전자상거래를 위한 멀티캐스트 그룹 키 관리 프로토콜 설계 및 구현

홍 종 준*, 김 태 우**
* 청강문화산업대학대학 컴퓨터소프트웨어과
** 성공회대학교 컴퓨터정보공학부

요 약

본 논문에서는 전자상거래 환경에서 멀티캐스트 그룹 통신의 사용자 정보 보호를 위한 멀티캐스트 그룹 키 관리 프로토콜을 제안한다. 이는 서브그룹의 단위인 RP에 멀티캐스트 그룹 키를 관리하는 키 관리자를 두어 송신자 고유의 그룹 키를 부여하고 데이터를 수신자에게 전송하기 이전에 RP는 인증된 수신자에게 송신자의 그룹 키를 전달한다. 송신자가 그룹 키로 암호화한 후 RP에게 전송을 하면 RP는 각 수신자에게 전송하고, 수신자는 미리 받은 송신자의 그룹 키로 데이터를 복호화 할 수 있다. 따라서 그룹 키에 의한 데이터 변환 작업이 불필요하여 데이터 전송 시간이 단축되며, 최소거리 경로로의 변경에도 새로운 키 분배 없이 데이터 전송이 가능하다.

Design and Implementation of Dynamic Group Key Management Protocol for Multicast Information Security

Hong, Jong-Joon, Kim, Tae-Woo

ABSTRACT

This paper proposes a group key management protocol for a secure of all the multcast user in PIM-SM multicast group communication under electronic commerce. Each subgroup manager gives a secure key to it's own transmitter and the transmitter compress the data with it's own secure key from the subgroup manager. Before the transmitter send the data to receiver, the transmitter prepares to encrypt a user's service by sending a encryption key to the receiver though the secure channel, after checking the user's validity through the secure channel. As the transmitter sending a data after then, the architecture is designed that the receiver will decode the received data with the transmitter's group key. Therefore, transmission time is shortened because there is no need to data translation by the group key on data sending and the data transmition is possible without new key distribution at path change to shortest path of the router characteristic.

1. 서 론

다양한 멀티캐스트 보안 프로토콜이 연구되면서 멀티캐스트 그룹 통신에서 서브그룹 단위로 그룹 키 등을 분배하는 계층적인 보안 프로토콜이 연구되었다[1]. 이는 기존의 유니캐스트에서 사용한 보안 프로토콜과는 다른 1:N 구조나 혹은 N:N 구조의 서브그룹 단위로 그룹 키를 관리하여 사용자의 가입/탈퇴에 따른 그룹 키의 재분배를 한다[4].

멀티캐스트 그룹은 PIM-SM(Protocol Independent Multicast-Sparse Mode) 라우팅 알고리즘을 사용하여 서비스를 제공받을 수 있다[5]. PIM-SM 라우팅 알고리즘은 많은 사용자를 갖는 CBT, DVMRP[6]와 같은 일정한 코어 트리도 없고, 최단거리 알고리즘을 위주로 하는 효과적인 라우팅 알고리즘이다. 또한 분산되어 있는 노드들을 서브그룹의 단위인 RP(Rendezvous-Point)로 분류하여 송신자에서 RP까지 유니캐스트로 전송하고, RP에서 수신자까지 멀티캐스트로 전송하는 혼합 멀티캐스트 라우팅에 적합한 그룹 키 관리 방식은 없다고 알려져 있다[7]. 따라서 본 논문에서는 PIM-SM 멀티캐스트 그룹통신에서 사용자의 정보 보호를 위한 동적 그룹 키 관리 프로토콜을 제안한다. 이는 RP에 멀티캐스트 그룹 키를 관리하는 키 관리자를 두어 송신자 고유의 그룹 키를 부여하고 데이터를 수신자에게 전송하기 이전에 RP는 인증된 수신자에게 송신자의 그룹 키를 전달한다. 송신자가 그룹 키로 암호화한 후 RP에게 전송을 하면 RP는 각 수신자에게 전송하고, 수신자는 미리 받은 송신자의 그룹 키로 데이터를 복호화 할 수 있다. RP에 멀티캐스트 그룹 키 관리자를 두어서 기존 PIM-SM 라우팅 알고리즘의 변형 없이 사용할 수 있게 된다. 또한 PIM-SM 멀티캐스트 라우팅에서 최소거리 경로 변경에 그룹 키를 미리 전송 받은 상태이므로 다른 키의 재분배 없이 바로 데이터 수신이 가능하고, 키 관리자 내에서 그룹 키에 의한 데이터 변환작업이 필요 없어 데이터의 전송시간이 단축된다.

