제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

보안 수준 비교 방식의 멀티캐스트 접근통제에서의 전송 효율성 분석

신동명*, 박희운*, 최용락**
*한국정보보호진흥원
**대전대학교 컴퓨터공학과
e-mail:dmshin@kisa.or.kr

Analysis of Traffic Effectiveness on Multicast Access Control Scheme with Security Level Comparison

Dong-Myung Shin*, Hee-Un Park*, Yong-Rak Choi**
*Korea Infomation Security Agency
**Dept of Computer Engineering, Daejeon University

요 약

멀티캐스트 기술은 다자간 비디오회의, 대화형 원격 강의, 소프트웨어 배포, 인터넷 게임 등 특정 사용자 그룹에게만 전송하는 효율적인 통신기술이다. 그러나, 멀티캐스트의 개방적 특성상, 언제 어디서나 임의의 그룹멤버가 메시지를 보낼 수 있다. 따라서 부적절한 데이터의 수신으로부터 그룹 멤버들을 보호하고 다양한 DOS 공격으로부터 멀티캐스트 트리를 보호하기 위해 송신자 접근통제를 수행하는 것이 중요하다. 소스기반과 단일지점 또는 랑데부 지점에서 인가되거나 인증되는 연구가 진행되어 왔다. 본 논문에서는 접근권한에 따라 전송 메시지가 라우터의 임의의 지점에서 사전에 통제될 수 있는 양방향 멀티캐스트 트리에 대한 다단계 송신자 접근통제 메커니즘을 제시한다. 다음으로 제시한 방식과 기존 전송 방식간의 메시지 전송 효율성 측면을 실험을 통하여 분석한다. 제안 방식이 라우터상에서 접근권한의 비교를 통하여 메시지를 사전에 걸러냄으로써 상대적으로 작은 메시지 전달 오버헤드를 갖는 것을 확인하였다.

1. 서론

멀티캐스트는 다자간 비디오회의, 대화형 원격 강의, 소프트웨어 배포, 인터넷 게임 등 특정 사용자 그룹에게만 전송하는 효율적인 통신 서비스를 제공한다. 그러나, 멀티캐스트의 개방적 특성상, 언제 어디서나 임의의 그룹멤버가 메시지를 보낼 수 있다. 따라서 부적절한 데이터의 수신으로부터 그룹 멤버들을 보호하고 다양한 DOS 공격으로부터 멀티캐스트 트리를 보호하기 위해 송신자 접근통제를 수행하는 것이 중요하다. 소스기반과 단일지점 또는 랑데부 지점에서 인가되거나 인증되는 연구가 진행되어 왔다. 특히, 양방향 라우팅에서의 접근통제 문제는 훨씬 더 어려운 문제이다. 왜냐하면 호스트들이 트리의 어느지점에서도 직접적으로 모든 그룹 멤버들에게 데이터를 전송할 수 있기 때문이다.

멀티캐스트 데이터가 권한없는 호스트 또는 사용자들에 의해 접근되는 것을 막는 방법에 대해 많은 연구가 진행되어 왔으나 해법들의 대부분은 응용레벨의 암/복호화에 기초하고 있다. 그러나, 응용레벨 메커니즘은 플러딩 공격과 같은 서비스 거부 공격에 대해 라우팅 인프라를 보호할 수 없다. 멀티캐스트 데이터가 수신자들에게 전송되는 선상에 있는 멀티캐스트 라우터들에게 계속 복제될 수 있기 때문에 이러한 공격들은 멀티캐스트 서비스에 치명적인 영향을 줄 수 있다. 따라서 서비스 거부 공격을 막기 위한 메커니즘은 응용계층 보다는 네트워크 계층에서 제공되어야 한다.

본 논문에서는 접근권한에 따라 전송 메시지가 라우터의 임의의 지점에서 사전에 통제될 수 있는 양방향 멀티캐스트 트리에 대한 동적 송신자 접근통제 메커니즘을 제시한다. 다음으로 제시한 방식과 기존 전송 방식간의 메시지 전송 효율성 측면에서 성능을 분석한다.

