

안전한 멀티캐스트 통신을 위한 그룹 관리 프로토콜

*서중운, *안태선, *강현국
*고려대학교 전자정보공학과
*{terryortony, cokein, kahng}@korea.ac.kr

Group Management Protocol for Secure Group Multicast Communication

*Jong Wun Seo, *Tae Sun An, *Hyun-Kook Kahng,
*Korea University

요약

다자간 그룹 통신에 참여하는 참여자는 멀티미디어 기술의 발달에 힘 입어 계속하여 증가하고 있다. 이에 따라, 증가하는 다자간 그룹 통신과 그 통신에 참여하는 참여자들의 정보를 관리해 주는 멤버십 관리 구조가 필요하며, 정보의 안전한 보호를 위해 그룹 보안 관리 구조가 필요하다. 본 논문은 이러한 다자간 그룹통신에서 그룹의 세션을 관리하는 세션관리(Session Management)와 참여자들의 정보와 현재 상태 등을 관리하는 멤버십 관리(Membership Management) 기능을 가진 GMP(Group Management Protocol)에 키 관리(Key Management) 기능을 추가하여 안전한 그룹 관리 통신을 위한 S-GMP(Secure GMP)를 제안하였다.

1 서론

현대의 통신환경은 시스템 및 네트워크 성능 향상의 영향으로 단순한 정보의 전달 뿐만이 아니라 음성, 영상 데이터와 같은 멀티미디어 데이터와 같은 다양한 형태의 정보 전달의 비중이 높아지고 있다. 멀티캐스트 프로토콜은 이러한 통신환경에서 대역폭 사용의 효율성을 증대시키기 위한 기술로서 사용되고 있다. 멀티캐스트 프로토콜은 정보의 양이 많아지고 멀티캐스트 통신에 참여한 사용자들이 많아질수록 대역폭의 효율성과 같은 멀티캐스트의 장점은 더욱 두드러지게 된다. 또한, 현대의 통신환경이 단순히 정보의 공유 및 활용을 넘어서 여러 사용자들이 화상 회의 시스템이나 원격 의료 시스템과 같은 공동 작업을 수행할 수 있는 응용 분야가 나타남에 따라 이러한 응용분야에 대한 멀티캐스트의 적용과 이에 따르는 보안에 대한 요구 사항 또한 점차 높아져 가고 있는 추세이다.

위와 같은 다자간 그룹 통신이 원활하게 제공되기 위해서는 여러 가지 서비스가 제공되어야 한다. 이러한 서비스 중에 통신에 세션의 관리를 위한 세션 관리(Session Management), 통신에 참여하는 사용자들에 대한 정보와 상태를 관리하는 멤버십 관리(Membership Management)가 필수적이다. 본 논문에서는 이러한 서비스를 제공하기 위한 멀티캐스트 프로토콜로서 그룹 관리 프로토콜(Group Management Protocol, GMP)을 고려하였다. 그룹 관리 프로토콜(GMP)에서 서버는 세션과 그룹 통신에 참여하는 모든 참여자들의 멤버십을 유지

관리하게 된다. 통신에 참여하는 참여자들(클라이언트)은 서버에 자신의 정보를 등록하고, 서버는 이를 통해 관리를 하게 된다. 서버는 주기적으로 클라이언트의 상태를 확인하여 통신 참여 상태를 확인한다. 또한, 클라이언트는 세션 정보와 사용자 정보를 서버에게 요청할 수 있다. 이와 같은 기능의 제공으로 송신자의 부담을 줄여주며, 세션별 멤버십 정보 교환이 용이하다. 또한 안전한 멀티캐스트 시스템을 설계하고 구현하는데 있어서 고려해야 할 보안 서비스는 인증과 접근제어, 비밀성, 무결성, 부인봉쇄 등이 있다. 멀티캐스트 보안 구조의 목적은 인증 받은 그룹 멤버들에게 안전한 그룹통신을 제공하도록 하는 것이다. 본 논문에서는 이러한 GMP 프로토콜에 대한 보안 사항을 추가하여 안전한 멀티캐스트 통신이 가능하도록 고려하였다.

본 논문의 구성은 다음과 같다. 2 장은 그룹 멤버십 프로토콜의 특징 및 기능에 대해서 설명하고, 3 장에서는 멀티캐스트 통신에서 필요한 그룹 키 관리 아키텍처에 대해서 설명한다. 4 장에서는 앞서 설명한 내용을 바탕으로 본 논문에서 제안하고 있는 안전한 그룹 관리 통신에 대한 아키텍처를 기술한다. 그리고 마지막으로 5 장에서는 결론을 맺는다.

2. 그룹 관리 프로토콜(GMP)

2.1 세션관리

그림 1 은 GMP 동작의 예를 보여주고 있다. 세션의 상