Mobile IP 기반 멀티캐스트 서비스 지원을 위한 메커니즘

박희운, 이임영
순천향대학교 정보기술공학부

A Mechanism based on Mobile IP for Multicasting Service

Hee-Un Park, Im-Yeong Lee
Division of Information Technology, Soon-chun-hyang University

요 약

정보 사회로의 빠른 성장으로 인해 기존의 단대단 서비스를 넘어서 다양한 요구 사항들이 제시되고 있다. 특히 다자간 멀티미디어 서비스를 제공하기 위한 멀티캐스트 방식은 좋은 예가 될 것이다. 이를 위해 현재 고정 IP에 기반한 다양한 멀티캐스트 방식들이 제안되고 있는 실정이다. 그러나 유선에서 무선으로 그 통신 범위가 확대되면서, Mobile IP에 기반한 멀티캐스트 서비스를 고려하지 않을 수 없다. 또한, 원격 호스트에서 서비스를 제공해야 하므로, 지불 관련 인증 서비스 및 사용자 익명성이 동시에 제공되어야 한다. 본 논문에서는 Mobile IP 상에서 멀티캐스트를 수행할 경우, 그룹 원의 인증 및 익명성을 제공할 수 있는 새로운 메커니즘을 제시한다.

1. 서 론

컴퓨터의 보급 확산과 개방형 통신 등의 발전을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있다. 이러한 상황에서 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의, 의료 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 그러나 기존의 일대일 통신 방식으로는 이러한 서비스를 제공하는데 제약 사항이 생길 수밖에 없다. 이를 해결하기 위하여 현재 각광 받고 있는 방식 중의 하나가 멀티캐스트 기법이다.[6]~[10]

멀티캐스트란 그룹에 참가한 멤버들을 대상으로 한 송신자로부터 그룹 참여자들 모두에게 안전한 데이터 전송을 수행하는 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을 떠나면 더 이상 정보를 수신할 수 없게 된다. 동시에 멀티캐스트 기법은 기존의 통신 방식에 대해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 제공한다. 그러나 멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 보안상의 취약성에 노출되고 있다. 특히 불법적인 제 3자의 도청이나 전송 정보의 위조는 그 대표적인 예가 된다. 동시에 기존의 멀티캐스트 서비스는 고정 IP에만 그 적용 범위를 두고 있었으나, 유선에서 무선으로 그 통신 범위가 확대되면서 Mobile IP에 기반한 멀티캐스트 서비스를 고려하지 않을 수 없다.

이러한 상황에서 불법 행위로부터 안전성과 신뢰성을 확보하기 위해 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져야 한다. 동시에 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다. 그 외에도 Mobile IP 기반 서비스를 위해서는 과금 관련 지불 인증을 받아야 하며, 개인 프라이버시를 보호하기 위해 익명성을 제공받아야 한다.[1]~[5]

현재 Mobile IP 기반 멀티캐스트 서비스 분야와 관련하여, 신뢰성과 안전성을 제공하기 위한 해결책들은 미흡한 상황이다. 따라서 본 연구는 향후 광범위하게 적용될 Mobile IP 기반 멀티캐스트 서비스에서 신뢰성, 확장성 및 익명성을 제공하기 위하여 요구되는 사항들을 고려한다. 특히 Mobile IP 기반에서 중요하게 취급되는 인증 및 익명성을 위한 수신자 지정 그룹 서명 방식을 제시함과 동시에 새로운 멀티캐스트 서비스 방식을 제안한다.

2. 고려 사항

멀티캐스트 구조는 그 특성상 다자간 통신을 전제로 하고 있기 때문에 여러 위협 요소에 노출되어 있다. 특히 Mobile IP상의 통신을 위해 사용되는 키의 관리는 매우 중요한 요소로서, 다음은 이를 위해 요구되는 사항을 기술한 것이다.