2. 관련연구

2.1 멀티캐스트 그룹 키 관리 방식

Naïve, Iolus, Nortel 방식의 멀티캐스트 그룹 키 관리 방식은 다수의 가입자 수에 중점은 둔 그룹 키 관리 방식으로 서브그룹의 규모가 매우 크다. 따라서 서브그룹 내에서 단 하나의 가입자가 탈퇴하여도 서브그룹 내에 모든 가입자에게 그룹 키의 재분배 과정을 수행하여야 하기 때문에 빈번한 이동이 있을 경우 키의 재분배 시간을 많이 요구한다. 또한 Naïve, Iolus 방식의 그룹 키 관리는 단일 노드의 결함이 전체 시스템 결함의 원인이 될 수도 있고, 동적으로 변하는 라우팅 경로에 대하여 원활하게 서비스 보호를 유지할 수 없다[2]. 또한 데이터 전송시 그룹이 바뀔 때마다 키 관리자로 하여금 그룹 키에 의하여 데이터의 변환이 필요하므로 많은 데이터 전송시간이 필요하다. 따라서 소규모 가입자만으로 능동적인 라우팅 프토토콜을 지원하는 그룹 키 관리가 필요하다[3,4].

2.2 PIM-SM 라우팅 알고리즘

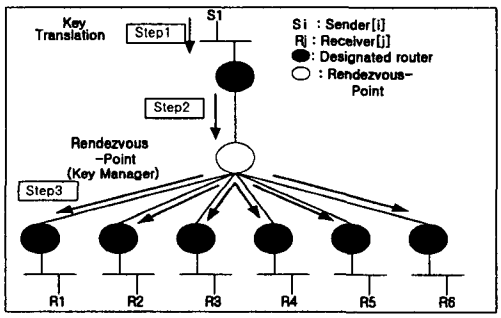
PIM-SM 라우팅 알고리즘의 수신자는 하나 이상의 RP를 가지고, 송신자와 RP사이의 공유트리를 두어 라우팅 경로를 공유하여 네트워크의 부하를 감소시킨다[6]. 각 RP의 정보와 멀티캐스트의 그룹에 대한 정보를 항시 가지고 있어야 하는 DR(Designated-Router)은 송신자로부터의 멀티캐스트 그룹에 속한 첫 번째 라우터로서 RP에 대한 정보를 가지고 송신자의 등록에 대한 정보를 RP에게 송신한다. 여기서 DR은 자신이 속한 그룹 내의 모든 RP의 정보를 부트스트랩 프로토콜로 정보를

수집한다. 자신에 속해져 있는 호스트로부터 그룹의 가입을 나타내는 IGMP를 수신시 어떤 RP로 송신해야 할지 미리 알고 있어야 한다. 한편 PIM-SM은 라우팅 경로에 있어서 최소거리경로를 사용한다. 원하는 QoS를 얻지를 못할 때는 수신자는 각 라우터에게 최단경로를 요구하여 송신자로부터 최단경로로 데이터를 수신할 수 있다[5].

3. 동적 멀티캐스트 그룹 키 관리 프로토콜 제안

3.1 PIM-SM 그룹 키 관리 구조

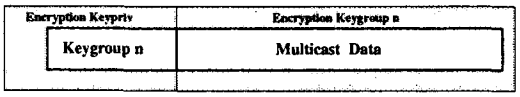
PIM-SM의 그룹 키 관리 구조는 그림 1과 같은 구성요소로 되어있다. 각 RP당 하나의 키 관리자를 두어 서브그룹으로 나누는 기준이 되고, DR(Designated Router)는 송신자와 수신자로부터 가장 근접한 라우터로서 RP에 대한 정보를 갖고 경로설정을 수행한다. 각 송신자는 Key Translation을 한 후 해당 그룹 키를 이용하여 데이터를 암호화하여 전송한다.



