2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

확장성을 제공하는 안전한 멀티캐스트 키 관리 구조에 관한 연구

박희운*, 이임영*, 박원주**, 이종태**, 손승원**
*순천향대학교 정보기술학부
**한국전자통신연구원 정보보호기술연구본부
e-mail:heeun@cse.sch.ac.kr

A Study on Scalable Secure Multicast Key Management Structure

Hee-Un Park*, Im-Yeong Lee*, Won-Joo Park**, Jong-Tai Lee**, Sung-Won Sohn**
*Division of Information Technology, Soon-chun-hyang University
**Information Security Technology Division, Electronic Technology Research Institute

요약

통신 및 컴퓨터의 보급 발전을 통해 공개 네트워크 상에서 그룹에 기반한 통신 응용 서비스의 요구가 증가하고 있다. 이러한 필요성에 따라 멀티캐스트 기반 구조에 대한 연구가 활발히 진행되고 있다. 하지만 멀티캐스트 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 기존의 대표적인 멀티캐스트 키 관리 구조를 고찰함과 동시에 안전성과 효율성 및 확장성을 분석한다. 이에 기초해 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안하고 기존 방식과 비교 분석한다.

1. 서론

컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 다가오는 산업 및 사회 일반에서 정보의 의존성이 한층 가속화되고 있다. 이에 따라 일반인 누구나 인터넷 등을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있다.

이러한 상황에서 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의 및 의료 분야에서 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 그러나 이와 같은 서비스는 기존의 일대일 통신 방식으로는 제약 사항이 생길 수밖에 없다. 이를 해결하기 위하여 현재 각광 받고 있는 방식 중의 하나가 멀티캐스트 기법이다.

멀티캐스트란 그룹에 참가한 멤버들 사이에서 한 송신자로부터 다수의 참여자에게 데이터 전송이 가능한 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을 떠나면 더 이상 정보를 수신할 수 없게 된다.

이 논문은 한국전자통신연구원의 인터넷 정보보호 IPSec 기술연구 지원사업에 의해 연구되었습니다.

동시에 멀티캐스트 기법은 기존의 통신 방식에 대해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 제공한다.

그러나 멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 많은 부분에서 취약성이 노출되고 있다. 특히 불법적인 제 3자의 도청이나 전송 정보의 위조는 그 대표적인 예가 된다.

이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위해 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져야 한다. 동시에 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다.

현재 멀티캐스트 그룹 키 관리 분야와 관련하여, 그 중요성에도 불구하고 해결책들은 미흡한 상황이다. 따라서 본 연구는 향후 광범위하게 적용될 멀티캐스트 서비스에서 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고려한다. 또한 기존의 멀티캐스트 키 관리 구조들을 고찰함과 동시에 새로운 방식을 제안하여 안전성, 효율성 및 확장성 부분에서 비교 분석을 수행한다.

2. 멀티캐스트 키 관리 요구사항

멀티캐스트 구조는 그 특성상 다자간 통신을 전제로 하고 있기 때문에 여러 위협 요소에 노출되어 있다. 특히 통신을 위해 사용되는 키의 관리는 매우 중요한 요소로서, 다음은 이를 위해 요구되는 사항을 기술한 것이다.

- 비밀성 : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.
- 무결성 : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- 인증 : 송·수신된 멀티캐스트 정보가 불법적인 변조 없이 정당한 참여자들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- 접근 제어 : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 멀티캐스트 서비스 참여자 사이에서 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자가 이를 확인 할 수 있어야 한다.
- 공정성 : 멀티캐스트에서 사용되는 키들은 허가된 그룹 참여자에게만 안전하게 전송되어야 한다. 또한 가입 및 탈퇴를 대비해 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단이나 제 3자와의 불법적 결탁을 방어하기 위한 공정성이 확보되어야 한다.
- 확장성 : 멀티캐스트 서비스는 다자간 통신을 전제로 하므로 그룹 참여자의 변동이 생기게된다. 따라서 참여자 변동에 따른 동적인 키 관리 기법이 필요하다.

