韓國 컴퓨터情報學會 論文誌
第9卷 第3號, 2004. 9.

2004-9-3-3-5

멀티캐스팅 정보보안을 위한 그룹키 관리 프로토콜 구현

홍 종 준*

Implementation of Group Key Management Protocol for Multicasting Information Security

Jong-Joon Hong *

요 약

소규모의 라우팅 구조에 적용된 기존 그룹키 관리 구조는 항상 키 분배에 따른 많은 부하를 갖는 문제점을 갖게 된다. 이에 본 논문에서는 소규모 라우팅 구조에 적합한 PIM-SM 라우팅을 이용하여, 안전한 멀티캐스트 통신이 가능한 그룹키 관리 구조를 제안한다. 제안한 방식은 멀티캐스트 통신 그룹을 RP단위의 부그룹으로 나누고, 각 RP에 부그룹 키 관리자를 부여하여 그룹키를 주고 받도록 한다. 이로서 송/수신자간에 보호채널이 설정되고, 그룹키에 따른 데이터 변환작업이 필요하지 않고 경로 변경에 따른 새로운 키 분배가 불필요하게 되어 데이터 전송시간이 단축되는 장점을 갖게 된다.

Abstract

The existing group key management architectures applied to a small scale routing protocols may have many overheads with key distribution. Therefore this paper proposes a group key management protocol in PIM-SM multicast group communication. This method divide multicast groups with RP, and subgroup key managers are established in each RP and can be transmitted groups keys. And this does not have needs of the data translation and the new key distribution for path change. This does not have needs of the data translation and the new key distribution for path change, so the data transmission time can be reduced.

▸ Keyword : Multicast, Group Key, PIM-SM

• 제1저자 : 홍종준
• 접수일 : 2004.08.14, 심사완료일 : 2004.09.01
* 평택대학교 정보과학부 정보통신학전공 교수

Ⅰ. 서 론

멀티캐스트상의 안전한 그룹통신[1,10,11]을 위해 그룹 내 멤버들이 메시지를 암호화/복호화하기 위하여 비밀키를 공유해야 하며, 그룹 내에서 공유되고 있는 비밀키는 backward secrecy와 forward secrecy를 만족하도록 새로운 멤버들이 그룹에 참여하거나 기존의 멤버가 그룹을 탈퇴할 때마다 새로운 그룹키로 변경되어야 한다[2][3][6][9]. 기존에 제안된 그룹키 관리 구조는 크게 중앙집중 방식과 분산 방식으로 분류할 수 있다[4]-[6]. 중앙집중 방식은 하나의 키 서버가 그룹 키를 관리하므로 멤버의 증가에 따른 부하가 키 서버에 집중되어 확장성에 문제가 있다. 이에 반해 분산된 키 서버에 각각의 그룹키를 갖는 분산 방식은 중앙집중 방식에 비해 확장성에 유리하다[7]. 이러한 방식들은 CBT (Core Based Tree)를 이용하여 코어를 중심으로 멤버들이 밀집되어 고정된 경로에 근거한 데이터 전송이 가능하다. 또한 이들은 키 관리자를 거칠 때마다 그룹키 변환이 필요하기 때문에 멤버들이 넓은 지역에 조밀하게 분포되어 있는 환경에 맞는 멀티캐스트 라우팅 방식에 적합하다[4].