(그림 1) PIM-SM 그룹 키 관리 구조

본 논문에서 제안한 PIM-SM 그룹키 관리는 먼저 송신자별 그룹 키를 키 관리자로부터 할당받아 송신자만의 키를 이용하여 메시지를 암호화 한 후 RP로 송신한다. 수신자는 RP로부터 수신한 데이터를 보호채널의 비밀 키를 갖고 메시지와 그룹 키를 복호화 한다. 이후 최소거리경로로 변경하여도 송신자의 그룹 키는 유효하므로 데이터의 복호화가 가능하다. 그림 2는 송신자가 데이터를 전송 할 때 멀티캐스트 데이터를 그룹 키로 암호화하고 그룹 키를 다시 보호채널의 비밀키로 암호화하는 것을 나타낸다.

Keypriv : 보호채널에서 비밀키
Keygroup n : 그룹 n에 대한 그룹키



(그림 2) 암호화된 데이터 형식

3.2 동적 멀티캐스트 그룹 키 관리 프로토콜

(1) 송신자의 멀티캐스트 그룹 등록 프로토콜

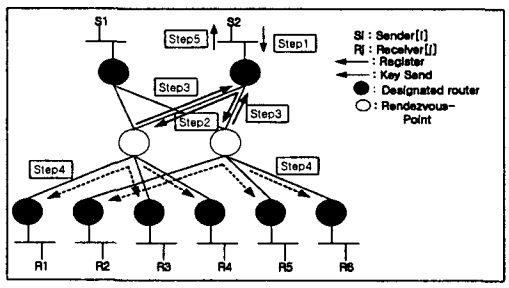
Step 1. 송신자는 DR에게 등록을 요구하는 IGMP를 전송한다.

Step 2. DR은 서브 그룹을 관리하는 각각의 RP에게 S2에 대한 그룹 가입을 알린다.

Step 3. 인증 절차를 거쳐 송신자가 확인되면 각각의 RP는 DR에 송신자에 할당된 그룹 키를 전송한다.

Step 4. 수신자에게 송신자 S2에 대한 보호채널을 통한 비밀 키로 그룹 키를 암호화하여 전송한다.

Step 5. DR은 송신자에게 각각의 RP에서 받은 그룹 키들을 송신자에게 전송한다.



(그림 3) 송신자 등록 과정

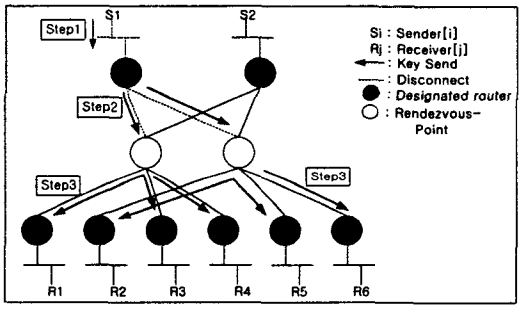
(2) 송신자의 멀티캐스트 그룹 탈퇴 프로토콜

Step 1. 송신자는 DR에게 탈퇴를 요구하는 IGMP를 전송한다.

Step 2. DR은 각각의 RP에게 송신자의 탈퇴를 알리는 IGMP를 송신하고, DR과 RP와의 경로를 종료를 요구한다.

Step 3. RP는 수신자에게 송신자 S1의 탈퇴를 알리는 메시지 송신 한 후 송신자 S1과의 경로를 종료한다.

S1을 가장한 침입자가 수신자에게 다른 데이터를 전송할 수 있기 때문에 송신자의 멀티캐스트 그룹 탈퇴 시 모든 수신자에게 더 이상 S1의 그룹 탈퇴를 각 수신자에게 전송하여야 한다.



(그림 4) 송신자 탈퇴과정

(3) 수신자의 멀티캐스트 그룹 가입 프로토콜

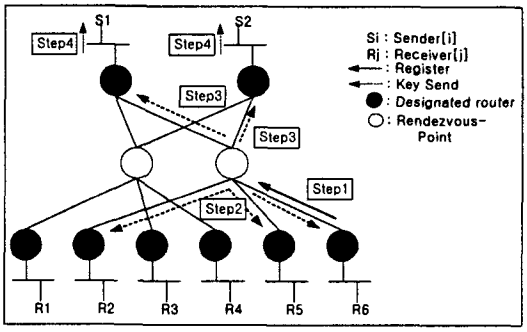
Step 1. 수신자는 DR을 거쳐 RP에게 등록을 요구하는 IGMP를 전송한다.