2. 멀티캐스트 보안수준 비교 방식

일반적인 네트워크 환경에서는 하나의 네트워크

라우터 인터페이스에 하나의 서브넷이 연결되어 있는 경우가 대부분이고, 하나의 서브넷에는 다수의 멀티캐스트 멤버들이 연결될 수 있다. 서브넷 내에서 멀티캐스트 그룹에 참여하고자 하는 호스트는 IGMP 프로토콜을 이용하여 지정된 라우터에 가입을 요청하게 된다. 가입요청에 따른 인증과 접근통제 권한부여는 멀티캐스트 코어 라우터에서 담당한다. 제안 방식에서는 CBT[1]와 같은 양방향 이진트리환경에서 멤버별 사용자 접근통제가 아닌 네트워크 세그먼트별로 접근통제가 수행된다. 그룹에 참여하고자 하는 멤버는 코어 라우터에 인증을 받은 후 접근권한 레벨을 부여받는다. 이때, 접근권한 승인 메시지가 코어에서 멤버에까지 전달되면서, 멤버의 접근권한 레벨이 지나가는 멀티캐스트 라우터의 Emax값과 비교하여 최대값을 갱신하게 된다. 그리고 멤버가 소속한 지정라우터에서는 Imax과 비교하여 최대값을 갱신하게 된다. 따라서, 네트워크 세그먼트내에 동일한 그룹에 가입한 멤버가 여럿 있는 경우에 지정된 라우터간의 데이터 전송은 네트워크 레벨의 접근통제를 수행하고, 동일한 세그먼트내에서의 멤버별 접근통제는 어플리케이션 레벨의 계층형 암/복호화 기법을 사용하여 해결할 수 있다. 먼저 네트워크 레벨의 다단계 접근통제를 수행하기 위하여 접근과 거부 2가지의 접근요소에서 확장하여 다단계의 보안 레벨(Security Level)을 고려한 접근통제 기법을 적용한다.

S는 멤버의 접근통제 레벨을 나타내고 EmaxR과 EmaxL은 각각 우측, 좌측 서브노드에 대한 접근레벨의 최대값을 나타낸다. EmaxR과 EmaxL을 통칭하여 Emax라하면 Emax는 자신의 하위 노드 전체에 대한 최대값이고 Imax는 자신의 노드 안쪽에 대해서만 최대값을 나타낸다. Emax ≥ (하위노드 Imax 와 하위노드 Emax)가 성립한다. Emax는 하위노드의 모든 Emax와 Imax의 최대값을 가져야 한다. 또한 Imax는 자신노드의 최대값을 가져야 한다. 단, 자신의 Emax와 자신의 Imax와는 상관관계가 없다. 임의의 호스트 또는 멤버는 자신의 접근통제 레벨에 상응하는 암호화된 메시지를 생성한다. 접근통제를 위한 계층형 키구조에서 각 멤버들은 해당 접근권한에 해당하는 키목록을 라우터와 공유했다고 가정한다. 암호화된 메시지는 멀티캐스트 라우터에서 상위노드 인터페이스와 우측, 좌측 하위 인터페이스로 전달할지를 결정한다. 이때, 상위노드로의 전달은 항상 이루어지고, 메시지의 보안레벨이 최대값보다 큰 경우에는 하위노드로 전달하지 않는다.

본 방식에서는 멀티캐스트 트리상에서 하위 레벨로 내려가면서 사전에 하위 노드에 대한 접근통제 레벨을 파악하여 불필요한 접근통제 연산과 전체 네트워크 트래픽을 줄일 수 있다. 접근통제 레벨에 따른 연결노드의 최적화가 이루어지면, 각 노드당 메시지 전달 확률은 더욱 낮아지며, 최악의 경우에도 서브넷내에서의 접근통제에 의해 1이하의 확률을 갖는다. 일반적인 환경에서는 높은 접근권한을 갖는 멤버가 낮은 권한을 갖는 멤버보다 적기 때문에, 트리의 깊이(depth)가 커질수록 메시지 전달 확률은 낮아진다.

