혼합 P2P 보안 멀티캐스트 구현

문정환*, 송기범*, 방극인*, 안성수**, 이 준***

*조선대학교 컴퓨터공학과
**동신대학교 컴퓨터과학과
***조선대학교 컴퓨터공학부

Implementation of Hybrid P2P Secure Multicast

Jung-Hwan Moon*, Gi-Beom Song*, Keug-in Bang*, Seong-Soo Ahn**, Joon Lee***

* Dept. of Computer Engineering, Chosun Univ.
** Dept. of Computer, Dongshin Univ.
*** School of Computer Engineering, Chosun Univ.

요 약

최근 수 년간 클라이언트/서버 모델에서 발생하는 문제인 서버 병목 현상, DoS(Denial of Service) 공격, 그리고 시스템의 확장성에 따르는 비용 증가 등의 문제를 해결하기 위한 방법으로 P2P (Peer-to-Peer)의 프로토콜 개선과 통신 모델 개선에 대해서 연구가 활발히 진행되고 있다. 본 논문에서는 기존의 멀티캐스트 프로토콜들을 살펴보고 제안하는 멀티캐스트 프로토콜인 GSAKMP(Group Secure Association Key Management Protocol)를 이용한 보안 멀티캐스트 환경을 구현한다.

1. 서론

인터넷은 개방성과 공개성 그리고 수평성을 지향한다. 이러한 특성을 기반으로 해서 인터넷은 디지털 경제를 구체화시키고 실현시키는 중요한 수단이 되고 있다. 현재 주목받고 있는 P2P(Peer-to-Peer) 인터넷의 이러한 이상을 실현해 가는데 중요한 위치를 차지하고 있다. 개인과 개인간의 정보공유 모델인 P2P는 인터넷을 통해서 다른 사용자들과 정보를 주고받을 수 있는 기술을 말한다. P2P가 발전함에 따라 단순한 파일전송만이 아닌 오디오/비디오등 멀티미디어 파일들이 Peer들간에 전송됨으로서 현 P2P 프로토콜은 네트웍의 대역폭을 많이 잠식하는 성향이 있다. 또한 Denial of service(DoS) 공격이나 Storage flooding 공격등에 취약성을 보인다. 이런 문제를 해결하기 위한 방법중 프로토콜 개선과 통신 모델 개선에 대해서 연구가 활발히 진행되고 있다. 이는 기존에 P2P환경에 보안 멀티캐스트 환경을 적용함으로서 어느 정도의 해결을 볼수 있다고 본다. 본 논문에서 제시하고 있는 보안모델은 혼합P2P 형식의 구조를 가진 분산자료관리시스템(Distributed Data Manager)에 적용된 것이다. 각각의 peer 간 통신에 SSL기술을 적용하여 메시지의 암호화 및 인증기능을 부여하고, 기존의 멀티캐스트 프로트콜을 살펴보고 제안하는 멀티캐스트 프로토콜인 GSAKMP(Group Secure Association Key Management Protocol)를 이용한 보안 멀티캐스트 환경을 제안한다.

2. P2P보안 모델

기본적인 네트웍 구성은 서버와 에이전트 기반으로 이루어지지만 각각의 사용자의 직접적인 자료의 공유를 위해서 Peer to Peer환경을 설정하여 분산되어진 멀티미디어 자료의 효과적인 관리를 위한 통신의 주체가 되는

각각 에이젼트들 간의 통신과 서버와 에이젼트의 통신에 있어 악의적인 침입에 의한 정보누출을 차단하기 위한 환경, 보안모델의 필수 요소인 암호화 할 수 있는 방법, Peer to Peer 환경에 적합한 암호화 프로토콜을 연구하고 이를 구현하였다.

