Wireless Mesh Networks의 보안 강화[1)]

박진호 조재익° 임을규 김정식 최경호 장현준
한양대학교 정보통신대학
{pjh0347, whisperi°, imeg}@hanyang.ac.kr, bisa1004@hanmail.net,
ckh820520@naver.com, iam@b4you.net

Improve security of Wireless Mesh Networks

Jin Ho Park, Jae Ik Cho°, Eul Gyu Im, Jung Sik Kim, Kyoung Ho Choi, Hyun Jun Jang
College of Information & Communications, Hanyang Univ.

요 약

기존의 무선 네트워크에 비해 빠르고 저렴하며 설치가 편리한 무선 메쉬 네트워크를 인터넷망 구성에 도입하려고 하는 것이 최근의 경향이다. 무선 메쉬 네트워크는 이종망간의 네트워크를 통합함으로 수많은 클라이언트들을 통제해야하며 기존의 IPv4 주소는 10년 내에 고갈이 됨으로, IPv6 주소 환경에 적합하게 연구 개발하여야 한다. 그러나 아직 무선 메쉬 네트워크는 개발 중인 기술로써 보완해야할 보안상의 문제점들이 발견되고 있다. 본 논문에서는 무선 메쉬 네트워크에 MIPv6를 어떻게 도입할지를 언급하고 MIPv6 도입 시에 발생하게 되는 보안상의 문제점을 SEND(SEcure Neighbor Discovery)와 MCGAs를 이용하여 해결하는 방법을 소개한다.

1. 서 론

최근 언제 어디서나 인터넷에 접속할 수 있는 유비쿼터스 시대를 만들기 위해 여러 방법들이 제안되고 있으며, 그 중에서 기존의 이기종 네트워크들을 쉽게 연결할 수 있는 무선 메쉬 네트워크 (WMN: Wireless Mesh Networks)[12]가 좋은 해결 방안으로 연구 개발 중에 있다. 무선 메쉬 네트워크는 Wireless Hot Spot (WHS)이라 불리는 무선 라우터와 Transit Access Point (TAP)이라 불리는 무선 AP를 기반으로 구성이 된다. 기존의 네트워크들과의 차이로는 WiFi 네트워크의 경우, 서비스 지역을 넓히기 위하여 무선 라우터의 수를 늘려야 하지만 무선 메쉬 네트워크에서는 WHS에 비해 가격이 저렴한 TAP의 추가 설치로 쉽게 서비스 지역을 넓힐 수 있다. 따라서 기존의 WiFi 네트워크에 비해 빠르고 간단하면서 네트워크를 구성하는데 드는 비용이 적은 것이 장점이다. Ad-Hoc 네트워크나 센서 네트워크의 경우는 노드들이 무선으로 연결되어 있으며, Multi - hopping 을 통하여 데이터를 전달한다는 유사점을 가지고 있으나, 무선 메쉬 네트워크의 경우 WHS나 TAP이 에너지의 제약을 가지지 않는다는 차이가 있다. 따라서 보안성을 높이기 위한 암호화 알고리즘이나 라우팅 알고리즘의 사용이 저전력이 요구되는 네트워크에 비해 용이하다. 그러나 무선 메쉬 네트워크는 아직 개발 중인 기술로써 보완해야할 기술적인 문제점들이 존재하며, 특히 이종망간의 연결로부터 발생하는 보안 문제들이 발견되고 있다. 또한, 유비쿼터스 시대의 IPv4의 점진적인 고갈 현상으로 인한 선결 문제인 무한한 IP 주소의 확보를 위해 무선 메쉬 네트워크 역시 128비트의 주소를 가지게 되는 IPv6에 맞춰서 개발을 해야 한다. IPv6 에서는 자동 주소 설정기능이 들어있어 네트워크에 접속만 하면 기본적으로 자동으로 주소가 결정이 되고, 이동형 장치를 지원하는 기능(mobility)이 향상 되었다. 그리고 기본적으로 통신내용을 암호화하여 통신의 보안성 (IPSec)을 향상시킬 수 있고 통신품질보장성 (QoS: Quality of Service) 기능을 자체적으로 지원한다. 본 논문에서는 무선 메쉬 네트워크에 MIPv6를 어떻게 도입할 것인지 그리고 MIPv6를 도입했을 경우에 발생하게 되는 보안상의 문제점을 SEND 프로토콜을 이용하여 해결하는 방법을 소개한다.

