오버레이 멀티캐스트 기반에서 유·무선 서비스를 위한 적응적 그룹키 관리 기법

이 광 겸° 박 상 진 김 대 원 김 경 민 신 용 태
숭 실 대 학 교 일 반 대 학 원 컴 퓨 터 학 과
{goodwin77°, parking, kdwon2002, kmkim, shin}@cherry.ssu.ac.kr

An Adaptive Group-Key Management Mechanism based Overlay multicast for Wired & Wireless services

Kwangkyum Lee° Sangjin Park Daewon Kim kyungmin Kim Yongtae Shin

Dept. of Computing, Soongsil University

요 약

본 논문은 오버레이 멀티캐스트 기반에서 유무선 서비스를 위한 적응적 키관리 기법을 제안한다. IP 멀티캐스트의 라우터 기능을 어플리케이션에서 처리하고, 적응적인 그룹관리를 위해서 유니캐스트와 멀티캐스트의 두 가지 통신기법으로 그룹키를 분배한다. 또한, 안전한 그룹키 관리를 위해 멤버의 그룹 가입과 탈퇴시에 키의 갱신을 수행하며, 주기적인 메시지 교환으로 멤버의 상태를 체크하여 비정상적인 그룹탈퇴의 경우에도 동적인 키의 갱신을 통하여 forward secrecy 와 backward secrecy의 보안적 요구사항을 충족시킨다. 그룹키는 갱신된 키의 분배를 우선적으로 하였으며, 대칭키를 이용한 암호화 기법과 이전의 그룹키를 사용하는 두 가지의 기법을 적응적으로 사용하는 기법에 대해서 제안한다.

1. 서론

멀티캐스트는 동시에 다수의 인원에게 같은 서비스를 제공하는 통신 기법이다. 일반적인 IP 멀티캐스트는 라우터에서 패킷을 복사하여 다수에게 전송할 수 있는 기능을 제공해야 한다. 그러나 고가의 장비와 교체의 어려움 때문에 어플리케이션 기반의 오버레이 멀티캐스트가 현실적으로 제시되고 있다. 그러나 멀티캐스트 통신은 특성상 일 대 다수에게 같은 메시지가 전달되기 때문에 보안적인 취약점을 가지고 있다. 따라서 본 논문에서는 오버레이 멀티캐스트 기반에서 유무선의 어떠한 환경에서도 적용이 가능하도록 동적인 키의 생성과 분배를 통하여 키의 교환을 최소화하고, 키의 보호를 위해서 이벤트성 키갱신이 이루어지도록 하는 적응적 키 관리 기법을 제안한다. 2장의 관련연구에서는 오버레이 멀티캐스트의 기본개념과[1], 키 관리 기법들[2, 3]에 대해 장단점을 비교한다. 3장에서는 본 논문에서 제안하고 있는 네트워크 구조와 키 관리의 세부 동작과정을 설명하고, 마지막으로 4장에서는 결론과 향후 연구과제를 제시한다.

2. 관련연구

기존 IP 멀티캐스트 기술은 네트워크 대역폭의 소비를 절약할 수 있지만 관리, 보안, 도메인간의 라우팅 등의 문제점을 가지고 있어 널리 전파되지 못하였다. 오버레이 멀티캐스트 기술은 IP 멀티캐스트만큼 효율적이지는 않지만 현재 인터넷 기반 구조의 어떤 변경도 필요하지 않으며 어플리케이션 계층에서 구현할 수 있기 때문에 IP 멀티캐스트의 문제점들을 간단히 해결 할 수 있다. [1]에서는 이러한 오버레이 멀티캐스트 기술과 IP 멀티캐스트 기술의 장단점을 비교, 분석하고 오버레이 멀티캐스트 기술에 대해서 고정 노드 기반과 동적 노드 기법으로 나누어 제안하고 있다.

GKMP(Group Key Management Protocol) 기법[2]은 멀티캐스트 그룹의 회원들을 관리하기 위한 대칭키를 생성하여 관리한다. 이 프로토콜에서는 각각의 멀티캐스트 그룹을 그룹 컨트롤러(Group Controller)가 관리한다. 그룹 컨트롤러 역시 그룹 회원으로서, 키 생성, 분배와 그룹 키 재생성(rekey) 메시지를 전달하는 역할 등의 주요한 프로토콜 동작을 수행하며, 진행 과정에 대한 보고도 담당한다. 그룹 컨트롤러는 선택된 그룹 회원과 JOINT를 통해 멀티캐스트 그룹 외부로부터 보안성을 제공해 주게 된다. 이 기법에서는 그룹 컨트롤러가 모든 그룹 회원에 대한 키 분배를 전담하므로 확장성이 떨어진다는 단점을 가진다.

[3]은 오버레이 멀티캐스트 기반에서 서버 처리량과 대역폭의 부담을 줄이기 위한 주기적인 배치 키 교환(periodic batch re-keying) 방법을 제안한다. 이 방법은 키 교환의 대역폭 부담을 줄이고 빠르게 처리하기 위해 키 교환 메시지를 한 단위씩 나누어 처리하는 기법을 통하여 오버레이 멀티캐스트의 주기적인 키 교환의 문제점을 해결한다. 그러나 단위로 나누는 기법은 주기적인 키 교환기법에 비해 보안 강도가 약해질 수 있다는 단점을 가지고 있다.

