논문 2005-42TC-11-5

Mobile IP에서 확장성과 실용성 있는 인증 프로토콜 제안 및 분석

(A Scalable and Practical Authentication Protocol in Mobile IP)

이 용*, 이 구 연**

(Yong Lee and Goo Yeon Lee)

요 약

Mobile IP 프로토콜에서는 이동 노드가 자신의 홈망이 아닌 다른 망에 이동할 경우에도 자신의 홈 IP 주소를 그대로 사용하기 때문에 이동 노드와 방문망, 홈망 사이의 상호인증은 중요한 문제이다. 지금까지 이와 관련된 여러 연구는 주로 비밀정보 공유를 기반으로 이동 노드와 HA간에 미리 대칭키를 나눠가지고 이를 이용하여 인증을 할 수 있도록 하거나, 공개키 방식을 적용할 경우도 복잡한 알고리즘으로 인하여 실제 환경에 적용하기 어려운 문제점을 가지고 있다. 또한 replay attack 등 네트워크 상의 공격이슈에 대한 문제를 해결하지 못하고 있다. 본 논문에서는 Mobile IP 프로토콜에서 발생하는 여러 가지 보안 이슈들에 대하여 설명하고, Mobile IP 프로토콜에 적용가능한 인증프로토콜을 제안한다. 제안하는 프로토콜은 공개키 알고리즘에 기반하여 기존의 Mobile IP 프로토콜의 수정없이 그대로 적용되어, 실제 환경에 적용가능하며 이동 노드들에 대한 확장성을 갖는다. 우리는 제안하는 프로토콜의 안전성을 증명하고 고유의 Mobile IP 프로토콜의 성능에 영향을 끼치지 않음을 보여줄 것이다.

Abstract

In Mobile IP protocol, because a mobile node still uses its home IP address even though it moves to foreign network from home network, authentication among mobile node, foreign network and home network is critical issue. Many researches about this issue have been based on shared secret, for example mobile node and home agent authenticate each other with pre-shared symmetry key. And they missed several security issues such as replay attack. Although public key scheme could be applied to this issue easily, since the public key cryptography is computationally complicated, it still has the problem that it is not practical to realistic environment. In this paper, we describe several security issues in Mobile IP protocol. And we propose new Mobile IP authentication protocol that is applicable to realistic environment using public key algorithm based on certificate. It has scalability for mobile nodes and is applicable to the original Mobile IP protocol without any change. Finally we prove security of the proposed protocol and that it might not affect performance of the original Mobile IP protocol.

Keywords: 인증프로토콜, 공개키 암호방식, 인증서, Mobile IP

* 정회원, Cornell University
(School of Electrical Eng. Cornell University)
** 정회원, 강원대학교 전기전자정보통신공학부
(Dept. of Electrical and Computer Eng. Kangwon National University)
※ 이 논문은 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원(해외방문연구)을 받아 연구되었으며(M01-2004-000-10101-0), 또한 강원대학교 정보통신연구소의 지원을 받아 연구되었습니다.
접수일자: 2005년3월31일, 수정완료일: 2005년11월14일

I. 서 론

인터넷 사용자에게 이동성을 지원하는 모바일 인터넷 기술의 발전에 따라, 인터넷 응용 환경이 이전보다 더 편리하게 변하고 있다. Mobile IP 프로토콜은 이동 노드가 홈망으로부터 다른 망으로 이동할 경우에도 자신의 홈 IP 주소를 그대로 사용하여 다른 노드들과 통

신하며 인터넷을 사용할 수 있도록 한다[1]. 이동 노드가 방문망에 머무를 경우 여러 가지 네트워크 자원을 사용할 필요가 있다. 이 경우 방문망은 자원 사용에 관한 권한을 이동 노드에게 주기 위해서 먼저 이동 노드를 인증해야 한다. 또한 이동 노드도 방문망으로부터 얻은 Care of Address (CoA)를 통하여 다른 노드들과 통신하게 되므로 자신이 접속한 방문망과 이 주소가 악의적인 서버에 의해 위장되지 않았는지 확인할 필요가 있다. 이동 노드가 홈망의 HA(Home Agent)에 CoA를 등록할 때에 HA는 이동 노드와 CoA를 인증한 후에 CoA 정보를 자신의 DB에 저장하고 다른 노드들의 호를 해당노드에 연결해 줄 때 사용하여야 한다. 따라서 이동 노드와 방문망, 홈망의 HA 사이의 인증은 노드들의 이동성을 지원하는 Mobile IP 프로토콜에서 중요한 주제이다[1][2].

