OTP를 이용한 개선된 다중접속 도메인 시스템에 관한 연구

한창남*, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
e-mail : pluto0142, mjun@ssu.ac.kr

A Study on Advanced Multi-connection Domain System using OTP

Chang-nam Han*, Moon-seog Jun*
*Dept of Computer, Soong-Sil University
e-mail : pluto0142, mjun@ssu.ac.kr

요 약

최근에 멀티미디어 환경을 기반으로 한 온라인 회의 시스템은 큰 발전을 가져왔지만 회의 통제 불가 같은 단점과 정보 보안에 있어서의 취약점이 존재한다.
이에 본 논문에서는 비대칭키 암호 알고리즘과 OTP 및 티켓 시스템을 이용해 기밀성과 회의 통제 기능을 추가하여 이전에 제안한 것보다 개선된 다중 접속 도메인 시스템을 제안하고자 한다.

1. 서론

최근 인터넷은 모든 컴퓨터 사용자들에게 다양한 서비스를 제공하고 있다. 웹의 기술은 멀티미디어 환경을 기본으로 다양한 정보를 전파할 수 있게 하였고 이와 같은 멀티미디어 환경을 기반으로 한 회의 시스템도 많은 발전을 거듭하고 있다. 그 예로 기업에서 많이 사용하고 있는 온라인 회의 시스템이 있다[1].

온라인 회의 시스템은 오프라인 회의와 달리 공간의 제약성을 극복했다는 점에서 큰 성과라고 할 수 있다. 오프라인 회의에서의 공간을 인터넷이라는 곳으로 이동함으로써 참여자들이 이동하지 않고 단지 컴퓨터와 통신수단만을 이용하여 쉽게 회의 시스템을 구축할 수 있게 되었다. 하지만 온라인 회의 시스템에는 대표적인 제약사항이 있는데 그것은 시간이 지나면서 참석자들의 회의 내용에 대한 일관된 의식과 현재 상황에 대한 인식이 부족해진다는 것에 있다[4]. 또한 눈으로 직접 맞대고 하는 시스템이 아니기 때문에 회의 자체의 통제가 불가능해질 수 있다[2][3].

이전에 제안되어진 논문에서는 비대칭 키 암호시스템과 OTP 및 토큰 시스템을 이용하여 온라인 회의 기밀성을 높이고 기존의 단점인 회의 통제 부분을 개선하는 내용이었다[5]. 하지만 이전의 논문에서는 회의 진행과정에서 회의의 진행자가 회의 진행을 원활하게 할 수 없었다.

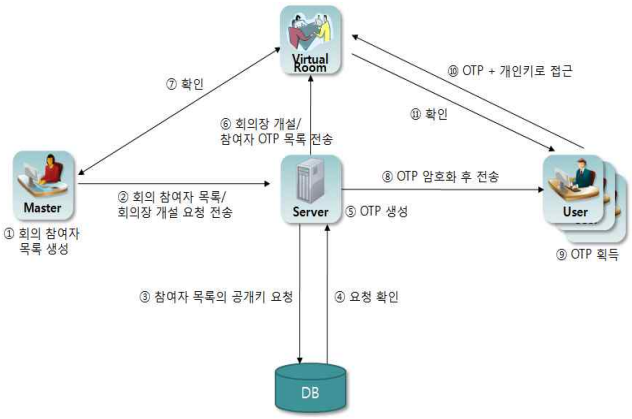
이에 본 논문에서는 이전에 제안되었던 회의 통제 부분을 개선하여 진행자로 하여금 더욱 효율적인 회의 진행을 유도하는 메커니즘을 제안한다.

2. 다중접속 도메인 시스템 설계

본 논문에서 제안하고자 하는 다중접속 도메인 시스템은 두 가지의 메커니즘으로 구성되어 있다. 첫 번째 메커니즘은 이전에 연구되었던 참여자 인증 및 로그인 과정의 메커니즘이고 두 번째는 이전의 것보다 개선된 회의 진행구조에 관한 메커니즘이다.