이에 본 논문에서는 적은 수의 사용자가 지역적으로 분산되어 있는 멀티캐스트 라우팅환경에 적합한 PIM-SM 라우팅 구조[5][6]를 이용한 그룹키 관리 방식을 제안한다. PIM- SM 라우팅은 대규모에 적합한 CBT, DVMRP[8]과 달리 소규모에 지역적으로 분산되어 있는 노드들을 RP(Rendezvous-Point) 단위로 나누고, 데이터를 송신자에서 RP까지 유니캐스트로 전송하고 RP에서 수신자까지는 멀티캐스트로 전송한다. 이러한 혼합적인 방식에 적합한 그룹키 관리 방식은 없다고 알려져 있다. 제안한 방식은 RP에 그룹 키를 관리하는 그룹키 관리자를 두어 송신자의 그룹 키를 RP에 부여하고 RP는 인증된 수신자에게 그룹키를 전달한다. 송신자는 데이터를 그룹키로 암호화하여 RP에 전송하고 RP는 암호화된 데이터를 부그룹 내 수신자에게 전송하고, 수신자는 이전에 받은 그룹키를 이용하여 데이터를 복호화한다. 따라서 제안한 방식은 PIM-SM 라우팅 구조의 변형 없이 사용하여 기존의 그룹 키 관리 구조에 비해 간단함을 알 수 있고 라우팅의 경로 변경에도 그룹키를 미리 받음으로 키의 재분배 없이 사용이 가능하고 키 관리자의 경유에 따른 데이터 변환작업이 불필요하여 데이터 전송시간이 단축됨을 알 수 있다.

Ⅱ. 관련 연구

2.1 멀티캐스트 그룹키

그룹키의 사용은 허용된 그룹의 멤버들만이 정보를 얻도록 하기 위한 것으로 그룹내 멤버가 아니면 그룹키를 알아내지 못하도록 하는 것은 멀티캐스트 정보보호의 기본 조건이라 할 수 있다. 따라서 멀티캐스트 그룹키는 멤버의 그룹 가입(Join)과 기존 멤버의 그룹 탈퇴(Leave)에 따라 현재 그룹키를 새로운 그룹키로 변환하는 키 재분배 과정을 거쳐야 한다. 이는 forward secrecy와 backward secrecy를 만족하기 위해서 이다[9].

2.2 기존 멀티캐스트 그룹키 관리 방식의 문제점

Naïve 방식[4], Iolus 방식[4], Nortel 방식[5][6]에서 제안된 방식은 많은 멤버를 갖는 대규모의 그룹키 관리 방식으로 부그룹의 규모가 매우 크다. 따라서 부그룹 내에 하나의 멤버가 탈퇴해도 부그룹 내에 모든 멤버들에게 그룹키의 재분배 과정을 수행하여야 하기 때문에, 빈번한 이동이 있을 경우 많은 키 재분배 시간을 요구한다. 또한, Naïve 방식, Iolus 방식의 그룹 키 관리는 단일 노드의 오류가 전체 시스템의 결함을 일으키는 원인이 될 수도 있다. 제시한 기존의 그룹키 관리 방식은 동적으로 변경되는 경로 설정에 대해서 원활한 보호유지가 가능하지 않고, 데이터의 전송의 경우 키 관리자 경유에 따른 빈번한 그룹 키 변환으로 많은 데이터 전송시간이 필요하게 된다. 따라서 이를 해결하고 소규모의 멤버 규모에 적합한 라우팅을 지원하는 그룹키 관리 구조가 필요하다[5][6].

III. PIM-SM 그룹키 관리 구조 및 프로토콜 제안

3.1 PIM-SM 그룹키 관리 구조

제안한 PIM-SM 그룹키 관리 구조는 그림 1과 같은 구성요소로 되어있다. 이중 RP(Rendezvous-Point)는 각 수신자에 대해 제어, 키 관리, 데이터 수신 등의 기능을 수행하며, 각 RP를 기준으로 부그룹을 분류하는 기준이 되고 하나의 키 관리자를 부여한다. DR(Designated-Router)은 송신자와 수신자에 가장 근접된 라우터로 RP에 대한 정보를 갖고 경로설정을 수행한다. 송신자는 키 변환기를 갖고 각 부그룹의 그룹키로 데이터를 암호화하여 전송한다. 키 관리자로부터 받은 송신자의 그룹키를 이용하여 메시지를 암호화하여 RP로 전달하고, 수신자는 RP로부터 받은 데이터를 설정된 보호채널의 비밀키를 이용하여 그룹키를 복호화한다. 여기서 보호채널은 멀티캐스트 그룹이 설정되기 이전에 수신자와 RP간에 미리 설정된 논리적인 경로를 의미한다. 제안한 그룹키 관리구조는 SPT(Shortest Path Tree)의 경로 변경에도 송신자의 그룹키가 변경되지 않으므로 변환과정 없이 쉽게 복호화가 가능하게 된다[7].