- 무결성 : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- 인증성 : 송·수신된 멀티캐스트 정보가 불법적인 변조 없이 정당한 참여자들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- 접근 제어 : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 멀티캐스트 서비스 참여자 사이에서 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자가 이를 확인 할 수 있어야 한다.

본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임

- 비밀성 : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.
- 안전성: 각 가입자의 등록 정보가 키 관리자의 DB에 저장되어 있을 경우, 제 3자의 가입자 정보에 대한 불법적 접속 및 유출이 방지되어야 한다.
- 익명성 : 멀티캐스트 멤버의 위치는 허가된 실체 외에는 확인할 수 없어야 한다.
- 공정성 : 멀티캐스트에서 사용되는 키들은 허가된 그룹 참여자에게만 안전하게 전송되어야 한다. 또한 가입 및 탈퇴를 대비해 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단이나 제 3자와의 불법적 결탁을 방어하기 위한 수단이 확보되어야 한다.
- Hand-Off 허용 : Mobile IP상에서 가입자는 이동성을 가지고 있다는 특성을 가지고 있다. 이때 가입자가 새로운 셀(Cell) 범위로 진입할 경우, 새로운 원격 호스트와 새로운 세션키를 통해 메시지를 송/수신해야 한다. 이를 위한 인증은 필수적이며 사용자 및 메시지에 대한 안전성 또한 확보되어야 하는데, 이러한 일련의 과정을 Hand-Off 과정이라 한다. 이동성을 갖는 사용자에 있어 Hand-Off 허용 여부는 중요한 의미를 갖는다.

3. 수신자 지정 그룹 서명 방식

다음은 Mobile IP 상에서 멤버들의 인증 및 익명성을 제공하기 위해 사용 가능한 수신자 지정 서명 방식에 대해 기술한다[1]~[3]. 다음은 본 방식에서 사용되는 시스템 계수 및 각 단계를 설명한 것이다.

1) 시스템 계수

- p, q : 큰 소수 p ≥512 bit, q ≥160 bit (q | p-1)
- g : 원시 생성자
- k_1, k_2 : 랜덤 수 $\{k_1, k_2\} \in {}_RZ_P$
- $D = Y_Z^{k2} \bmod p$
- $e = g^{k2-k1} \bmod p$
- H : 160비트 출력을 내는 안전한 일방향 해쉬 함수
- $R = H(g^{k1} \bmod p \,\|\, M \,\|\, e \,\|\, D)$
- M : 메시지 M
- K_{PG} : 서명자의 소속 확인용 공개키 리스트
- K_{SU} : 서명자의 소속 서명 키 리스트
- X_Z : 수신자 Z의 비밀키
- Y_Z : 수신자 Z의 공개키
- S : 서명

2) 소속 등록 및 키 분배 단계

소속의 등록은 TC(Trusted Center)가 관할하며, 소속에 등록 및 키를 분배받기 위해서는 다음과 같은 일련의 과정을 거친다.

(1) 서명자는 자신의 신상 정보 (서명자 이름, ID, 소속, 기타)를 TC에게 제공한다.

(2) TC는 서명자의 소속 확인이 끝난 후 비밀키 리스트를 안전한 방식으로 전달한다.

$K_{SU} = K_{SL1}, \ldots, K_{SLn}$ (비밀키 리스트)

$K_{SUk} = K_{SL1}, \ldots, K_{SLk}$ (단, $1 \le k \le n$)

서명자의 비밀키는 총 n개의 분할된 키를 갖게된다. 이 키는 TC에서 만든다고 가정하며, 각 서명자의 공개키로 암호화해 분배되거나, IC 카드와 같은 물리적인 형태로 분배된다. 각 서명자는 서명 수행을 위해 분배된 키 리스트 중에서, 날짜 또는 TC의 권고에 따라 k개를 선택해 서명 수행이 가능하다.

따라서 서명 확인을 위한 공개키는 수시로 변화되므로 안전성을 확보할 수 있으며, 별도의 키 생성을 위해 TC가 연산을 수행할 필요가 없기 때문에 효율적이다. 이러한 방식은 새로운 신규 멤버 가입 역시 쉽게 이뤄지는 장점을 가진다.

