HMIPv6 기반의 모바일 멀티캐스트 환경에서 송신자에 대한 멀티캐스트 분배 트리 접근제어에 관한 연구*

한병진*, 정수진**, 한영주**, 정태명*
*성균관 대학교 정보통신공학부
**성균관 대학교 정보통신공학부 컴퓨터공학과
e-mail : {bjhan, sjjung, yjhan}@imtl.skku.ac.kr , tmchung@ece.skku.ac.kr

A Study on Access Control over Multicast Distribution Tree for Sender in Mobile Multicast Environments based on HMIPv6*

Byung-Jin Han*, Soo-Jin Jung**, Young-Ju Han**, Tai-Myoung Chung*
*School of Information & Communication Engineering, Sungkyunkwan Univ.
**School of Computer Engineering, Sungkyunkwan Univ.

요 약

인터넷과 무선통신 기술의 발달로 Mobile IP 에 대한 관심이 높아지고 있는 가운데 이동 중에도 멀티캐스트 서비스를 이용하기 위해 여러 가지 기술이 연구되고 있다. 인터넷과 멀티캐스트는 열린 모델이라 보안위협에 취약하다. 특히 멀티캐스트에서는 멀티캐스트 분배트리에 대한 접근제어가 중요하다. 본 논문에서는 이동 멀티캐스트에서 멀티캐스트 분배트리에 대한 송신자의 접근제어를 제공하여 서비스의 신뢰성을 높일 수 있는 MSAC (Multicast Source Access Control) 메커니즘을 제안한다. MSAC 과정은 이동하는 멀티캐스트 송신자의 정보들을 MSAC 서버를 통해 인증을 받아 허가되지 않은 노드의 멀티캐스트 분배 트리에 대한 접근을 방지하는 기법이다. MSAC 는 인터넷의 계층적인 특성을 이용하여 인증 회수를 줄이고, 토큰 인증방식을 사용하여 인증 시 메시지를 교환하는 횟수를 줄인다.

1. 서론

인터넷 컨텐츠의 다양화와 컴퓨터 사용환경의 발달은 인터넷 사용자의 급격한 증가를 낳았다. 또한 최근들어 다양한 종류의 서비스를 동시에 즐기는 멀티미디어 서비스에 대한 요구가 증가하고 있다.

멀티캐스트는 이러한 멀티미디어 전송에 알맞은 서비스로 그 중요성이 부각되고 있다. 멀티캐스트는 동일한 패킷을 다수의 수신자에게 동시에 전달하여 대역폭과 패킷 전달의 효율성을 높이기 위해 만들어진 서비스다. 멀티미디어 서비스에 대한 요구가 다양해지는 만큼 멀티캐스트 기술도 더욱 중요시 된다.

한편 무선 기술의 발달로 무선 인터넷의 보급도 빠른 속도로 증가하고 있다. 하지만 현재의 무선 인터넷은 이동성을 보장하지 못하기 때문에 이동 중에도 인터넷을 사용하고자 하는 요구에 부응하지 못하고 있다. 이러한 요구에 발맞추어 Mobile IP 개념이 도입되었다[1][2].

차세대 인터넷은 유무선이 혼합된 초고속 네트워크와 실시간 멀티미디어 중심의 서비스를 지향할 것으로 예상된다. 따라서 이동컴퓨팅 환경에서 멀티캐스트를 지원하는 이동 멀티캐스트 기술이 요구된다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성・지원사업의 연구결과로 수행되었음

이동 멀티캐스트는 몇 가지 문제점을 가지고 있는데 크게 수신자의 이동, 송신자의 이동, 이동 노드의 멀티캐스트 분배 트리에 대한 접근제어 관련 문제로 나눌 수 있다[3].