3. 오버레이 멀티캐스트 기반의 동적 그룹키 관리기법

본 논문은 오버레이 멀티캐스트 기반에서 동적인 그룹키 관리기법을 제안한다. 멤버의 요청에 따라 그룹관리 호스트에서는 그룹키를 생성하고 분배하며, 안전한 그룹키의 관리를 위해 키를 갱신하고, 갱신된 키를 암호화하여 멤버들에게 멀티캐스트로 분배한다.

3.1 그룹키 관리를 위한 네트워크 구조

본 논문에서 제안하는 오버레이 기반의 멀티캐스트 서비스를 위한 키 관리 구조는 다음과 같다. 오버레이 멀티캐스트를 위하여 일반적인 IP 멀티캐스트 라우터의 역할을 대신하는 그룹관리 호스트와 그룹관리 호스트를 관리하는 메인 호스트, 그리고 그룹 서비스를 이용하고자 하는 멤버들로 구성된다. 그룹관리 호스트들은 자신의 그룹 멤버들의 가입 탈퇴와 키 분배를 담당하고, 메인 호스트는 그룹관리 호스트로부터 받은 정보들을 이용하여 그룹관리 호스트와 그룹 멤버들의 관리를 위한 키관리 기능을 담당한다. 이러한 계층적인 구조를 이용하여 중앙 집중형 방식의 단점을 보완하였다. 그림 1은 제안하는 네트워크의 구조도를 나타낸다.

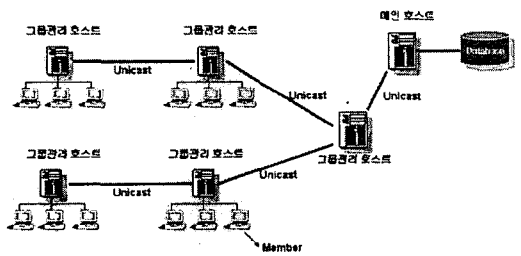

그림 1. 네트워크 구조도

3.2 멤버의 그룹 가입 요청시 그룹키 분배 기법

본 논문은 멤버의 그룹 가입 요청시 안전한 그룹키의 분배를 위해서 대칭키를 사용하며, 그룹관리 호스트에서 갱신된 키를 유니캐스트로 분배하도록 한다. 또한, 메인 호스트와 그룹관리 호스트들은 서로간에 안전한 채널이 설정되어 있으며, 서로간의 정보를 교환하여 외부의 침입에 대해 견고하다고 가정한다. 멤버는 그룹키를 획득하기 위해서 그룹가입 요청을 그룹관리 호스트로 자신의 개인키와 함께 전송한다. 이 때 개인키는 사전 프로세스에 의해 그룹관리 서버와 멤버간의 공유키로 암호화된다. 멤버의 개인키를 획득한 그룹관리 호스트는 멤버의 가입 여부를 판단하여 이상이 없을 경우 이전에 사용하던 그룹키 K_i 를 K_{i+1}로 갱신하고 멤버의 개인키로 그룹키를 암호화해서 멤버에게 유니캐스트로 전송한다. 새로운 멤버는 그룹관리 서버로부터 자신이 보낸 개인키로 암호화되어 온 그룹키를 개인키로 복호화하여 갱신된 그룹키 K_{i+1}을 획득한다. 그림 2와 그림 3은 그룹 가입을 요청하는 멤버의 그룹키 획득과정을 나타낸 그림과 메시지 흐름도이다.

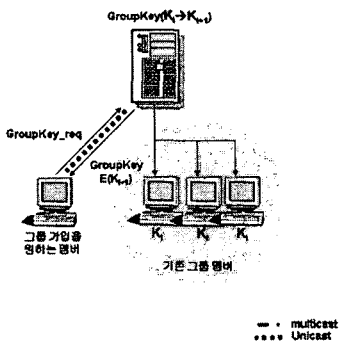

그림 2. 새로운 멤버의 갱신된 그룹키 획득과정

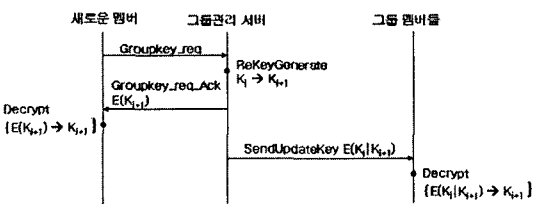

그림 3. 메시지 흐름도

표 1. 변수 및 메시지의 정의와 기능

변수 및 메시지	설명
K_i	현재 사용중인 그룹키
K_i->K_{i+1}	i 번째 사용중인 그룹키를 갱신
$E()$	멤버의 개인키로 암호화
Groupkey_req	그룹키 요청 메시지
ReKeyGenerate	키의 갱신
Decrypt	암호화된 그룹키의 복호화