(3) TC는 서명자의 공개키 들을 공개키 리스트에 등록한다.

$K_{PGk} = g^{KSUk} \bmod p$ (단, $1 < k \le n$)

3) 서명 수행 단계

(1) 서명자는 다음과 같은 정보를 생성한다.

. 큰 소수 p와 q를 생성한 다음 공개한다.

. 생성자 g를 계산한다.

: $h \in \{1,\ldots,p-1\}$를 선택한다.

: $g = h^{(p-1)/q} \bmod p$가 되는 g를 계산하여 공개한다.

(2) 수신자는 자신의 비밀키와 공개키를 생성한다.

. 자신의 일반 서명용 개인키를 생성한다.

: X_Z (단, $0 < X_Z < q$인 난수)

. 공개키는 다음과 같이 생성한다.

: $Y_Z = g^{XZ} \bmod p$

(3) 서명자는 다음과 같이 서명 정보를 생성하여 수신자 Z에게 전송한다.

. 랜덤 수 k_1, k_2를 다음과 같이 생성한 후 e를 계산한다.

: $\{k_1, k_2\} \in {}_RZ_P$

: $e = g^{k2-k1} \bmod p$

. 수신자 Z의 공개키를 이용하여 다음을 계산한다.

: $D = Y_Z^{k2} \bmod p$

. 해쉬 함수를 이용하여 다음을 계산한 다음 서명 정보를 생성한다.

: $R = H(g^{k1} \bmod p \,\|\, M \,\|\, e \,\|\, D)$

: $S = k_1 - K_{SUk} * R \bmod q$

. 다음을 수신자에게 전송한다.

: (M, R, e, D, S) => 수신자

4) 서명 검증 단계

(1) 수신자는 다음을 확인함으로서 서명자의 신분을 확인한다.

. 해쉬를 이용하여 R이 정확한지 확인한다.

: $H(g^S * K_{PG}^R \bmod p \,\|\, M \,\|\, e \,\|D) = R$

(2) 확인된 R을 통해 다음 수식이 만족한다면 서명은 유효하다고 판단한다.

: $(g^S K_{PG}^R e)^{XZ} = D \bmod p$

5) 서명 프로토콜 검증

서명 프로토콜 검증은 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

$$
\begin{aligned}
D &= (g^S K_{PG}^R e)^{XZ} \bmod p \\
&= (g^{k1} g^{(-R*KSUk)} g^{KUSk*R} e)^{XZ} \bmod p \\
&= (g^{k1} e)^{XZ} \bmod p \\
&= (g^{k1} g^{k2-k1})^{XZ} \bmod p \\
&= (g^{k2})^{XZ} \bmod p \\
&= Y_Z^{k2} \bmod p \\
&= D
\end{aligned}
$$

그림 1은 제안된 수신자 지정 그룹 서명 방식에 대한 개략적인 흐름도를 나타낸 것이다.

TC(Trusted Center)	서명자	공개정보 K_{PGk}, p, q, g, Y_Z	검증자 (수신자)
비밀키 리스트 ==> K_{SU}-K_{SL1},...,K_{SLn}	<==신상정보 (서명자 이름, ID, 소속, 기타) 서명 정보 생성 ==> $(k_1, k_2) \in {}_RZ_P$ $e = g^{k2-k1} \bmod p$ $D = Y_Z^{k2} \bmod p$ $R=H(g^{k1} \bmod p \ \|\| M\|\|e\|\|D)$ $S = k_1 - K_{SUk} * R \bmod q$	(M, R, e, D, S)=->	서명 검증 : $H(g^S * K_{PG}{}^R \bmod p \|\| M \|\| e \|\| D) - R$: $(g^S K_{PG}{}^R e)^{XZ} = D \bmod p$

그림 1. 수신자 지정 그룹 서명 방식 흐름도

4. Mobile IP 기반 멀티캐스트 메커니즘 제안

다음에서는 Mobile IP 환경에서 적용 가능한 멀티캐스트 서비스 구조를 제안한다.