지금까지 이에 관한 많은 연구가 진행되어 왔으나, 대부분 AAA(Accounting, Authorization, Authentication)나 KDC(Key Distribution Center) server 같은 비밀정보 공유를 이용하는 방법에 기반하고 있다. 이동 노드와 HA는 비밀 정보로서 대칭키를 공유하며 이를 이용하여 서로를 인증한다. 그러나 이러한 방법은 키 관리와 확장성 등 대칭키 암호의 전통적인 문제를 해결하지 못하고 있다[3]. 공개키 알고리즘에 기반한 인증 프로토콜을 적용한 경우에도 계산이 오래 걸리는 공개키 암호 연산을 그대로 적용하였고, 인증서 검증이 복잡한 문제를 해결하지 못하여 여러 곳을 움직이며 빈번하게 인증 프로토콜을 수행하여야 하는 이동 노드에게는 실용적이지 못하다[4]. 이러한 방법들은 이동 노드가 CoA를 얻기 위해 방문망에서 보내는 Advertisement 메시지를 어떻게 신뢰하여야 하는 지에 대한 방법을 언급하지 않고 있다.

앞에서 언급한 바와 같이, 이동 노드가 Mobile IP 프로토콜에 따라 방문망으로 이동했을 때 먼저 서로 인증한 후에, 이동 노드는 방문망으로부터 CoA를 획득하고 방문방도 이동 노드가 네트워크 bandwidth 같은 자원을 사용할 수 있도록 권한을 주어야 한다. 이동 노드가 홈망에 자신의 위치를 등록할 때에도 HA가 이동 노드가 자신의 도메인이 미리 등록된 노드인지를 확인하고 등록을 요청한 노드가 주장하는 노드가 맞는지를 인증한 후에 등록 절차를 수행하고 노드의 CoA를 이동 노드와 통신하기를 원하는 노드(CN)에 주어야 한다.

이 논문에서는 공개키 알고리즘을 이용한 Mobile IP에서의 인증 프로토콜을 제안한다. 제안하는 프로토콜은 이동 노드가 방문망으로부터 CoA를 얻기 위해 방문망을 인증하는 메커니즘과 HA가 네트워크를 통해 전송된 이동 노드의 현재 위치 정보를 어떻게 신뢰할 것인지에 대한 방안을 소개한다. 이 프로토콜은 본래의 Mobile IP 프로토콜의 스텝을 수정하지 않고 공개키 인증서를 사용하는 간단한 인증 프로토콜로서 초기 인증 후에 각 객체들은 비밀키를 공유하여 복잡한 공개키 연산을 피할 수 있고 인증 단계를 최적화할 수 있다. 또한 이동 노드가 다른 망에 있는 CN과 통신하고자 할 경우에, CN이 정말로 자신이 통신하고자 하는 노드인지를 인증하는 프로토콜을 제안하고 이에 대한 안전성을 검증하고자 한다.

Ⅱ. Mobile IP 인증 프로토콜

이 장에서는 현재 IETF에서 논의되고 있는 Mobile IP 인증 프로토콜과 관련된 연구들에 대하여 소개하고 그 문제점에 대하여 논의하고자 한다.

1. IETF Mobile IP 프로토콜에서의 보안 문제들

Mobile IP 프로토콜에서의 보안에 관련된 주요이슈는 Home Address Destination option을 사용한 DoS(Denial of Service) Attack 과 Binding Update에 대한 인증이 대표적이다. 현재 Mobile IPv6에서 이러한 주제를 주요 보안 이슈로 다루고 있다.

Home Address Destination option을 사용한 DoS Attack의 경우, 공격자가 자신의 정체를 숨긴 채로 A라는 노드의 홈 IP 주소를 사용하여 CN에 메시지를 보낼 경우, 노드 A는 공격자로부터 예상치 못한 DoS 공격을 받게 된다. 이러한 DoS 공격에 대한 해결방안으로는 CN이 home address의 유효성을 확인할 수 있어야 한다. 즉, CN이 home address의 소유자인 이동 노드가 정말로 이 메시지를 보냈는지를 검증할 수 있어야 한다.