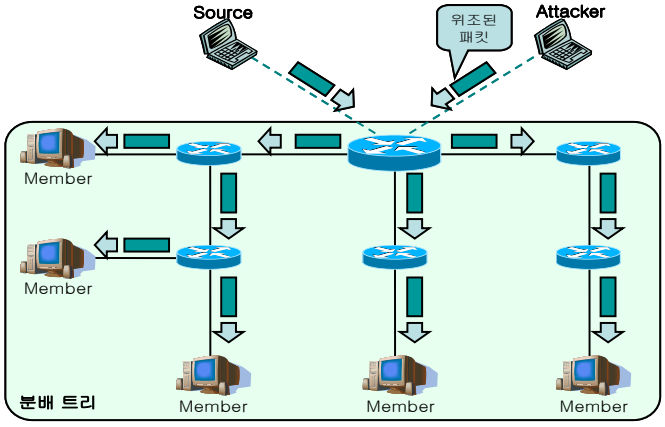
본 논문은 멀티캐스트 분배 트리에 대한 송신자의 접근 제어 문제를 해결할 새로운 방안을 제안한다. 2 장에서는 멀티캐스트 분배 트리에 대한 접근제어의 중요성과 관련 연구를 설명하고, 3 장에서는 본 논문에서 제안하는 멀티캐스트 분배 트리 접근제어 방안인 HMIPv6 기반의 MSAC 메커니즘을 다룬다. 4 장에서 성능의 향상을 보이고, 5 장에서 결론을 맺는다.

2. 관련 연구

멀티캐스트 분배 트리에 대한 접근제어

인터넷과 멀티캐스트 기술은 열려있는 기술이기 때문에 위조나 도청, DoS(Denial of Service)공격을 비롯한 각종 악의적인 공격에 취약하다.

특히, 멀티캐스트 트리에 대한 접근제어는 멀티캐스트 트리가 특정 공격에 대해 일종의 확성기 역할을 할 수 있는 특성을 가지기 때문에 매우 중요하다.



(그림 1) 멀티캐스트 분배트리와 보안 취약점

멀티캐스트 접근제어는 수신자의 접근제어와 송신자의 접근제어로 나누어 생각할 수 있다.

우선 수신자의 접근제어는 수신자가 멀티캐스트 패킷을 받을 수 있는 권한이 있는가에 관한 문제이다. 해결 방식으로는 그룹 키 분배 센터를 두고 그룹 키를 토큰생성에 이용하는 SMKD(Scalable Multicast Key Distribution)[4]방식과 PKI 기반구조를 사용하고 접근제어서버를 두어 증명서를 생성하는 Gothic(Group Access Control Architecture for Secure Multicast and Anycast) [5]방식 등이 있다.

송신자의 접근제어는 송신자가 멀티캐스트 분배트리에 멀티캐스트 패킷을 전송할 수 있는 권한이 있는지를 판단하는 과정이다. 송신자의 위치는 멀티캐스트 분배 트리를 이용하여 수신자보다 능동적인 공격을 할 수 있기 때문에 멀티캐스트 분배트리에 대한 송신자의 접근 제어는 매우 중요하다.

송신자 접근제어 관련 연구 기술로는 IGMP RAC &SAC(IGMP Extension for Authentication of Receivers and Senders)[6] 기술이 있다. 이 기술은 CR (Challenge Response)방식을 사용한다. 작동 방식은 다음과 같다.

멀티캐스트 송신자가 멀티캐스트 패킷을 보내고자 할 때, 송신자는 멀티캐스트 패킷을 제일처음 받는 라우터인 Ingress Router 에게 송신자의 ID 와 그룹 ID 가 담긴 Sender Start 메시지를 보낸다. Ingress Router 는 임의의 Challenge 값을 담은 Challenge 메시지를 송신자에게 보내고, 송신자는 계산한 Response 값과 송신자 ID, 그룹 ID 을 Response 메시지에 담아 Ingress Router 에게 보낸다. Response 메시지를 받은 Ingress Router 는 RADIUS 서버에게 Access Request 메시지를 보내고, RADIUS 서버는 Response 값 확인절차를 통해 인증을 하고 Ingress 라우터에게 유효 기간을 담은 Access Accept 메시지를 보낸다. 마지막으로 Ingress Router 는 송신자에게 Success 메시지를 보낸다.