4.1 구성 요소 및 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성 요소를 기술하고 있다.

- DKM_i : 도메인 키 관리자 i
- DKA_i : 도메인 키 중간 관리자 i
- GML : 그룹 멤버 리스트
- SGB_i : Subgroup Border i
- R, DMB_i : 라우터 및 도메인 Border i
- MGB_i : 멀티캐스트 그룹 Border i
- PKM : 각 관리자들 및 Border의 공개키 관리자
- MBR_i, GI : 그룹 멤버 i 및 그룹 초기자
- MKey : PKM에 의해 생성된 멀티캐스트 키
- K_{DPi}, K_{DAPi} : DKM_i의 공개키 및 DKA_i의 공개키
- K_{BPi} : 각 B_i의 공개키
- K_{D_DAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MSi} : 그룹 멤버 MBR_i의 비밀키
- K_{DAi_Ms} : 각 DKA_i가 관리하는 멤버들과의 공통키
- Hdr : 각 그룹의 식별 정보
- ID_*, Sig_*, IP_* : *의 식별자, 서명 및 IP 주소
- K_{GS}, K_{GV} : 수신자 지정 그룹 서명용 키 및 확인 키
- M : 멀티캐스팅 메시지
- T, Tr : 멤버가 생성하는 Time-Stamp 및 원격 호스트가 제공하는 Time-Stamp
- RH_i : 원격 호스트 i
- K_{RPi}, K_{RSi} : 원격 호스트 i의 공개키 및 개인키

4.2 시스템 프로토콜

1) 도메인 초기화 단계

(1) DKM_i, DKA_i 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 PKM으로부터 수신한다.

(2) 각 도메인은 DKM_i를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

2) 그룹 초기화 단계

(1) GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 ID_{GI}와 함께 서명을 수행하여 PKM에게 전송한다.

$$Sig_{GI}(ID_{GI}||GML) \rightarrow PKM,\ GML = (ID_{MBR1}||\cdots||ID_{MBRn})$$

(2) PKM은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들에게만 제공함으로서 신뢰성을 높이고 있다.

(3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

3) 그룹 멤버 가입 단계

(1) DKM_i는 도메인 내에서 DKA_i와 통신 시 사용할 K_{D_DAi}를 생성하여 유니캐스트 채널을 통하여 안전하게 DKA_i에게 전송한다.

(2) 그룹에 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{MSi}를 K_{DAPi}로 암호화하여 안전하게 전송한다.

(3) DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 그룹 가입 멤버 리스트를 생성해 DKM_i에게 전송한다.

(4) DKM_i는 각 DKA_i로부터 수신된 그룹 가입 멤버 리스트에 대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.

(5) DKA_i는 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{DAi_Ms} 및 수신자 지정 그룹 서명 키 K_{GS}를 안전하게 전송해 준다. 동시에 이 K_{DAi_Ms} 및 K_{GS}는 DKM_i 및 SGB_i에게 안전하게 전송된다.

4) 원격 호스트 접속 및 인증

이동성을 가지는 MBR_i는 원격 호스트를 통해 멀티캐스트 서비스를 지원받아야 하므로, 자신을 인증 받아야한다. 이때, 자신의 익명성을 제공받기 위해 가명 ID와 수신자 지정 서명을 수행한다.

(1) 멤버는 원격 호스트에서 사용할 자신의 가명 식별자 ID_N를 생성한다. 또한 서비스 개시를 위한 Time-Stamp를 생성하여, 지불 인증을 받을 DKM_i와 가명 식별자를 수신자 지정 서명을 수행해 다음과 같이 원격 호스트에게 전송한다. 가명 식별자를 사용하는 이유는 제 3자로부터 자신의 신분을 숨기기 위해서이다.

$$ID_N||K_{GS}(ID_N||ID_N||DKM_i||T) \rightarrow RH_i$$

(2) 원격 호스트는 수신자 지정 서명을 확인한 다음, 멀티캐스트 서비스 수행을 위해 도메인 Border와 채널을 형성한다.

