IGMPv3 인증을 위한 키 분배기법

강현선*, 김민경*, 박창섭*
*단국대학교 전자계산학과
e-mail : sshskang@dankook.ac.kr

A Key Distribution Scheme for IGMPv3 Authentication

Hyun-Sun Kang*, Min-Kyoung Kim*, Chang-Seop Park*
*Dept. of Computer Science, Dankook University

요 약

IGMP(Internet Group Management Protocol)는 멀티캐스트 그룹의 멤버쉽 관리를 위한 프로토콜로서, 임의의 호스트가 멀티캐스트 라우터에게 특정한 멀티캐스트 통신의 수신을 요청할 경우에 사용된다. 본 논문에서는 이와 같은 IGMP 메시지를 이용한 정당하지 않은 호스트의 DoS 공격 등으로부터 멀티캐스트 분배트리의 보호를 위한 수신자 접근제어 기법을 제안한다. 또한 제안기법은 수신자 접근제어 기능뿐만 아니라, 실제 다양한 상업적인 멀티캐스트 서비스에도 적용될 수 있는 비즈니스 모델을 기반으로 하며 과금과 관련하여 활용이 가능하다.

1. 서론

멀티캐스트 통신은 일대다(one-to-many)와 다대다(many-to-many) 통신을 위한 효율적인 전송 메커니즘을 제공한다. 즉, 하나의 그룹주소를 목적지로 하여 다수의 그룹멤버에게 패킷을 전달하기 위한 통신으로 효율적인 전송 메커니즘으로써, 이와 관련하여 다양한 멀티캐스트 라우팅 프로토콜이 존재한다. 멀티캐스트 라우팅 프로토콜은 그룹멤버에게 패킷을 전달하기 위해 네트워크 내에 존재하는 그룹멤버에 대한 정보를 유지해야 하며, IGMP(Internet Group Management Protocol)[1][2]가 이를 위한 메커니즘이다. IGMP 는 멀티캐스트 그룹의 멤버쉽 관리를 위한 프로토콜로서, 임의의 호스트가 특정한 멀티캐스트 그룹통신의 수신을 멀티캐스트 라우팅 시스템으로 요청할 경우에 사용된다. 호스트의 특정 그룹에 참여를 요청하는 메시지를 수신하면 멀티캐스트 라우터는 멀티캐스트 라우팅 프로토콜을 이용하여 멀티캐스트 분배트리로 요청 메시지를 전송하고, 멀티캐스트 분배트리가 해당 멀티캐스트 라우터까지 효율적으로 확장되며 호스트는 그룹통신을 수신할 수 있게 된다.

현재 멀티캐스트 환경에서는 IGMP 메시지를 통하여 어떠한 호스트라도 쉽게 멀티캐스트 그룹멤버가 될 수 있다. 따라서 멀티캐스트 통신의 도청이 발생할 수도 있으며, 멀티캐스트 통신의 보호를 위해 일반적으로 멀티캐스트 데이터를 암호화하여 송신하고, 정당한 그룹멤버에게 복호화키를 분배하여 멀티캐스트 서비스를 제공받는 방식을 사용한다. 하지만 암호화된 통신만으로는 정당하지 않은 호스트에 의한 트래픽 분석이나 악의를 가진 호스트의 DoS(Denial of Service) 공격에는 여전히 취약하다. 즉, 해당 네트워크로 다수의 멀티캐스트 분배트리를 확장하여 네트워크 대역폭과 멀티캐스트 라우터의 리소스의 낭비를 초래할 수 있으며, 이를 통해 궁극적으로는 DoS 공격도 가능하게 된다. 이러한 멀티캐스트 모델에서의 문제점을 해결하기 위해서는 [3]에서 처음 수신자 접근제어가 언급되었으며, 현재 수신자에 대한 접근제어 뿐 아니라 송신자에 대한 접근제어도 다양한 방식으로 연구되고 있다.