3. 전송 효율성 분석

제안된 방식은 완전전송(Full Forwarding) 방식에 비해 네트워크 트래픽에서 많은 이득을 준다. 완전전송 방식의 멀티캐스트 라우터는 입력된 모든 메시지를 말단 노드의 멤버들에게까지 모두 전송한다. 그러나 제안된 방식은 Emax 와 Imax에 따라 하위노드 및 서브넷 내로의 전송여부를 결정한다. 먼저, 멤버들로 구성된 트리에서 임의의 노드를 잡아 어느 정도 전송되는지 살펴보자. 각 노드를 멀티캐스트 라우터라고 볼 때 라우터가 결정하는 것은 그 노드 내의 멤버들에게 전송을 하는지 여부와 자식 노드에게 전송을 하는지 여부이다. 노드에 입력되는 메시지의 보안등급이 1 ~ L_0 사이에 난수로 구성되어 있고 각 등급의 출현빈도가 $1/L_0$ 로 균일하다고 가정한다.

L_0 보안등급 수

l : 입력된 메시지의 보안등급

n : 각 노드에 딸린 멤버 수

우선 멤버 수가 1인 경우를 살펴보자. 라우터가 받은 임의로 메시지의 보안레벨을 x1이라고 하고 전송여부를 결정할 멤버의 보안레벨을 x2라고 하자. 그러면 라우터는 x1 ≤ x2 인 경우만 전송해야 한다. 계산을 간편하게 위해 우선 각 멤버들은 1에서 L_0 사이에 고르게 분포한다고 가정한다. 그러면 보안 등급 l을 가질 확률은 $1/L_0$ 이다.

$$P(x_1 \le x_2) = \sum_{r=1}^{L_0} \frac{1}{L_0} \frac{L_0-(r-1)}{L_0} = \frac{1}{L_0^2}\left(L_0^2 + L_0 - \frac{L_0(L_0+1)}{2}\right) = \frac{L_0+1}{2L_0} \quad (1)$$

다음은 멤버의 수가 n개인 내부 노드에 전송하게 되는 확률을 구해보자. 전송이 일어나는 경우는 입력된 메시지의 보안레벨보다 큰 보안레벨을 가진 멤

버가 하나 이상 존재할 때이다.

$P(x_1 \le Max(x_2 \in I))$

멤버들 중 r개만 l보다 크거나 같고 나머지는 작은 경우,

$$\frac{{}_nC_r(L_0-l+1)^r(l-1)^{n-r}}{L_0^n} \quad (2)$$

구하고자 하는 식은 모든 경우에서의 식이므로 각각의 (2)를 합산한다.

$$P(x_1 \le Max(x_2 \in I)) = \sum_{r=1}^{n} \frac{{}_nC_r(L_0-l+1)^r(l-1)^{n-r}}{L_0^n} \quad (3)$$

식 (3) 은 노드의 내부 멤버들에 대해 브로드캐스트할 확률이다.

다음으로 자식 노드들에게 브로드캐스트할 확률을 구해보자. 자식 노드에게 브로드캐스트할 확률은 결국 자식 노드들의 모든 멤버들 중 입력받은 메시지의 보안레벨보다 큰 보안레벨을 갖는 멤버가 존재하는 경우이다. 따라서 식 (3)에서 n에 전체 멤버수를 대입하면 된다.

트리의 높이가 H이고 깊이가 d 인 노드는 h' = H - d + 1 의 높이를 갖는다. 한편, 우리가 관심을 갖고 있는 노드는 그 노드의 왼쪽이나 오른쪽 노드이기 때문에 높이가 하나 만큼 낮아 h = H - d + 1 -1 = H - d 의 높이를 갖는다. 높이가 h인 트리의 자손 노드 수는 2^h-1 이다. 따라서 각 노드의 멤버수를 N_0 라고 한다면, 트리에서 깊이가 d 인 노드의 왼쪽이나 오른쪽 자손에 포함된 멤버 수는 다음과 같다.

$$N_0(2^h-1) \quad (4)$$

(4)를 (3)에 대입하면 왼쪽이나 오른쪽 자손에 대해 브로드캐스트할 확률이 된다. 최악의 경우는 모든 멤버들이 같은 보안레벨을 갖거나 부모보다 자손의 보안레벨이 항상 클 경우인데, 이 경우는 이전의 방법처럼 전송할 확률이 무조건 1이된다. 최상의 경우는 부모 노드의 멤버들이 자손 노드의 멤버들보다 항상 클 경우인데 이 경우는 메시지가 위로만 전달되고 아래로는 전달되지 않는다.

