안전한 멀티캐스트 전송을 위한 효율적인 그룹 관리 방법

(An Effective Group Management Method for Secure Multicast Transmission)

고 훈 † 장 의 진 †† 김 선 호 ††† 신 용 태 ††††
(Hoon Ko) (Uijin Jang) (Sunho Kim) (Yongtae Shin)

요 약 많은 중요한 정보들이 인터넷을 통해 전송 되고 있으나, 이들은 정보는 수많은 위험에 노출되어 있다. 그리고 멀티캐스트 서비스도 다양해지고 보편화 되고 있는 만큼 서비스의 종류도 다양해지고 있다. 그룹에 새로운 멤버가 가입하거나 탈퇴하는 경우 기존 멤버들이 사용하던 그룹 키는 갱신되어야 한다. 그러나 기존의 방법은 키 교환 때문에 성능이 저하되는 문제가 있다. 본 논문에서는 안전한 멀티캐스트 데이타 전달을 위해서 가입과 탈퇴가 빈번한 멀티캐스트 그룹에 대해서 안전한 데이타 전달을 위한 효율적인 그룹 관리 기법을 제안한다.

키워드 : 그룹전송, 암호화, 세션키, 공개키, 개인키

Abstract While a lot of important information is being sent and received on the Internet, the information could be exposed to many threats, and the more the Multicast Service is various and generalized, the more the service range is widened. When a new member joins in or leaves from the Multicast Group, the Group Key, which the existing member use for, should be newly updated. The existing method had a problem that the performance was depreciated by the key exchanging. This paper proposes the effective group management mechanism for a secure transmission of the Multicast Data on the Multicast Group

Key words : Group Communication, Cryptograph, Session Key, Public Key, Private Key

1. 서 론

인터넷이 금융, 증권 등의 다양한 분야에 활용되면서 새로운 서비스가 제공되고 있다. 멀티캐스트는 네트워크의 대역낭비를 최소화 시켜주기 때문에 많은 인터넷 서비스에서 이용된다. 인터넷 화상회의, 화상교육, 화상강의 등에서 많이 사용된다. 그룹에 새로운 멤버가 가입하거나 기존의 멤버가 탈퇴하는 경우 멤버들이 사용 중인 그룹키와 세션키는 갱신되어야 한다. 그러나 많은 그룹들이 이러한 키 갱신 절차를 계속할 경우, 즉 그룹갱신이 빈번하다면 이로인해서 발생되는 문제로 정상적인 서비스와 그룹 확장에 큰 문제가 발생된다.

안전한 멀티캐스트를 설계함에 있어서 고려되어야 할 사항은 인증과 접근제어 그리고 비밀성, 무결성, 부인봉쇄 등을 제공하는 것이다[1-3]. 특히 동적인 멀티캐스트 그룹과 같이 가입과 탈퇴가 빈번한 그룹에서 기존에 사용하던 그룹키를 이용해서 서비스를 하고 있다가 멤버가 탈퇴할 경우, 그룹키는 필요없어지기 때문에 새로운 그룹키를 갱신해서 전달해야 한다.

본 논문에서는 분산/계층 그룹 모델을 제안하여 그룹 관리와 데이타의 비밀성 측면에 초점을 맞추어 통신에 참여하는 수신자와 새로운 멤버 가입하기 위한 멤버 인증 방안 등을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 제안한 방법인 안전한 그룹관리 방법에 대해서 설명 및 분석을 하고, 3장에서는 제안한 모델을 실험을 통하여 산출된 결과를 설명하고, 마지막으로 4장에서는 향후 과제 및 결론을 맺는다.

† 정 회 원 : 대진대학교 컴퓨터공학과 교수
skoh21@daejin.ac.kr
†† 비 회 원 : 숭실대학교 컴퓨터학과
neon@cherry.ssu.ac.kr
††† 비 회 원 : 서울소방방재본부 전산개발팀
shkim2005@fire.seoul.kr
†††† 종신회원 : 숭실대학교 컴퓨터학과 교수
shin@cherry.ssu.ac.kr
논문접수 : 2003년 11월 5일
심사완료 : 2005년 11월 16일