3. 기존 방식 분석

본 장에서는 기존에 제안되어진 멀티캐스트 키 관리 구조에 대한 주요 사항 및 문제점을 기술한다.

3.1 Clique 방식

이 방식은 선형 또는 Ring 형 네트워크 구조에서 적용 가능한 기법이다[1][2]. 키 분배를 위해서 각 멤버는 공개키 방식에 기반한 Diffie-Hellman 방식을 적용하고 있다. 이때 멀티캐스트 통신을 위해서 모든 멤버가 키 생성에 관여하므로, 새로운 멤버 가입 및 기존 멤버 탈퇴시 전 멤버 사이에 새로운 키를 생성 해야하는 번거로움이 발생한다. 또한 제 3자의 도청이 man-in the-middle attack에 의해 가능하다는 문제점을 안고 있다.

3.2 Iolus 방식

본 방식은 각 멤버쉽이 Tree-Based 계층 구조로 구성된다[3]. 각 멤버의 가입/탈퇴시 Sub-Group 내에서만 키의 변경이 일어나므로, Clique 방식의 문제점을 개선하고 있다. 그러나 보안 관리 센터(GSC)의 오류 및 부정이 발생할 경우 멀티캐스트 서비스가 불가능하다. 동시에 각 Sub- Group간의 통신시 중간 관리자간에 메시지 암/복호화를 별도로 수행해야 하는 단점이 발생한다.

3.3 Domain GKMP 방식

이 방식은 각 그룹을 도메인 형식으로 구성함으로서 동적인 멤버쉽 변화에 유연성을 제공하고 있다[4]. 그러나 멀티캐스트 메시지 전송을 위해 각 도메인 별로 각각의 멀티캐스트 키를 보유하고 있다. 따라서 도메인간의 메시지 전송 시 매번 암/복호화 과정을 수행해야 하는 번거로움이 발생한다.

3.4 DK 방식

이 방식은 Iolus 방식에서 지적되었던, 멀티캐스트 메시지 전송시 중간 관리자 사이에 발생되는 암/복호화 과정을 줄이기 위하여 제안된 방식이다[5]. 즉 모든 멤버가 동일한 멀티캐스트 키를 보유함으로서, 중간 관리자의 번거로움이 해결되고 있다. 그러나 새로운 멤버 가입/탈퇴시 전 멤버의 멀티캐스트 키를 새로이 생성 및 전송해 주어야 하는 문제점이 생기고 있다.

4. 새로운 방식 제안

본 방식은 상기 제시되었던 요구 사항을 만족함과 동시에 기존 방식들 - Clique 방식, Iolus 방식, DK 방식 및 D-GKMP 방식 - 이 안고 있던 문제점들을 해결하고 있다.

4.1 구성 요소 및 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성 요소를 기술하고 있다.

- DKM_i : 도메인 키 관리자 i
- M_i : 멤버 i
- BKM_i : Border 키 관리자 i
- R : 라우터
- DKA_i : 도메인 키 중간 관리자 i
- PKLM : 관리자들의 공개키 리스트(APL) 관리자
- GI : 그룹 초기자

- Sig_{GI} : 그룹 초기자의 서명
- MKey : PKLM에 의해 생성된 멀티캐스트 키
- APL : 각 관리자의 공개키 리스트
- K_{DPi} : 각 DKM_i의 공개키
- K_{DPAi} : 각 DKA_i의 공개키
- K_{BPi} : 각 BKM_i의 공개키
- K_{SDP_DPA} : DKM_i와 DKA_i 사이의 비밀키
- K_{SM} : 그룹 멤버의 비밀키
- Ks_{ubi} : 각 KDA_i가 관리하는 멤버들과의 비밀키

4.2 시스템 프로토콜

본 방식은 멤버쉽 가입/탈퇴시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 도메인 형식으로 분류하여 동적인 관리를 수행한다. 또한 구조적으로 제어부와 데이터 전송부로 구분함으로서 키 관리 담당자의 부담을 줄이고 메시지 전송 과정에서 발생 가능한 부정 및 오버헤드를 막고 있다. 동시에 본 방식은 인증 및 메시지 암호화를 위하여 현재 국제 표준화 작업이 활발한 IPSEC을 적용한다. 이는 이질적인 통신망 상에서 안전하면서도 적용이 용이하여 효율성을 높이는 효과를 제공한다.