송, 수신자 접근제어와 관련하여 제안된 기법으로는 디지털 서명을 기반으로 하는 [6][7][8]과 공유한 비밀키를 기반으로 하는 [5][9][10][11][12] 등이 있다. 본 논문에서는 안전한 멀티캐스트 통신을 위해 반드시 수행되어야 하는 IGMP 접근제어 메커니즘을 제안한다. 해당 프로토콜은 실제 다양한 상업적인 멀티캐스트 서비스에도 적용될 수 있는 비즈니스 모델을 기반으로 하므로, 수신자 접근제어 기능뿐만 아니라, 과금과 관련하여 활용이 가능하다. 2 장에서는 수신자 접

근제어와 관련한 기존연구를 소개하고, 3 장에서 제안 프로토콜의 설계원리와 동작과정을 제안한다. 4 장에서는 제안 프로토콜과 기존연구와 간단히 비교하고, 결론을 맺는다.

2. 기존연구

일반적으로 IGMP 인증을 위해서는 이미 구축된 PKI 기반의 공개키 또는 공유된 비밀키를 사용한다. 공개키를 사용하는 방식은 이미 구축된 PKI 를 기반으로 하므로 인증과 관련한 키의 관리는 수월하지만, 인증자는 계산량이 큰 서명확인 작업을 수행해야 하며, 이를 통해 DoS 공격이 발생할 수 있다는 문제점이 있다. 반면 비밀키를 사용하는 방식은 계산량 측면에서는 비교적 효율적이지만, 사전에 개체간에 비밀키 공유에 따른 키 관리의 어려움이 있다. 따라서, IGMP 인증을 위해서는 안전성 측면과 함께 함께 키 관리 방안이 고려되어야 한다.

[6][7][8]은 이미 구축된 PKI 를 기반으로 사전에 공개키가 공유되었음을 전제로 프로토콜을 소개한다. 즉, 개인키로 계산한 서명값을 제시함으로써 IGMP 인증을 수행하게 된다. 특히, [8]에서는 CBA 를 기반으로 제안된 방식으로 GCKS 는 자신이 생성한 개인키/공개키 쌍을 안전한 채널을 통해 호스트에게 분배하고, 분배 받은 개인키로 계산한 서명값과 공개키를 IGMP 인증에 사용하게 된다. 이 방식들은 공개키 방식으로 DoS 공격이 발생할 수 있다.

[9][10][12]에서는 IGMP 인증을 위해 비밀키를 사용하므로 위에서 발생 가능한 공격에 비교적 대응적이다. 시도-응답 메커니즘을 사용하며, 사전에 AAA 서버와 호스트 간의 비밀키 공유를 전제로 프로토콜이 소개되는 제약이 있다. 반면 [5][11]은 IGMP 인증에 비밀키를 사용하며, [5]에서는 토큰(token)을 통한 비밀키 분배에 대해 다루고 있다. 위의 방식은 다른 기존기법들에 비교적 DoS 공격에 대응적이며 현실성이 있다. 하지만, 실제 다양한 상업적인 서비스에 활용 가능한 멀티캐스트 비즈니스 모델로 적용하기에는 여전히 부족한 면이 있다.

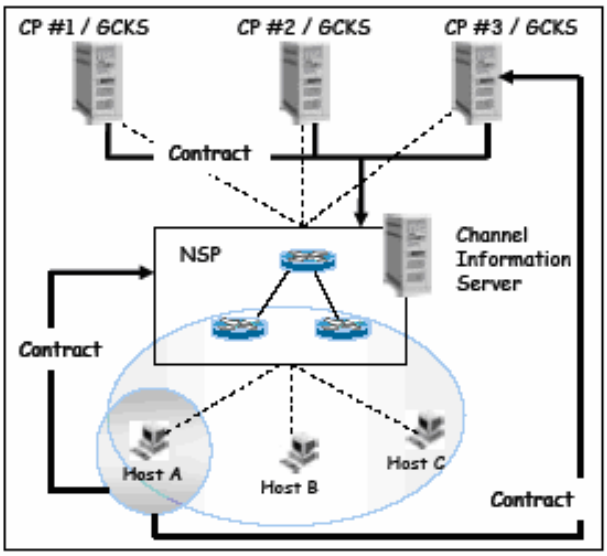
3. 제안 프로토콜

이번 장에서는 본 논문에서 제안하는 프로토콜에 대해 소개한다. 프로토콜의 이해를 돕기 위해 우선 프로토콜의 설계원리를 간단히 소개한 후, 제안 프로토콜을 단계별로 설명한다.