Binding update에 대한 공격의 경우는 공격자가 CN에 대한 binding update 메시지에 노드 A의 CoA를 실어 보낼 경우, CN은 binding update가 노드 A로부터 온 것으로 착각하여 노드 A로 패킷을 보내게 되고 노드 A는 예상치 못한 패킷을 받게 된다. 이러한 binding

update를 통한 공격을 방지하기 위해서는 CN측에서 이동 노드부터 온 binding update 메시지를 인증하여 이것이 진정으로 노드 A로부터 온 요청인지를 확인할 수 있어야 한다.

이외에도 공격자가 이동노드의 binding update(BU) 메시지를 가로채어 자신의 CoA를 삽입한 후 이를 노드 A의 HA나 CN으로 보낼 경우, HA는 공격자의 CoA를 노드 A와 통신하고자 하는 CN들에게 알려주게 될 것이며, CN들도 공격자의 CoA를 노드 A의 CoA로 잘못 알게 되고 노드 A는 원하는 CN들과 통신할 수 없게 될 것이다. 따라서 Mobile IP 프로토콜이 안전하게 수행되어 이동 노드에게 이동성을 제공하기 위해서는 위와 같은 주요 보안 이슈에 대한 해결방안이 필요하며 그러한 해결방안들은 기존의 Mobile IP 프로토콜 스텝에 영향을 주지 않고 성능에 영향을 주지 않는 범위 내에서 적용되어야 한다. 다음 절에서는 IETF에서 제안되고 있는 Mobile IP 인증 프로토콜과 관련 연구들에 대하여 소개하도록 한다.

2. IETF Mobile IP 인증 프로토콜

IETF RFC3775에서는 기본적으로 이동 노드와 HA 사이의 인증을 위해 IPsec을 사용하도록 정하고 있다[1][5]. 또한 HA를 통해 전달되는 Return Routability 메시지와 Mobile Prefix Discovery 메시지가 IPsec을 통하여 보호되어야 한다[1].

[2]에서는 IETF RFC3775에서 IPsec을 적용하여 보안 문제를 해결함에 따라 이동 노드에서의 IPSec 처리의 어려움을 지적하고 있다. 또한 IPsec이 이동 노드의 Home address에 결합되어 동작하기 때문에 이동노드가 이동함에 따라 새로운 주소를 얻는 Mobile IP 환경에는 적합하지 않음을 지적하여, 이러한 문제를 해결하고자 하였다. 위와 같은 문제를 해결하기 위하여 [2]에서는 AAA 기반의 비밀정보 공유 결합을 사용하여 이동 노드와 상대 노드간의 인증을 해결하도록 제안하였다. 그러나 비밀정보 공유 결합을 이용한 이 방안은 비밀정보 공유가 가지는 근본적인 문제를 해결하지 못하고 있다. 이 방안에 따를 경우 이동 노드가 Home AAA(HAAA)와 비밀정보를 공유할 수 있지만, 이동성에 따라 여러 네트워크에 접속하는 다른 노드들과의 문제는 해결할 수 없게 된다. 또한 앞 절에서 지적한 문제를 해결하지 못하고 있다.

3. 관련 연구들

현재 Mobile IP 프로토콜은 제어 메시지의 인증을 위해 여전히 직접적인 키 공유를 통한 비밀정보 공유를 사용하고 있다. 이러한 접근은 알려진 바와 같이 키 관리에서 확장성의 문제를 가지며 많은 수의 노드를 가지는 경우에 적용하기 어려워 인터넷과 같은 글로벌 네트워크에는 적당하지 않다. [3]에서는 공개키 암호방식을 이용한 확장성 있는 인증 메커니즘을 제공하기 위한 방안을 제안하고 있다. 그러나 이 제안은 이동 노드가 인증서 기반의 복잡한 공개키 암호 연산을 수행하도록 하는 복잡한 요구사항들로 인한 문제점을 가지고 있다.

[4]에서 제안하는 Mobile IP 등록 프로토콜은 공개키 암호 알고리즘의 사용을 최소화 하여 위의 문제점들을 제거하고자 하였다. 그러나 이 논문에서도 역시 공개키 알고리즘 적용의 부담을 줄이고자 이동 노드와 HA간에 비밀키의 사용을 전제로 하고 있으므로 비밀키 사용에 따른 키 관리와 확장성의 문제를 해결하지 못하고 있다. 또한 이동 노드가 방문망에서 CoA를 얻고 HA로의 등록에 foreign agent가 관련하지 않는 Mobile IPv6 프로토콜에는 HA가 foreign agent를 직접 인증하는 이 방안은 적절하지 않다.