2. 제안하는 안전한 그룹관리 방법

2.1 기존의 문제점

안전한 멀티캐스트 연구와 관련된 기존의 방법은 Wong[2], Iolus[3] 그리고 Doneti[4] 방법이 있다. Wong과 Dondeti의 방식은 모든 MH는 중앙 키 분배 센터에서 분배한 하나의 KS를 사용하기 때문에 일시적인 키 갱신이 빈번하게 발생되어 전체 시스템 성능에 영향을 준다. Iolus는 서브그룹간에 서로 다른 지역 세션키를 사용하기 때문에 MH의 이동에 따른 오버헤드는 적지만 송신자와 수신자 사이에 여러개의 서브그룹 관리자가 존재하는 경우에 서브 그룹의 수만큼 재암호화, 재분배로 인한 데이타 전송 지연이 발생되는 문제가 있다[5-7].

2.2 그룹구조

그룹키를 이용해서 그룹 가입과 탈퇴 등에서 인증을 하기 때문 보안기법이 추가된 그룹 환경에서의 그룹키는 아주 중요하다. 그러나 빈번한 가입과 탈퇴는 과도한 그룹키 및 세션키 생성을 유도하게 되어 멀티캐스트 서비스와 그룹 확장에 많은 부담이 가중된다. 멀티캐스트는 그룹 멤버쉽을 관리하고 멤버들의 접근 제어와 키 분배를 수행하기 위한 제어 관련과 데이타에 암호, 복호 등 보안 메커니즘을 적용하여 전송하는 데이타 전송 측면으로 이루어진다[9]. 그림 1은 본 논문에서 제안하기 위한 계층적 그룹 구조를 보여주고 있다.

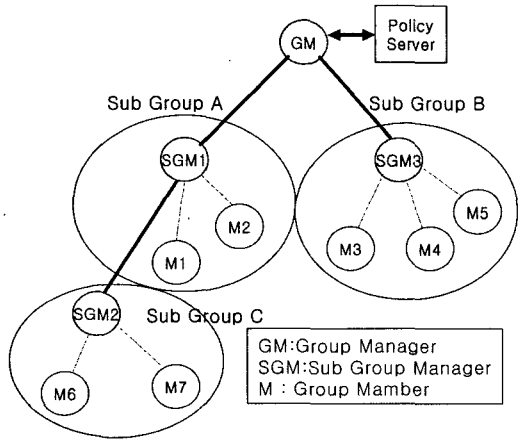

그림 1 계층적 그룹 구조

[기호설명]

M : 그룹가입요청 멤버
GM : 그룹 멤버
SGMn : 서브 그룹 멤버(n)
SGKn : 서브그룹 키(k)
SK : 세션키
K : DH를 이용한 교환 키
E : 암호수행
D : 복호수행
IDn : n의 ID
Xa, Xb : 개인키
Ya, Yb : 공개키

(1) 그룹 가입을 위한 키 획득(생성)

q : *prime number*
α : $\alpha < q$ and α *a primitive root of* q
① $M \rightarrow GM$: X_A 선택, $Y_A = \alpha^{X_A} \bmod q$
② $GM \rightarrow M$: X_B 선택, $Y_B = \alpha^{X_B} \bmod q$
③ M : $K = (Y_B)^{X_A} \bmod q$
④ GM : $K = (Y_A)^{X_B} \bmod q$
⑤ $M \rightarrow GM$: $E_K(ID_M \| SGM_n)$
⑥ GM : $D_K(ID_M \| SGM_n)$
⑦ $GM \rightarrow M$: $E_K(SK \| SGK_n)$
⑧ M : $D_K(SK \| SGK_n)$, Get SK, SGK_n

그룹 가입을 위한 키 획득 및 생성 단계에서는 키교환 방법인 DH 방법을 활용한다.

①~④단계는 M과 GM의 공통 값인 K를 생성하는 단계이다. 먼저, 각자 $Y_A = \alpha^{X_A} \bmod q$, $Y_B = \alpha^{X_B} \bmod q$를 처리해서 각각 X_A, X_B를 선택하고, 이를 이용하여 K를 생성한다.

⑤단계는 K를 이용하여 $(ID_M \| SGM_n)$를 암호화 하여 GM에게 전송하는 단계이다. 마찬가지로 ⑥단계는 K를 이용하여 $(ID_M \| SGM_n)$를 암호화 하여 M에게 전송하는 단계이다. ⑦⑧ 단계에서는 서로 K값을 이용하여 암호화 후 전송된 값들을 복호화 해서 SK, SGK_n 값을 획득한다.