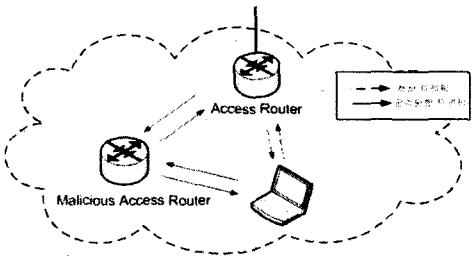
본 논문의 구성은 다음과 같다. 먼저, 제2장에서 무선 메쉬 네트워크 관점에서의 MIPv6와 보안 문제에 대하여 소개하고 제3장에서는 MIPv6의 취약점을 보완해줄 SEND 프로토콜에 대해 설명한 후, 제 4장에서는 무선 환경에서 SEND의 취약점을 보완하는 MCGAs기법을 소개하며, 마지막으로 제5장에서는 결론과 향후 연구 계획에 대해 언급하였다.

2.1 IPv6 보안 문제

무선 메쉬 네트워크에서는 수많은 모바일 클라이언트들을 관리하기 위해 IPv6[1,10] 체계를 사용하여야 한다. IPv6 보안 문제점은 대표적으로 주소 자동 설정 기능의 취약점을 들 수 있다. 노드가 네트워크에서 별도의 IP관리 서버의 도움 없이 라우터에서 보내주는 정보를 받아 IP를 설정하는 주소 자동 설정 기능[3]은 ICMPv6 프로토콜 기반의 이웃 탐색(Neighbor Discovery) 프로토콜[2]의 한 기능으로서 보안 메커니즘이 없는 ICMPv6 기반의 ND는 메시지의 위변조가 가능하다. 즉, 아래 [그림

1) 본 연구는 한국과학재단 특정기초연구(과제번호 : R01-2006-000- 11196-0)지원으로 수행되었음.

1]처럼 악의적인 라우터에서 거짓된 정보를 노드에게 광고하여 그 노드가 악의적 라우터를 통해 외부로 통신하게 하는 Man In The Middle(MITM) Attack이 가능하다. 이에 대한 해결책으로 SEND(Securing Neighbor Discovery)[4]는 ND에 대하여 인증 및 무결성을 제공한다.



[그림 1] Man In The Middle(MITM) Attack

2.2 Mobile IPv6 보안 문제

무선 메쉬 네트워크는 사용자들이 이동을 할 경우에도 끊임없는 서비스를 제공해야 하며 다양한 이종망간에서도 이동성을 지원해줘야 한다. 따라서 이동성이 고려된 Mobile IPv6 환경이 무선 메쉬 네트워크에 가장 적합하다고 할 수 있다. 기존의 MIPv4의 경우 Triangle Routing 문제가 지적되었는데, Triangle Routing 문제는 다음과 같은 현상을 의미한다. 외부 네트워크에 위치한 모바일 클라이언트는 통신하려는 상대 클라이언트에게 직접 데이터를 전송할 수 있다. 그러나 상대 클라이언트가 외부 네트워크에 위치한 모바일 클라이언트로 데이터를 전송할 때에는 모바일 클라이언트가 위치했던 홈 네트워크의 홈 에이전트를 거쳐 전달된다. 상대 클라이언트가 전송한 패킷이 항상 홈 에이전트를 거쳐서 전달되어 통신의 효율성을 떨어트리는 현상을 Triangle Routing 문제라고 한다.

