실시간 멀티캐스팅 정보보안을 위한 그룹키 관리

홍 종 준** 황 교 철**

요 약
실시간 데이터를 사용자 그룹내에 전송하는 멀티캐스트는 유니캐스트에 비해 일괄의 수가 많으므로 부담적인 접점자로부터 신부문장, 사무소, 거주 공간 등에 많은 공익을 받기 쉽다. 이를 방지하기 위해 세분화된 기존의 그룹키 관리 구조는 비교적 규모가 큰 규모에 맞는 라우팅 프로토콜에 적합하도록 설계되었다. 따라서 소규모의 라우팅 구조에 적용된 기존 그룹키 관리 구조는 항상 기본적인 고속 트래픽 요구사항이나 키 문제, 키 복잡성, 키 관리 문제를 갖는 문제점들을 갖게 된다. 이에 본 논문에서는 소규모 라우팅 구조에 적합한 PIM-SM 방식을 이용하여, 안전한 멀티캐스트 통신이 가능한 그룹키 관리 구조를 제안한다. 제안한 방식은 멀티캐스트 통신 그룹의 Rendezvous Point에 기반하여 구조로, 각 Rendezvous Point 관리자에 의해 전송을 부여하여 송수신자간에 그룹키를 주고 받도록 한다. 이로서 송수신자간에 보호체계가 설정되고 안전한 데이터 전송이 가능하게 된다. 이는 그룹키의 특성 데이터 전송방법이 필요하고 있고 경로 변경에 따른 새로운 키 분배가 불필요하게 되어 데이터 결손시간에 단축되는 장점을 갖게 된다.

A Group Key Management for Real-Time Multicasting Information Security

Jong-Joon Hong** Kyo-Chul Hwang**

ABSTRACT

The multicast transmitting the real-time data to groups may easily have many attacks from abnormal attackers because it has many links as compared to the unicast. The existing group key management architectures for preventing these problems are designed for protocols suitable for a large scale. Thus these architectures applied to a small scale routing protocols may have many overheads with key distribution and a constant core tree. Therefore this paper proposes a group key management protocol for a secure multicast in PIM-SM multicast group communication. The proposed method divide multicasts groups with Rendezvous Point, and subgroup key managers are established in each RP and can be transmitted groupkeys between senders and receivers, so the security channel is set up for secure data transfer. And this does not have needs of the data translation for group keys and the new key distribution for path change. As a result of this, the data transmission time can be reduced.

