

LBT 트리 기반의 멀티 캐스트 그룹 네트워크 관리 방식 제안

*서대희, *이임영, **나학연, **김춘수
*순천향대학교 정보기술공학부
**국가보안기술연구소

A Proposed scheme Multicast Group Network Management Based on LBT Tree

*Dae-Hee Seo, *Im-Yeong Lee, **Hac-Yun Na, **Chun-Su Kim
*Division of Information Technology Engineering, SoonChunHyang University
**National Security Research Institute

요약

최근 인터넷의 급속한 발전은 다양한 서비스를 창출하였으며, 모든 사용자에게 제공되던 브로드캐스팅 서비스에서 일부 사용자만을 위한 여러 가지 새로운 서비스로 변화하고 있다.

새로운 형태의 서비스의 경우 그룹 형태의 사용자들의 안전성을 보장하면서 효율적인 관리 구조에 대한 연구보다는 그룹의 서비스의 효율성에 목적을 두어 사용자의 프라이버시 침해에 대한 논란을 야기 시키고 있다.

따라서 본 논문에서는 기존의 멀티캐스팅 그룹 설정에 기반한 LBT 트리에 그룹 네트워크가 설정될 경우 그룹원들간의 안전성을 제공하면서 관리의 효율성과 확장성 갖는 관리 방식을 제안하고자 한다. 제안 방식은 LBT트리의 특징을 그대로 유지하면서 기존 방식에서의 안전성에 대한 취약점을 보완하여 보다 안전하고 효율적인 방식을 제안하였다.

다음은 기존의 멀티 캐스트 그룹 키 관리에 대한 연구를 분석한다.

1. 서론

최근 인터넷의 급속한 발전은 그룹이 다이나믹하게 변화할 때 멀티캐스트 그룹간의 신뢰성을 두고 연구를 촉진시키고 있다. 특히, 고정된 멤버와 다이나믹하게 변화하는 멤버와의 구분을 통한 신뢰 모델의 제시는 급속한 기술과 서비스 변화에 따른 요구사항이다.

모든 사용자가 아닌 일부 사용자만을 위한 멀티캐스트 개념은 1988년 최초 제기된 이후 많은 연구가 수행중에 있으나, 현재의 멀티캐스트 그룹 서비스에 대한 문제점으로는 키의 관리 뿐만 아니라 데이터의 전송에 따른 안전성과 확장성에서 공통된 문제점으로 제기되고 있다.

따라서 본 논문에서는 기존의 멀티캐스트 키 분배에서 키 설립과 분배에 따른 취약성을 보완하면서 빈번한 그룹키 갱신시 예측되는 보안 요구사항을 제시하고 이를 만족하는 방식을 제안하고자 한다.

① A Framework for Scalable Secure Multicasting 방식

1997년 Mittra에 의해 제안된 방식으로 많은 서브그룹과 이질적인 환경에서의 에이전트를 적용한 방식이다. 그러나 다음과 같은 문제점을 지적할 수 있다.

- GSA(Group Security Agent)를 이용하여 자 많은 서브그룹의 관리에 효율성을 유지하고자 하였으나 에이전트 활용에 따른 보안 취약성이 존재한다.

- 암호화 통신이 최상위 객체에서만 제공함으로써 하위 객체의 데이터 전송에 따른 보안 서비스를 제공하지 못한다.

- 많은 신뢰 객체와 서로 다른 암호/복호화 수행에 따른 전송 데이터의 신뢰성 문제가 발생한다.

② A Dual Encryption Protocol for Scalable Secure Multicasting 방식

LBT 방식을 이용하여 KEK(Key Encryption Key)을 이용해 키를 갱신하는 방법을 선택하였

2. 기존 네트워크 공격자 추적 방법

다. 그러나 다음과 같은 보안 취약점을 지적할 수 있다.

- 모든 멤버들이 루트의 그룹키를 사전에 공유해야 하는 문제점이 존재한다.
- 키를 갱신하기 위해 또 다른 암호화 키를 생성하여 갱신함으로써 키의 효율성이 저하된다.
- 멀티캐스트 그룹 멤버들이 서브 그룹으로 확장했을 경우 발생하는 계산량의 증가에 따른 비효율성이 문제시 된다.