인증과정이 성공적으로 끝나면, Ingress Router 는 송신자로부터의 멀티캐스트 패킷을 받아들이고, 인증이 실패하면 패킷을 버린다.

CR 방식은 매번 임의의 Challenge 값과 그에 대한 Response 를 통해 인증하므로 Replay attack 으로부터 안전하지만, 너무 많은 컨트롤 메시지를 오가게 하므로 지연시간이 길어지게 된다. 또한, 송신자가 이동하는 환경에서는 핸드오프를 할 때마다 CR 과정을 해야 하므로 오버헤드가 크다.

본 논문은 2 장에서 언급한 멀티캐스트 분배 트리 접근제어를 위해 적은 오버헤드로 송신자 접근제어를 수행하는 HMIPv6 기반의 MSAC 메커니즘을 제안한다.

3. HMIPv6 기반의 MSAC 메커니즘

3.1 MSAC 프레임워크

MSAC(Multicast Source Access Control)메커니즘은 멀티캐스트 송신자가 이동 중에도 정당한 멀티캐스트 트리의 사용권한이 있음을 증명하는 메커니즘이다. 즉, 처음 전송을 시작할 때 송신자 자신이 가지는 고유정보를 기반으로 MSAC 서버에 인증을 받고, 송신자의 이동으로 핸드오프가 일어나 송신자의 주소가 바뀌었을 때, 기존에 해당 멀티캐스트 그룹으로 패킷을 보내던 송신자와 일치한다는 것을 증명하여 멀티캐스트 트리에 대한 사용권한을 획득 하는 과정이다.

MSAC 프레임워크는 핸드오프를 할 때 마다 인증과정을 수행하게 되는 오버헤드를 줄이기 위해 인터넷의 계층구조를 이용하는 HMIPv6(Hierarchical MIPv6) [7]를 기반으로 한다.

MSAC 프레임워크의 구성요소는 MSAC 서버, MAP (Mobility Anchor Point) 그리고 단말 노드로 구성되며, 각각에 대한 기능은 다음과 같다.

- MSAC 서버: 멀티캐스트 송신자의 정보를 받아 정당한 사용자임을 인증하는 역할을 하는 외부에 있는 Trusted Party 로서 송신자 노드와 키를 공유한다.
- MAP: HMIPv6 의 MAP 에 필터링 기능을 추가한 것으로써, MSAC 로부터 접근제어 권한을 위임 받아 멀티캐스트 송신자로부터 멀티캐스트 트리의 루트

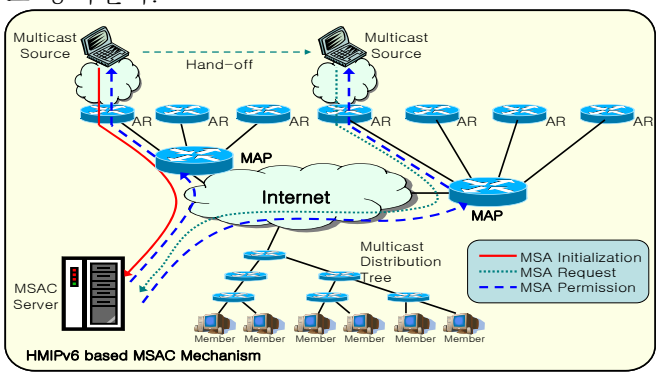
(Root)로 가는 패킷 필터링을 수행한다.

● 단말 노드: 송신자 노드와 수신자 노드가 있다. 송신자는 MSAC 서버로부터 정당성을 인정 받아 멀티캐스트 분배 트리에 멀티캐스트 패킷을 전송하고, 수신자는 멀티캐스트 패킷이 정당한 송신자로부터 온 것임을 믿고 서비스를 받는다.