3.1 설계원리

3.1.1 비즈니스 모델

멀티캐스트 서비스는 무료의 정보를 효율적으로 분배하기 위해 사용 되어질 수도 있지만, 실제 다양한 상업적인 서비스에도 활용될 수 있다. 유료로 서비스되는 상업적인 멀티캐스트 서비스 환경에서 서비스 제공자는 해당 서비스에 대한 수신자 접근제어 기능은 물론 과금과 관련한 정보도 확보해야 한다. 하지만 현재의 IGMP 표준은 물론 기존의 관련연구에서는 이러한 요구사항을 충분히 만족시키지 못하며, 때문에 실제 상업적인 서비스 모델에 적용하기에는 한계가 있다. [4]에서는 현실적인 접근과 관련하여 제공되어야 할 과금, 접근제어 등의 기능들에 대해 언급하였으며, 이와 관련하여 멀티캐스트 서비스 네트워크 모델을 제시하였다. 다음의 그림은 [4]에서 제시한 멀티캐스트 서비스 네트워크 모델을 나타내며, 본 논문에서는 아래의 모델을 기반으로 프로토콜을 제안한다.



(그림 1) 네트워크 아키텍처

위의 모델은 크게 CP(Content Provoder), NSP(Network Service Provider), Host 등 세 부분으로 구성된다. CP 는 NSP 의 네트워크를 통해 각 그룹멤버들에게 멀티캐스트 서비스를 제공하고, NSP 는 네트워크 리소스를 유지, 관리하는 개체로서 멀티캐스트 서비스를 그룹멤버에게 전달하는 역할을 담당한다. CIS(Channel Information Server)에서는 모든 멀티캐스트 채널에 대한 정보를 유지한다.

3.1.2 Kerberos 프로토콜

Kerberos 는 특정 개체의 인증 및 세션키 분배를 위한 시스템으로써, 클라이언트-서버 환경 하에서 여러 유형의 응용 서버로부터 서비스를 요구하는 워크스테이션의 사용자들에 대한 인증 목적으로 사용된다. Kerberos 에서 클라이언트는 여러 응용 서버들과 인증에 요구되는 각각의 공통된 비밀키를 유지하는 대신, 중앙 집중적인 Kerberos Server(KS)와 대칭키를 공유함으로써 특정 응용 서버의 인증에서 요구되는 티켓을 부여받고 일정기간 응용 서버의 서비스를 제공받을 수 있다. 즉, 특정 응용서버의 서비스를 요구하는 클라이언트는 먼저 KS 에게 서비스 제공을 위한 일종의 티켓을 요청한다. KS 는 클라이언트를 확인한 후 클라이언트와의 대칭키를 이용하여 자신이 생성한 세션키를 암호화한 후 응용서버로의 티켓과 함께 클라이언트에게 보낸다. 클라이언트는 자신의 대칭키를 이용하

여 KS 가 보낸 세션키를 얻을 수 있으며, 특정 응용서버의 서비스를 받을 수 있는 티켓을 응용 서버에게 보낸다. 응용서버는 티켓을 통해 클라이언트를 인증하게 되고, 클라이언트는 티켓의 유효기간 동안 해당 응용서버로부터 서비스를 제공받을 수 있게 된다.

3.2 제안 프로토콜

이번 절에서는 IGMPv3 를 기반으로 하는 멀티캐스트 네트워크에서의 수신자 접근제어 프로토콜을 제안한다. IGMPv3 에서 그룹멤버는 *Query* 메시지에 대해 모두 응답해야 하며, 본 논문에서는 이러한 특성을 접근제어 메커니즘에 이용한다.