③ Multicast Security : A Taxonomy and Some Efficient Constructions 방식

Canneti에 의해 제안된 방식의 경우 ②의 방식을 확장하여 신뢰할 수 있는 제 3의 객체를 이용해 각 멤버들간의 통신을 통해 안전한 멀티캐스트 보안을 제공하고자 하였다.

그러나 제안된 방식의 경우 다음과 같은 문제점을 내포하고 있다.

- 그룹 크기의 결정에서 송신자의 수를 고려하지 않은채 그룹의 크기를 결정함으로써 키 설정과 키 갱신 방식에 매우 비효율적이다.
- 다이나믹한 그룹 멤버들의 가입과 탈퇴에 따른 보안성을 고려하지 않는다.
- 멤버의 ID나 쿠키를 이용한 인증 정보 획득 공격이 가능하다.

3. 분산 네트워크에서 공격자 추적 기법의 보안요구사항

LBT 트리 기반의 멀티 캐스트 그룹 네트워크 관리 방식은 다음과 같은 요구사항을 만족할 수 있어야 한다.

① 객체간 통신의 기밀성

기존 방식과 같이 객체간의 통신은 기밀성이 유지되어야 한다. 그러나 KEK와 같이 기밀성 제공을 위한 키 이외에 또 다른 키를 설정 및 분배하여 키의 효율성을 저하시켜서는 안된다.

② 그룹 객체간의 인증

LBT 트리를 기반으로 멀티캐스트 그룹이 설정될 경우 그룹 객체간의 인증은 단일 인증 혹은 상위 객체에서 하위 객체로의 인증이 반드시 요구된다.

③ PFS 보장

멀티캐스트 그룹이 설정되어 보안 서비스를 위해 키를 설정할 경우 설립된 키의 경우 설립된 비밀 키가 노출되어도 키 설정에 대해 과거에 설립된 키가 노출되지 않아야 한다.

④ 객체 탈퇴에 대한 그룹의 효율성 유지

멀티캐스트 그룹에서 객체 탈퇴 이벤트가 발생할 경우 현재 탈퇴하는 노드에서만 탈퇴와 관련된 갱신과 객체 이동의 수행으로 전체적인 그룹 관리의 효율성을 제공할 수 있어야 한다.

4. LBT 트리 기반의 멀티 캐스트 그룹 네트워크 관리 방식 제안

본 논문에서는 LBT 트리를 기반으로 하여 그룹원 가입에 따른 멀티캐스트 그룹이 설정되었을 경우 각 그룹원에 대한 가입과 탈퇴시에 발생하는 이벤트와 통신의 안전성을 유지할 수 있는 방식을 제안하고자 한다.

4.1 가정사항

- LBT 트리를 기반으로 SM과 DM의 초기화 설정이 완료된 그룹이다.
- SM(Static Member)은 가입과 탈퇴가 제한된 객체로써 하위에 DM을 하위 그룹원으로 관리할 수 있는 객체이다.
- DM(Dynamic Member)은 이동성을 갖는 객체로써 SM의 하위 객체로 소속된 그룹원이라 한다.
- SM은 초기 설정 과정에서 각각의 하위 DM에 해당되는 A와 B 값을 생성하여 A는 SM이 안전하게 저장하고, B는 비밀 통신로를 통해 해당 DM에 이를 전송한다.

$$A = g^e \text{ mod } p$$

$$B = d^e \text{ mod } p$$

- SM은 DM에 비밀 통신로를 통해 전송한 B값을 생성한 d값의 리스트를 안전하게 저장한다.

4.2 시스템 계수

다음은 LBT트리를 기반의 멀티캐스트 관리 방식을 제안하기 위한 시스템 계수를 설명한다.

ID : 멀티캐스트 객체 식별자

α, w, x, y : 의사난수

Sig : 서명 알고리즘

MAC : 메시지 인증 코드

n, p : 공개계수

E() : 대칭키 암호 알고리즘

H() : 안전한 해쉬 함수

T : 타임 스탬프

4.3 제안방식 프로토콜

LBT 트리를 이용해 안전하고 효율적인 멀티캐스트 그룹 관리를 제공하기 위한 프로토콜은 다음과 같이 이루어진다.

(1) SM-SM, DM-DM간의 통신

동등 레벨의 SM-SM, DM-DM간의 통신을 위해 인증 및 세션키 설립은 SIGMA 프로토콜을 기반으로 이루어진다.