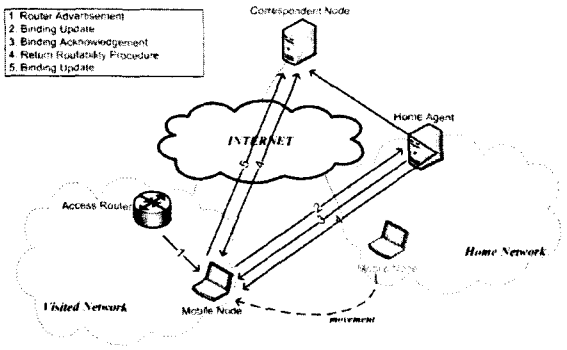
그러나 Mobile IPv6[8]에서도 MIPv4의 문제점은 해결하였으나 2장에서 언급한 IPv6에서 발생하는 문제점 외에도 이동성을 중시하기 때문에 파생된 보안 문제들이 있다. 먼저, 바인딩 메시지를 주고받는 과정에서 발생할 수 있는 문제점으로 무선 메쉬 네트워크에서 모바일 클라이언트가 기존에 위치하고 있던 네트워크에서 다른 네트워크로 이동했을 때 이동한 네트워크에 위치하는 WHS 또는 홈 에이전트로 바인딩 메시지를 전송하여 자신이 다른 네트워크에서 이동해왔음을 등록하여야 하는데, 악의적인 목적을 가진 공격자는 자신을 피해자의 모바일 클라이언트가 이동해 온 네트워크의 홈 에이전트라는 거짓된 정보를 제공함으로써 이동해 온 모바일 클라이언트를 속일 수가 있다. 피해자의 모바일 클라이언트는 공격자를 거쳐서 통신을 하기 때문에 데이터들이 공격자에게 인터셉트 당하게 된다.

다음으로, 모바일 클라이언트가 타 네트워크로 이동한 후 홈 에이전트로 바인딩 메시지를 전송할 때, 공격자가 이동해 온 모바일 클라이언트의 위치를 속여서 바인딩 메시지를 홈 에이전트에게 보낼 수 있다. 홈 에이전트가 이와 같은 거짓된 정보를 수신하게 되면, 모바일 클라이언트는 데이터를 수신하지 못하게 되고 다른 임의의 모바일 클라이언트가 데이터를 수신하게 된다. 이를 방지하기 위해서는 이동 노드가 다른 도메인의 서브넷으로 이동하는 경우 먼저 이동 노드와 서브넷간에 상호 인증이 우선되어야 한다. 이는 BTS(Base Transceiver Station) 공격 및 악의적인 외부 노드의 링크 사용을 방지하기 위한 기본적인 요구사항으로서 일반적으로 AAA(Authentication, Authorization and Accounting) 등의 인프라 구조상에서의 인증 과정을 수행한다. Mobile IP 작업 그룹에서 AAA 통합 인증 방법에 관한 연구는 아직 초기단계이지만 지속적인 관심을 가지고 실험적인 시도가 진행되고 있으며 향후 AAA 작업 그룹 및 3GPP 등의 다른 작업 그룹과의 협력을 통해 보다 구체화된 인증방식이 정의될 것이며 여기에 한 단계 더 나아가 동적 SA 설정을 위한 기반 구조로 사용될 수 있도록 하는 보완 작업이 진행될 것이다. 앞에서 기술한 성능 개선 작업이 제안되면서 그에 따르는 보안 위협도 증가하고 있는데 이는 보안성 향상과 성능 개선의 이득이 서로 상반된 것으로서 높은 보안을 유지하고 최적화된 성능을 제공하는 것이 그만큼 어렵다는 반증이 된다.