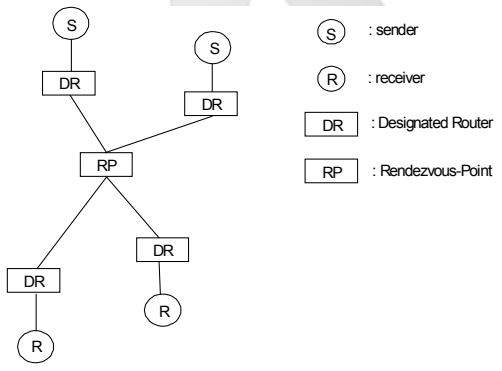

그림 1. PIM-SM 그룹키 관리 구조
Fig. 1 The Architecture of managing PIM-SM Group Key

3.2 PIM-SM 그룹키 관리 프로토콜

3.2.1 송신자의 멀티캐스트 그룹 등록

송신자의 멀티캐스트 등록은 부그룹을 관리하는 RP를 통한 그룹키 전달에 따른다.

① 송신자 S`는 등록을 요구하는 IGMP를 DR에게 전송한다.
② DR은 부그룹을 관리하는 각 RP에게 S`에 대한그룹 가입을 알린다.
③ 송신자 S' 인증이 승인되면, 각 RP는 DR에송신자에 할당된 그룹키를 전송한다.
④ 송신자 S'은 설정된 보호채널을 통해 그룹키를 암호화하여 수신자에게 전송한다.
⑤ DR은 각 RP에서 받은 그룹키들을 송신자 S`에게 전송한다.

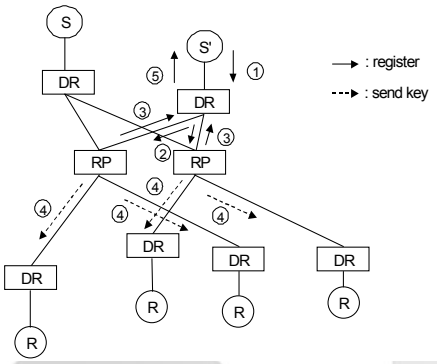

그림 2. 송신자의 그룹 등록 과정
Fig. 2 Sender Registration

3.2.2 송신자의 그룹 탈퇴

그룹을 탈퇴한 송신자 S'을 가장한 침입자가 그룹 내 수신자에게 데이터를 전송할 수 있기 때문에 송신자의 멀티캐스트 그룹 탈퇴시 모든 수신자에게 S'의 그룹 탈퇴 메시지를 각 수신자에게 전송하여야 한다.

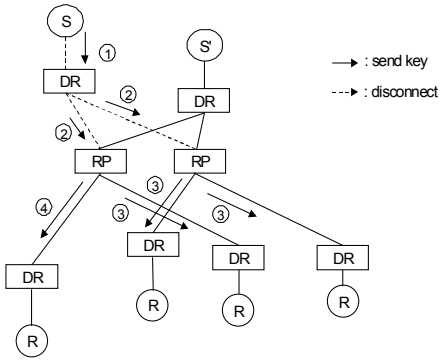

그림 3 송신자의 그룹탈퇴 과정
Fig. 3 Sender Leave Phase

① 송신자 S′는 DR에게 탈퇴를 요구하는 IGMP를 전송한다.
② DR은 각 RP에게 송신자의 탈퇴를 알리는 IGMP를 전달하고, DR과 RP와의 경로 취소를 요구한다.
③ RP는 수신자에게 탈퇴 메시지를 전달한 후, 송신자 S′과의 경로연결을 해제한다.

3.2.3 수신자의 멀티캐스트 그룹 가입 프로토콜

새로 가입한 수신자 R′은 가입하기 이전에 존재하는 그룹키를 알 수 없도록 하기 위해서 부그룹 전체에 새로운 키를 재분배해야 한다. 이는 backward secrecy를 만족하도록 하기 위한 절차이다.