① 초기 객체중 송신자는 수신자에게 인증 요구 메시지를 이용해 다음과 같은 계산을 하여 S, g^z 전송한다.

$$S = M^w \text{ mod } n$$

② 수신자는 전송되어온 S, g^z 를 임시 저장하고 다음과 같은 서명값 SIG를 생성하고 SIG와 대응되는 MAC을 계산하여 송신자에게 $S, g^v, ID_{\text{수신자}}, SIG, MAC$ 을 전송한다.

$$k_0 = PRF_k(1)$$

$$SIG = Sig(1, S, g^z, g^v)$$

$$MAC = MAC_{k_0}(1, S, ID_{\text{수신자}})$$

③ 송신자는 수신자로부터 전송되어온 $S, g^v, ID_{\text{수신자}}, SIG, MAC$ 에서 g^v 를 이용해 세션키 Z를 다음과 같이 생성한 뒤 서명에 대한 검증과 MAC에 대한 검증 과정을 수행한다.

$$Z = (g^v)^z = g^{zv}$$

$$k_0' = PRF_{k_0}(1)$$

$$MAC' = (1, S, ID_{\text{송신자}})$$

$$MAC' = MAC$$

수신된 정보에 대한 검증 과정이 올바른 경우 송신자는 수신자에게 전송할 값 SIG_1, MAC_1 을 생성한 뒤 $S_1, ID_{\text{수신자}}, SIG_1, MAC_1$ 을 전송한다.

$$S_1 = M^{w_1} \text{ mod } n$$

$$SIG_1 = (0, S, g^z, g^v)$$

$$MAC_1 = MAC_{k_1}(0, S, ID_{\text{수신자}})$$

④ 수신자는 송신자로부터 전송되어온 $S_1, ID_{\text{수신자}}, SIG_1, MAC_1$ 을 송신자와 같은 검증 과정으로 전송 정보의 검증 과정을 수행한다.

$$Z = (g^z)^v = g^{zv}$$

$$k_0' = PRF_{k_0}(0)$$

$$MAC' = (1, S, ID_{\text{수신자}})$$

$$MAC_1' = MAC_1$$

(2) SM-DM간의 통신

상위 SM와 하위 DM과의 통신 과정을 수행할 경우 다음과 같은 수행된다.

① SM_1 이 송신자로 설정된 경우 SM_1 은 다음을 계산하여 DM_1 에 A, S, β 를 전송한다.

$$S = (\alpha + 1)$$

$$\beta = e^{-1}$$

② A, S, β 를 수신한 DM_1 은 다음의 검증 과정을 거쳐 그 정당성을 확인한다.

$$\begin{aligned} - (A^{\alpha} * B * g^{e\alpha})^{\beta} &= (g^{e\alpha} * r^{e\alpha} * g^{-(e\alpha - e)})^{\beta} \\ &= (g^{(-e\beta)} * r^{e\beta}) \\ &= g^{-1} * r \end{aligned}$$

이상의 검증 과정이 올바른 경우 C 를 다음과 같이 생성하여 VD_S 를 계산한 뒤 VD_S, T_D 을 SM_1 에 전송한다.

$$C = G^{(g^{-1} * r)} \text{ mod } p$$

$$VD_S = E_C(M || w_0)$$

③ SM_1 은 VD_S, T_D 에서 C 를 생성하여 VD_S 를 복호화 한 뒤 올바른 경우 하위 통신과의 안전한 암호 통신을 위해 세션키 S 를 생성하여 M 에 대한 응답 메시지 M_{res} 를 타임 스탬프 T_S 와 함께 암호화 하여 전송한다.

$$S = H(g^{w_0} || g^{-1} * r)$$

$$V_{S,M} = E_S(M_{res} || T_S)$$

(3) DM의 그룹 탈퇴 프로토콜

DM이 탈퇴할 경우 해당 SM은 DM의 고유 g, d 값을 저장 리스트에서 삭제하는 과정을 수행한다.

① 탈퇴하고자 하는 DM은 탈퇴 메시지 M_{res} 를

(2)에서 공유된 세션키로 암호화 하여 자신의 ID , 타임 스탬프와 함께 상위 SM에 이를 전송한다.

$$VD_{S,DEL} = E_S(M_{DEL})$$

② 이를 전송 받은 상위 SM은 (2)에서 공유된 세션키 S 를 이용해 이를 복호화 한 뒤 탈퇴를 원하는 DM의 g, d 를 저장된 리스트에서 삭제함으로써 탈퇴 과정을 수행하고 이를 하위 DM에 브로드캐스팅 한다.

