MOFT : Mobile-IP네트워크에서 확장성을 제공하는 멀티캐스트 그룹 키 관리.

윤미연[0] 김기영 신용태
숭실대학교 컴퓨터학과
myyoon@hpcn.ssu.ac.kr

MOFT : Scalable Key management of secure multicast using OFT mechanism for mobile-IP network

Miyoun Yoon[0] Kiyoung Kim Yongtae Shin
Dept. of Computer Science, Soongsil University

요 약

멀티캐스트 정보보호 기술은 순수한 멀티캐스트 기술을 실용화 하는데 있어서 없어서는 안 될 기술이다. 멀티캐스트 정보보호 기술에서 이슈가 되는 것은 여러 가지가 있으나, 본 논문에서는 인증된 수신자만이 데이터를 볼 수 있도록 하기 위해 필요한 키의 분배 및 rekey 연산에 대해 제안된 몇 가지 기술을 알아보고, 무선환경에서도 확장성을 제공할 수 있는 방안으로 기존의 OFT(One-way Function Tree) 메커니즘을 토대로 하는 MOFT(Mobile OFT) 메커니즘을 제안하고 제안하는 MOFT 메커니즘의 효율성을 분석한다.

1. 서론

초기 인터넷은 연구소간의 전문적인 지식을 공유하는 통신망으로 출발하여 80년대 WWW의 등장으로 일반인들도 쉽게 사용할 수 있는 통신망으로 발전하게 되었다. 사용자의 증가는 서비스에 대한 요구사항을 다양화하였고 이런 사용자의 요구를 충족하기 위한 결과로 멀티캐스트, Mobile-IP의 WG이 구성되었으며, 연구가 진행 중에 있다.

멀티캐스트는 동일한 데이터를 수신 노드별로 전송하지 않고 네트워크 계층에서 패킷을 한번만 전송하도록 하여 대역폭의 효율성을 높일 수 있으며, Mobile-IP의 경우는 단말기에 이동성을 부여하여 이동 중에도 인터넷 서비스를 지원할 수 있는 기술이다. 하지만, 이와 같은 차세대 기술의 실제적인 수용을 위해서는 데이터의 불법적 사용과 공격을 방지해야 하며, 이를 위해 데이터의 기밀성, 무결성 지원이 선행되어야 한다.

현재 고정된 노드로 구성되는 멀티캐스트 환경에서의 키 관리에 관한 연구는 IETF 및 IRTF에서 WG을 결성하여 활발히 진행 중이지만, 멀티캐스트를 지원하는 Mobile-IP에서의 키 관리에 관한 연구는 미약한 실정이다. 특히 멀티캐스트를 지원하는 Mobile-IP의 경우 멀티캐스트 그룹의 가입과 탈퇴 동작 외에 노드의 이동에 따른 키 관리가 필요하기 때문에 멀티캐스트에서의 키 관리를 적용할 경우 빈번한 키 분배로 인해 확장성에 문제가 발생하게 된다. 따라서 본 논문에서는 멀티캐스트 환경에서의 키 분배 알고리즘인 OFT(One-way Function Tree)을 기본으로 하여 데이터의 기밀성과 무결성을 지원하고 멀티캐스트를 지원하는 Mobile-IP 환경에서 멀티캐스트 그룹의 가입/탈퇴와 노드의 이동 횟수가 증가하여도 확장성을 보장할 수 있는 MOFT 알고리즘을 제안한다.

2장에서는 고정 노드에서의 그룹 키 관리에 대해 알아보고, 3장에서는 OFT 메커니즘에 대해 알아보고, 4장에서는 MOFT 메커니즘을 제안하며, 5장에서는 결론 및 향후 연구방향을 제시한다.