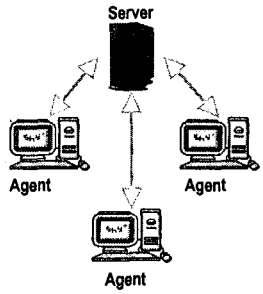

그림 1 Server-Client 모델

서버의 기본적인 역할은 에이젼트들의 주소 목록을 저장했다가 요청하는 에이젼트에게 그 목록을 반환하며 에이젼트는 서버로부터 다른 에이젼트 목록을 받아서 에이젼트들 간의 데이터 전송 및 목록전송을 담당한다. 사용자 인증은 에이젼트가 서버로부터 하게 된다. 하지만 각각의 에이젼트들간의 보안성이 제공되는 통신환경을 위해 SSL프로토콜을 사용하였다. 메세지를 블럭 단위로 분할하여 선택적으로 압축하고 MAC(Message Authentication Code)를 계산하여 암호화 한다. 암호화된 데이터가 송신되면 수신측은 복호화, MAC검증, 압축풀기, 역분할 과정을 거쳐 메세지를 재생하고 상위 계층으로 전달한다. 암호화된 SSL 연결은 보내는 쪽 Application에서 암호화하고 받는 쪽 Application에서 암호를 해독하기 위해서 보내지는 모든 정보의 기밀성을 유지하기 위해서 필요하다. 암호화된 SSL의 연결에 의해서 보내지는 모든 데이터는 부정 행위를 탐지하고, 통과되는 데이터가 변경되었는지를 확인하는 방법에 의해서 보호된다.

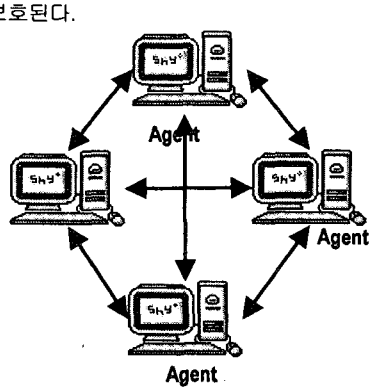

그림 2 SSL을 이용한 Peer to Peer 모델

기존의 서버 클라이언트 모델에서는 서버는 웹 상에서 새로운 클라이언트 등록을 받게 되고 기존 회원에게 정보를 제공하게 된다. 따라서, 보안이 보장되는 웹 환경에서 정보를 주고받기 위해서는 https, PKI(Public Key Infrastructure)등을 이용하는 환경이 필요하다.

3. 그룹 키와 키 관리에 관한 기존연구

멀티캐스트 세션은 멀티캐스트 그룹 주소로 이루어지며 어떠한 호스트이든지 해당 멀티캐스트 주소를 통해 간단하게 멀티캐스트 그룹으로 전송이 가능하다. 멀티캐스트 그룹의 가입 및 탈퇴와 같은 그룹관리 메커니즘은 IGMP(Internet Group Management Protocol)에 의해 이루어진다. 하지만, 이러한 멀티캐스트 통신 그룹은 데이터를 받는 수신자의 가입 및 탈퇴가 자유로운 상태로 보안에 취약한 점을 보인다. 보안 멀티캐스트 환경은 하나의 그룹 키를 사용하여 특정 멀티캐스트 그룹회원에게 보내어지는 메시지를 암호화함으로써 멀티캐스트 통신을 보호하는 것으로 멀티캐스트 그룹 키 분배 기법의 관련 연구로는 GKMP(Group Key Management Protocol), SMKD(Scalable Multicast Key Distribution scheme) MKMP(Secure Scalable Multicast Key Management Protocol), Iolus가 있다.