Step 2. RP 인증 절차를 거쳐 수신자가 확인되면 RP는 멀티캐스트 그룹의 다른 수신자에게 그룹 키를 재분배한다.

Step 3. RP는 서브 그룹 송신자들에게 그룹 키를 재분배하기 위해 DR에게 새로운 그룹 키를 전송한다.

Step 4. DR은 송신자에게 RP에게 새로운 그룹 키들을 받는다.

새로운 수신자 R6은 가입 이전의 데이터를 복호화 하지 못해야 하기 때문에 서브 그룹 전체에 키를 재분배를 해야 한다.



(그림 5) 수신자 등록과정

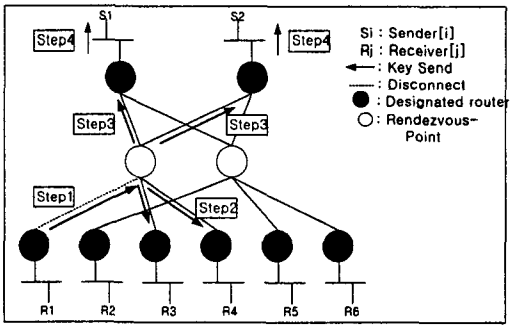
(4) 수신자의 멀티캐스트 그룹 탈퇴 프로토콜

Step 1. 수신자는 RP에게 탈퇴를 요구하는 IGMP를 전송한다.

Step 2. RP는 서브 그룹의 다른 수신자들에게 보호채널을 통하여 새로운 키를 재분배한다.

Step 3. RP는 서브 그룹 송신자들에게 그룹 키를 재분배하기 위해 DR에게 새로운 그룹 키를 전송한다.

Step 4. RP는 Backward/Forward Secrecy에 어긋나기 때문에 송신자와 수신자에게 그룹 키를 재분배해야 한다.



(그림 6) 수신자 탈퇴 과정

(5) 최소거리 경로 설정

Step 1. 수신자는 RP에게 최소거리경로를 요구하는 ICMP를 받는다.

Step 2. RP는 DR에게 수신자1에 해당하는 최소거리경로 변경 명령하고, DR은 수신자1에 대한 최소거리경로를 결정한다.

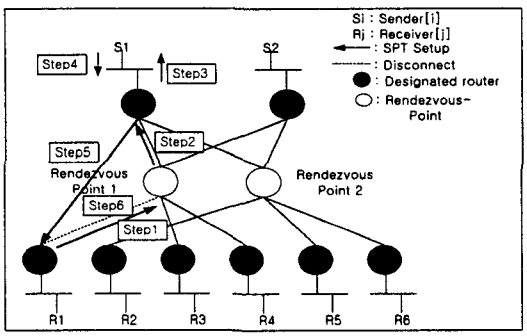
Step 3. DR은 송신자에게 수신자에 대한 데이터 전송을 명령한다.

Step 4. 송신자는 기존의 전송 방식과 동일하게 데이터를 DR에게 각각의 그룹 키로 암호화하여 전송한다.

Step 5. DR은 수신자1에게 최소거리경로로, 나머지 수신자들에게 멀티캐스트로 데이터를 전송한다.

Step 6. 데이터를 수신한 수신자는 RP1과의 경로를 중단한다.

송신자는 기존의 그룹 키를 그대로 사용하므로 수신자는 다른 경로로부터 받은 데이터에 대하여 새로운 키의 분배 없이 데이터를 복호화 할 수 있다.



(그림 7) 최소거리 경로 설정

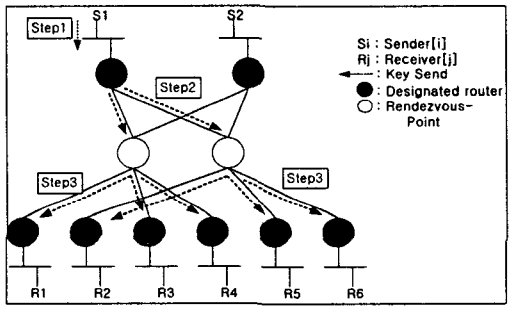
(6) 데이터 전송과정

멀티캐스트 그룹은 그림 8과 같이 두 개의 그룹으로 나누어진다. (R1, R3, R4)가 그룹 1에 속하고, (R2, R5, R6)가 그룹2에 속한다. 키 관리자 상호간의 직접적인 정보 교환이 없는 관계로 추가적인 경로도 필요 없다. 데이터의 전송과정은 다음과 같다.