2. 멀티캐스트에서의 그룹 키 관리

그룹 키 관리 알고리즘들은 중앙 집중형, 분산 환경형, 그리고 복합적으로 사용하는 방식이 있다. 중앙 집중 방식은 하나의 키 서버가 관리한다. 중앙 집중 방식은 효율적이나 그룹에 가입한 호스트의 수의 증가에 따라 서버의 오버헤드가 커지는 확장성의 문제가 있다. 분산 환경 방식은 복수 개의 키 서버를 두어 그룹 키를 관리한다. 키 서버를 위한 별도의 그룹 키의 관리가 필요하므로 중앙 집중 방식에 비해 복잡해지지만 뛰어난 확장성을 가진다.

멀티캐스트 특성상 그룹 멤버의 동적인 가입/탈퇴가 발생하므로 키의 재생성 및 재분배 등의 키 관리 또한 필요하다. 이러한 멀티캐스트 환경에서의 키 관리 기법은 다음 두 가지 조건을 만족해야 한다[1].

- Forward secrecy : 멀티캐스트 그룹을 떠나는 사용자는 그룹을 떠난 이후의 메시지를 복호 할 수 없어야 한다.
- Backward secrecy : 멀티캐스트 그룹에 새로 가입한 사용자는 가입하기 이전의 메시지를 복호 할 수 없어야 한다.

위의 두 조건을 만족하기 위해서는 그룹 전체에 대한 rekey 연산이 필요하다. 또한 외부의 공격을 막기 위해서, 키 구조는 멀티캐스트 세션에서 배제된 멤버들의 그룹이 결탁하여 새로운 그룹 키의 생성 및 재생성을 막을 수 있는 구조를 가지고 있어야 한다.

멀티캐스트 정보보호를 위해 제안된 키 분배 구조는 크게 다음과 같이 4가지로 나눌 수 있는데, 수동 키 분배 방식[5]과 Pairwise Keying 방식[3,4,5], Secure Lock 방식[5,6,7] 그리고 계층적 트리 방식이다.

계층적 트리 방식에서 참가자들은 자신만이 사용하는 키를 가지고 있으며, 해당 키를 가지고 트리 구조를 구성한다. 이러한 방식을 사용하는 경우에 확장성이 좋으며, 초기 키 동작이 선형적인 효율을 제공하며, rekey 메시지의 크기 또한 작다[5]. 또한, 멀티캐스트 통신은 다중 통신이기 때문에 확장성은 매우 중요한 요소이다. 따라서, 관리하기 쉽고, 확장성을 보장하기 위해 계층적 트리 방식을 많이 이용한다.

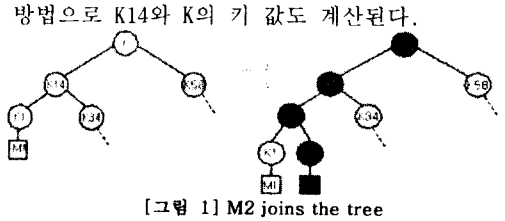
3. OFT 메커니즘의 개요

OFT 메커니즘은 McGrew와 Sherman[6,8]에 의해 제안되었으며, 이는 키 트리를 유지하는 GC(Group Controller)를 가지고 있다. 키 트리는 이진 트리로 구성되며, 트리의 leaf는 그룹의 멤버로 구성된다. 또한, 키 트리의 루트는 그룹 키를 가지고 있다. 각각의 내부 노드는 자신의 자식 노드에 의해 생성된다. 각각의 키 값은 one-way 함수와 혼합(mixing) 함수를 이용하여 만들어진다.

$$k_i = f(g(k_{left(i)}), g(k_{right(i)}))$$

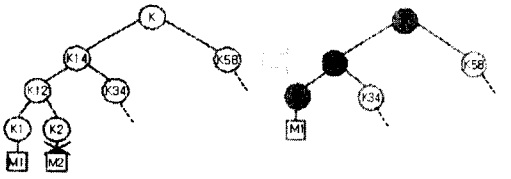
여기서, g는 one-way 함수이고, f는 혼합함수이며, $left(i)$와 $right(i)$는 노드 i의 자식 노드들이다. 각각의 멤버들은 $log_2 n+1$개의 키를 저장하고 있어야 한다.