3.2 동작과정

3.2.1 전체 동작과정

HMIPv6 기반 MSAC 메커니즘은 다음과 같은 단계로 동작한다.



(그림 2) RS-HMIPv6 기반의 MSAC 메커니즘

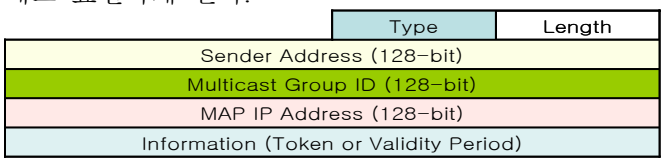
1. 이동성을 가진 멀티캐스트 송신자가 최초 멀티캐스트 패킷을 보내기 전에 MSAC 초기화 메시지를 MSAC 서버로 보내어 인증 및 등록하고 MSAC 서버는 MAP 에게 멀티캐스트 분배 트리 접근을 허가하는 MSAC 허가 메시지를 보내고, MAP 은 그 메시지를 송신자에게 전달한다. 송신자는 허가 메시지를 받은 후 멀티캐스트 패킷 전송을 시작한다.
2. 멀티캐스트 송신자가 이동하여 핸드오프가 발생하면 송신자는 새로운 MAP 도메인에서 MAP 의 IP 주소와 RCoA(Regional Care of Address)를 얻어 해당하는 멀티캐스트 그룹 ID 와 고유 식별 정보를 MSAC 요청 메시지에 담아 MSAC 로 보낸다.
3. MSAC 는 송신자의 고유 식별 정보를 통해 해당 노드의 멀티캐스트 그룹 접근을 허가한다. MSAC 는 MAP 에게 허가 메시지를 보내고, MAP 은 그 메시지를 받아 접근 허가 유효 기간을 설정하고, 송신자에게 허가 메시지를 전달한다.
4. MAP 은 MSAC 서버로부터 받은 허가메시지를 근거로 멀티캐스트 분배 트리 접근을 필터링 한다.
5. 접근 허가 유효 기간이 다 지나게 되면 멀티캐스트 분배트리에 접근할 수 없으므로, 송신자는 유효기간이 다 지나기 전에 MSAC 요청 메시지를 보내어 재 인증을 받는다.
6. 전송이 종료되면 송신자는 MSAC 서버에게 종료 메시지를 보낸다. MSAC 서버는 MSAC 허가 메시지에 접근 허가 유효 기간을 0 으로 하여 보내고, MAP 은 그 메시지를 송신자에게 전달한다.

3.2.2 MSAC 메시지 형식

MSAC 과정에는 4 가지의 메시지 타입이 필요하다. 이는 각각 MSAC 초기화, MSAC 요청, MSAC 허가, MSAC 종료 메시지이며, Destination 옵션에 4 가지 타입을 새로 정의 한다. 모든 MSAC 메시지는 보낼 때 HoA 를 얻기 위해 HA(Home Address)옵션을 같이 사용해야 한다.

MSAC 메시지에는 송신자 자신의 주소 (HoA, RCoA), 멀티캐스트 그룹 ID, MAP 의 IP 주소, 접근 허가 유효기간, 그리고 송신자의 고유 식별 정보가 담긴다. 송신자 자신의 고유 식별 정보는 토큰(Token)이라고 하며, MSAC 서버가 멀티캐스트 송신자를 구별하는 단서다. 토큰에 대해선 다음절에 상세히 설명한다.

MSAC 메시지 옵션들의 형식은 (그림 3)과 같은 형태로 표현하게 된다.