Step 1. 송신자는 각 서브그룹에 받은 그룹 키로 데이터를 암호화하여 데이터를 DR에게 전송한다.

Step 2. DR은 각 서브그룹 RP에게 그룹 키에 의한 데이터 변환없이 RP에게 전송한다.

Step 3. RP는 서브그룹에 속한 모든 수신자에게 그룹 키에 의한 데이터 변환 없이 수신자에게 전송한다.



(그림 8) 데이터 전송 과정

4. 실험 및 평가

4.1 실험 모델

본 실험에서는 제안한 동적 멀티캐스트 그룹 키 관리 프로토콜을 분석하기 위하여 그림 8의 실험모델에서 기존의 그룹 키 관리 방식과의 성능 비교를 하였다. 실험 모델은 PIM-SM 라우팅 프로토콜의 특징인 소수의 송신자와 원거리에 있는 RP에 속한 다수의 수신자 상태를 고려하여, 두 개의 송신자와 두 개의 RP 그리고 하나의 RP당 송신자 1개와 수신자 3개를 구성하였다. 다른 그룹 키 관리 방식에 적용한 실험과 동일하게, 사용한 실험 파라미터는 표 1과 같다.

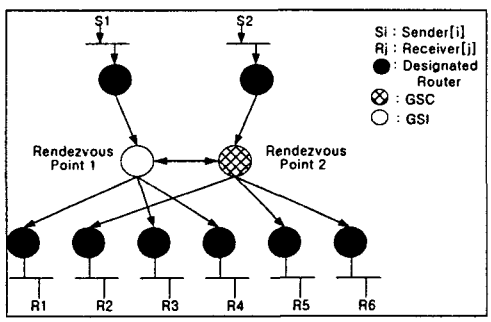
<표 1> 실험 파라미터

종 류	변 수 명
데이터의 암호화 시간	T_{En}
데이터의 복호화 시간	T_{De}
각 노드당 데이터전송시간	$T_{DataSend}$
가입/탈퇴에 대한 IGMP 수신 시간	T_{IGMP}
등록 소요시간	$T_{Register}$

데이터의 전송은 10Mbps Ethernet을 이용하여 UDP로 전송하였다. 10Kbyte의 데이터를 DES 알고리즘으로 암호화시 110ms 지연이 생긴다. 망에서 키 분배하는데 소요되는 시간은 다음과 같다. 키의 전송시간과 키 설정시간은 10ms로 정한 후, Iolus 그룹 키 관리 방식과 Nortel 그룹 키 관리 방식에 적용하여 각 데이터를 산출한다. 10Kbyte의 데이터를 송신자 S1에서 전송하여 각 수신자 그룹에게(R3, R5, R6)에게 전송함을 가정하고, 키 관리자에서 수신별 키 설정시간을 TKeySet, 키 전송시간 TKeySend을 각각 정하여 놓는다.

4.2 기존 그룹 키 관리 방식과의 비교

Iolus에서 제안된 그룹 키 관리는 코어구조를 요구하는 멀티캐스트 그룹 키 관리로서 적용된 실험모델은 그림 9와 같다.

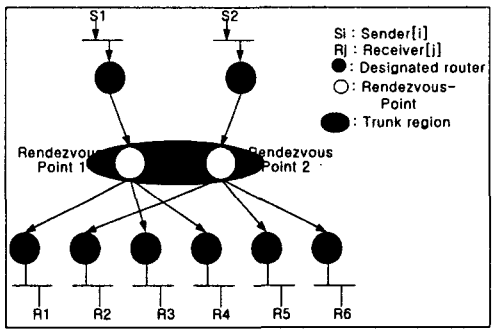


(그림 9) Iolus 방식의 데이터 전송과정

데이터 전송과정에서 데이터가 S1에서 R6까지 전송되기 위해서는 우선 RP간의 복호화 키를 RP 상호간 미리 전송하고, S1→DR→RP1→RP2→R6순서로 데이터가 전송된다. 데이터는 S1의 그룹 키로 암호화한 후 RP1에서 RP2에게 데이터를 그룹 키에 의해 키 변환작업이 수행되고, 데이터를 받은 RP2는 다시 자신이 관리하고 있는 서브그룹 키로 데이터에 키 변환 작업을 거쳐 R6에 전송하고 R6는 자신의 복호화 키로 복호를 하는 데이터 전송과정을 거친다.