(2) 그룹 가입

① $M \rightarrow SGM$: Request Join SGM_n, $E_{SK}(ID_M \| SGK_n)$
② SGM : $D_{SK}(ID_M \| SGK_n)$
③ $SGM \rightarrow M$: Member Authentication Join OK Message

그룹 가입 단계에서는 서로 생성한 SK, SGK_n를 이용하게 된다.

①단계에서는 M이 먼저 SGM에게 가입 요청을 하면서, SK를 이용하여 $(ID_M \| SGK_n)$를 암호화 해서 전송하게 된다. 이를 수신한 SGM은 SK를 이용하여 복호화 한다②. ③단계에서는 복호화 한 값을 SGM이 가지

고 있는 SGK_n과 비교하는 단계로 값이 같으면 그룹 가입을 허락하게 된다. 만약 값이 틀리면 그룹 가입을 허락하지 않게 된다.

(3) 멤버 탈퇴

① $M \rightarrow SGM$: Request Leave SGM_n
② $SGM \rightarrow GM$: Request New SGK_n, $E_{GK}(ID_{SGMn})$
③ $GM \rightarrow SGM$: Generate new SGK_n, $E_{GK}(newSGK_n)$
④ SGM : $D_{GK}(newSGK_n)$, Update SGK_n
⑤ $SGM \rightarrow$ All SubGroup M : $E_K(SGK_n)$

본 단계는 멤버 탈퇴 단계로서, ①먼저 M이 SGM에게 탈퇴 요청을 하게 된다. ②단계에서는 탈퇴 메시지를 수신한 SGM은 GM에게 새로운 SGK_n를 요청 한다. 이때 정상적인 SGM를 증명하기 위해서 SGM과 GM이 미리 공유하고 있던 GK를 이용해서 SGM의 정보 ID_{SGMn}을 암호화 해서 전송한다.

③단계는 복호화 후, 정상적인 SGM의 메시지인지 확인한 후, 새로운 $newSGK_n$을 생성해서 GK를 이용해서 암호화 후에 전송한다. ④단계는, 이를 수신한 SGM은 GK로 복호화 해서 SGK_n를 갱신한다. ⑤단계는 서브 그룹의 모든 멤버들에게 새로운 SGK_n를 전송해 주는 단계이다. 물론 이때 그룹 멤버가 아닌 다른 멤버들에게 키의 유출을 방지하기 위해서 K를 이용해서 암호화 후에 전송하게 된다.

(4) 재가입

① $M \rightarrow GM$: $E_K(ID_M \mid SGM_n)$
② $GM \rightarrow M$: $D_K(ID_M \mid SGM_n)$, $E_K(SGK_n)$
③ $M \rightarrow SGM$: Request Join SGM_n, $E_{SK}(ID_M \| SGK_n)$
④ $SGM \rightarrow M$: Member Authentication Join OK Message

재가입 단계는 기존에 탈퇴했던 멤버가 다시 그룹에 가입하는 단계이다. ①먼저, GM에게 가입 요청을 하면서 이전에 전송했던 방식 그대로 자신의 개인 정보와 가입하고자 하는 서브그룹의 정보를 K로 암호화 후에 전송하게 된다. ②단계는 GM이 M에게 요청하는 서브그룹의 SGK_n를 전송하는 단계이다. ③은 새롭게 획득한 SGK_n를 해당 SGM에게 보내서 가입 요청을 하는 단계이다. ④단계는 SGM가 암호화 해서 수신된 값 $(ID_M \| SGK_n)$을 복호화 해서 가입을 허락하는 단계이다.

(5) 데이타 전송

① $GM \rightarrow M$: $E_{SK}(Data)$, Multicast $E_{SK}(Data)$ to M
② M : $D_{SK}(Data)$

데이타 전송 부분은 각각이 보유하고 있는 세션키 SK를 이용하여 데이타를 암호화 후 멀티캐스트로 전송하면(①) 이를 수신한 각 멤버 M은 보유하고 있는 SK를 이용하여 복호화하는 단계이다(②).

2.3 키 관리

각 분산/계층 모델에서 해당 그룹에 해당되는 키는 바로 상위 계층에게 요청하게 된다[7,8].