(그림 3) MSAC 옵션 형식

1. MSAC 초기화: 멀티캐스트 패킷을 처음 보낼 때 인증을 위해 보내는 메시지로써, 각 필드의 값은 {Sender_Address, Group_ID, MAP_IP, Token}이다.
2. MSAC 요청: MAP 도메인간의 핸드오프가 일어났을 경우 새로운 RCoA 를 인증하기 위하여 보내는 메시지로써, 각 필드의 값은 {Sender_RCoA, Group_ID, MAP_IP, Token}이다.
3. MSAC 허가: MSAC 초기화 메시지나 MSAC 요청, MSAC 종료 메시지에 대한 MSAC 서버의 응답으로써, 메시지의 각 필드는 {Sender _HoA, Group _ID, MAP_IP, Validity_Period}이다. MAP 은 송신자에게 MSAC 허가 메시지를 전달한다.
4. MSAC 종료: 송신자가 멀티캐스트 패킷을 모두 전송하였을 때나 접근 허가 유효 기간이 만료되었을 때 사용한다. 필드의 값은 MSAC 요청메시지와 같다.

3.2.3 토큰의 구조 및 생성

앞서 언급하였듯이 토큰은 사용자를 구분하는 단서이다. 토큰은 해쉬 함수에 HoA 의 정보, RCoA 정보, MSAC 서버와 공유한 키 값, 그룹 ID, 순서 번호 등을 입력하여 얻어지는 값이다.

$$Token = H\{HoA||RCoA||Key||Group\_ID||Seq\_num\}$$

순서 번호는 Replay attack 에 대비한 요소다. 순서번호는 MSAC 초기화 메시지를 보낼 때 MSAC 서버와 공유한 키 값의 하위 32 비트를 순서번호로 정하여 보내게 되고, 이후 MSAC 요청 메시지를 보낼 때 마다 1 씩 증가시키면서 사용한다.

3.2.4 MSAC 서버의 동작 과정

MSAC 서버는 HoA, RCoA, Group ID, MAP IP 주소, 순서번호 등을 테이블로 유지한다.

최초 MSAC 초기화 메시지를 받게 되면 MSAC 는 공유하고 있는 키 값에서 하위 32 비트를 순서번호로 등록하고 토큰 확인절차를 통해 인증을 한 다음, 해당 HoA 와 Group ID 새로운 엔트리를 만들어 유지시킨다. 새로운 엔트리가 생성되면 MAP 에 MSAC 허가 메시지를 보낸다.

MSAC 요청 메시지가 들어오면 순서번호를 하나 늘린 다음, 토큰을 확인하여 송신자를 인증한다. 인증이 성공하면 엔트리 내의 RCoA 와 MAP IP 를 변경한 뒤, 유효 기간을 다시 설정하여 MAP 에게 MSAC 허가 메시지를 보낸다.

MSAC 종료 메시지가 들어오면 토큰 확인절차를 통해 송신자를 인증하고 허가메시지의 접근 허가 유효 기간을 0 으로 하여 MAP 에게 보내고, 송신자에게는 응답 메시지를 보낸 후, 해당 엔트리를 삭제한다.

3.2.5 MAP 의 동작 과정

MAP 은 기본적으로 가지는 LCoA(Local Care of Address)와 RCoA 에 대한 바인딩 정보 유지 기능에 추가적으로 MSAC 서버로부터 넘겨받은 MSAC 허가 메시지를 바탕으로 필터링을 행한다.

멀티캐스트 분배 트리로의 접근은 기본설정을 불가로 해놓는다 즉, 엔트리에 있는 경우만 허가 한다.

접근 허가 유효 기간이 0 이 아닌 MSAC 허가 메시지를 받으면 접근 허가 엔트리에 해당 송신자의 정보를 추가 혹은 수정을 하고, 접근 허가 유효 기간이 0 인 MSAC 허가 메시지를 받거나 유효 기간 타이머가 만료되면 접근 허가 엔트리를 삭제한다.