키워드: 멀티캐스트(Multicast), 그룹키(Group Key), PIM-SM

1. 서론

멀티캐스트는 유니캐스트나 브로드캐스트에 비해 효과적인 그룹 접근이 어렵고 트래픽을 많은 링크를 경유하기 때문에, 신문광고, 사무소 간 공익, 재충전 공익 등에 위협이 증가하고 있어 많은 공익기관을 제공하고 있다(2,3,6). 이러한 멀티캐스트의 전송한 루트를 통한 공유에 위와 같은 악용의 방식을 방지하기 위해 멀티캐스트가 공유해야 하며, 그룹 내에 공유하고 있는 백워드 서서히 전송에 사용이는 백워드 공유의 백워드 secrecy와 Forward secrecy를 만족하도록 새로운 엔트리가 그룹에 참여하게 기존의 백워드 그룹을 탈락할 때마다 새로운 그룹키로 변경되어야 한다(1,6,11). 기존에 제안된 그룹키 관리 구조는 크게 중앙집중 방식과 분산 방식으로 분류할 수 있다(4,6). 중앙집중 방식은 하나의 서버가 그룹키 관리하므로 블레이크 증가로 블레이크가 서버에 집중되는 확장성에 문제가 있다. 이에 반해 분산인 서버에 각각의 그룹키를 갖는 분산 방식은 중앙집중 방식에 비해 확장성에 우려한다(7,9). 이러한 방식들은 CBT (Core Based Tree)를 이용하여 코어를 중심으로 멀티캐스트와 블레이크가 밀집되어 고정된 경로에 근거한 데이터 전송이 가능하다. 또한 이들은 기 관리를 거절하기 때문에 그룹키 변경이 필요하기 때문에 멀티캐스트 브러우징 환경에 적합한 PIM-SM 브러우징 구조(5,6)를 이용한 그룹키 관리 방식을 제안한다.
SM 라우팅은 대규모에 적합한 CBT, DVMRP[6]에 달리 소규모에 저소득이 분산되어 있는 노드들에 RP(Rendezvous-Point) 단위로 나누고, 데이터를 송신하지만 RP까지 유니캐스트로 전송하고, RP에서 수신자까지는 멀티캐스트로 전송한다. 이러한 혼합적 방식에 적합한 그룹키 관리 방식은 없다고 알려져 있다. 제안한 방식은 RP에 그룹 키를 관리하는 그룹키 관리자 두어 송신자의 그룹키, 그룹키를 부여하고 RP는 인증된 수신자에게 그룹키를 전달한다. 송신자는 데이터를 그룹키로 암호화하여 RP에 전송하고 RP는 암호화된 데이터를 부그룹 내 수신자에게 전송하고, 수신자는 이전에 받은 그룹키를 이용하여 데이터를 복호화한 다. 따라서 제안한 방식은 PIM-SM 라우팅 구조의 변형 없이 사용하여 기존의 그룹키 관리 구조에 비해 간단함을 알 수 있고, 라우팅의 경로 변경에도 그룹키를 미리 관리함으로 하여, 네트워크의 전송 시간이 단축될 수 있다.

2. 관련 연구

2.1 멀티캐스트 그룹키

그룹키의 사용은 허용된 그룹의 멤버들만이 정보를 얻을 수 있도록 하기 위한 것으로 그룹내 멤버가 아닌 그룹키를 알아 내지 못하도록 하는 것은 멀티캐스트 정보보조의 기존 조건이란 할 수 있다. 따라서 멀티캐스트 그룹키는 멤버의 그룹 가입(Join)과 기존 멤버의 그룹 탈퇴(Leave)에 따라 현재 그룹키를 새로운 그룹키로 변경하는 기 재본체 구성을 가져야 한다. 이는 forward secrecy와 backward secrecy를 만족하기 위해서이다[11]. forward secrecy는 멤버가 탈퇴할 경우 탈퇴된 멤버가 이전에 공유하고 사용하던 그룹키로부터 탈퇴 이전의 그룹키를 생성할 수 없도록 하기 위한 조건이며, backward secrecy는 새로운 멤버가 합법적으로 가입하여 그룹키를 공유하게 되더라도 가입이전의 그룹키는 알아낼 수 없도록 하기 위한 조건이다.

2.2 기존 멀티캐스트 그룹키 관리 방식의 문제점

Naive 방식[3], Iolus 방식[4], Nortel 방식[5,6]에서 제안된 방식은 많은 멤버가 갖는 대규모의 그룹키 관리 방식으로 부그룹의 구조가 매우 크다. 따라서 부그룹 내에 하나의 멤버가 탈퇴해야 부그룹 내에 모든 멤버들에게 그룹키의 재본체 시간이 수반되어야 하는데, 반면의 이전이 있 경우 많은 시간이 앞으로 시간을 요구한다. 또한, Naive 방식, Iolus 방식의 그룹키 관리자는 단일 노드의 오류가 전체 시스템의 경향을 인하기도 한다. 하지만 기존의 그룹키 관리 방식은 동적으로 변경되는 경로설정에 대해 완전한 보호가 제공하지 않고, 데이터의 전송의 경우 기 관리자에 따른 반변한 그룹키 변환으로 많
32 PIM-SM 그룹기 관리 프로토콜
3.2.1 송신자의 멀티캐스트 그룹 등록
송신자의 멀티캐스트 등록은 부그룹을 관리하는 RP를 통한 그룹키 전달에 따른다. 이에 세부적인 절차는 아래와 같이 이루어진다(그림 2)에 포함하였다.