5) 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 Border들만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정과 타 도메인 및 다른 멀티캐스트 그룹에 속한 멤버들에게 보내는 외부 전송 과정으로 분류된다. 본 문서에서는 내부 전송 과정 중 도메인 전체 메시지 전송에 대한 내용을 기술한다.

(1) 각 멤버들은 K_{DAi_Ms}를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 Border SGB_i에게 전송한다.

$$K_{DAi\_Ms}(M) \rightarrow SGB_i$$

(2) SGB_i는 암호화되어 수신된 정보를 복호화하여 Hdr를 확인하고 Hdr이 없다면 멀티캐스트 메시지 M을 MKey로 암호화하여 각 SGB_i'에게 전송한다.

(3) 각 SGB_i'는 수신된 정보를 복호화하고 이를 자신이 속한 그룹의

공통키로 암호화하여 그룹 멤버들에게 전송한다.

(4) 각 Subgroup의 멤버 MBR_i'는 K_{DAi_Ms}'로 수신된 정보를 복호화하여 메시지를 확인한다. 기타 메시지 전송은 상기 프로토콜에 기초해 수행된다.

6) 원격 호스트 Hand-off 및 지불 인증

(1) 멤버 MBR_i가 이동성이 빨라 Hand-off가 발생될 경우, 원격 호스트 RH_i는 다음 원격 호스트 RH_{i+1} 및 DKM_i에게 다음의 정보를 전송해 준다.

$$K_{RHPi+1}(ID_{Ni}||Tr)||K_{GS}(ID_N||ID_{Ni}||T) \rightarrow RH_{i+1}$$

$$K_{DPi}(ID_{Ni}||Tr)||K_{GS}(ID_N||ID_{Ni}||DKM_i||T) \rightarrow DKM_i$$

(2) 멤버 정보를 수신하면, DKM_i는 다음과 같이 지불 확인 정보를 RH_i에게 전송한다. 이를 통해 RH_i는 지불 인증을 받게 된다.

$$ID_{Ni}||Sig_{DKMi}(ID_N||Tr-T) \rightarrow RH_i$$

(3) RH_{i+1}은 수신된 정보를 확인한 다음, 4)-(2)의 과정을 수행한다. 사용자 요구에 의해 멀티캐스트 접속이 완료되면, 멤버 MBR_i에게 다음의 정보를 각각 전송한다.

$$ID_{Ni+1}||Tr_{+1}||K_{RSi+1}(ID_N||ID_{Ni+1}||Tr||Tr_{+1}) \rightarrow MBR_i$$

(4) MBR_i는 수신정보를 확인한 후에, 다음 정보를 생성해 RH_{i+1}에게 전송한다.

$$ID_N||K_{GS}(ID_N||ID_{Ni+1}||DKM_i||Tr||Tr_{+1}) \rightarrow RH_{i+1}$$

(5) RH_{i+1}은 다음의 정보를 DKM_i에게 전송한다.

$$K_{DPi}(ID_{Ni+1}||Tr_{+1})||K_{GS}(ID_N||ID_{Ni+1}||DKM_i||Tr||Tr_{+1}) \rightarrow DKM_i$$

(6) DKM_i는 6)-(2) 과정을 수행함으로서 지불 인증을 수행한다.

7) 신규 멤버 가입 및 기존 멤버 탈퇴 단계

(1) 신규 멤버 가입은 3) 그룹 멤버 가입 단계와 같은 과정을 수행한다.

(2) 기존 멤버 탈퇴 시에는 DKA_i가 새로운 K_{DAi_Ms}' 및 K_{GS}'을 생성하여 남아 있는 기존의 멤버들 MBR_i', DKM_i 및 SGB_i에게 안전하게 전송함으로서 키 갱신을 수행한다.