본 논문에서 *CP/GCKS*, *CIS*, *Host*는 CP/GCKS, CIS, Host 각각의 IP 주소를 나타내고, $h(\ )$는 일방향 해쉬함수를 나타낸다. $MAC(K)$는 선행하는 모든 데이터를 키 K를 이용하여 계산한 MAC(Message Authentication Code) 값을 의미하고, $[m_1, m_2]K$는 데이터 m_1과 m_2를 연결하여 키 K를 이용하여 암호화한 값을 의미한다. K_{GC}는 CP/GCKS와 CIS의 공유한 대칭키를, K_{MR}은 CIS와 몇몇의 멀티캐스트 라우터 사이의 공유한 대칭키를 나타낸다. (P_R, S_R)과 (P_G, S_G)는 각각 멀티캐스트 라우터와 CP/GCKS의 공개키/개인키 쌍을 나타내며, $Sig(S)$는 모든 선행하는 데이터를 서명용 개인키 S로 디지털 서명값을 나타낸다. 다음에서는 새로운 IGMP와 함께 주소할당(Address Allocation) 프로토콜, 등록(Registration) 프로토콜, 티켓-발행(Ticket-Issuing) 프로토콜을 함께 제안한다.

3.2.1 주소할당 프로토콜

CP/GCKS는 멀티캐스트 서비스에 사용할 멀티캐스트 주소를 주소할당 프로토콜을 통하여 CIS에게 요청한다. 이 과정을 통해 CP/GCKS는 CIS와 공유한 K_{GC}를 통해 안전하게 CIS로부터 *Exp*를 유효기간으로 갖는 멀티캐스트 주소 *m_address*를 할당 받는다. 여기서 SAP(Session Announcement Protocol)[17]에서 사용하게 될 채널정보 *Channel_Info*는 (*CP*, *m_address*, *Exp*)와 같다.

3.2.2 등록 프로토콜

특정 멀티캐스트 그룹통신에 가입을 원하는 호스트는 CP/GCKS와 등록 프로토콜을 수행하며, 이 과정에서 호스트는 암호화된 멀티캐스트 통신과 암호화된 키의 복호화를 위한 그룹키와 KEKs를 제공 받는다. 본 논문의 등록 프로토콜에서는 위의 두 키와 함께 다음과 같은 접근제어를 위한 정보를 제공받는다. K_{Net}은 *Authentication_Ticket*을 통해 호스트와 CIS가 공유하게 될 키를 나타낸다. x_n은 CP/GCKS가 해쉬체인 생성을 위해 임의로 선택한 seed 값으로 이를 바탕으로 길이가 n인 해쉬체인을 생성하며, x_0은 생성한 해쉬체인의 루트(root) 값을 나타낸다.

Channel_Info, (K_{Net}, n, x_n), *Authentication_Ticket*.
Authentication_Ticket = [*Host*, *Channel_Info*, K_{Net}, P_G, $(n, x_0, Sig(S_G))]K_{GC}$.

3.2.3 티켓-발행 프로토콜

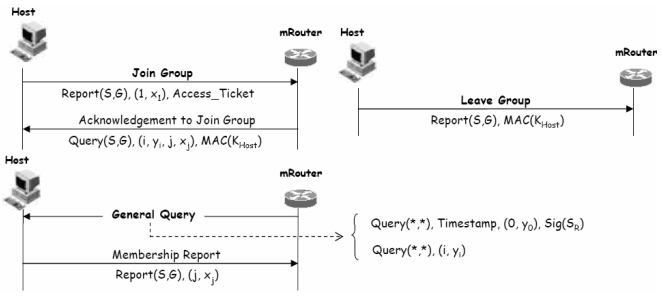
티켓-발행 프로토콜은 호스트와 멀티캐스트 라우터의 대칭키 공유를 위해 호스트와 CIS 사이의 메시지 교환을 나타낸다. 호스트가 *Access Ticket Request* 메시지를 CIS로 보내면 CIS는 해당 메시지에 포함된 티켓을 복호화하고, 호스트를 위한 새로운 티켓을 생성하여 *Access Ticket Grant* 메시지를 구성하여 호스트에게 전송한다. K_{Host}는 호스트와 라우터의 공유키로 호스트는 *Exp* 때까지 *Channel_Info*, K_{Host}, P_R, (n, x_n), *Access_Ticket*의 정보를 유지하며, 해당 티켓은 처음 그룹통신에 참여할 때 사용한다.