1. 송신자 S'는 동록을 요구하는 IGMP를 DR에게 전송한다.
2. DR는 부그룹을 관리하는 각 RP에게 S'에 대한 그룹 가입을 알린다.
3. 송신자 S'의 인증이 승인되면, 각 RP는 DR에게 송신자에 할당된 그룹키를 전송한다.
4. 송신자 S'는 정의된 보호체널을 통해 그룹키를 암호화하여 수신자에게 전송한다.
5. DR은 각 RP에서 받은 그룹키들을 송신자 S'에게 전송한다.

(그림 2) 송신자의 그룹 등록 과정

3.2.2 송신자의 그룹 탈퇴
송신자의 그룹 탈퇴는 다음의 단계에 따라 수행되며, 이는 (그림 3)과 같다. 그룹을 탈퇴한 송신자 S'를 가정한 절차가 그룹 내 수신자에게 데이터를 전송할 수 있기 때문에 송신자의 멀티캐스트 그룹 탈퇴시 모든 수신자에게 해당 S'의 그룹 탈퇴 메시지를 각 수신자에게 전송하여야 한다.

1. 수신자 R는 DR에게 데야하는 IGMP를 전송한다.
2. RP는 각 RP에게 송신자의 탈퇴를 알리는 IGMP를 전달하고, DR과 RP의 경로 채소를 요구한다.
3. RP는 송신자에게 탈퇴 메시지를 전달한 후, 송신자 S'의 경로연결을 해제한다.

3.2.3 송신자의 멀티캐스트 그룹 가입 프로토콜
새로운 수신자의 그룹 가입에 대한 절차는 다음과 같다. 새로 가입한 수신자 R는 가입하기 전에 존재하는 그룹 키를 알 수 없도록 하기 위해서 부그룹 전체의 새로운 키를 재분배해야 한다. 이는 backward secrecy를 만족하도록 하기 위한 절차이다.

1. 수신자 R는 DR에게 데야하는 IGMP를 전송한다.
2. 수신자 R이 승인되면, RP는 수신자들에게 그룹키를 재분배한다.
3. RP는 송신자들에게 그룹키를 재분배하기 위해 DR에게 새로운 그룹키를 전송한다.
4. DR은 송신자에게 RP에게 받은 새로운 그룹키를 전송한다.

(그림 4) 수신자의 그룹 등록 과정

3.2.4 수신자의 멀티캐스트 그룹 탈퇴 프로토콜
수신자 그룹 탈퇴는 다음의 단계를 수행하여야 하며 (그림 5)와 같이 진행된다. 그룹 탈퇴에 따른 그룹키의 재분배는 forward secrecy를 위해 필요하기 때문이다.

1. 수신자는 RP에게 탈퇴를 요구하는 IGMP를 전송한다.
2. RP는 부그룹의 다른 수신자들에게 보호체널을 통하여 새로운 키를 재분배한다.
3. RP는 송신자들에게 그룹키를 재분배하기 위해, 새로운 그룹키를 DR에게 전송한다.
4. DR에서 수신받은 DR은 송신자들에게 그룹키를 재분배한다.

(그림 3) 송신자의 그룹 탈퇴 과정
3.2.5 SPT의 경로 설정
SPT(Shortest Path Tree)의 경로 설정과정은 아래의 5단계를 거쳐 수행된다. 여기서 송신자는 기존의 그룹키를 그대로 사용하게 되며, 수신자는 SPT의 경로로부터 받은 데이터에 대하여 새로운 키를 발급하여 데이터를 복호화할 수 있다. 아래 그림은 SPT에 의한 경로 설정에 대한 그룹키 설정에 대한 설명이다.

1. 수신자는 RP에게 SPT의 경로를 요구하는 ICMP를 전송한다.
2. RP는 DR에게 SPT의 경로변경 메시지를 전송하고, DR는 전송자에 대한 SPT의 경로를 결정한다.
3. DR는 전송자에게 수신자에 대한 데이터 전송메시지를 전송한다.
4. 송신자는 데이터를 각각의 그룹키로 암호화하여 DR에게 전송한다.
5. DR은 수신자에게 설정된 SPT의 경로로, 나머지 수신자들에게는 멀티캐스트로 데이터를 전송한다.
6. 데이터를 수신한 수신자는 RP와의 경로 연결을 해제한다.