또 다른 보안 문제로는 라우팅 헤더 문제로 라우팅 헤더는 Mobile IPv6에서 모바일 클라이언트로 패킷을 전송할 때 상위계층에 투명하게 통신할 수 있도록 지원하기 위해서 사용된다. 또한, 소스 라우팅에 사용되기 때문에 트래픽 라우팅 헤더를 이용해서 동적으로 ISP를 선택할 수 있다. 하지만, 현재 Mobile IPv6에서 사용하도록 한 Type 0의 라우팅 헤더는 호스트나 라우터에서 모두 처리 가능하며, 여러 개의 주소를 담아서 전송될 수 있기 때문에 reflection attack에 이용될 수도 있다.[11]

마지막으로 HAO(Home Address Option)을 사용할 경우 발생할 수 있는 보안상의 문제점이 있다. 공격자가 HAO를 이용하여 자신의 위치를 숨기고 서비스 거부 공격 (DoS: Denial of Service)이 가능하다. 공격자는 공격 대상으로 특정 모바일 클라이언트를 선택하고 도달 가능한 다른 모바일 클라이언트를 선택한다. 공격자는 MIPv6 패킷 헤더의 소스 주소와 목적지 주소를 공격자 자신의 주소와 도달 가능한 다른 모바일 클라이언트의 주소로 설정하고 HAO 에는 공격대상이 되는 모바일 클라이언트의 주소를 포함하여 패킷을 전송한다. 도달 가능한 모바일 클라이언트는 공격자로부터 도착한 MIPv6 패킷을 처리하여 응답메시지를 전송하는데, 수신한 패킷에 HAO가 포함되어 있으면, 소스 주소와 HAO의 주소를 바꾸게 된다. 그 결과 도달 가능한 모바일 클라이언트는 공격대상으로부터 패킷이 전송되었다고 판단하고 응답 메시지를 공격 대상으로 전송한다. 공격 대상인 모바일 클라이언트는 소스 주소가 도달 가능한 모바일 클라이언트인 패킷을 받게 되는데 원 송신자였던 공격자의 주소는 알 수 없게 된다. 위에 언급된 IPv6 및 Mobile IPv6의 보안 문제들은 현재 여러 보안 프로토콜들을 중점으로 연구되고 있다. 홈 에이전트와 모바일 클라이언트 사이의 보안 프로토콜로는 IPsec을 사용 중이고 보완하고 있는 중이다. 바인딩 갱신 및 바인딩 응답메시지의 인증을 위해서 RR (Return Routability) 프로토콜을 사용을 RFC 문서에서는

명시하고 있다. 그러나 보다 보안성이 향상된 프로토콜이 요구되어 지고 있으며, 기존의 ND 프로토콜에 보안 요소들을 추가한 SEND (Securing Neighbor Discovery)이 MIPv6에서 중요한 연구로 떠오르고 있다.



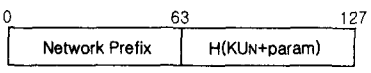
[그림 2] MIPv6 동작 과정

3. SEcure Neighbor Discovery

앞서 기술한바와 같이 IPv6의 Neighbor Discovery를 보호하기 위해 SEND 프로토콜이 사용된다. 먼저 어떤 기능을 제공하는지를 살펴보면 다음과 같다.

Cryptographically Generated Addresses (CGA)[5]를 사용하여 전송하는 ND 메시지의 송신지 주소가 ND 메시지를 전송한 노드의 주소임을 증명하는 주소 소유권 증명 기능과 공개키 기반 서명을 통해 송신자를 인증하고 메시지의 무결성을 제공하는 기능 그리고 Redirect와 같은 단방향 메시지는 Time stamp값을 이용하고, neighbor solicitation / neighbor advertisement와 같은 양방향 메시지는 임의의 수 Nonce를 이용하여 이전에 전송된 메시지를 다시 사용하는 위장 공격, 즉 재연 공격을 방지한다. 또한 라우터 탐색을 보호하기 위해서 각 라우터는 자신의 권한(Authority)에 대해 인증 받을 수 있는 인증 경로(Certification path)를 가지는데, 인증 경로는 경로상의 최종 객체에 대한 공개키를 얻기 위한 인증서들이 순서대로 정렬된 것을 의미한다. 라우터는 신뢰 앵커(Trust anchor)로부터 인증서를 얻고 호스트는 신뢰 앵커와 설정을 맺어 인증서 사슬(Certificate Chain)을 형성하게 되어 호스트는 라우터를 신뢰할 수 있게 되며 이를 권한 위임 탐색이라고 한다.