멀티캐스트 보안 프로토콜은 주로 멀티캐스트 키 분배 프로토콜에 관해서 언급하고 있다. 이는 새로운 회원에게 그룹 키를 분배해 주는 것을 말하며 그룹의 회원이 변경되었을 경우에 키를 재분배해야 한다. 이와 관련된 대부분의 프로토콜은 중앙 집중화된 구조를 가진다. 즉 보안성이 제공되는 각 멀티캐스트 그룹은 그룹 제어자(Group Controller)를 두고 이 그룹 제어자가 모든 가입 처리를 하여 그룹 키인 Kgrp를 신규 회원에게 전달한다. 이러한 프로토콜 중 하나인 GKMP(Group Key Management Protocol)는 그룹 단위별로 GC를 만드는 특징이 있다. GKMP 프로토콜은 멀티캐스트 그룹의 회원들을 위해 대칭 키를 생성하고 관리한다. 이 프로토콜에서 각 멀티캐스트 그룹은 그룹 키를 관리하기 위한 전용 그룹 제어자(Group Controller)를 가진다. 이 그룹 제어자는 선택된 그룹 회원과 공동 작업으로 그룹 키를 생성한다. 즉 각 그룹 회원들이 아직 유효한지 확인한 뒤 그룹 제어자와 그 회원만이 아는 키로 암호화된 그룹 키를 보낸다. 그런데 이 프로토콜은 하나의그룹 제어자(GC)가 모든 그룹 회원들에게 키를 보내야 되므로 확장성이 부족하다. 이 방식은 키관리나 확장성에 대한 언급이 없어서 중앙 집중화된 그룹 제어자가 확장성을 가지기 힘들다.

Iobus는 보안성이 제공되는 분배 트리를 구성하여 확장성을 용이하게 한다. 멀티캐스트 그룹은 계층적으로 정렬된 서브 그룹으로 나뉘어진다. 최상위 레벌에서는 그룹을 관리하기 위한 그룹 보안 제어자(Group

Security Controller)가 있가 각기 다른 서브 그룹을 관리하기 위한 그룹 보안 중계자(Group Security Intermediarise)가 있다. 각 서브 그룹은 각기 다른 서브 그룹키를 가진다. GSI는 그 서브 그룹의 키와 상위 레벨 서브 그룹의 키를 알기 때문에 메시지를 상위 레벨로 전송하거나 하위 레벨로 전송할 때 키로 풀어서 다른 키로 암호화하여 보는 작업이 필요하다. 이 연구의 단점은 GSI가 각 데이터 패킷을 복호화한 다음 다시 재암호화해야 하므로 이때 지연이 생긴다는 점이다. 그리고 신뢰할 수 없는 GSI를 제거하는 과정도 복잡하다. Iobus는 키의 재분배 시에 한계를 가지는 중앙 집중식 구조를 개선하여 서브 그룹으로 이루어진 계층적인 구조를 가진다. 다른 레벨의 계층에서 키 관리는 각기 다른 제어자에 의해 이루어진다. 그래서 서브 그룹 내에서 키를 재분배하면 단지 그 서브 그룹내의 회원들에게만 영향을 미치게 된다. 이 연구가 키의 재분배에 대해 개선점을 제시했으나 서브 그룹으로 데이터가 전송될 때마다 트래픽을 복호화 하여 다시 서브 그룹의 키로 암호화해야 하는 단점이 있다.

4. 사용자 인증이 가능한 그룹 키 분배 프로토콜(GSAKMP)

멀티캐스트 그룹의 경우 회원 변화가 다양하므로 그룹 키의 재분배가 원활해야 한다. 또한 많은 회원이 가입할 수 있으므로 확장성이 있어야 한다. 확장성을 만족하기 위해서는 특정 단위에서의 그룹 키 분배가 이루어져야 한다. 멀티캐스트 그룹을 서브 그룹으로 나누어 서브 그룹별로 그룹 키를 나누어 계층적으로 관리하는 것이 바람직하다.