4. 실험 및 성능 분석
본 논문에서 제안한 그룹키 관리 구조를 분석하기 위하여 실험을 수행하였다. 실험은 그룹의 구성과 데이터 전송, 그리고 그룹키를 변경할 때의 성능을 비교하였다. 실험은 SOAP(Simple Object Access Protocol)을 사용하여 데이터 전송을 수행하고, 그룹키를 변경할 때의 성능을 비교하였다.
표 1 실험 파라미터

<table>
<thead>
<tr>
<th>종류</th>
<th>변수 명</th>
</tr>
</thead>
<tbody>
<tr>
<td>데이터 활성화 시간</td>
<td>$T_m$</td>
</tr>
<tr>
<td>데이터 비활성화 시간</td>
<td>$T_d$</td>
</tr>
<tr>
<td>데이터 전송시간</td>
<td>$T_{total}$</td>
</tr>
<tr>
<td>KMP 수신 시간</td>
<td>$T_{mp}$</td>
</tr>
<tr>
<td>동작 소요시간</td>
<td>$T_{ex}$</td>
</tr>
<tr>
<td>커 기적시간</td>
<td>$T_{rel}$</td>
</tr>
<tr>
<td>커 전송시간</td>
<td>$T_{total}$</td>
</tr>
</tbody>
</table>

Iolus에서 제안된 그룹키 관리의 제시한 실험모델을 적용한 결과 데이터를 전송하는데 걸리는 시간은 데이터에 대한 암호화/복호화 과정이 $3 \times (T_m + T_d)$ 이 소요된다. 또한 Nortel 방식의 제시한 실험모델을 적용한 결과, 데이터를 전송하는데 걸리는 시간은 데이터에 대한 암호화/복호화 과정이 $3 \times (T_m + T_d)$ 이 소요된다. 제안된 그룹키 방식은 데이터에 대한 암호화/복호화 과정이 $2$회 발생하여, 데이터 전송시간은 $4 \times (T_m + T_d)$ 시간이 소요된다.

각 라우터에 속한 호스트가 데이터를 전송할 때, 각 부그 루에서 데이터를 수신하는데 걸리는 시간을 측정한 결과는 각 라우터에 속한 호스트까지 데이터가 전달되는 평균시간과 최대소요시간을 (그림 8)와 (그림 9)에 나타낸다. 측정한 시간은 데이터 전송시간뿐 아니라 기 관리에 의해 이뤄지는 <표 1>에 제시한 각 파라미터의 시간을 포함하고 있다.

(그림 8) 데이터 전송 평균시간

(그림 9) 데이터 전송 최대소요시간

제안한 PIM-SM 그룹키 관리 방식은 분산된 구조로서 Iolus 그룹키 관리 방식의 단점은 단일 노드 오류에 대한 결함이 없고, 기존의 그룹키 관리 방식에서 제공할 수 없는 SPT의 경로에 대한 데이터의 보안을 지원할 뿐만 아니라, 실험 모델을 적용한 경우 추가적인 구성 요소가 없어 간단한 구조가 되며, 그룹키와 관련된 데이터 수작업이 이루어지지 않기 때문에 데이터의 전송시간이 단축된다. 또한 비교실험에서 데이터 전송시간과 최대전송시간에서 가장 적게 소요되는 것을 보였다.

제안한 그룹키 방식을 이용하여 발생하는 부하를 기존의 방식과 비교하기 위해 다음의 실험을 수행하였다. 제안한 방식은 소규모의 라우팅 구조에 적합하므로 50개 이하의 정적 작업도 제시하였고, 본 실험 모델로 구축된 50개의 그래프를 기본으로 하여 수행하였다. 각 그룹키 방식의 실험 결과에서 수행시간은 일정하게 저항하지만 평균값의 반도는 1회, 각 범위에서 수행하는 기존 개수와 평균값을 구하고, 이에 대한 최대값과 평균값을 구하였다. 결과는 <표 3>와 같으며, 이 를 (그림 10)과 (그림 11)에 나타내었다.

