멀티캐스트 환경에서 Dynamic Grouping을 이용한 키 관리 프로토콜†

문종식, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:jsmoon@sch.ac.kr

Key Management Protocol using Dynamic Grouping in Multicast Environment

Jong Sik Moon, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

인터넷 및 서비스 환경의 발전으로 인해 컴퓨터 통신의 환경이 변함에 따라 기존의 유니캐스트 전송 방식에서 멀티캐스트 전송 방식을 이용한 그룹 통신이 증가하고 있다. 그러나 멀티캐스트 전송 방식의 취약점 및 키 관리의 어려움으로 인해 많은 문제점이 발생하면서 멀티캐스트 환경에서 안전하고 효율적인 키 관리 방법에 대한 연구의 필요성이 대두되고 있다. 따라서 본 연구에서는 멀티캐스트 환경에서 dynamic grouping을 이용한 키 관리 프로토콜을 제안하여 안전성과 효율성을 제공하고자 한다.

1. 서론

최근 디지털화의 가속 및 통신 인프라의 확충 등으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보 등 데이터를 서로 공유할 수 있는 환경이 제공되고 통합 서비스에 대한 수요가 증가하면서 멀티캐스트 전송 방식을 이용한 그룹 통신이 증가하고 있다[2]. 그러나 이와 같은 환경에서는 IP 멀티캐스트의 취약점 및 키 관리의 어려움으로 인한 정보노출 등 다양한 보안 위협이 이슈화 되고 있다. 따라서 본 연구에서는 기존의 문제점을 해결할 수 있는 멀티캐스트 환경에서 dynamic grouping을 이용한 키 관리 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 요구사항에 대하여 분석하고, 3장에서는 기존 방식에 대하여 분석한다. 4장에서는 제안방식을 기술하고 5장에서는 제안방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구방향으로 논문을 마치도록 한다.

2. 멀티캐스트 키 관리 요구사항

멀티캐스트 환경에서 키 관리를 위한 요구사항은 다음과 같다.

- 전방향 안전성 : 멀티캐스트 통신 환경에서 그룹을 탈퇴한 멤버를 포함하여 이전 그룹키를 알고 있는 공격자는 새 그룹키를 알 수 없어야 한다.
- 후방향 안전성 : 멀티캐스트 통신 환경에서 그룹을 새롭게 가입한 멤버를 포함하여 현재 그룹키를 알고 있는 공격자는 이전 그룹키를 알 수 없어야 한다.
- 키 갱신 효율성 : 멀티캐스트 키 관리 프로토콜은 키 갱신 시 효율성을 감소하는데 초점이 맞추어져 있다. 따라서 기존 연구는 대칭키 방식 및 해쉬 기반의 방식을 사용하여 연산량을 줄이고자 하였으나 안전성에 문제가 발생함에 따라 공개키 기반 방식을 사용하는 추세이다. 그러나 공개키 방식의 특성상 연산량이 증가하기 때문에 경량화된 공개키 방식을 사용하여 안전성뿐만 아니라 갱신의 효율성을 제공해야 한다.

3. 기존연구

기존에 연구된 멀티캐스트 키 관리 프로토콜 연구는 다음과 같다.

3.1 계층적 멀티캐스트 구조에서 이중 키 관리 프로토콜

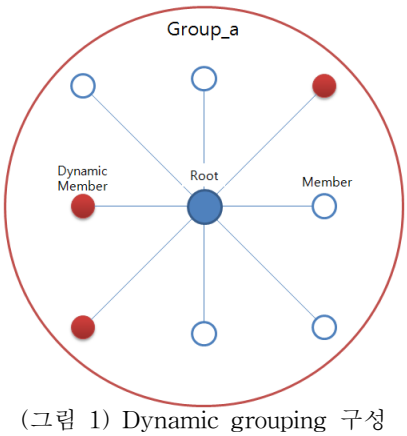
본 연구는 모바일 인터넷 환경에서 대규모 그룹통신을 위한 안전한 멀티캐스트 구조 기반의 키 관리 프로토콜을 제안하였다[3]. 그러나 일괄 키 갱신방식 및 테이블을 통해 멤버를 관리함으로써 전방향 안전성에 노출되는 단점을 가지고 있다. 즉, 모바일 환경에서 디바이스가 서브 그룹 간의 이동 시 키 갱신을 즉시 실행하지 않고 테이블 구성으로 일정시간 및 이동 횟수에 따라 키 갱신 연산을 수행하기 때문에 완벽한 전방향 안전성을 제공하지 못한다. 또한 PKI 기반 구조를 사용함으로써 CA가 추가되어 통신 횟수가 증가한다.

3.2 키 분배의 효율성을 위한 계층적 그룹키 관리 방식

IP 멀티캐스트를 이용한 그룹 통신 증가에 따른 보안 문제가 대두됨에 따라 본 연구는 멀티캐스트 환경에서 그

† 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구 결과임.

룹키 관리를 위한 효율적인 프로토콜과 알고리즘을 제안하였다[1]. 그룹키를 구성하는데 있어 멤버의 비밀값과 서버의 비밀값을 기반으로 생성하기 때문에 멤버의 탈퇴 시 탈퇴 멤버의 비밀값을 제외함으로써 그룹키를 관리한다. 그러나 이와 같은 효율성은 탈퇴 연산에만 해당하며, 멤버의 가입 연산에는 기존의 방식과 동일한 연산량을 가진다.