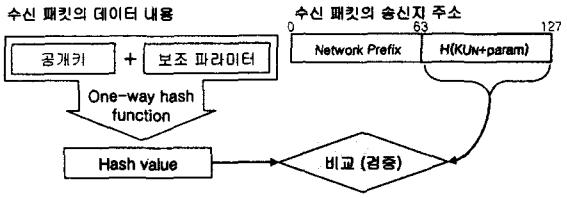
SEND 프로토콜의 핵심은 공개키를 IPv6 주소에 바인딩 시킬 수 있다는 점이다. SEND는 내부적으로 CGA 개념을 도입하여 주소 소유권 증명, 메시지에 대한 무결성, 인증 등의 보안성을 제공한다.



KU_N : 노드 자신의 공개키
param : 보조 파라미터

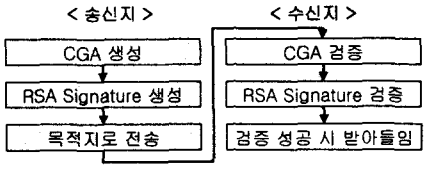
[그림 3] CGA 형식

CGA는 앞의 64bit는 네트워크 프리픽스를 사용하고 뒤의 64bit는 기존의 주소 자동 설정에서 사용되었던 인터페이스 식별자 대신에 노드에서 생성한 공개키와 보조파라미터로부터 얻은 해시 값을 사용하여 만들어진다.[9] CGA를 사용한 ND 메시지를 받았을 때 공개키와 보조파라미터로부터 해쉬값을 재검출하여 CGA와 일치하는지 확인함으로써 IP주소와 공개키 사이에 바인딩 시킬 수 있게 된다.



[그림 4] CGA 검증 수행 방법

전송할 ND메시지를 개인키로 RSA Signature를 만들어 붙여 보내면 ND메시지에 대해 인증과 무결성을 제공할 수 있다. 전체적인 동작 흐름을 정리하면 다음과 같다.



[그림 5] CGA관련 SEND 동작 흐름

이렇게 IPv6 환경에서 SEND를 적용하면 안전하게 ND를 보호할 수 있지만 Mobile IPv6 환경에 바로 적용하면 CGA주소가 프록시(Home Agent)에 의해 보호되어지지 못하는 문제점이 발생하는데, 이 부분에 대한 해결을 위해 다음에 소개하는 MCGAs 기법이 있다.

4. Multi-Key Cryptographically Generated Addresses

MCGAs는[7] DoCoMo USA Labs에서 2005년에 표준 스펙으로 제안했었던 내용으로 기존 CGA에서 하나의 키를 사용하는 반면에 MCGAs는 여러 개의 키를 사용하여 주소 프록시 문제를 해결한다는 점에서 SEND의 취약점을 보완하기 위해 제시된 내용으로 볼 수 있다. 이와 함께 위치 보호(location privacy)기능을 갖는 이점도 있다.

CGA주소가 프록시에 의해 보호되지 못하는 이유는 MN만이 자신의 개인키를 갖고 있기 때문이다. MCGAs의 동작 과정을 살펴보면 다음과 같다.

라우터에서의 처리 방법은 먼저 AES encryption key를 생성하여 node-specific RSA Ring signature의 개인키 부분을 암호화하여 그 노드에게 전달한다. 라우터가 RS 메시지를 받았다면 RSA Ring signature를 사용하여 RA 메시지를 서명하여 응답한다. 이때 필요한 RSA Ring signature와 multi-key CGA는 라우터의 인증된 공개키

와 라우터에 RS메시지를 요청한 노드의 공개키를 이용하여 생성된다.