결국, 노드의 수 2^h-1 이 증가할수록 루트노드에 가까운 노드의 Emax가 증가할 가능성이 커지고 최대전송 확률은 1에 가까워진다. 그러나, 하단의 노드로 갈수록 전송할 확률은 점점 낮아진다. (그림1)은 실험을 통한 결과를 보여준다. 가로축은 트리의 높이가 h에 해당하는 최하단의 노드이고 세로축은 최하단의 노드에 메시지가 전송되는 수를 가리킨다. 전송 메시지로는 1,000,000개를 $1/L_0$ 확률의 보안 등급을 갖도록 무작위로 생성하였다. (그림1)과 (그림2)는 트리의 깊이가 커질수록 전달 메시지 수가 감소하고 높이가 커질수록 전송확률이 증가하나 완전전송 방식의 확률 1 보다 낮게 나옴을 보여준다.

좀 더 높은 효율을 얻기 위해서는 Emax 가 큰 노드를 위쪽으로 보내고 낮은 노드들은 아래로 보내는 최적화가 수행될 필요가 있다. 최적화를 통해 자식노드에서 루트노드까지의 완만한 Emax 값 상승을 유도할 수 있고, 메시지 송신 횟수를 줄일 수 있게 된다. 최적화가 수행되지 않은 최악의 경우에는 모든 자식노드들이 루트노드의 Emax 값과 동일한 경우이다. 이러한 경우에 최대전송 확률은 1이 된다.

3.1 트리노드의 최적화

최적화를 위해 제시한 방법은 각 노드의 최대 보안 레벨에 따라 전송 여부를 결정하므로, 트리를 최대 효율이 되도록 하기 위해, 보안 레벨이 높은 노드를 상위로 보내고 낮은 노드들을 하위로 보내도록 트리를 재조정한다.

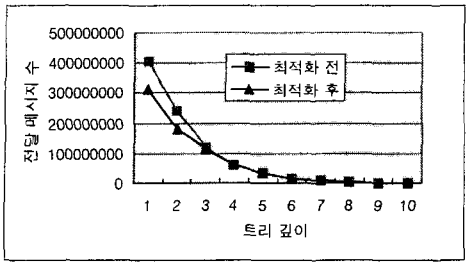
노드 정렬 시 고려해야 할 값은 한 노드의 최대 보안 레벨을 나타내는 Imax 이다. Imax 에 따라 노드들을 순차적으로 배열하면 되므로 일반 정렬 알고리즘을 그대로 사용할 수 있다.

노드의 개수가 n 인 트리에서 한 노드를 위치시키는 데 필요한 시간은 O(n) 이다. n 개의 노드를 가진 트리를 정렬하는 데 소요되는 시간을 T(n)이라 하면, 한 노드가 정확한 위치에 놓이게 될 때마다 트리는 거의 똑같은 크기를 갖는 두 개의 부분으로 나누어질 때 다음과 같은 식을 얻을 수 있다.

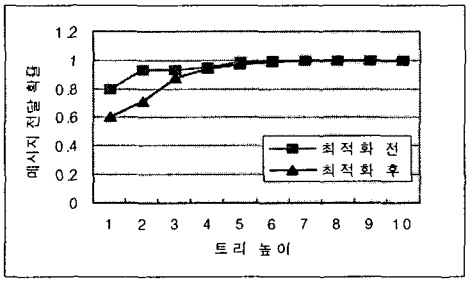
$$\begin{aligned} T(n) &\le cn + 2T(n+2) \\ &\le 2cn + 4T(n/4) \\ &\le cn + 2(cn/2 + 2T(n/4)) \\ &\vdots \\ &\le cn\ \log_2 n + nT(1) \\ &= O(n \log_2 n) \end{aligned}$$

따라서 평균 $O(n \log_2 n)$ 의 시간 안에 노드들을 최적의 상태로 정렬할 수 있다.