- 그룹 관리자 : 그룹 키 생성, 서브그룹 키 생성, 세션 키 생성 / 전달
- 서브그룹 관리자 : 그룹에 서브그룹 키 요청

① 중앙집중식 방법 : 그룹 제어자가 모든 멤버의 가입과 탈퇴에 따른 키 관리를 하게 된다. 하지만 이는 그룹의 크기에 비례해서 암호화 처리 증가 및 네트워크의 트래픽이 발생하기 때문에 만약 크기가 큰 그룹이라면 구동에 많은 오버헤드가 발생.

② 분산/계층식 방법 : 지역적으로 서브그룹을 묶고 서브그룹 멤버 중 특정 서버가 그 지역의 키 관리를 담당

표 1 구조 분석

비교 항목	중앙집중식 구조	Iolus	제안구조
구조 유형	중앙 집중구조	다중 계층의 분산 구조	분산/계층 구조
제어자	단일 제어자	서브 그룹 제어자	그룹 제어자, 서브 그룹 제어자
키	단이 그룹키	서브 그룹키	그룹 키, 세션키, 서브 그룹키

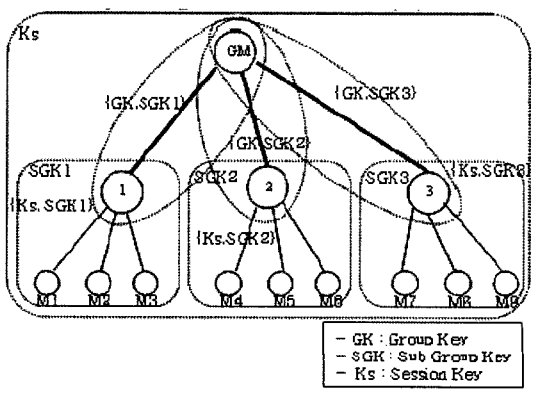

그림 2 분산/계층 키 트리

멤버 $M_1 \sim M_7$ 은 각각 세션키 SK와, SGK_1, SGK_2, SGK_3의 서브그룹 키를 가지고 있고 서브그룹 관리자는 그룹키 GK와 관리자 자신의 서브그룹 키를 가지고 있다.

$$GroupMember = \{(SGK_1, SGK_2, SGK_3) \| GK\}$$
$$GroupKey = \{GK\}$$
$$SubGroupKey = \{SGK_1, SGK_2, SGK_3\}$$
$$SubGroupMember\ 1 = \{(M_1, M_2) \| SGK_1\}$$
$$SubGroupMember\ 2 = \{(M_6, M_7) \| SGK_2\}$$
$$SubGroupMember\ 3 = \{(M_3, M_4, M_5) \| SGK_3\}$$
$$SessionKey = \{SK\}$$

Case 1 : 가입

M_8은 그룹 관리자GM으로부터 세션키 SK와 서브그룹 키 SGK_2를 받게 된다. GM이 SK로 암호화해서 전송한 멀티캐스트 데이타를 M_8은 SK를 이용해서 복호화 하면 된다. 그룹은 그룹 인증키인 그룹키와 서브그룹 인증키인 서브그룹 키, 그리고 데이타의 암/복호화에 사용되는 세션키로 구성이 되어 있다.

Case 2 : 탈퇴

분산/계층적인 키 트리 방법은 그룹의 가입보다는 탈퇴 시에 많은 장점이 있다. 왜냐하면 그룹 가입시에는 기존에 사용하던 세션키, 서브그룹 키를 그대로 멤버에게 전송하면 되기 때문에 특별한 키 갱신 절차는 필요하지 않다.

표 2 키 갱신 비교

항목	중앙집중식	분산/계층식
키 갱신 회수	n-1	d×(h-1)

※ n:멤버수, d:트리의 degree, h:트리의 높이

만약 중앙 집중식 방식일 경우 경우는 각 멤버들은 GK와 SK 하나만 가지고 있으면 된다. 이때 한 멤버가 탈퇴하게 된다면 키 갱신 메시지는 남은 멤버들의 수만큼 암호화되어 보내지게 된다. 따라서 멤버수가 n일 경우$(n-1)$만큼의 키 갱신 메시지가 발생하게 된다. 결국 시스템 측면이나 네트워크 자원 측면에서 많은 오버헤드가 발생된다.