먼저 backward secrecy를 만족하기 위해서는, 그룹에 새로운 멤버가 가입했을 때, GC는 임의로 새로운 멤버에 게 키를 부여하고 rekey 연산을 수행한다. 예를 들어, [그림 1]과 같이 M2가 그룹에 가입하였을 때, K12는 K1과 새로운 멤버 K2에 의해 조상 노드의 키 값을 다시 계산하고, 같은 방법으로 K14와 K의 키 값도 계산된다.



[그림 1] M2 joins the tree

또한 forward Secrecy를 만족하기 위해서는, 기존의 그룹 멤버가 그룹에 탈퇴하면 rekey 연산을 수행한다. 예를 들어, [그림 2]와 같이 M2가 그룹에서 탈퇴를 하면, K1, K14, K는 새로운 키를 생성하는 것이다.



[그림 2] M2 leaves the tree

OFT메커니즘은 rekey 연산 횟수를 해당 트리의 한 줄기만을 수행함으로써 상당히 줄였다. 다음은 OFT 메커니즘을 나타낸 것이다.

```
==============================
OFT Mechanism

If(MH joins G or MH leaves G)
Do
  node : send g(K_node) to parent.
  parent : create new key using g(K_node)
       and g(K_sibling of node).
  node=parent
until(node==root node)
==============================
```

4. MOFT 메커니즘

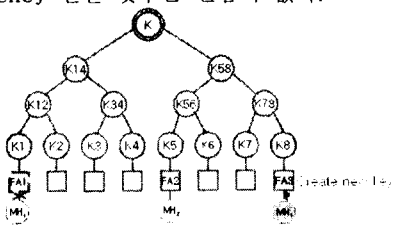
본 논문에서 제안하는 메커니즘은 기존의 계층적인 트리를 사용하는 OFT 메커니즘을 사용하며, 무선 환경에서의 확장성을 높인 것이다. 무선 환경의 잦은 이동성으로 인해 기존의 OFT 메커니즘을 적용하는 경우, MH(mobile host)가 이동할 때마다 rekey 연산을 해야 하기 때문에 확장성이 떨어진다. 따라서, 새로운 FA로의 이동 시마다 새로운 키를 생성하고 분배한다는 것은 비효율적일 수 있다.

MOFT 메커니즘은 멀티캐스트 멤버가 FA(Foreign Agent)가 된다. FA가 처음 그룹에 가입할 때에는 기존의 OFT 메커니즘과 같이 동작하며, 이미 그룹의 멤버인 FA로 MH가 이동 했을 때는 새로운 rekey 연산을 수행하지 않고 단지 FA에서 새로운 키를 생성함으로써 해결될 수 있다. OFT메커니즘과 다른 추가적인 것은 MH는 HA(Home Agent)에게서 받는 유일한 키를 가지고 있다는 것이다.

MOFT 메커니즘은 크게 두 가지 경우로 나눌 수 있다. FA가 그룹에 새로 가입/탈퇴를 하는 경우와, 이미 그룹 멤버인 FA에 새로운 MH가 이동하는 경우이다.

전자의 경우는, OFT 메커니즘의 가입/탈퇴시의 rekey 연산을 그대로 적용하고, FA는 새로운 비밀키를 생성한다.

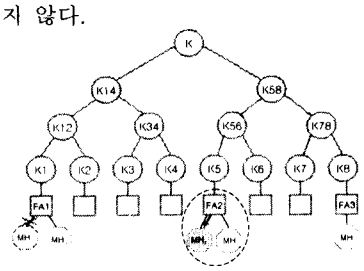
따라서, rekey 연산 횟수는 변함이 없다.