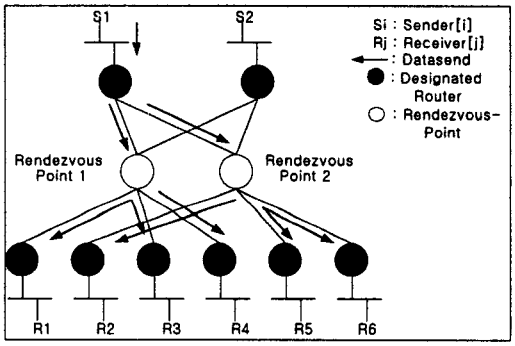
데이터를 전송하는데 걸리는 시간은 데이터에 대한 암호화/복호화 과정이 총 3번 거쳐 일어나게 되므로 3*(TEn+TDe)시간이 소요된다.

Nortel 멀티캐스트 그룹 키 관리에서 적용된 실험모델은 그림 10과 같다. Nortel 방식의 그룹 키 관리의 특징은 중간의 특정 라우터들을 트렁크 지역으로 만들고 트렁크 그룹 키를 설정하여 라우터 상호간 키 변환작업이 생략될 수 있으나, 각 리프당 다른 그룹 키를 두어 각각의 리프키에 맞게 키 변환작업이 필요하다. 전송순서는 S1→DR→RP1→RP2→R6로서 트렁크 키로 암호화/복호화된 후, 다시 각각의 리프키에 맞는 암호화/복호화 작업이 필요하다. 데이터를 전송하는데 걸리는 시간은 데이터에 대한 암호화/복호화 과정이 총 2번 일어나므로 2*(TEn+TDe)시간이 소요된다.



(그림 10) Nortel 방식의 데이터 전송과정

제안된 그룹 키 관리에서 적용된 실험모델은 그림 11과 같다. 제안된 그룹 키 관리의 특징은 중간의 라우터에서 데이터를 그룹 키에 의한 키 변환이 없이 수신자에게 전송이 가능하므로 송신자와 수신자가 수행하는 단 1번만의 데이터 암호화/복호화 작업을 거치면 된다. 전송순서는 다음과 같다. S1→DR→RP1→RP2→R6의 순서로 데이터를 전송하는데 걸리는 시간은 데이터에 대한 암호화/복호화 과정이 총 1번 일어나게 되므로 1*(TEn+TDe)시간이 소요된다.



(그림 11) 제안된 방식의 데이터 전송과정

4.3 실험 결과

각각의 그룹 키 관리 방식에 대한 실험 결과, Iolus 그룹 키 관리 방식은 3회 키 변환이, Nortel 그룹 키 관리방식은 2회 키 변화가 일어난다. 실험 모델을 적용한 3가지 그룹 키 관리로 송신자가 등록 과정을 거쳐 10 Kbyte의 데이터 전송시의 총 소요 시간 TTotal은 다음과 같다.

$$T-Total = T-Register + T-Data$$
$$T-Register = T-IGMP + T-KeySet + T-KeySend$$
$$T-Data = T-DataSend + T-KeyTra$$
$$T-KeyTra = T-En + T-De$$

여기서 $T-Register$의 시간은 모든 구조에서 동일하기 때문에 구조에 따른 데이터 전송 시간 $T-DataSend$는 다음과 같다.

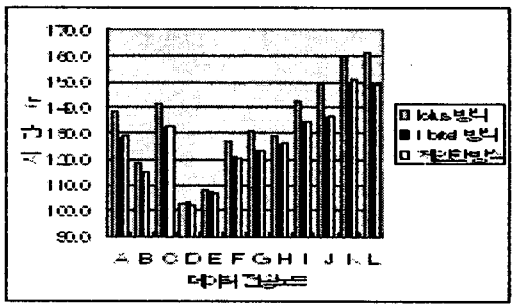
$$T^{IIM-SM}-Data = 2T-DataSend + T-KeyTra$$
$$T^{Iolus}-Data = 3T-DataSend + 3T-KeyTra$$
$$T^{Nortel}-Data = 3T-DataSend + 2T-KeyTra$$

따라서 총 소요시간 TTotal은 아래와 같다.