분산/계층적인 키 트리일 경우에는 $d \times (h-1)$만큼의 키 갱신 메시지만 필요하게 된다. 키 갱신은 멤버의 탈퇴신호에 의해서 시작되기 때문에 멤버 탈퇴에 대한 자료는 시스템 설계와 구현을 위해서 매우 중요한 요소가 된다.

3. 실험 및 결과

3.1 실험환경

본 논문은 사이버 교육 환경에서 분산되어 있는 50명에서 300명 사이의 학생이 인터넷상에서 화상을 이용한 교육을 받고 있다고 가정한 상태에서 실험하였다. 화상과 음성이 추가된 멀티미디어 데이타의 가장 큰 특징 중 하나는 대용량성에 있다. 멀티캐스트의 경우 TCP에서 사용하는 ACK 기반의 오류복구를 사용할 경우 송신자에게 응답을 위한 폭주 현상이 발생된다. 따라서 이를 해결하는 방안인 Hybrid ARQ나 Reed Solomon Encoding을 사용한 FEC를 이용할 수 있다. 그러나 부호화를 위한 블록의 단위가 8비트일 경우 최적을 이루게 된다[4]. 이런 최적에 맞추기 위해 미들웨어에서 부호화 과정이 필요하다. 이를 사용하면 잦은 전송호출로 인한 오버헤드가 발생되어 전송율에 문제가 생긴다[9]. 이러한 문제를 해결하기 위해 SRM(Scalable Reliable Multicast)을 이용한다. 그룹 환경에서 동적인 멤버쉽 변화를 지원하는 효율적인 그룹 관리 측면과 안전한 데이타를 전송하는 데이타 전송 측면에 초점을 맞추어 실험을 진행하였다. 실험 프로그램은 nsII를 이용하였고 보안 메커니즘은 Crypto++ 4.1을 사용하였다. 기타 실험 환경은 아래의 표 3에서 정의하였다.

표 3 실험 환경 변수

멀티캐스트 라우팅프로토콜	DVMRP
CBR 트래픽	0.06초
데이타 크기	64bytes-5Kbytes
암호 알고리즘	Rijndael
키 길이	56bits
해쉬 알고리즘	SHA1
서명 알고리즘	RSA
서명 / 인증 키 길이	512bits
노드 개수	4개
호스트 개수	50,150,200,300
실험시간	300초
링크지연	10ms
대역폭	1.5mb, 10mb

3.2 실험결과

그림 3은 그룹 통신에 참여하는 멤버들의 수를 증가시키면서(n=50, 150, 200, 300) 실험한 결과를 보여주고 있다.

그림 4는 서브 그룹키 획득 시간을 보여주고 있다. 그룹의 크기가 50인 경우 서브 그룹키 획득 시간이 평균 1.63sec이고 그룹의 크기가 가장 큰 300인 경우 4.63sec이다. 그룹의 크기는 그룹 멤버의 수로 정하기 때문에 많은 그룹 멤버들이 키가 동시에 생성되기 때문에 그룹 크기가 작을 때보다 많은 시간이 소요되었다.