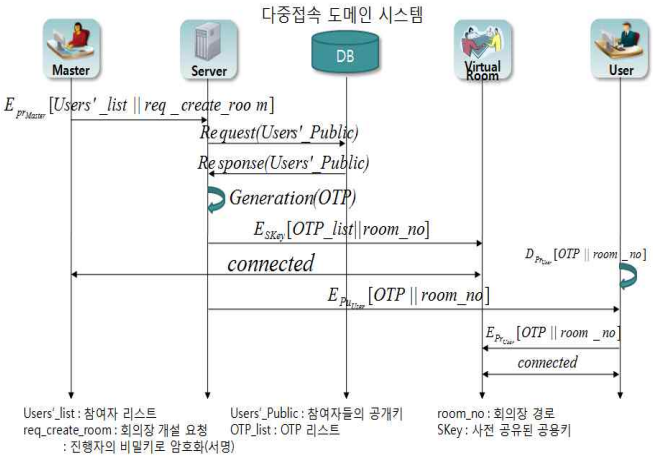
2.1. 참여자 인증 및 로그인 메커니즘

회의 진행자가 회의에 참여하게 될 대상자를 선정하는 참여자 인증 및 참여자들이 회의장에 접속하게 되는 로그인 과정은 [그림 1]과 같다.



[그림 1] 참여자 인증 및 로그인 과정

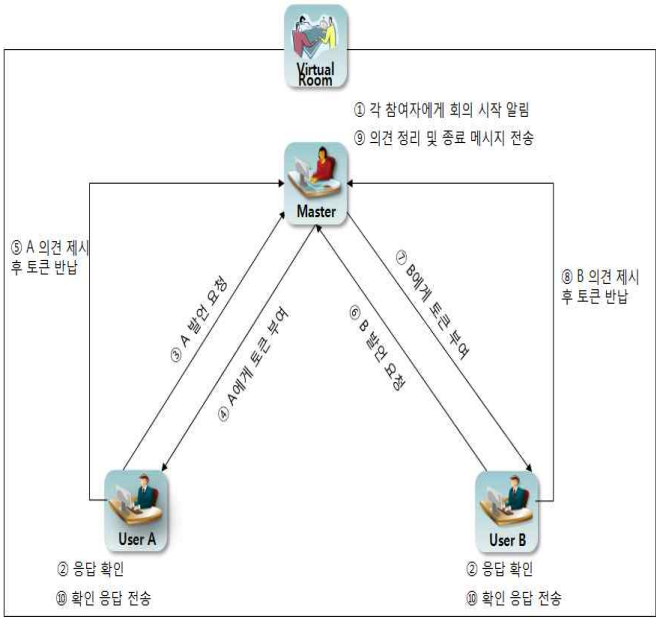
진행자는 회의를 진행하게 되는 사람이다. 진행자는 첫 번째 단계로 회의에 참여하게 될 참여자 대상을 선정해 목록을 생성하여 그 목록과 회의장 개설 요청을 온라인 회의 서버에게 전송한다. 온라인 회의 서버는 참여자의 공개키를 사원 데이터베이스에 요청을 한다. 사원 데이터베이스가 응답 메시지로 온라인 회의 서버에게 회의 참여자의 공개키를 보내준다. 온라인 회의 서버는 공용키를 생성한 후 온라인 회의장에 참여자들의 키를 전송하고 회의장 개설 요청을 한다. 또한 각 참여자들에게 참여자의 공개키로 암호화한 공용키와 회의장의 경로를 전송해준다. 참여자는 회의 서버로부터 받은 내용을 복호화하여 자신의 개인키와 공용키로 회의장에 접속을 하게 된다. 회의장은 참여자에게 접속되었다는 메시지를 전송하고 회의 서버는 진행자에게 완료되었다는 메시지를 전송하게 된다. 참여자 인증 및 로그인 과정에 대한 알고리즘은 [그림 2]와 같다.