① 수신자 R′는 DR을 거쳐 RP에게 등록을 요구하는 IGMP를 전송한다.
② 수신자 R′이 승인되면, RP는 수신자들에게 그룹키를 재분배한다.
③ RP는 송신자들에게 그룹키를 재분배하기 위해 DR에게 새로운 그룹키를 전송한다.
④ DR은 송신자에게 RP에게 받은 새로운 그룹키를 전송한다.

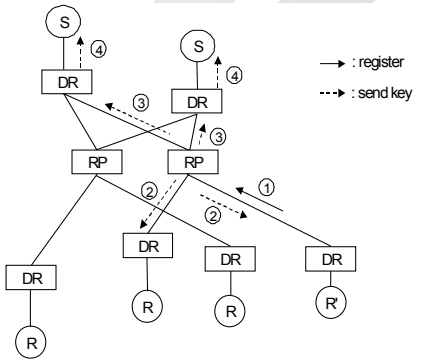

그림 4. 수신자의 그룹 등록 과정
Fig. 4 Receiver Registration

3.2.4 수신자의 멀티캐스트 그룹 탈퇴 프로토콜

그룹 탈퇴에 따른 그룹키의 재분배는 forward secrecy를 위해 필요하기 때문이며, 다음과 같이 진행된다.

① 수신자는 RP에게 탈퇴를 요구하는 IGMP를 전송한다.
② RP는 부그룹의 다른 수신자들에게 보호채널을 통하여 새로운 키를 재분배한다.
③ RP는 송신자들에게 그룹키를 재분배하기 위해, 새로운 그룹키를 DR에게 전송한다.
④ RP에서 전송받은 DR은 송신자들에게 그룹키를 재분배 한다.

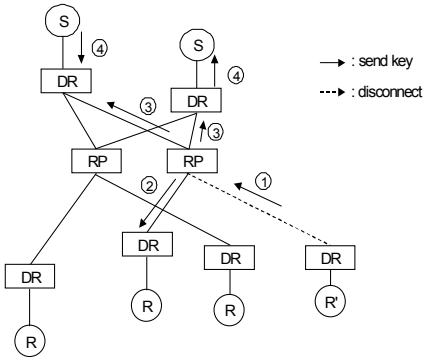

그림 5. 수신자의 그룹 탈퇴 과정
Fig. 5 Receiver Leave Phase

3.2.5 SPT의 경로 설정

SPT(Shortest Path Tree)의 경로 설정과정에서 송신자는 기존의 그룹키를 그대로 사용하게 되어, 수신자는 SPT의 경로로부터 받은 데이터에 대하여 새로운 키 분배 없이 데이터를 복호화 할 수 있다.

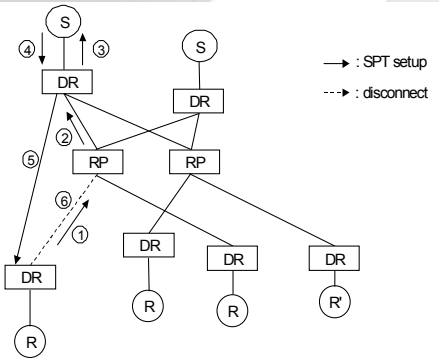

그림 6. SPT의 경로설정 과정
Fig. 6 SPT Establishment

① 수신자는 RP에게 SPT의 경로를 요구하는 ICMP를 전송한다.
② RP는 DR에게 SPT의 경로변경 메시지를 전송하고, DR은 수신자에 대한 SPT의 경로를 결정한다.
③ DR은 송신자에게 수신자에 대한 데이터 전송메시지를 전송한다.
④ 송신자는 데이터를 각각의 그룹키로 암호화하여 DR에게 전송한다.

⑤ DR은 수신자에게 설정된 SPT의 경로로, 나머지 수신자들에게는 멀티캐스트로 데이터를 전송한다.
⑥ 데이터를 수신한 수신자는 RP와의 경로연결을 해제한다.