$$T^{IIM-SM}-Total = T-IGMP + K-Set + K-Send + 2T-DataSend + T-KeyTra$$
$$T^{Iolus}-Total = T-IGMP + K-Set + K-Send + 3T-DataSend + 3T-KeyTra$$
$$T^{Nortel}-Total = T-IGMP + K-Set + K-Send + 3T-DataSend + 2T-KeyTra$$

제안한 동적 멀티캐스트 그룹 키 관리 방식의 전송시간은 Iolus 그룹 키 관리방식보다 $T-DataSend + 2T-KeyTra$, Nortel 그룹 키 관리방식보다 $T-DataSend + T-KeyTra$ 만큼 적게 소요된다.

다음은 데이터 전송 평균 시간을 나타낸 것이다.



(그림 12) 데이터 전송 평균 시간

실험결과 각 그룹 키 관리의 특징을 비교한 결과는 다음과 같다.

<표 2> 그룹 키 관리의 비교 결과

구 분	Iolus	Nortel	제안한 방식
구 조 형 태	다중구조	분산구조	분산구조
그룹 확장성	매우높음	높 음	높 음
단일 실패에 대한 결함	있 음	없 음	없 음
최소거리경로 지원	지원하지 않음	지원하지 않음	지원함
실험 모델 적용사 추가 구성요소	경로, GSC, GSI	경로, Trunk Region	없음
그룹키에 의한 데이터변환	3 회	2 회	1회

제안한 PIM-SM 그룹 키 관리 방식은 분산된 구조로서 Iolus 그룹 키 관리 방식의 단점인 단일 실패에 대한 결함이 없고, 기존의 그룹 키 관리 방식에서 제공할 수 없는 최소거리경로에 대한 데이터의 보안을 지원할 뿐만 아니라, 실험 모델을 적용할 경우 추가적인 구성 요소가 없어 간단한 구조가 되며, 그룹 키에 대한 데이터 변환작업이 1회로서 데이터의 전송시간이 단축된다. 또한 비교실험에 데이터 평균 전송시간이 가장 적게 소요되는 것을 보였다.

5. 결 론

본 논문에서 제안한 전자상거래를 위한 멀티캐스트 그룹 키 관리 프로토콜은 서브그룹을 RP 단위로 나누고, RP는 유일한 그룹 키를 두어 최소거리경로로의 데이터 수신 시 새로운 키 분배 없이 바로 전송이 가능하다. 또한 RP간 데이터 전송이 없으므로 분산구조의 형태가 되어 서브그룹에 따른 키 변환 작업이 불필요하여 전송시간이 다른 구조에 비해 단축이 된다.

실험결과 기존의 Iolus, Nortel 그룹 키 방식과 달리 최소거리경로를 지원함을 알 수 있었고, PIM-SM 라우팅의 구조에 다른 추가 구성 요소 없이 그대로 사용할 수 있다는 장점을 갖게 되었다. 또한 데이터 변환 횟수가 1회로 전송시간의 단축되고, 전송시간이 적게 소요됨을 알 수 있었다.

참고문헌

[1] Moyer MJ, Rao JR, Rohatgi P., "A Survey of Security Issues in Multicast Communications," IEEE Network , V.13 No.6, pp.12-23, 1999.

[2] Suvo Mittra. "Iolus:A Framework for Scalable Secure Multicasting," Computer Communication Review, V.27 N.4, pp.277-288, 1997.

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

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

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

[6] Sahasrabuddhe L H, Mukherjee B, "Multicast Routing Algorithms and Protocol: A Tutorial", IEEE Network, V.14 N.1, pp.90-102, 2000.

[7] Boivie R, Feldman N, Metz C, "Small group multicast: A new solution for multicasting on the Internet", IEEE Internet Computing , V.4 N.3, 75-79, 2000.

홍 종 준

1991년 인하대학교 전자계산공학과(공학사)
1993년 인하대학교 전자계산공학과(공학석사)
2002년 인하대학교 전자계산공학과(공학박사)
1999 ~ 현재 청강문화산업대학 컴퓨터소프트웨어과 교수

김 태 우

1984년 인하대학교 전자공학과 (공학사)
1990년 인하대학교 전자계산공학과(공학석사)
1996년 고려대학교 전산과학과(공학박사)
1997 ~ 현재 성공회대학교 컴퓨터정보공학부과 교수