주소설정 노드에서 처리 방법은 multi-key CGA사용을 위해 라우터에서 생성한 node-specific 공개키와 암호화된 개인키를 얻어야 한다. 이는 링크내의 모든 라우터에게 멀티캐스트 방식으로 요청하게 된다. 이렇게 얻은 node-specific 공개키와 노드 자신이 생성한 공개키를 이용하여 Multi-key CGA 주소를 생성한다. 그리고 노드 자신의 개인키와 전에 얻은 node-specific 암호화된 개인키를 저장해놓고 주소 프록시 서비스가 필요할 때 사용한다. 그런 후 DAD과정을 거쳐 다른 노드가 사용 중인지 확인한 후 사용 한다.

주소검증 노드에서 처리 방법은 ND관련 메시지를 받았을 때 확장된 SEND관련 옵션을 이용하여 검증을 수행한다.

Multi-key CGA 주소 생성 방법은 CGA 방법과 대체로 같지만 예외적으로(CGA주소 생성 step 2단계) 공개키를 연결할 때 키가 복수 개이므로 각 키를 차례로 연결하여 해시 값을 얻어(concat-val) 공개키 대신에 사용한다. 검증 방법도 몇 가지를 제외하고는 크게 다르지 않다. CGA주소 검증 step 3단계에서 Hash1값을 계산하기 전에 확장 필드를 제외시킨다는 점과 step 6단계에서 Hash2의 확장 필드 대신 앞에서 설명한 바와 같이 concat-val값을 계산하여 사용한다.

5. 결론 및 향후 연구 방향

기존 무선 LAN의 한계를 극복하기 위해 제안된 무선 메쉬 네트워크는 유비쿼터스 환경 구축을 위한 인프라로써 앞으로 필요성이 증대될 것이다. 그러나 아직 이종망간의 통합으로 인한 서로 사용 환경이 다른 상황에서 해결해야할 보안 문제점들이 존재하고 있다. 또한 앞에서 언급한 것과 같이 MIPv6의 도입이 필요로 하나 MIPv6 자체에서 재기 되는 보안 문제도 해결해야 한다는 과제를 남겨 두고 있다.

DoCoMo USA Labs에서는 "Open Source SEND project"라는 이름으로 Linux OS상의 사용자 레벨에서 SEND를 이미 구현하여 테스트와 연구를 진행하고 있다. 앞으로 Secure Neighbor Discovery와 관련하여 활발한 연구가 이루어질 것으로 생각된다.

MCGAs는 비대칭키를 사용한 암호화 기법을 무선 환경에 적용함으로서 신뢰하기 힘든 무선 메쉬 네트워크에서 적절한 보호 메커니즘으로 사용될 수 있을 것이다.

참 고 문 헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[2] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[3] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[4] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005

[5] T. Aura, "Cryptographically Generated Addresses (CGA)". RFC 3972, March 2005

[6] P.Nikander, J.Kempf, E.Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004

[7] J.Kempf, C.Gentry, "Secure IPv6 Address Proxying using Multi-Key Cryptographically Generated Addresses (MCGAs)", IETF Working Document, RFC 3668 (SEND), Aug 2005

[8] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC3775, June 2004

[9] "IPv6 보안 기술 해설서", KISA, Oct 2005

[10] IPv6 포럼 코리아, "차세대 인터넷 프로토콜 IPv6", 다성 출판사, March 2002

[11] 권혁찬, 나재훈, 정교일, "Mobile IPv6 표준화 및 기술 동향", May 2004

[12] Ben Salem, N. Hubaux, J.-P., "Securing wireless mesh networks", Wireless Communications, IEEE Volume 13, Issue 2, April 2006 Page(s):50 - 55