[5]에서는 무선 인터넷 응용에서의 보안과 인증을 목표로 하여 공개키 알고리즘과 전자 서명을 적용하였다. 여기에서는 복잡한 공개키 연산을 이동 노드에 비하여 성능이 좋은 HA에서 수행하도록 하여 HA에서 상대 HA에 대한 인증을 수행하도록 하고 이동 노드는 자신의 홈망의 HA를 신뢰하도록 하여 HA가 인증한 상대 HA의 CN을 인증하는 scheme을 적용하고 있다. 여기에서는 이동 노드와 CN간의 인증에만 필요한 프로토콜만을 제시하고 있으며 이동 노드가 HA에 자신의 위치를 등록하는 등록 프로토콜에서 발생하는 보안 이슈들을 다루고 있지 않다. 여기서도 또한 HA와 이동 노드간에는 비밀 키 방식을 적용하여 다른 연구들과 마찬가지의 문제점을 안고 있다.

Ⅲ. Mobile IP 인증 프로토콜의 요구사항

이 장에서는 Mobile IP에서 필요한 보안 요구사항들을 정의하고 뒤에서 이러한 요구사항을 기반으로 본 논문에서 제안하는 프로토콜이 이러한 요구사항을 만족하는 지를 검증하도록 할 것이다.

1. 인증 프로토콜의 요구사항

Mobile IP 인증 프로토콜은 다음과 같은 요구사항을 만족하여야 한다.

(가) 인증

우선 이동 노드가 홈망을 떠나 방문망으로 이동하는 경우, 이동 노드는 방문망으로부터 CoA를 획득하여야 한다. 이 때 이동 노드는 방문망을 인증한 후 방문망이 보내는 Advertisement로부터 CoA를 획득할 수 있어야 한다. 또한 방문망에서는 미리 등록되지 않는 이동 노드가 외부로부터 이동해 와서 자신의 영역의 IP 주소를 획득하여 그 망의 자원들을 사용하고자 할 경우, 그 이동 노드에 대한 인증절차를 우선적으로 실행하여야 한다. 이동 노드가 방문망을 인증하지 않은 경우, 이동 노드는 방문망으로부터 잘못된 CoA를 획득하여 HA에 등록하게 되고, 이동 노드는 이로 인하여 원하는 패킷을 받지 못할 수 있으며 실제 그 주소의 사용자는 원하지 않는 패킷을 받게 될 수 있다. 또한 방문망에서 이동 노드를 인증하지 않을 경우 악의적인 노드가 해당 망에 들어와서 망 내의 자원을 악의적으로 사용할 수 있게 된다.

다음으로 이동 노드가 HA에 자신의 위치를 알리고자 등록에 해당하는 binding update를 보낼 경우도 HA는 등록을 요청한 이동 노드가 정말로 자신의 홈망에 등록된 노드인지를 인증할 필요가 있다. 악의적인 노드가 이동 노드의 identity를 사용하여 제3노드의 CoA를 등록할 경우, 제3노드는 HA를 통하여 원하지 않는 패킷을 받을 수 있으며 앞에서 언급한 DoS 공격이 발생할 수 있다. 따라서 HA는 binding update를 보내는 이동 노드를 인증할 필요가 있다. 이동 노드의 경우 HA가 자신이 보낸 등록 요청을 받았는지를 확인할 필요가 있다.

이동 노드와 CN이 통신할 경우에, 이동 노드가 CN에 binding update를 보내면, CN은 이 메시지가 진정으로 이동 노드로부터 온 것인지를 검증할 수 있어야 한다. 만약 악의적인 노드가 CN에게 이동 노드의 identity를 이용하여 잘못된 CoA를 삽입한 binding update를 보낸다면, 이동 노드는 CN과 더 이상 통신할 수 없게 되며 삽입된 CoA의 소유자 역시 원하지 않는 패킷을 받게 될 것이다.

위에서 언급한 바와 같이 Mobile IP 프로토콜에서는 이동 노드와 방문망, 이동 노드와 HA, 이동 노드와 CN 간에 인증 과정이 필수적이다.