회원이 1000명인 멀티캐스트 그룹에서 동일한 그룹 키를 사용한다고 가정해보자. 10분 단위로 회원이 변동이 생긴다면 10분마다 1000명의 회원에게 새로운 그룹 키를 분배해야한다. 그러나 이 그룹을 10명 단위로 100개의 서브 그룹으로 나누어 서브 그룹별로 그룹 키를 관리한다면 10분마다 하나의 서브 그룹에서만 키를 재분배하면 된다. 전자의 경우 키를 한 회원에게 나누어 주는 비용을 M이라 하면 M * 1000 비용이 필요하지만 후자의 경우 M *10 비용만으로 족하다. 반면 그룹 키로 한번 암호화 하는 비용을 Me, 복호화하는 비용을 Md라 하면 전자의 경우 한번의 암호화와 복호화로 메시지를 전송할 수 있으므로 각각 1 * Me, 1 * Md의 암호화/복호화 비용이 드는 반면 후자의 경우 10개의서브 그룹을 거친다고 가정하면 10 * Me, 10 * Md 정도의 부가적인 비용이 들게된다. 그러나 후자와 같이 계층적인 구조로 그룹 키를 각기 관리하고 멀티캐스트 라우터에 하나의 LKDC(Local Key Distribution Center)를 두어 복호화/재암호하 과정이 이루어진다면 Iobus와 같이 경로 배정된 후 GSI에서 다시 복호화/재암호화 과정이 일어나는 것보다 처리 속도가 빨라진다. 또한 서브 그룹별로 그룹 키를 관리할 경우 공개키를 이용한 전자 서명을 통해 송신자 인증이 가능하고 가입된 회원에게 키를 쉽게 재분배할 수 있다.

이 방법은 Iobus에서 제기된 것으로 확장성이 좋으나 멀티캐스트 라우터를 통과할 때마다 부가적인 처리 과정(복호화/재암호화)이 필요하므로 지연이 길어진다. 그러나 멀티캐스트 내부와 외부에서의 그룹 키 관리를 분리시키고 보안성이 강화된 그룹 관리를 통해 사용자 인증이 가능하다. 또한 서브 그룹별로 나누어 송신자가 공개키에 기반한 전자 서명을 하여 트래픽을 전송하면 서브그룹 내에서 인증을 하여 다른 서브그룹으로 전송할 수 있다. 따라서 본 논문에서 제안하는 메커니즘은 계층적인 구조를 가지며 보안성이 강화된다.

4.1 그룹 키 분배

멀티캐스트 라우터에 LKDC를 두어 그룹 키를 분배하고 관리한다. 또한 각 회원의 공개키를 등록하여 멀티캐스트 그룹의 회원 정보를 저장한다. 이 LKDC는 멀티캐스트 라우터나 호스트가 새로 그룹에 가입하면 그 멀티캐스트 라우터나 호스트의 공개키를 등록한다. 이미 다른 그룹으로 등록되어 있는 멀티캐스트 라우터라면 공개키를 등록하지 않고 가지고 있는 그룹 회원 정보를 갱신한다. 서브 그룹 내에서는 그룹 키와 공개키를 동시에 사용한다. 멀티캐스트 라우터에서 받은 데이터그램을 LKDC가 가지고 있는 그룹 키를 이용해 암호화하여 보낸다. 그룹에 속한 회원은 공유하고 있는 그룹 키를 이용해서 데이터그램을 확인할 수 있다. 반면 회원이 아닌 호스트는 데이터그램을 가진다 하더라도 그룹 키가 없으므로 이를 확인할 수 없다. 이 때 그룹 키를 공유하는 방법이 중요한 문제가 되는데, 특히 그룹의 회원 변화가 심하면 그룹 키를 재분배하기가 쉽지 않다. 회원이 그룹을 떠난다면 그룹 키를 재분배해야 되는데 이때 떠난 회원을 제외한 나머지 회원들 각각에게 공개키로 암호화하여 새로운 그룹 키를 유니캐스트로 보낸다. 떠난 회원을 제외한 모든 회원이 새로운 그룹 키를 받아 사용할 수 있다. 멀티캐스트 그룹 관리를 위한 IGMP 이외에 LKDC에게 회원 등록, 해지 및 키 재분배를 할 수 있도록 관리해 주는 IMMP 프로토콜을 사용한다.