(그림 1) Dynamic grouping 구성

4. 제안방식

제안방식은 그림 1과 같이 멀티캐스트 환경에서 그룹을 구성된 상태에서 그 중 데이터를 보내고자 하는 멤버로만 dynamic 그룹 새로 구성을 하고 키를 갱신한다. 멀티캐스트 환경에서 고정적 그룹을 구성하고 데이터를 전송하는 것은 매우 비효율적이기 때문에 데이터를 전송받고자 하는 멤버로만 dynamic 그룹을 구성하고 키를 갱신한다. 따라서 키가 그룹 구성동안만 사용되기 때문에 그룹 멤버의 탈퇴 및 가입에 따른 키 갱신이 필요하지 않다. 제안방식의 흐름은 다음과 같다.

step1. 그룹의 멤버는 미리 구성되었다고 가정하며, 전체 멤버를 위한 그룹키는 공개키 방식을 통해 분배한다.

step2. 그룹의 관리자가 멀티캐스트 통신을 위해 데이터를 전송하고자 할 때 데이터를 전송받는 멤버의 공개키를 기반으로 그룹키를 생성하고 그룹키 생성 인자를 전체 그룹키로 암호화하여 브로드캐스팅한다.

step3. 각 멤버는 그룹키로 메시지를 복호화하고 데이터를 전송받고자 하는 멤버는 dynamic grouping 그룹키를 생성한다.

step4. 키생성 인자를 브로드캐스팅 하더라도 참여하지 않는 멤버는 dynamic grouping을 위한 키를 생성할 수 없기 때문에 정보 노출에 대한 위협이 발생하지 않는다.

step5. 그룹 관리자는 dynamic grouping 그룹키로 데이터를 암호화하고 dynamic 그룹 멤버들에게 전송한다. 멤버들은 그룹 관리자가 브로드캐스트한 메시지의 키 생성 인자를 통해 생성한 dynamic 그룹키로 복호화하여 서비스를 제공받을 수 있다.

step6. 데이터 전송이 완료되면 dynamic grouping 그룹키는 삭제하며, 이후 데이터 전송 시 위와 같은 단계를 통해 그룹키를 생성하고 통신한다.

step7. Dynamic grouping 그룹키는 경량화 기반 공개키 방식을 사용하기 때문에 기존 연구에서의 멤버의 가입 및 탈퇴에 따른 키를 갱신하는 방법보다 더욱 효율적이다.

5. 제안방식 분석

제안방식은 dynamic grouping을 사용하여 데이터를 전송하고자 할 때 멤버의 가입과 탈퇴에 따른 키 갱신 필요하지 않다. 즉, 데이터를 전송할 때 마다 동적 그룹을 구성하고 키를 분배하기 때문에 전방향 및 후방향 안전성으로부터 안전하다. 그러나 기존에 구성된 그룹에서의 멤버의 가입 및 탈퇴에 따른 키 갱신은 기존의 batch re-keying 키 갱신 기법을 사용한다. 이와 같은 방법을 사용하면 멤버의 가입 및 탈퇴 시 마다 키를 갱신할 필요가 없으며 dynamic grouping을 기반으로 하기 때문에 키 갱신 지연으로 인한 정보노출이 발생하지 않는다. 또한 이로 인해 키 갱신 시 계산 효율성을 제공할 수 있으며, 경량화된 공개키 방식으로 인해 키 갱신의 효율성을 제공할 수 있다.

6. 결론

기존에 연구된 멀티캐스트 키 관리 방식은 대칭키 방식의 키 분배 문제와 계산 효율성을 높이고자 공개키 방식을 이용한 키 분배와 해쉬 기법을 이용한 키 생성이 연구되었다. 그러나 공개키 방식의 높은 연산량과 해쉬 기법의 취약점으로 인해 많은 문제점이 제기되고 있다. 따라서 제안방식은 멀티캐스트 환경에서 경량화된 공개키 방식을 적용하여 오버헤드를 줄일 수 있도록 하였으며 dynamic grouping을 이용한 관리 기법으로 인해 효율성을 높이고자 하였다. 향후 중복 grouping이 가능한 키 관리 기법에 관한 연구가 필요할 것으로 사료된다.

참고문헌

[1] Alireza Nemaney Pour, Kazuya Kumekawa, Toshihiko Kato, and Shuichi Itoh, "A Hierarchical Group Key Management Scheme for Secure Multicast Increasing Efficiency of Key Distribution in Leave Operation," Computer Networks, Vol. 51, No. 17, pp. 4727-4743, 2007.

[2] Iuon-Chang Lin, Shih-Shan Tang, and Chung-Ming Wang, "Multicast Key Management without Rekeying Prcesses," The Computer Journal, Vol. 53, No. 7, pp.939-950, 2010.

[3] Jiannong Cao, Lin Liao, Cuojun Wang, and Bin Xiao, "A Novel Dual-Key Management Protocol Based on a Hierarchical Multicast Infrastructure in Mobile Internet," ICCNMC 2005, LNCS 3619, pp. 560-569, 2005.