5. 제안 방식 분석

다음은 제안 방식의 특성 및 요구 사항 만족도를 분석한 결과이다.

- 무결성 : 전송 정보는 각 세션 키 및 멀티캐스트 키를 통해 암호화되므로, 무결성을 보장한다.
- 인증성 : 각 관리자 및 멤버 그리고, 원격 호스트간에 서명 및 수신자 지정 그룹 서명을 통해 자신을 인증하므로, 불법적 변조는 불가능 하다.
- 접근 제어 : 정당한 그룹의 소속원만이 분배된 세션키를 통해 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 디지털 서명을 통해 인증이 진행되므로, 부인 봉쇄는 불가능하다.
- 비밀성 : 멀티캐스트 전송 정보는 대칭키 암호 기법을 이용해 보호된다.
- 안전성: 각 가입자의 멤버 리스트는 오직 DKM_i 및 PKM에 의해 안전하게 관리된다.
- 익명성 : 제안 방식은 Mobile IP 상에서 가명 ID와 수신자 지정 그룹 서명 방식을 이용하여, 제 3자 및 홈 도메인으로부터 익명성을 보장받는다.
- 공정성 : 멤버 탈퇴시 새로운 K_{DAi_Ms}'를 안전하게 전송받으므로서, 키 갱신을 수행한다.
- Hand-Off 허용 : 멀티캐스트 서비스 도중, 멤버의 Hand-Off가 발생할 경우, 새로운 원격 호스트에서 Border와 안전하게 채널을 형성하며, 인증상의 부담을 줄이기 위해 이전 원격지에서 사용자 인증 정보를 복사해주고 있다.

제안 방식은 상기 모든 요구 사항을 만족함으로서 Mobile IP 기반 멀티캐스트 서비스에서 안전성과 신뢰성을 제공하고 있다. 특히 원격 호스트와 멤버간에 수신자 지정 그룹 서명을 사용함으로서 인증 및 익명성을 제공하고 있다.

6. 결 론

현대 사회는 정보 통신 분야의 발전과 더불어 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 기존의 멀티캐스트 서비스는 기본적으로 고정 IP상에서 다자간 통신을 요구함으로서 안전성, 확장성, 익명성 및 이동성 부분에서 취약성을 드러내고 있다.

본 논문에서는 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았으며, Mobile IP 상에서 이동성을 고려하여 인증 및 익명성을 제공하기 위해 수신자 지정 그룹 서명 방식을 제시하였다. 동시에 요구 사항 및 기존 방식들의 문제점을 해결할 수 있는 새로운 Mobile IP 기반 멀티캐스트 메커니즘을 제안하고 분석하였다. 이를 통해 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참고문헌

[1] D. Chaum, "Group Signature," Advances in Cryptology -EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp.257-265.

[2] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC'95, pp.II-68 ~ II-71, 1995.

[3] 박희운, 이임영, "안전한 수신자 지정 그룹 서명 방식에 대한 고찰," 한국멀티미디어학회 추계학술발표논문집, 1999, 11

[4] C. Perkins, "IP mobility support," RFC 2002.

[5] R. Lin and Kai-Min Wang, "Mobile Multicast Support in IP Network," INFOCOM 2000, Vol3, pp.1664-1672, 2000.

[6] M. Steiner, G. Tsudik and M. Waidner, "Diffie -Hellman Key distribution extended to group," In ACM Symposium on Computer and Communication Security, 1996.

[7] G. Caronni, M. Walldvoge l and D. Plattner, "Efficient Security for Large Dynamic Multicast Groups," WETIC '98, 1998.

[8] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," 1997.

[9] H. Harney and C. Muckenhirn, "Group Management Protocol(GKMP) Architecture," IETF RFC 2094, 1997.

[10] 박희운, 이임영, "효율적인 회의용 키 분배 방식에 관한 연구," 한국통신정보보호학회 충청지부, 1999.