(나) 무결성

인증과정에서와 마찬가지로 이동 노드, 방문망, HA, CN은 각각 상대방으로부터 온 메시지가 위·변조 되지 않고 제대로 도착한 것임을 검증할 수 있어야 한다. 악의적인 공격자에 의하여 binding update 메시지가 위조된 경우 이동 노드는 원하는 CN과 제대로 통신할 수 없으며 임의의 노드는 원하지 않는 패킷을 받게 된다.

(다) 부인방지

이동 노드, 방문망, HA, CN은 메시지 전송에 대한 부인방지를 확인할 수 있어야 한다. 예를 들어, 과금 등이 적용되는 경우, 이동 노드가 HA에게 등록 요청을 보낸 후 HA가 CN으로부터 오는 메시지를 등록된 이동 노드의 CoA로 전송하였으나, 이동 노드가 자신의 등록을 부인하고 이로 인한 책임을 HA에 추궁하게 된다면 HA는 등록요청에 대한 부인방지 확인 기능이 필수적이다. 또한 이동 노드가 CN에게 더 이상 패킷을 받고 싶지 않아 잘못된 주소로 binding update를 보낸 후, CN으로부터 패킷을 받지 못했다고 주장할 경우, CN은 이동 노드로부터 그 주소에 대한 binding update를 받았음을 증명할 필요가 있다.

(라) Replay attack 방지

이동 노드가 방문망으로부터 CoA를 획득한 후에, 공격자가 이 메시지를 이용하여 방문망에서 또 다른 CoA를 획득할 경우, 방문망에서는 합법적인 노드에게 CoA를 준 것으로 생각하지만, 실제로는 공격자가 이동 노드의 이름으로 CoA를 획득하여 그 망의 자원을 사용하게 된다. 따라서 이러한 replay attack을 방지할 수 있어야 한다.

또한 이동 노드가 방문망 A에서 방문망 B로 이동한 후에, 공격자가 이동 노드가 방문망 A에서 HA나 CN에 보냈던 binding update를 저장해 두었다가 이를 이용하여 다시 HA나 CN에 binding update를 보내게 되면 HA나 CN은 이것이 합법적인 binding update로 생각하여 이동 노드의 위치를 잘못 알게 된다. 따라서 이동 노드는 자신에게 오는 패킷을 수신하지 못하게 되고, 다른 노드들은 이동 노드와 통신할 수 없게 되는 문제가

발생한다. 따라서 binding update에 대한 replay attack을 방지할 수 있어야 한다.

2. Assumptions 와 Notations

본 논문에서는 제안하는 모델을 위하여 다음 사항을 가정한다.

- 제안하는 모델에서 이동 인터넷은 HA_1에 등록된 이동노드(MN), 방문망(FN), HA_2에 등록된 노드(CN)으로 구성된다.
- 간단한 설명을 위해 CN은 이동하지 않고 자신의 홈망(즉, HA_2)에만 위치한다.
- MN, HA_1, FN, CN, HA_2는 미리 offline으로 CA에 공개키를 등록하고 인증서를 발급받는다.
- 모든 객체들은 CA의 공개키를 미리 알고 있다. 인증서는 객체의 identity와 공개키를 연결하는 것을 목적으로 하며 CRL(Ceritificate Revocation List) 검증을 하지 않는 short-lived certificate을 사용한다[6]. 목적에 맞는 인증서 프로파일을 정의하는 것은 이 논문의 영역 밖이다. 또한 각 노드가 각각 다른 CA들로부터 인증서를 발급받을 경우 CA들간의 상호인증에 대한 논의는 PKI(Public Key Infrastructure) 영역에서 이루어지고 있으므로 역시 이 논문의 영역 밖으로 하고 여기서는 단일 CA로부터 인증서를 발급받는 모델에 대해서만 고려한다.
- 제안하는 프로토콜의 모든 메시지는 본래의 Mobile IP 프로토콜 메시지에 삽입되어 전달된다.

Short-lived 인증서의 경우, CRL을 발급하지 않으므로, CRL을 검증하지 않고 인증서의 서명과 유효기간만을 검증한다. 따라서 인증서 검증의 복잡성을 피할 수 있으므로 복잡한 인증서 검증 과정이 부담스러운 단말기 등에 주로 사용될 수 있다[6][7]. 또한 인증서에는 각각 객체의 identity를 확인할 수 있는 정보가 포함되어 있다. 본 논문에서는 제안하는 프로토콜을 설명하기 위하여 다음의 표기를 사용한다.