Access Ticket Request message:
CP/GCKS, *Authentication_Ticket*
Access Ticket Grant message: *Access_Ticket*, $[K_{Host}, P_R,$ *Timestamp*$]K_{Net}$
Access_Ticket = [*Subnet_Prefix*, *Channel_Info*, K_{Host}, $(n, x_0)]K_{MR}$

3.2.4 Authenticated IGMP

제안 프로토콜에서는 질의 인덱스와 그룹 인덱스가 각각 존재한다. 멀티캐스트 라우터는 해당 서브넷에 그룹멤버의 존재여부를 위해 주기적으로 *General Query* 메시지를 멀티캐스트 하는데, 해당 메시지에 대한 인증을 위해 사용 가능한 해쉬체인 값과 관련한 것이 질의 인덱스이고, 최초의 *General Query* 메시지에 포함되어 호스트에게 전해진다. 해당 메시지에 대한 *Report* 메시지의 인증을 위해 사용 가능한 해쉬체인 값과 관련한 것이 그룹 인덱스이다.

$Host_1$이 $(S, G) = (CP, m\_address)$ 통신에 처음으로 참여를 원할 경우, 다음의 그림과 같이 *Join Group* 메시지를 멀티캐스트 라우터에게 전송한다. 해당 메시지에서 Report(S, G) 는 멤버쉽 report 메시지와 관련된 파라미터를 나타내고, *Access_Ticket*은 티켓-발행 프로토콜에서 CIS로부터 제공받은 것이다. 라우터는 CIS와 K_{MR}을 공유하고 있으므로 *Access_Ticket*을 복호화할 수 있고, 메시지내의 해쉬체인 값과 티켓내의 해쉬체인 값을 확인한다. 라우터는 *Join Group* 메시지에 대한 응답 메시지를 생성하여 호스트에게 전송한 후 그룹에 대한 정보 < $(CP, m\_address)$, $(x_0, j = 1, x_j, Exp)$, $\{(Host_1, K_{Host_1})\}$ >를 유지한다.



(그림 2) Authenticated IGMP

만약 호스트가 (*S*, *G*) 통신의 수신을 중지할 경우, 호스트는 라우터에게 *Leave Group* 메시지를 송신한다. IGMPv3 에서는 suppression 기능이 제공되지 않기 때문에 라우터는 모든 그룹멤버를 유지할 수 있으며, *Leave Group* 메시지를 수신하면 라우터는 (*S*, *G*)의 정보에서 해당 호스트만 삭제하면 된다.

4. 기존기법과 비교 및 결론

이번 장에서는 제안 프로토콜과 기존연구에서의 수신자 접근제어 기법을 비교한다. 비교를 위해 접근제어를 위해 사용한 인증방식, DoS 공격에 대한 안전성, 키 관리 등으로 각각 구분하여 설명한다.

4.1 인증방식과 안전성

기본적으로 IGMP[1][2]에는 인증방식이 제공되지 않는다. 디지털 서명을 사용하여 접근제어를 수행하는 방식으로는 [6][7][8] 등이 있으며, 이 방식들은 서명을 확인해야 하는 개체에서 발생하는 계산 오버헤드가 크므로 DoS 공격이 발생할 수도 있다. DoS 공격은 최근 인터넷 환경에서 가장 빈번히 발생하는 공격 중 하나이기도 하다. [9][10]에서는 시도-응답 방식과 [5]에서는 MAC 을 사용하며, 실제 [5][11]을 제외한 모든 방식들 역시 DoS 공격에 안전하지 못하다. 반면, 제안 프로토콜은 인증을 위해 해쉬체인을 사용한다. 따 DoS 공격에 안전하며, 본 논문에서 해쉬체인은 인증을 위한 목적 외에도 상업적인 멀티캐스트 서비스에서의 과금과 관련한 정보로 활용될 수 있다.

4.2 키 관리

위 절에서 살펴본 것과 같이 디지털 서명을 이용하여 인증을 수행하는 방식은 DoS 공격이 발생할 수 있으며, 이에 비해 비밀키를 이용하여 인증을 수행하는 방식은 비교적 DoS 공격에는 안전하다. 하지만, 서로 다른 개체 사이에 비밀키를 공유하는 것은 어려움이 있다. 몇몇 기존연구에서는 비밀키를 미리 공유함을 가정[9][10][11][12]하고 프로토콜을 제안하기도 하며, [5][6]은 토큰을 이용하여 키 분배를 수행한다. 본 논문에서는 실제 멀티캐스트 서비스에 적용을 위해 티켓을 이용하여 개체 사이의 공유키 분배를 제시하였다.