1) 도메인 초기화 단계

①DKM_i, DKA_i 및 BKM_i은 자신의 공개키를 APL에게 등록하고, PKLM에게 인증을 수행한다.

②각 관리자들은 자신의 공개키를 확인한다.

③각 도메인은 DKMi를 정점으로 멤버들을 분할하여 담당하는 각 DKAi를 계층적으로 관리한다. 공개키 등록이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

2) 그룹 초기화 단계

①GI는 그룹 멤버 리스트(ACL)를 작성하여 자신의 식별자 ID_{GI}와 함께 서명을 수행하여 PKLM에게 전송한다.

$$SigGI(ID_{GI}||ACL)$$

②PKLM은 서명 확인을 통해 GI 및 ACL을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 BKMi에게만 제공함으로서 신뢰성을 높이고 있다.

③PKLM은 해당 Domain에게 공개키를 이용하여 안전하게 ACL을 전송한다.

3) 그룹 멤버 Join 단계

①DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{SDP_DPA}를 생성하여 안전하게 DKA_i에게 전송한다.

②그룹에 멤버로 가입할 사용자들은 IPSec을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{SM}를 K_{DPAi}로 암호화하여 안전하게 전송한다.

③DKM_i는 각 DKA_i를 통해 그룹에 가입할 멤버를 재확인한다.

④DKA_i는 수신된 비밀키를 이용하여 각 멤버에게 Ks_{ubi}를 안전하게 전송해 준다. 동시에 이 Ks_{ubi}는 DKM_i 및 Border에게 안전하게 전송된다.

4) 멀티캐스트 메시지 전송 단계

①이 단계는 도메인 간 데이터 전송부로서 오직 멤버들과 Border만이 관여한다.

②각 멤버들은 멀티캐스트 메시지 전송 시 Ks_{ubi}를 이용하여 암호화한다.

$$Ks_{ubi}(M)$$

③암호화된 메시지는 Border를 통해 복호화된 다음 MKey로 암호화되어 인접 도메인 Border로 전송된다.

④전송된 메시지는 복호화되어 각 K_{subi}로 암호화되어 전송된다.

⑤각 Sub 그룹의 멤버는 K_{subi}로 복호화하여 메시지를 확인한다.

5) 신규 멤버 가입 및 기존 멤버 탈퇴 단계

①신규 멤버 가입은 멤버 Join과 같은 과정을 수행한다.

②이 때 신규 멤버 가입 시 기존의 K_{subi}의 노출을 방지하기 위하여 이 키는 새로이 갱신하여 분배되어진다.

③기존 멤버 탈퇴 시에는 남아 있는 멤버들을 위해 새로운 K_{subi}를 갱신하여 분배한다.

4.3 새로운 방식의 특징

본 제안 방식은 다음과 같은 특징을 가지고 있다.

1) Clique 방식의 문제점 해결

: 새로운 멤버 가입 및 기존 멤버 탈퇴 시 모든 멤버에게 새로운 키를 생성 및 분배하는 문제점을 해결하고 있다.

: 멤버를 도메인 상의 sub 그룹으로 나누는 기법 적용함으로서 가입 탈퇴가 발생하는 Sub 그룹

의 K_{subi}만 갱신하면 된다.

2) Iolus 방식의 문제점 해결

: 도메인 관리를 위한 제어부와 메시지 전송을 위한 데이터 전송부로 구분함으로서 메시지 전송시 중간 과정에서 노출되는 것을 막는다.