그림 5는 그룹 키 갱신시간을 보여주고 있다. 그룹 키는 그룹 대표자가 탈퇴 하였을 경우를 해결하기 위해서

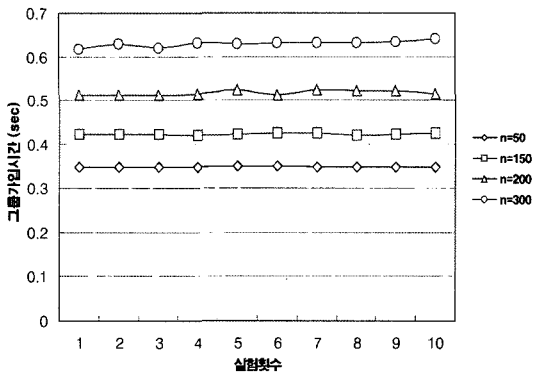

그림 3 그룹가입시간

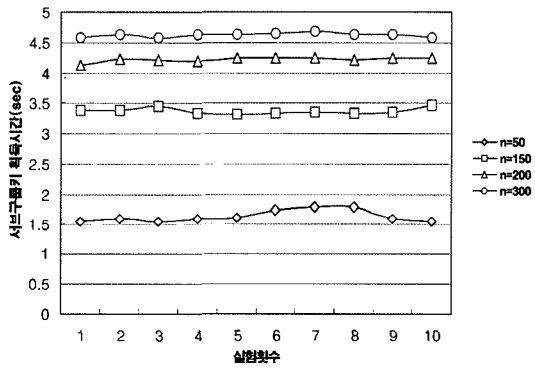

그림 4 서브그룹키 획득 시간

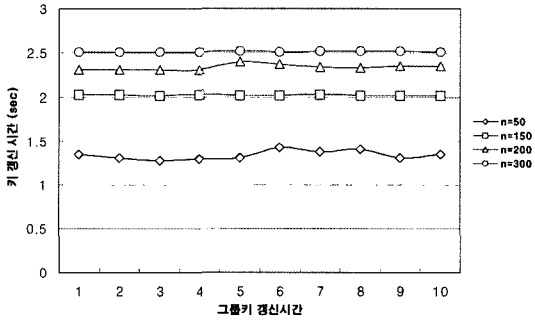

그림 5 그룹 키 갱신시간

대표자가 탈퇴하였을 경우 새로운 그룹 키로 대체하기 위한 시간을 의미한다.

3.3 키 갱신 횟수

암화화 과정은 데이타의 기밀성을 유지하기 위함이고, 세션키는 이런 암화화 과정에서 반드시 필요한 암호화 키가 된다.

그러나 본 논문에서 세션키는 한 멀티캐스트 세션이 수행되는 동안은 특별한 일이 있지 않으면 갱신되지 않는다.

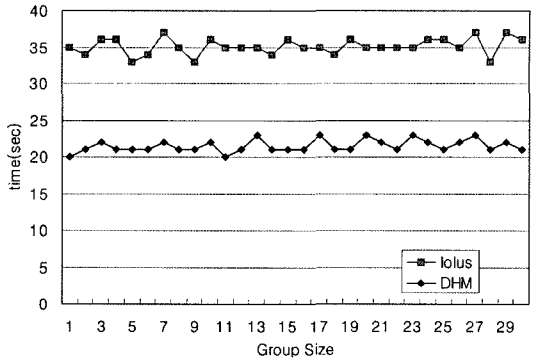

그림 6 키 교환 회수

기존 멤버가 탈퇴 후에도 세션키를 가지고 있지만, 해당 서브 그룹의 가입을 위한 서브 그룹키는 탈퇴와 동시에 갱신된다.

그림 6은 기존의 방법과 제안한 방법을 실험을 통한 결과를 보여주고 있다.

제안한 방법은 멤버가 탈퇴해도 세션키가 갱신되지 않기 때문에 적은 교환회수를 보여주고 있다. 또한 탈퇴해도 기존 멤버의 서브 그룹키만 갱신되기 때문이다.

3.4 기존 모델과의 비교

표 4는 안전한 멀티캐스트 프로토콜을 위한 키 분배 방식을 Wong[7], Iolus[8] 그리고 Dondeti[14]와 제안한 방식을 비교한 결과이다. Wong과 Dondeti의 방식에서 모든 MH는 중앙 키 분배 센터에서 분배한 하나의 KS를 사용하기 때문에 빈번하게 일시적인 키 생신을 해주어야 하기 때문에 전체 시스템 성능에 많은 영향을 주게 된다. Iolus는 서브그룹간에 서로 다른 지역 세션키를 사용하기 때문에 MH의 이동에 따른 오버헤드는 적지만 송신자와 수신자 사이에 여러 개의 서브 그룹 관리자가 존재하는 경우에 서브그룹의 수만큼 재암호화 재분배로 인한 데이타의 전송 지연이 발생하게 되어 그룹 확장하는데 한계가 있다.

그러나 제안한 방법은 Iolus와 유사하지만 송신자와 모든 MH의 암호화와 복호화는 단 한번만 수행하게 되고, 각 서브그룹별로 자치적인 키 생성을 수행하기 때문에 확장성 측면에서 기존방식보다 유리하다. 따라서 제안하는 분산/계층형 방식은 Iolus 방식의 문제점인 반복되는 재암호화와 재분배 과정을 줄일 수 있고, Wong, Dondeti에서 발생되는 빈번한 키 갱신 문제를 해결할 수 있다.