[그림 2] 참여자 인증 및 로그인 과정 알고리즘

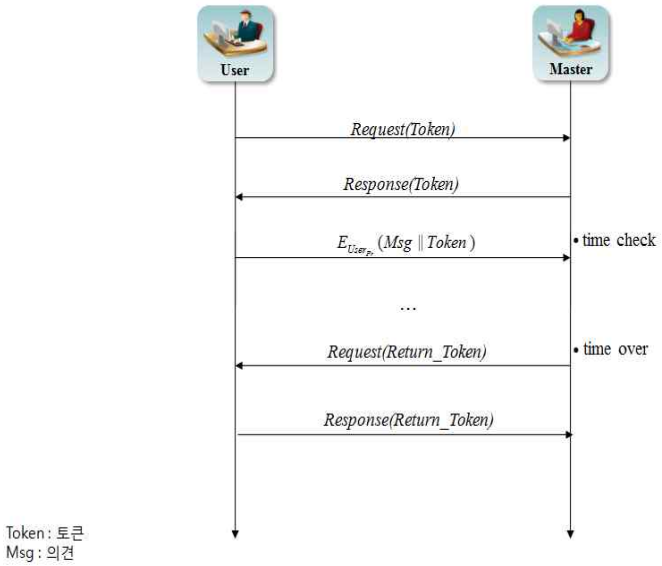
2.2. 회의 진행 메커니즘

회의장에 입장하게 된 진행자와 참여자들이 회의를 진행하는 과정은 [그림 3]과 같다.



[그림 3] 회의 진행과정

2.1의 참여자 인증 및 로그인 과정이 끝나면 진행자와 참여자들은 회의장에 입장하게 된다. 진행자는 각 참여자에게 회의 시작을 알리고 참여자들은 각각의 확인 응답 메시지를 전송한다. 참여자 A가 발언을 요청하면, 진행자는 A에게 응답으로 발언할 수 있는 권리를 부여하는 티켓 즉, 토큰을 전송한다. 토큰을 전송받은 A는 자신의 발언 내용을 토큰과 함께 A자신의 전자서명을 이용하여 의견 제시를 하게 된다. 의견 제시를 마치게 된 참여자 A는 토큰을 반납하게 된다. 참여자 A가 발언시간이 길어져서 회의 진행에 어려움이 있을 때도 진행자가 시간이 지났다는 메시지를 참여자 A에게 보내 토큰을 반납하게 한다. 이어서 참여자 B와 같은 경우도 참여자 A의 의견 제시 과정과 마찬가지로 진행하며 다만 참여자 B의 경우는 참여자 B 자신의 전자서명을 이용한다는 것이다. 의견 교환이 끝나면 진행자는 회의 내용을 정리하고 종료 메시지를 참여자들에게 전송하게 된다. 참여자들은 확인 응답을 진행자에게 전송함으로써 회의를 마치게 된다. 회의 진행과정에 대한 알고리즘은 [그림 4]와 같다.



[그림 4] 회의 진행과정 알고리즘

이전의 회의 진행과정 알고리즘은 참여자들의 발언 시간을 고려하지 않은 것이었지만 위에 제안한 진행과정의 알고리즘은 참여자의 발언권을 진행자가 통제하게 됨으로써 이전의 것보다 더욱 효율적으로 회의를 진행할 수 있다.

4. 결론

최근에 발전을 거듭하고 있는 멀티미디어 환경에서 온라인 회의 시스템도 발전하고 있다. 이 온라인 회의 시스템은 오프라인이 아닌 온라인에서 진행되는 것으로써 참여자에게 회의 장소까지 가게 되는 불편을 줄여줄 뿐만 아니라 단지 컴퓨터와 통신 수단만을 이용하여 쉽게 회의 시스템을 구축 및 이용할 수 있게 되었지만 시간이 지나면서 참석자들의 회의 내용에 대한 일관된 의식과 현재 상황에 대한 인식이 부족해진다는 것에 있다. 또한 눈으로 직접 맞대고 하는 시스템이 아니기 때문에 회의 자체의 통제가 불가능해지는 등의 단점이 존재한다.

이에 본 논문에서는 이전에 제안된 것보다 회의 진행과정에서 참여자의 발언권을 회의 진행자가 더욱 통제할 수 있게 하였다.

추후 연구에서는 회의 참여자 목록 및 회의장 개설 요청 문서를 XML 형태로 개발하여서 실제로 구현하게 될 때 어느 시스템이던지 호환될 수 있는 것으로 만들고자 한다.

참고문헌

[1] 고기원 외 2인, "전자상거래를 위한 멀티미디어 회의 응용서비스", 1998

[2] 홍현우 외 3인, "XML 기반 의사결정 시스템 설계 및 구현", 2005

[3] 김태현 외 5인, "지식기반 회의관리 시스템 아키텍처에 관한 연구", 2006

[4] 임영태 외 2인, "XML 기반 온톨로지 의사 결정 시스템 설계 및 구현", 2004

[5] 한창남 외 2인, "OTP를 이용한 다중접속 도메인 시스템에 관한 연구", 2009