1].