3.3 그룹키의 갱신 기법

본 논문은 오버레이 멀티캐스트 기반에서 안전한 그룹키의 관리를 위한 그룹키 갱신 기법을 제안한다. 그룹키의 갱신은 멤버의 그룹 가입과 탈퇴시에 이루어지게 되며, 동적인 그룹키 갱신을 통하여 forward secrecy 와 backward secrecy의 보안적 요구사항을 만족시킨다. 새로 가입하려는 멤버는 그룹에 가입하기 이전의 서비스에 대해 알지 못해야 하며, 탈퇴한 멤버는 탈퇴한 그룹에 대해서 어떠한 것도 알지 못해야 한다. 멤버가 그룹에 가입할 경우에는 그룹관리 서버로부터 갱신된 키를 암호화해서 유니캐스트로 전송받는다. 기존 멤버들은 그룹관리 서버에서 갱신된 그룹키 K_{i+1}를 이전의 그룹키 K_i로 암호화되어 온 키값을 멀티캐스트로 전송받는다. 암호화되어 온 그룹키는 현재 그룹의 멤버들이 가지고 있는 키값 K_i를 사용하여 복호화된다. 이 때, 그룹에서 탈퇴하는 멤버는 이전의 키를 가지고 탈퇴할 수 없다고 가정하고, 그룹 탈퇴의 경우를 정상적인 탈퇴 메시지를 보내고 탈퇴하는 정상 탈퇴와 네트워크상의 문제로 인한 비정상적인 탈퇴의 두 가지 경우로 정의한다. 또한 그룹관리 서버는 멤버의 비정상적인 탈퇴를 감지하기 위해서 주기적으로 멤버의 상태를 체크하는 메시지를 브로드캐스팅 하여 상태 정보가 일정시간이 지나도 오지 않는 경우를 비정상적인 탈퇴로 간주하고 그룹키 갱신을 실행한다. 탈퇴의 이벤트가 있을 경우에만 키의 갱신을 실행하여 일정 시간마다 키의 교환으로 인한 주기적인 키 갱신의 단점을 보안하였다. 그림 4와 그림 5는 그룹 탈퇴시 그룹키의 갱신과정과 기존 멤버의 그룹키 획득과정을 나타낸 그림과 메시지 흐름도이다.

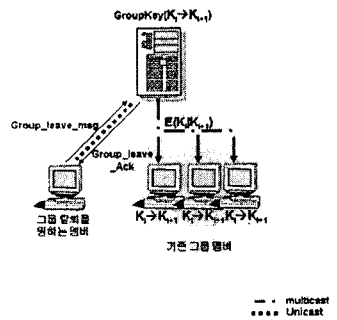

그림 4. 그룹 탈퇴시 그룹키의 갱신과정

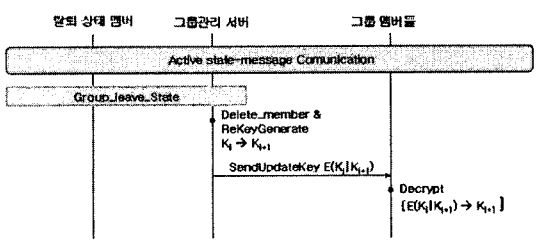

그림 5. 메시지 흐름도

표 2. 변수 및 메시지의 정의와 기능

변수 및 메시지	설명
K_i, K_i->K_{i+1}, $E()$, Decrypt	표 1. 참조
Group_leave_state	정상 비정상적인 멤버의 탈퇴상태
Delete_member	그룹멤버 리스트에서 멤버 삭제
ReKeyGenerate	키의 갱신
SendUpdatekey	멀티캐스트 그룹키 전송
$E(K_i/K_{i+1})$	K_i로 K_{i+1}을 암호화

4. 결론 및 향후 과제

본 논문은 오버레이 멀티캐스트 기반에서 유무선 서비스를 위한 적응적인 키관리 기법을 제안한다. 또한 네트워크의 구조를 계층화하여 독립적인 키관리가 이루어지질 수 있도록 하였다. 멤버의 그룹 가입시 그룹키 요청에 따라 유니캐스트로 이루어지는 키의 갱신과 분배, 정상탈퇴와 비정상적 탈퇴시 키의 갱신과 기존 멤버에 대하여 안전한 멀티캐스트 키 분배를 통하여 멀티캐스트에서 적응적인 키관리를 수행할 수 있도록 하였다. 향후 멀티캐스트의 특징인 그룹관리와 함께 제안에 대한 보안성의 성능분석에 대한 연구가 추가되어야 할 것이다.

참고문헌

[1] Zhi Li, Yongjoo Shin "Survey of Overlay Multicast Technology" Course Project

[2] Sencun Zhu, Cao Yao, Donggang Liu, Sanjeev Setia, Sushil Jajodia "Efficient Security Mechanisms for Overlay Multicast-based Content Distribution" In Proc. of Applied Cryptography and Network Security (ACNS) conference, New York, June, 2005

[3] X. Brain Zhang, Simon S. Lam, Huaiyu Liu "Efficient Group Rekeying Using Application-Layer Multicast" Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05) - Volume 00 Pages 303 - 313