: GSC의 오류 및 부정에 대한 해결 방안 제시 - Iolus 방식은 집중형 Tree Based 구조를 가지고 있으므로 최상위 노드의 오류에 대해 멤버 전체의 통신 단절을 가져 올 수 있다는 문제점이 발생하고 있다. 그러나 본 방식은 각 Sub 그룹을 그물형 도메인 내에 계층적으로 분포시킴과 동시에 오류에 대한 새로운 path를 지정함으로서 이 문제를 해결하고 있다.

3) GKMP 방식의 문제점 해결

: 이 방식은 도메인간의 멀티캐스트 메시지 전송시 각 인접 도메인의 키로 암/복호화가 이뤄지기 때문에 n개의 도메인에 대해 n번의 암/복호화가 이뤄진다. 그러나 제안 방식은 단 2번의 암/복화가 수행되므로 효율성을 높이고 있다.

4) DK 방식의 문제점 해결

: DK 방식은 Iolus에서 문제가 되고 있는 중간 관리자의 메시지 암/복호화의 문제점을 해결하기 위해 각 멤버가 그룹 키를 가지게 하고 있다. 그러나, 이 방식은 새로운 멤버 가입 또는 기존 멤버 탈퇴시 모든 멤버에게 새로운 그룹 키를 전송해야하는 문제점을 가지고 있다. 이에 대해 본 방식은 멤버 가입/탈퇴 시 Sub 그룹의 K_{subi}만 변경하면 되므로 DK 방식의 문제점을 해결하고 있다.

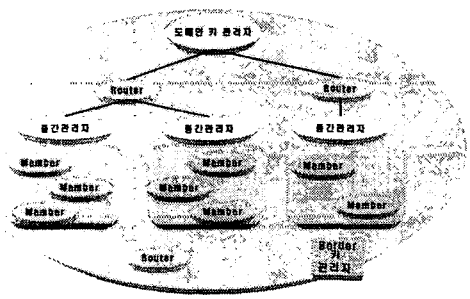

그림 1. 제안된 멀티캐스트 키 관리 구조도

5. 각 방식별 비교 분석

다음은 멀티캐스트 키 관리 구조 요구 사항에 기초하여 기존 방식과 제안 방식은 비교 분석한 결과이다.

표 1. 각 방식별 비교 분석

항목 \ 대상	Clique	Iolus	GKMP	DK	제안 방식
암호키의 수	3	3	5	7	3
암호 방식 (대칭, 비대칭)	(O,O)	(O,O)	(O,X)	(O,O)	(O,O)
참가자 증가에 따른 키 증가	X	X	X	X	X
탈퇴자에 대한 참가자 보안성	O	O	O	O	O
참가자 수에 따른 중계 라우터 키의 양	변화 없음	증가	증가	증가	변화 없음
상호 인증성	O	O	O	O	O
통신 신뢰성	X	X	O	O	O
병목현상 극복	O	X	O	O	O
키 갱신 범위	ALL	Sub-Group	Sub-Group	ALL	Sub-Group
메시지 전송시 암/복호화 회수	1	m	n	1	2

n : 도메인 수 m : 중간 관리자(중계 라우터) 수

6. 결론

현대 사회는 정보 통신 분야의 발전과 더불어 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 멀티캐스트 서비스는 기본적으로 다자간 통신을 요구함으로서 안전성, 효율성 및 확장성 부분에서 취약성을 드러내고 있다.

본 논문에서는 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았으며, 기존의 방식이 이에 어떻게 대처하는지 고찰하였다. 또한 요구 사항 및 기존 방식의 문제점을 해결할 수 있는 새로운 멀티캐스트 키 관리 구조를 제안함으로서 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참고문헌

[1] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key distribution extended to group," In ACM Symposium on Computer and Communication Security, 1996.

[2] G. Caronni, M. Walldvoge l and D. Plattner, "Efficient Security for Large Dynamic Multicast Groups," WETIC '98, 1998.

[3] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," 1997.

[4] H. Harney and C. Muckenhirn, "Group Management Protocol(GKMP) Architecture," IETF RFC 2094, 1997.

[5] "멀티캐스트를 위한 키 분배 메커니즘 설계 및 구현" ETRI 최종 보고서, 1999.