4. 향후 과제 및 결론

기존의 멀티캐스트 구조와는 달리 본 논문에서 제안한 분산/계층 구조가 시스템의 오버헤드를 최소화 하면

표 4 기존 모델과의 비교

구분	Wong[7]	Iolus[8]	Dondeti[14]	제안 모델
그룹 세션의 수	1	l	1	l
전체 키의 수	$\frac{dn-1}{d-1}$	$n+l+1$	$n+l+1+c$	$n+2m-1$
GM이 관리하는 키의 수	$\frac{dn-1}{d-1}$	2	c+2	3
SGM이 관리하는 키의 수	-	l+1	2	2
멤버가 관리하는 키의 수	$\log_d n$	2	2	2
가입 시 메시지의 전송 수	$\log_d n$	2	2	2
탈퇴시 메시지의 전송 수	$d\log_d n$	s	s	s
SGM의 세션키 암호화 회수	1	1	c	0
세션키 분배시 전체 암호화 횟수	1	ls	$l+c$	l
송/수신자간의 최대 재암호화 횟수	0	D	0	0
서브 그룹의 자치성	×	○	△	○
빈번한 멤버 가입/탈퇴에 따른 전체 시스템의 오버헤드	많음	적음	많음	적음
데이타 전송 지연의 주 원인	키 분배	재 암호화	키 분배	서브그룹의 멤버인증
세션키 생성의 주체	그룹 관리자	그룹관리자, 서브그룹 관리자	그룹 관리자	그룹 관리자
세션키 갱신의 빈도	많다	중간	많다	적다
(재)가입을 위한 멤버인증	×	×	×	○
서브 그룹키 갱신	×	○	×	○
중간 노드의 신뢰성 조건	필요	필요	불필요	필요
멤버의 프라이버시	-	-	-	○

※ n : 전체 그룹의 멤버(그룹 관리자 수+서브그룹 관리자의 수+전체 사용자 수), l : 서브그룹 수, ls : 서브그룹의 평균 크기, d : 가지 수, c : 송신자의 서브그룹의 크기, D : 키 분배 트리의 깊이

서 전체 적인 키 갱신 횟수 및 키의 수도 적음을 실험을 통해서 확인했다. 이를 설명하면 제안 구조는 그룹에 재 가입할 때, 그룹 관리자에게 그룹 키를 획득하고 이 키를 이용하여 서브그룹에 가입해야 하는 인증 절차로 인해서 약간의 지연시간이 발생한다. 그러나 서브그룹 관리자는 단지 멤버들에게 데이타를 전달하는 역할만 하고 기존의 서브그룹의 많은 처리 임무에 비교해 볼 때 단순해 졌기 때문에 그 만큼 추가적인 멤버의 가입 요청에 효과적으로 대처할 수 있는 장점이 있다. 제안된 방법은 보다 안전하고 효율적인 방식으로 멀티캐스트 서비스를 제공하고, 효율적인 서비스 관리 구조를 이용하여 보안 자원으로 인한 네트워크 부하 및 성능 저하를 최소화하는데 유용한 정보를 제공한다. 향후 과제는 제안된 모델의 구현과 이동성을 지원하는 구조와 병행 연구가 필요하다.

참 고 문 헌

[1] M. J. Moyer, J. R. Rao and P. Rohotgi, "A Survey of Security Issues in Multicast Communications," *IEEE Network, November/December*, 1999.

[2] C. K. Wong, M. Gouda, S.S. Lam, "Secure Group Communication Using Key Graphs," *Proceedings of CMSIGCOMM'98*, 1998.

[3] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," *Proceedings of ACM SIGCOMM'97*, 1997.

[4] Lakshminath R. Donditi and Sarit Mukherjee, "A Dual Encryption Protocol for Scalabel Secure Multicasting," *Proceedings of IEEE International Symposium on Computer Communication*, pp.667-673, Jun. 1998.

[5] J. Huang and S. Mishra. "Mykil: A highly Scalable and Efficient Key Distribution Protocol for Large group Multicast," *IEEE 2003 Global Communications Conference*, Vol.3 pp.1476-2480, 2003.