SPT의 경로 설정은 RP를 중심으로 한 부그룹 관리를 우선으로 한 것이 아니라 최단 경로를 찾는데 중점을 두고 있다. 따라서 SPT의 경로설정을 위해 RP와의 경로 연결 해제를 하고, 이로서 데이터 전송시간을 단축할 수 있게 한다.

3.2.6 데이터 전송 프로토콜

분리된 그룹의 각 키 관리자는 서로 직접적인 정보전달이 필요 없으므로 추가적인 경로 설정이 필요 없게 된다.

① 송신자는 각 부그룹에게서 받은 그룹키로 데이터를 암호화하여 DR에게 전송한다.
② DR은 각 부그룹의 RP에게 그룹키에 의한 데이터 변환 없이 RP에게 전송한다.
③ RP는 부그룹에 속한 모든 수신자에게 그룹키에 의한 데이터 변환과정 없이 전송한다.

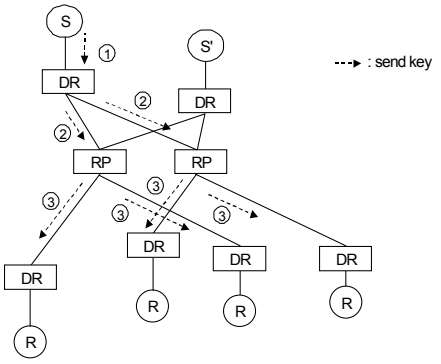

그림 7. 데이터 전송 과정
Fig. 7 Data Transmission

Ⅳ. 실험 및 성능 분석

실험 및 성능분석을 위하여, 실제의 네트워크 위상을 갖는 네트워크를 모델링하기 위한 Waxman의 그래프 모델[8]에 근거한 그래프를 구성하였다. 이는 PIM-SM 라우팅 프로토콜의 특징인 소수의 송신자와 원거리에 있는 RP에 속한 다수의 수신자 상태를 고려하였다. 본 실험에서는 제안한 그룹키 관리 방식과 기존의 그룹키 관리 시스템인 Iolus 방식, Nortel 방식과의 성능을 비교 평가하기 위하여 제시한 모델에서 멀티캐스트 트래픽 전송속도와 키 변환에 필요한 소요시간을 비교하였다. 본 실험에서는 라우터에서의 전송지연 시간, 키의 생성시간은 별도로 고려하지 않았다. 실험은 범용 시뮬레이션 언어인 SIMSCRIPT II.5를 사용하였다.

각 라우터에 속한 호스트가 데이터를 전송할 때, 각 부그룹에서 데이터를 수신하는데 걸리는 시간을 측정한 결과는 각 라우터에 속한 호스트까지 데이터가 전달되는 평균시간을 (그림 8)에 나타냈다.

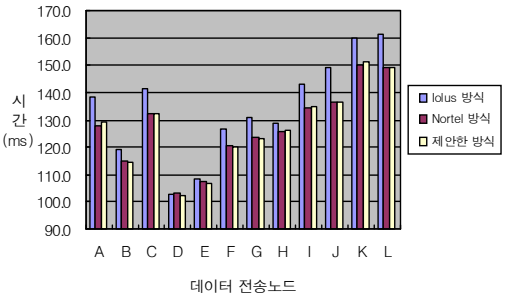

그림 8 . 데이터 전송 평균시간
Fig. 8 Average Time of the Data Transmission

제안한 PIM-SM 그룹키 관리 방식은 비교실험에서 데이터 평균 전송시간에서 가장 적게 소요되는 것을 보였다.

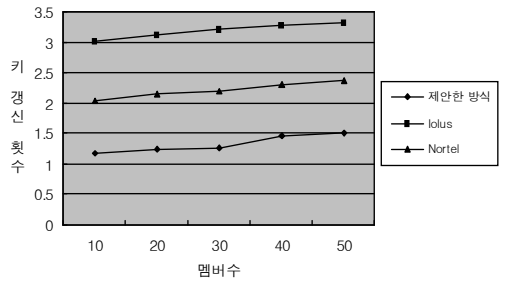

그림 9. 멤버의 평균 키 갱신 횟수의 평균값
Fig 9. Average values of average key update counts

또한 제안한 그룹 키 방식을 이용하여 발생하는 부하를 기존의 방식과 비교하기 위해 다음의 실험을 수행하였다. 제안한 방식은 소규모의 라우팅 구조에 적합하므로 50개 이하에서 임의로 제시하였다. 각 그룹키 방식의 시뮬레이션