[그림 3] FA가 그룹에 속하지 않는 경우

후자의 경우는, rekey 연산이 필요 없이, 새로운 MH가 FA로 이동하면 FA는 MH의 키 정보를 전달 받아서 FA가 일종의 GC가 되어 자신에게 속한 이동 노드들의 키를 관리한다. 따라서, rekey 연산이 필요하지 않으며, 단지 한번의 키 생성만이 필요한 것이다. MH가 그룹에 가입한 FA로의 이동이 많을수록, 본 메커니즘의 확장성은 더욱 높아진다.

MOFT 메커니즘의 추가적인 키 생성은 가입 시에만 이루어지며, 탈퇴 시에는 FA가 탈퇴하지 않는 한 어떤 절차도 필요하지 않다.



[그림 4] FA가 그룹에 속한 경우

다음은 MOFT메커니즘을 나타낸 것이다.

==========

MOFT Mechanism

If FA∉G.
then OFT
FA : create key which is different to FA's private key
else if FA∈G
FA : create key which is different to FA's private key

==========

기존의 OFT 메커니즘의 rekey 연산 횟수를 수식으로 나타내면 다음과 같다.

$$f(x) = \lambda Tx \ln N \bullet P(\tau = 0) \qquad (1)$$

N은 그룹에 속한 멤버의 수를 나타낸다. λ는 단위 시간당 이동 노드의 평균 이동 횟수이고 포아송 분포를 따른다. T는 일정시간을 나타낸다. τ는 특정한 FA에 위치하는 MH의 개수이다. 그리고, $P(\tau = 0)$는 이항분포를 따르며, 이미 그룹에 가입된 FA가 없을 확률이다.

본 논문에서 제안한 MOFT 메커니즘의 rekey 연산 횟수를 수식으로 나타내면 다음과 같다.

$$g(x) = \lambda Tx \bullet P(\tau \neq 0) \qquad (2)$$

이는 FA가 그룹의 멤버가 아닐 때에는 기존의 OFT 메커니즘과 같음으로 이동한 MH가 속하는 FA가 이미 그룹의 멤버일 때만을 나타낸 것이다. 여기서, $P(\tau \neq 0)$는 특정 FA에 이동 노드가 위치할 확률이다.

도출된 수식에서도 알 수 있듯이, $f(x)$ 보다 $g(x)$의 연산회수가 적다. 즉, $f(x)$는 기하급수적인 증가를 보이며, $g(x)$는 선형적인 증가를 보임을 알 수 있다.

5. 결론 및 향후 연구방향

본 논문에서는 Mobile-IP상의 이동 노드에 대한 키 관리 방안으로 MOFT 메커니즘을 제안하였으며, rekey 연산 횟수를 줄일 수 있음을 보여주었다. 무선노드의 증가에 따라 MOFT 메커니즘은 유용하게 쓰일 수 있을 것이다.

그러나, 이동 노드의 인증문제와 핸드오프시의 데이터 처리를 향후 연구과제로 남긴다.

참고문헌

[1] T. Hardjono et. al, " *IP Multicast Security: Issues and Directions,*" Technical Report, Univ. of Southern California, September 1999.

[2] A. Billardie, " Scalable Multicast Key distribution," RFC1949, May 1996.

[3] H. Harney et. al, " Group key management protocol(GKMP) Architecture," RFC2094, July 1997.

[4] P. Kruus et. al, "*Techniques and Issues in Multicast Security,*" Proc. IEEE MILCOM 98.

[5] D. Wallner et. al, " Key Management for Multicast : Issues and architectures," RFC2627, July 1999.

[6] D. McGrew et. al, " *Key Establishment in Large Dynamic Groups Using One-Way Function Trees,*" IEEE Transactions on Software Engineering, May 20, 1998.

[7] G. H. Chiou et. al, " *Secure Broadcasting using the Secure Lock,*" IEEE Trans. on Software Engineering, vol. 15, pp. 929-934, 1989.

[8] D. Balenson, et. al, " *Key management for large dynamic groups: One-way function trees and amortized initialization,*" Internet Draft, draftirtf-smug-groupkeymgmt-oft-00.txt, IETF, August 25, 2000.