[6] S. Mishra. "Key management in large group multicast. Technical report CU-CS-940-02," Department of Computer Science, University of Colorado, Boulder, CO., 2002.

[7] 박준하, 황용호, 이필중 "효율적인 하이브리드 그룹키 관리 프로토콜", 한국정보보호학회 동계정보보호학술대회 논문집, Vol.14, No.2 pp.115-120, 2004.

[8] 권정옥, 황정연, 김현정, 이동훈, 임종인 "일방향 함수와 XOR을 이용한 효율적인 그룹키 관리 프로토콜: ELKH", 정보보호학회논문지, 제12권 제6호, pp.92-112, 2002.

[9] H. Liu and Magada, Zarki "Data and Synchronization Control Middleware to Support Real time Multimedia Services over Wireless PCS Networks," *IEEE journal Communication*, Vol.17, No.9, pp.1660-1672, 1999.
[10] R. Canetti and B.Pinkas, "A taxonomy of Multicast security issues," draft-irtf-smug-taxonomy-01.txt, August., 2000.
[11] Pekka Pessi, "secure Multicast," *Proc. of Helsinki University of Technology Seminar on Network Security*, 1995.
[12] G. Caronni, M. Waldvogel, D. Sun and B. Plattner, 'Efficient Security for Larget and Dynamic Multicast Groups," *Proceedings of 7th Workshop on Enabling Technologies,(WETICE '98), IEEE Computer Society Press*, 1998.
[13] P. McDaniel, A. Prakash and P. Honeyman, "Antigone:A Flexible Framework for Secure Group Communication," *Proceedings of th 8th USENIX Security Symposium*, pp.23-36, August, 1999.
[14] M. Handley and V. Jacobson, "SDP: Session Description Protocol," IETF RFC 2327, 1998.
[15] M. Handley, C. Perkins and E. Whelan, "SAP: Session Announcement Protocol," IETF RFC 2974, 2000.
[16] P. S. Kruus and J. P. Macker, "Techniques and Issues in Multicast Security," *Proc. IEEE MILCOM*, 1998.

고 훈

1998년 2월 호원대학교 전자계산학과 졸업 학사. 2000년 2월 숭실대학교 컴퓨터학과 통신연구실 석사. 2004년 8월 숭실대학교 컴퓨터학과 통신연구실 박사 2000년 5월~2002년 7월 (주)지오나스 주임연구원. 2003년 1월~현재 한국정보보호학회 편집위원. 2002년 9월~현재 대진대학교 컴퓨터공학과 초빙교수. 관심분야는 홈 네트워크 보안, 홈 게이트웨이 보안, 암호화프로토콜, 정보보안, 인터넷보안, 전자서명, 네트워크 보안

장 의 진

1999년 9월 숭실대학교 컴퓨터학과 졸업 학사. 2002년 9월 숭실대학교 컴퓨터학과 통신연구실 석사. 2002년 12월~현재 디지캡 기술연구소 선임연구원. 관심분야는 DRM, 네트워크 보안, 암호화 프로토콜, 정보보안, 인터넷보안, 전자서명

김 선 호

1987년 2월 이화여자대학교 수학교육전공 학사. 1992년 9월 이화여자대학교 교육대학원 전자계산교육전공 석사. 2004년 8월 숭실대학교 컴퓨터학과 박사. 1987년 1월~1989년 12월 대우전자부품(주) 전산실. 1990년 1월~1993년 10월 한국생산성본부 정보화 사업부. 1998년 3월~2004년 8월 동덕여자대학교 정보과학대학 강의전임교수. 2004년 9월~현재 서울소방방재본부 전산개발팀. 관심분야는 DRM, 네트워크 보안, 암호화 프로토콜, 정보보안, 인터넷보안, 전자서명

신 용 태

1985년 2월 한양대학교 산업공학 학사 1990년 12월 Univ. of Iowa 전산학 석사. 1994년 5월 Univ. of Iowa 전산학 박사. 1994년 5월~1994년 8월 Univ. of Iowa computer Science Dept. 객원교수. 1994년 8월~1995년 1월 Michigan State Univ Computer Science Dept. 객원교수. 1995년 3월~현재 숭실대학교 컴퓨터학과 부교수. 2000년 4월~현재 (주) 디지캡 대표이사. 관심분야는 암호화프로토콜, 정보보안, 인터넷보안, DRM