환경에서 수행횟수를 임의적으로 제시하고 멤버의 가입 및 삭제의 발생을 랜덤하게 발생하도록 한 후, 각 멤버가 수행하는 키 갱신 개수의 평균을 구하고, 이에 대한 평균값을 구하였다.평균 키 갱신 횟수의 평균값은 제안한 방식에 비해 대략적으로 Iolus가 약 3배, Nortel이 약 2배가 많은 것으로 분석되었다. 따라서 키 갱신에 따른 부하는 제안한 방식이 기존의 방식에 비해 부하가 적음을 알 수 있다.

V. 결 론

본 논문에서 제안한 PIM-SM 그룹키 관리 방식은 RP 단위로 부그룹을 나누고, 각 RP는 송신자에게 송신자 고유의 그룹 키를 두어 SPT 경로로의 데이터 전달에도 새로운 키 분배 없이 바로 전송이 가능하다. 또한 각 RP간 데이터 전송이 없으므로 분산구조의 형태가 되어 PIM-SM에서도 모든 사용자가 정당한 보호를 받고, 부그룹에 따른 키 변환 작업이 불필요하여 전송시간이 기존의 방식에 비해 적게 소요됨을 알 수 있다. 또한 실험결과 기존의 Iolus, Nortel 그룹키 방식에 비해 키 갱신에 따른 부하가 적고 데이터 전송 시간이 단축됨을 알 수 있었다.

제안한 그룹키 관리 구조는 소규모 서비스를 요구하는 시스템에도 적용이 가능할 뿐만 아니라 건물 내에 화상회의 시스템, 캠퍼스와 같은 지역적으로 독립된 네트워크 환경에서 다른 서비스에 대한 대역폭 점유 없이 사용되어야 할 때 적합한 그룹키 관리 모델로 활용 될 수 있다.

참고문헌

[1] 홍종준, "RTP를 위한 보안 제어 프로토콜 구현", 한국컴퓨터정보학회, 제8권 제3호, pp. 144-149, 2003.

[2] 한근희, "멀티캐스트의 정보보호", 정보처리학회학회지, 제7권 제2호, pp.34-40, 2000.

[3] 이동철, 홍종준, "온라인게임에서 QoS 라우팅을 위한 부하균등 비용산정 방식", 한국컴퓨터정보학회, 제8권 제1호, 2003.

[4] Suvo Mittra, "Iolus : A Framework for Scalable Secure Multicasting," Computer Communication Review, Vol.27, No.4, pp.277-288, 1997.

[5] Thomas Hardjono, Brad Cain, N. Doraswamy., "A Framework for Group Key Management for Multicast Security," draft-ietf-ipsec-gkmframework-03.txt, Aug., 2000.

[6] Thomas Hardjono, Brad Cain, "Intra-Domain Group Key Management Protocol," draft-ietf-ipsec-intragkm-02.txt, Feb., 2000.

[7] D. Estrin, "Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification," RFC 2362, Jun., 1998.

[8] B. M. Waxman, "Routing of Multipoint Connections," IEEE J. Select. Areas Commun., Vol.6, No.9, pp.1617-1622, Dec., 1988.

[9] A. Perrig, D. Song, J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution," 2001 IEEE Symposium on Security and Privacy, 2001.

[10] J. Cui, M. Faloutsos, D. Maggiorini, M. Gerrla, and K. Boussetta, "Measuring and Modeling the Group Membership in the Internet," IMC2003, 2003

[11] R. Chalmers and K. Almeroth. On the topology of multicast trees. UCSB Technical Report, Mar. 2002.

저 자 소 개

홍 종 준

현재 평택대학교 정보과학부 정보통신학전공 교수

<관심분야> 네트워크보안, QoS라우팅, 분산시스템