(4) SM의 탈퇴의 경우

SM의 탈퇴에 따른 하위 DM의 상위 SM 재설정 과정은 다음과 같이 수행된다.

① SM_{DEL} 은 SM_2 에 탈퇴 메시지 M_{DEL} 과 하위 DM의 초기 dlist를 (1)에서 설정한 세션키로 암호화

호화 하여 전송한다.

$$VS_{DEL_S,2} = E_X(dlist | M_{DEL})$$

② SM_2 는 dlist를 자신의 dlist와 같이 구분하여 저장한 뒤 새로운 dlist에 설정된 DM을 자신의 새로운 DM으로 설정하는 인증 및 키 설정에 대한 갱신 메시지를 전송하여 (1)과 (2)의 과정을 수행한다.

5. 제안방식 분석

본 논문에서는 LBT 트리 기반의 멀티 캐스트 그룹 네트워크 관리 방식 제안하였으며, 다음과 같이 기존 방식과는 차별화된 특징을 가지고 있다.

① 객체간 통신의 기밀성

기존 방식에서 사용되는 KEK와 같이 기밀성 보호 키를 위한 또 하나의 키가 필요하는 비효율성을 배제하였다. 제안 방식에서는 통신 레벨에 따라 새로운 세션키를 설정하는 방식을 이용하여 기존 방식에서 제공되는 기밀성 서비스보다 효율성을 높게 하였다.

② 그룹 객체간의 인증

제안방식은 LBT 트리를 기반으로 멀티캐스트 그룹이 설정 될 경우 SIGMA 프로토콜의 서명값과 이를 보장해줄 MAC를 이용하여 상호 인증이 가능하게 하였다. 따라서 상호 인증에 따른 계산량 증가는 최소화 하고 상하위 객체간의 상호인증이 가능하게 하였다.

③ PFS 보장

제안 방식은 SM에서 초기 설정된 고정된 g, r 값 뿐만 아니라 DM에서 설정된 w_0 값을 이용하여 세션키의 PFS를 보장하도록 하였다.

④ 객체 탈퇴에 대한 그룹의 효율성 유지

본 제안 방식의 경우 DM의 탈퇴에 따라 전체 멀티캐스트 그룹에 영향을 최소화 하도록 하였으며, SM이 탈퇴할 경우 인접한 SM과의 통신을 통해 탈퇴를 요구하는 SM의 하위 DM을 인계받아 지속적인 그룹 설정이 이루어지도록 하였다.

6. 결론

본 논문에서는 멀티캐스트 그룹의 초기 설정에 따른 인증과 키 설정 방법을 분석하고 이를 보완할 수 있는 기법을 제안하였다. 제안된 방식은 기존 방식에서 고려되지 않았던 멀티캐스트 구조상의 특징을 고려하였으며, 기존 방식에서 제기되고 있는 다양한 형태의 보안적 취약점을 보완할 수 있는 안전한 형태의 멀티캐스트 그룹 네트워크

관리 방식을 제안하였다. 그러나 제안 방식의 경우 기존 방식보다 많은 가정 사항을 기반으로 하였으며, SM의 계산량은 고려되지 않아 확장성에 한계성을 나타내고 있다. 따라서 향후 본 논문에서 제안되었던 방식을 기반으로 하여 가정사항을 최소화하면서 SM의 계산량을 고려한 확장성을 제공하는 멀티캐스트 그룹 네트워크 관리 방식에 대한 연구를 지속적으로 수행하고자 한다.

7. 참고 문헌

- [1] T. Sander and C. F. Tshudin, "Towards Mobile Cryptography", International Computer Science Institute TR-97-049, 1997
- [2] <http://www.kisa.or.kr>
- [3] D. S. Alexander et al., "A Secure Active Network Environment Architecture: Realization in SwitchWare", IEEE Network Magazine, 1998
- [4] Dan Sterne, "Active Network Intrusion Detection and Response", Boeing and NAI Lab., DARPA DARPA FTM PI Meeting, Jul. 20. 2000
- [5] D. S. Alexander et. al., "Active Network Encapsulation Protocol(ANEP)" <http://www.cis.upenn.edu/~switchware/ANEP/docs/ANET.txt> 1997
- [6] 이임영 "전자상거래와 보안 입문", 생능출판사, 2001.7
- [7] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.11