(그림1)과(그림2)는 최적화의 수행전과 수행후의 전달메시지 수와 진달 확률의 변화를 나타내었다.



(그림 1)



(그림 2)

3.2 피라미드형 분포

위의 수식에서는 멤버들의 보안레벨 분포가 균일하게 $1/L_0$로 가정했지만 일반적인 상황에서는 보안레벨이 높은 멤버들의 수는 적고 낮은 멤버들의 수는 많다. 이 경우 트리의 노드들이 최상의 경우로 정렬되어 있다면, 훨씬 좋은 성능을 예측할 수 있다. 일반적인 보안등급의 분포를 결정할 때, 조직은 높은 등급의 구성원의 수가 적고 낮은 등급의 구성원의 수가 많은 피라미드형 분포를 따른다.

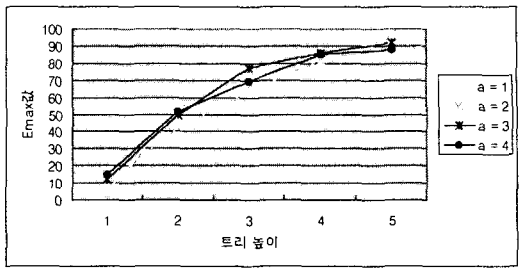
제안 논문에서는 피라미드형 분포를 적용하여 제안 모델의 효율성을 평가하여 보았다. 피라미드형 분포를 나타내기 위해, 다음과 같이 정의하였다.

$$f(x) = -ax + b \quad (a>0, b>0, x>0, y>0)$$

단, $0 \le f(x) \le 1$, $\int_{x=0}^{b} f(x)dx = 1$

x : 보안등급
f(x) : 보안 등급이 x일 확률
a : 보안등급 구성 비율

위 수식에서 a값이 크면 각 보안등급에 해당하는 구성원(멤버)가 적은 경우이고, a값이 작은 경우 각 보안등급당 구성원의 수가 많은 분포를 갖는 경우이다. (그림3)는 기울기 a 값의 변화에 따른 Emax값의 변화를 보여준다. 기울기 a 값에 관계없이 트리 높이가 낮은 경우 낮은 Emax 값을 갖는다. 기울기 a 값에 따른 Emax값의 편차는 확률적인 입력으로 인해 나타나는 특성이며, 더 많은 반복실험을 통해 정규화될 수 있다. 보안등급의 확률을 기울기가 a인 피라미드형 분포에서도 Emax의 값의 증가율이 일정하게 나왔으며 이는 제안 모델이 실제 환경에 적합한 모델임을 보여준다.



(그림 3)

4. 결론

본 논문에서는 다단계 네트워크 접근통제를 이용한 접근권한별 비밀성 서비스를 제공한다. 또한 멤버가 코어에 등록하는 과정에서 자신이 속한 서브넷의 최대 접근레벨과 하위 노드 각각에 대한 최대 접근레벨을 등록함으로써, 접근권한이 높은 메시지의 불필요한 전달을 사전에 차단하여 상대적으로 작은 메시지 전달 오버헤드를 갖는 것을 확인하였다.

다단계 비밀성 레벨은 멀티미디어 서비스 제공시 멤버별로 멀티캐스트 서비스에 대한 제공범위를 제한하는데 응용할 수 있다. 현재, 멀티캐스트상에서의 접근통제에 대한 전문적인 연구는 극히 미진한 상태이며, 향후 멀티캐스트 서비스의 활성화 및 활용범위 확대와 함께 활발한 연구가 진행되리라 예상된다.

참고문헌

[1] A. Ballardie, "Core Based trees(CBT) Multicast Routing Architecture", IETF RFC 2201, 1997.

[2] T. Hardjono, B. Cain and I. Monga, "Intra-Domain Group Key Management Protocol", Internet Draft, 2001.

[3] Ning Wang & George Pavlou, "Towards Dynamic Sender Access Control for Bi-directional Multicast Trees", Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE , Volume: 3 , 2001

[4] Thomas Hardjono, "Router-Assistance for Receiver Access Control in PIM-SM", Proceedings. ISCC 2000. Fifth IEEE Symposium 2000