3.2.6 송신자 노드의 동작 과정

송신자가 멀티캐스트 패킷을 보내려면 먼저 MSAC 서버에 MSAC 초기화 메시지를 보내어 인증을 받아야 한다. 인증 후 핸드오프가 발생하거나 유효기간이 다 되면 MSAC 서버에 MSAC 요청 메시지를 보내어 재인증을 받는다.

MSAC 초기화 메시지를 보낼 때, 송신자는 MSAC 서버와 공유한 키 값을 이용해 순서번호를 생성한 후 토큰을 생성하여 보낸다.

MSAC 요청 메시지를 보내는 경우는 두 가지다. 첫 번째는 핸드오프가 일어나는 경우이고, 두 번째는 유효기간이 다 되었을 경우이다. 핸드오프가 일어나면 순서번호를 하나 늘리고, 새로운 RCoA 와 MAP IP 를 얻어낸 다음, 토큰을 생성하여 MSAC 서버에게 보낸다. 한편 유효기간이 다 되어 MSAC 요청 메시지를 보낼 경우에는 순서번호만 하나 증가시킨 후 토큰을 생성하여 보낸다.

멀티캐스트 패킷 전송이 끝난 경우 송신자 노드는 MSAC 서버에게 MSAC 종료 메시지를 보내어 더 이상 멀티캐스트 분배 트리를 사용하지 않음을 알린다.

4. 성능평가

이번 장에서는 본 논문에서 제안한 HMIPv6 기반 MSAC 메커니즘과 IGMP RAC&SAC 기술과의 비교를 통해 성능향상을 보인다.

<표 1> HMIPv6 based MSAC vs. IGMP RAC&SAC

	인증빈도	인증시 교환하는 메시지 수	인증 주체	유선망과의 연동가능성
HMIP based MSAC mechanism	MAP 간의 핸드오프시	2	MSAC Server	X
IGMP SAC&RAC	AR 간의 핸드오프시	4	RADIUS Server	O

이처럼 인증 빈도와 교환하는 메시지 수에서는 본 논문에서 제안한 HMIPv6 기반 MSAC 메커니즘의 성능이 월등하다. 특히 MAP 도메인 안에서의 이동 시에는 그 성능이 더욱 월등해진다. 하지만 새로운 기법은 MAP 이라는 요소가 필요하므로 유선 망과의 연동은 불가능한 단점이 있다.

5. 결론

본 논문에서는 이동 멀티캐스트에서 멀티캐스트 분배 트리에 대한 송신자의 접근제어 문제를 해결하기 위하여 HMIPv6 기반의 MSAC 메커니즘을 제안한다. 이 기법은 기존의 송신자 접근제어 방식보다 인증 빈도와 교환 메시지 수에서 월등한 성능을 보인다.

향후 수학적인 성능 분석을 이용하여 보다 정량적인 성능향상을 보이도록 하고, 기존 유선 망에서의 멀티캐스트 서비스 방식과 통합 할 수 있는 방안에 대해 연구해야 하겠다.

참고문헌

[1] C. perkins, “IP Mobility Support for IPv4”, RFC 3344, August 2002

[2] D. Johnson, C. perkins, and j. Arkko, “Mobility Support in IPv6”, RFC 3775, June 2004

[3] I. Romdhani et al., “IP Mobile Multicast Challenges and Solution”, IEEE Communications Surveys, Volume 6, no.1, First Quarter 2004

[4] A. Ballardie, “Scalable Multicast Key Distribution”, RFC 1949, May 1996

[5] P. Judge and M. Ammar, “Gothic : A group Access Control Architecture for Secure Multicast and Anycast”, IEEE INFOCOM, pp. 1547-56, June 2002

[6] N. Ishikawa, N. Yamanouchi, and O. Takahashi, “An Architecture for User Authentication of IP Multicast and Its Implementation”, IEEE/Japan Internet Workshop. ’99 (IWS’99), pp.687-692, Feb 1999

[7] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6)”, RFC 4140, Aug 2005