4.2 전자 서명을 이용한 사용자 인증

서브 그룹 내에서는 송신자는 그룹 회원 권한을 확인하기 위해 멀티캐스트 데이터그램을 공개키를 이용해 전자 서명한 뒤 그룹 키로 암호화하여 멀티캐스트 한다 LKDC는 전자 서명된 송신자를 인증한 후 그룹 키를 이용해 복호화/재암호화하여 다른 멀티캐스트 라우터로 데이터그램을 전송한다. LKDC는 각 그룹에 속한 회원 정보와 공개키, 그룹 키를 유지하여 송신자를 인증하고 그룹 키를 이용해 전송한다. LKDC는 그룹 회원 권한을 확인하기 위해 공개키를 사용하여 전자 서명을 하므로

송신자 인증과 수신자 인증이 가능하다. 전자 서명 기법은 전자 문서에 대한 서명을 생성하는 방법이다. 디지털 데어터의 특성상 전자 서명은 쉽게 복제가 가능하기 DEOAN 문서 및 서명 위조의 위험성이 크다. 서명자는자신이 서명한 전자 문서에 대한 서명 사실을 부인할 수 없고 문서 수신자는 서명된 문서에 대한 정당성을 부인할 수 없다.

① 공개키 서명 방식

암호화 및 복호화에 사용되는 키가 서로 다른 방식으로, 비밀키 kd와 공개키 ke로 구성된다. Ke로부터 kd를 유추하는 것은 계산상 불가능하기 때문에 사용자는 공중망상에 ke를 공개할 수 있다. 공개키 ke를 공개할 수 있다. 공개키 ke로 암호화된 메시지는 비밀키 ke를 소유한 사용자만이 복호화할 수 있다. 공개키 서명 방식은 공통키 서명 방식에서의 키 분배의 쿤제점 및 센터 의존도를 해결한 방법이다. 단점은 모듈러 지수 연산을 수행하기 때문에 서명 생성 및 검증 시간이 비례하게 된다. 따라서 공개키 서명 방식에서는 일반적으로 일방향 해시 함수를 사용하여 서명 대상 메시지의 크기를 일정 길이로 줄여서 서명하게 된다. 메시지 내용의 무결성은 해시 함수의 일방향성에 기반한다.

② 송신자 인증

멀티캐스트 그룹 키 관리에서 필수적으로 해결해야 할 것이 송신자 인증이다. 왜냐하면 실시간으로 전송되어야 할 많은 양의 데이터를 다른 사용자가 가로채거나 방해한다면 송신자의 정보를 제대로 이용할 수 없기 때문이다. 서브 그룹 내에서 송신자 인증이 이루어지면 멀티캐스트 라우터가 서명된 부분을 제거하고 메시지를 그 서브 그룹과 다른 서브 그룹으로 전송한다. 따라서 메시지를 인증한 LKDC가 송신자에 대한 합법적인 권한을 인정한 것이다. 만약 침입자가 LKDC로 가장하고 인증하지 않은 메시지를 인증한 것처럼 가장한다면 이를 막을 수 없다. 그러므로 멀티캐스트 라우터가 LKDC의 역할을 하려고 한다면 증명서를 가진 합법적인 멀티캐스트 라우터에게만 서브 그룹을 관리하는 권한을 부여한다. 이는 LKDC뿐 아니라 그룹의 회원으로 가입하려는 호스트에게도 동일하게 적용되어 LKDC뿐 아니라 그룹의 회원으로 가입하려는 호스트에게도 동일하게 적용되어 LKDC에게 호스트가 합법적인 권한이 있음을 증명해야 한다.