(그림 8) 데이터 전송 평균시간

(그림 9) 데이터 전송 최대소요시간

제안한 방식은 Iolus가 약 3배, Nortel이 약 2배 많은 것으로 분석되었다. 따라서 기존에 따른 하나의 제안한 방식이 기존의 방식에 비해 부하가 적을 것을 알 수 있다.

표 2 그룹키 관리 방식의 비교

<table>
<thead>
<tr>
<th>구분</th>
<th>Iolus</th>
<th>Nortel</th>
<th>제안한 방식</th>
</tr>
</thead>
<tbody>
<tr>
<td>특장성</td>
<td>배수율음</td>
<td>높음</td>
<td>높음</td>
</tr>
<tr>
<td>단일노드오류에 대한 결함</td>
<td>없음</td>
<td>없음</td>
<td>없음</td>
</tr>
<tr>
<td>SPT 경로 지원</td>
<td>지원 없음</td>
<td>지원 없음</td>
<td>지원함</td>
</tr>
<tr>
<td>실험 모델 적용시 추가 구성요소</td>
<td>경로, GSC, GSI</td>
<td>경로, Trunk Region</td>
<td>없음</td>
</tr>
<tr>
<td>그룹키에 의한 데이터 손실</td>
<td>3회</td>
<td>2회</td>
<td>1회</td>
</tr>
</tbody>
</table>

표 3 그룹별로의 등록 및 활성화에 대한 경선 분석 실험

<table>
<thead>
<tr>
<th>실험 파라미터</th>
<th>범위수</th>
</tr>
</thead>
<tbody>
<tr>
<td>실험 파라미터</td>
<td>50</td>
</tr>
<tr>
<td>범위수</td>
<td>100</td>
</tr>
<tr>
<td>20</td>
<td>150</td>
</tr>
<tr>
<td>30</td>
<td>200</td>
</tr>
<tr>
<td>40</td>
<td>250</td>
</tr>
<tr>
<td>50</td>
<td>300</td>
</tr>
</tbody>
</table>

제안한 방식 | 최대값 | 평균값 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Iolus</td>
<td>1.32</td>
<td>1.45</td>
</tr>
<tr>
<td>Nortel</td>
<td>1.18</td>
<td>1.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>제안한 방식</th>
<th>최대값</th>
<th>평균값</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iolus</td>
<td>3.20</td>
<td>3.24</td>
</tr>
<tr>
<td>Nortel</td>
<td>3.02</td>
<td>3.13</td>
</tr>
</tbody>
</table>

(그림 10) 실험 결과

(그림 11) 실험 결과

(그림 12) 실험 결과
5. 결 론

본 논문에서 제안한 PIM-SM 트리를 관리 방식은 RP 단위로 부프로필을 나누고, 각 RP에 송신자에게 송신자 고유의 그룹을 두어 SPT 경로로의 데이터 전달에도 새로운 커리큘럼 없이 바로 전송이 가능하다. 또한 각 RP간 데이터 전송이 없으므로 분산구조의 형태가 되어 PIM-SM에서도 모든 사용자가 정상의 보호를 받고, 부프로필에 따른 편리한 작업이 불필요하며 전송시간이 기존의 방식에 비해 적게 소요됨을 알 수 있다. 또한 실험결과에 의하면 Iolus, Nortel 그룹을 방식에 비해 기존 방식에 따른 부하가 적고 데이터 전송 시간이 단축됨을 알 수 있었다.

제안한 그룹의 관리 구조는 소규모 서비스를 요구하는 시스템에도 적용이 가능한 뿐만 아니라 전통 내에 확성체의 시스템, 컴퓨터와 같은 지역으로 독립된 네트워크 환경에서 다른 서비스에 대한 대역폭 정체 없이 사용되어야 할 때 적합한 그룹의 관리 모델로 활용될 수 있다.

참 고 문 현