위에서 본 것과 같이 제안 프로토콜은 수신자 접근제어를 위해 해쉬체인을 사용하며, 이로써 DoS 공격에 대응적일 수 있다. 또한 상업적인 비즈니스 모델에 기반하여 프로토콜을 설계하였으므로, 실제 멀티캐스트 서비스로의 적용에 현실성이 있다.

참고문헌

[1] W. Fenner, "Internet Group Management Protocol, Version 2," RFC 2236, Nov. 1997.

[2] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Inter-net Group Management Protocol, Version 3," RFC 3376, Oct. 2002.

[3] L. Gong and N. Shacham, "Elements of trusted multicasting," in Proceed-ings of the 2nd ACM Conference on Computer and Communications Secu-rity, Fairfax, Virginia, 1994, pp. 176-183.

[4] T. Hayashi, H. He, H. Satou, H. Ohta, S. Vaidya, "Accounting, Authenti-cation and Authorization Issues in Well Managed IP Multicasting Services", Internet Draft, draft-hayashi-maccnt-02.txt, Feb. 2005

[5] T. Hardjono and B. Cain "Key Establishment for IGMP Authentication in IP Multicast," ECUMN, France, Oct. 2000, pp. 247-52.

[6] H. He, T. Hardjono, and B. Cain, "Simple Multicast Receiver Access Control," Internet draft, draft-irtf-gsec-smrac-00.txt, Nov. 2001.

[7] P. Judge and M. Ammar, "Gothic: A Group Access Control Architecture for Secure Multicast and Anycast, " IEEE INFOCOM, New York, June 2002, pp. 1547-56

[8] C. Castelluccia and G. Montenegro, "Securing Group Management in IPv6 with Cryptographically Based Addresses, "Proc. 8th IEEE International Symposium on Computer and Communication, Turkey, July 2003, pp. 588-93.

[9] N. Ishikawa, N. Yamanouchi, O. Takahashi, "IGMP Extension for Au-thentication of IP Multicast," Internet Draft, draft-ishikawa-igmp-auth-01.txt, Aug. 1998.

[10] N. Yamanouchi, N. Ishikawa, Takahashi, "RADIUS Extension for Mul-ticast Router Authentication," Internet Draft, draft-yamanouchi-radius-ext-00.txt, Mar. 1998.

[11] H. Ueno, H. Suzuki, N. Ishikawa, and O. Takahashi, "A Receiver Au-thentication band Group Key Delivery Protocol for Secure Multicast", IEICE Trans. on Comm.., vol. E88-B, no. 3, Mar. 2005, pp.1139-1148.

[12] T. Hayashi, D. Andou, H. He, W. Tawbi, and T. Niki, “IGMP for user Authentication Protocol (IGAP),” Internet Draft, draft-hayashi-igap-00.txt, Oct. 2002.

[13] B. Coan, V. Kaul, S. Narain, W. Stephens, "HASM: Hierachical Appli-cation-Level Secure Multicast," Internet Draft, draft-coan-hasm-00.txt, Nov. 2001.

[14] R. M. Needham and M. D. Schroeder, “Using Encryption for Authentica-tion in Large Networks of Computers,” Communications of the ACM, vol.21, 1978, pp.993-999.

[15] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, “Multicast Secu-rity (MSEC) Group Key Management Architecture,” RFC 4046, Apr. 2005.

[16] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no.11, 1981, pp. 770-772.

[17] M. Handley, C. Perkins, and E. Whelan, “Session Announcement Proto-col,” RFC 2974, Oct. 2000.

[18] M. Baugher, B. Weis, T. Hardjono, H. Harney, “The Group Domain of Interpretation,” RFC 3547, July 2003.

[19] T. Hayashi, H. He, H. Satou, H. Ohta, S. Vaidya, “Issues Related to Re-ceiver Access Control in the Current Multicast Protocols,” Internet Draft, draft-ietf-mboned-rac-issues-00.txt, July 2005.