③ 수신자 인증

멀티캐스트에서 보안성을 제공하기 위해서 주로 그룹 키 분배와 사용자 인증에 대한 연구가 진행되어 왔다. 그룹 키 분배 프로토콜은 멀티캐스트그룹의 모든 회원들에게 공통키를 안전하게 전달해 주는 목적으로 사용된다. 그룹 내의 회원들은 공통키를 통해 멀티캐스트 그룹 내에 전송되는 데이터를 암호화하여 보안성을 유지할 수 있다. 그룹 키의 장점은 송신자가 각각의 수신자에게 개별적으로 암호화해서 전송할 필요가 없다는 점이다. 그러나 새로운 회원이 가입하거나 기존 회원이 그룹을 탈퇴한다면 그룹 권한을 보호하기 위해서 그룹 키를 재분배해야 한다. 수신자 인증은 그룹 키를 통해서 가능하므로 그룹의 회원 변동이 생기면 키를 재분배해야 한다. 이 경우 키의 재분배가 수신자인증 면에서 매우 어려운 작업이 되며 확장성을 유지하면서 키의 재분배가 용이해야 한다. 유니캐스트와 달리 멀티캐스트는 사용자가 끊임없이 가입하고 탈퇴하므로 현재 회원들만이 그룹 키를 소요할 수 있도록 부단히 키를 재분배하는 매커니즘이 필요하다. 수신자가 보낸 멀티캐스트 메시지는 각 서브 그룹 키로 암호화되어 전송된다. 각 그룹 키는 서브 그룹 내에서 그룹의 회원들끼리만 공유하는 비밀키이므로 이 키를 가진 회원들만이 송신자가 보낸 멀티미디어 메시지를 확인할 수 있다. 그룹 키는 네트워크 상에서 암호화되지 않은 채로 돌아다니지 않으므로 안전하다. 또한 LKDC가 그룹 키를 재분배할 때 각 회원들의 공개키로 암호화하여 보내므로 권한이 없는 호스트가 그룹 키를 가로챌 수 없다.

5. 결론 및 향후과제

Peer to Peer 환경에서 SSL 프로토콜을 사용함으로써 신뢰성 있는 통신환경을 제공하였으며 또한 여러 가지 그룹 키 분배 기법들에 대해 살펴보았다. GSAKMP를 응용함으로서 보안 멀티캐스트 환경을 구축할수 있었다. 그룹 키 관리에서는 안전한 인터넷 멀티캐스트 그룹에 가입한 유저는 회원 인증과 메시지 무결성을 통해 안전한 멀티캐스트 통신을 할 수 있을 뿐만 아니라 대규모의 회원을 관리해야 하는 경우, 가입과 탈퇴에 따른 그룹 키 분배자의 부하를 줄여 확장성을 제공해 준다.

향후 연구 방향은 Rekey interval에 관련하여 기존 Tree_base방식이나 CBT(Core-base Tree)등을 연구하여 효율적인 키 관리 메커니즘의 구현과 좀더 안정적인 P2P에서의 보안 멀티캐스트 환경에 대하여 지속적인 연구가 필요하다.

[참고문헌]

[1] Kan. G., "Gnutella", in Andy Oram(ed), Peer-to-Peer: Harnessing the Power of Disruptive Technologies, 2001,

[2] H. Harney, and C. Muckenhirn, Group Key Management Protocol (GKMP) Specification . R F C 2093, July 1997.

[3] H. Harney, and C. Muckenhirn, Group Key Management Protocol (GKMP) Architecture , R F C 2094, July 1997.

[4] S. Mittra, " Iolus : A Framework for Scalable Secure multicasting" , Proceedings of the ACM SIGCOM M ' 97, pp. 277- 288, September ,1997.

[5] H. Harney, A. Colegrove, E. Harder , U. Meth, and R. Fleischer , "Group Secure Association Key Management Protocol" , Internet Draf t, draft-ietf-msec-gsakmp-sec-00.tx t, March 2001.

[6] myns, http://www.cs.umd.edu/~suman/research/myns