- $Cert_x$: CA가 발급한 객체 x의 인증서, 객체 x의 identity 정보, 공개키 정보를 가지고 있음. x = MN, HA_1, HA_2, CN, FN
- PK_x: 객체 x의 공개키, $Cert_x$ 에 의해 인증되어 있음
- SK_x: 객체 x의 개인키
- $session_{x-y}$: x-y 사이의 세션키로서, 여기서 x, y = MN, HA_1, HA_2, CN, FN
- $sign_x[\ ]$: [ ]를 x가 개인키로 서명함
- $E[\ ]_{SKx-y}$: $session_{x-y}$로 [ ]를 암호화 함
- $E[\ ]_{PKx}$: PK_x로 [ ]를 암호화 함
- ID_x: 객체 x의 identity
- IP_x: 객체 x의 Home IP address, 여기서 x = MN, CN
- hash[ ] : [ ]에 대해 해쉬 함수를 수행함
- | : concatenation
- CoA_{MN}: MN의 CoA
- nonce: 일회성 정보
- $Auth_{req}(\ )$: 인증 요청 메시지
- $Auth_{res}(\ )$: 인증 응답 메시지

Ⅳ. 확장성과 실용성 있는 Mobile IP 인증 프로토콜

1. 이동 노드에 의한 CoA 획득 과정

이동노드가 방문망으로 이동할 때, 이동노드는 다음과 같이 방문망을 인증하고 방문망의 Advertisement를 통하여 CoA를 획득하여야 한다.

$$FN \rightarrow MN : sign_{FN}[CoA|nonce] \mid Cert_{FN} \quad (1)$$

- MN은 $Cert_{FN}$을 이용하여 메시지 (1)을 보낸 주체가 FN임을 확인할 수 있다. 또한 이 메시지는 FN에 의한 서명을 가지므로, MN은 이 메시지가 FN이 보낸 것임을 인증할 수 있다. nonce를 이용하여 MN은 악의적인 노드에 의한 replay attack을 방지할 수 있다. Mobile IP 프로토콜에 따르면 모든 객체들은 규칙적으로 nonce를 생성하므로 이 값을 그대로 사용할 수 있다. 물론 nonce를 사용하지 않더라고 FN은 자신의 DB에 이미 노드들에게 할당된 CoA에 대한 정보를 가지고 있고, 같은 CoA에 대한 중복된 요청을 감지하고 replay attack에 의한 CoA 요청을 거절할 수 있다. 그러나, MN은 이를 알지 못하므로 어떤 노드가 네트워크에 접속하고자 할 경우, Advertisement가 nonce를 갖지 않는다면, replay attack에 의해 잘못된 주소를 획득할 수 있다.

$MN \rightarrow FN$: $sign_{MN}[ID_{MN}|CoA|hash[nonce]] \mid Cert_{MN}$ (2)

- 이 메시지는 ID_{MN}을 포함하며 MN의 비밀키로 서명되어 있으므로 메시지가 위·변조 되더라도 FN은 이를 알 수 있다. 이 메시지는 다음의 기능을 갖는다.
  ① MN의 identification에 대한 인증 : FN은 $Cert_{MN}$과 서명을 통해 MN을 인증할 수 있다.
  ② 메시지의 무결성 : 공격자는 서명을 위조할 수 없으므로 메시지에 대한 MN의 서명을 이용하여 FN은 메시지의 위·변조 여부를 확인할 수 있다.
  ③ 부인방지 : MN의 서명으로 인하여 MN은 자신이 이 메시지를 보냈음을 부인할 수 없다.
  ④ Replay attack의 방지 : hash[nonce]를 이용하여 FN은 이 메시지가 (2)의 메시지와 관련이 있음을 알 수 있다.

2. 이동 노드의 등록 프로토콜

FN으로부터 CoA를 획득한 MN은 HA_1에 다음의 등록 요청 메시지를 보낸다.

$MN \rightarrow HA_1$: $BU|sign_{MN}[IP_{MN}|CoA_{MN}|nonce] \mid Cert_{MN}$ (3)

- HA_1는 $sign_{MN}[]$과 $Cert_{MN}[]$을 이용하여 BU를 MN이 요청하였는지를 확인한다. 또한 IP_{MN}을 이용하여 MN의 Home address를 확인할 수 있다. MN의 Home address가 $Cert_{MN}$에 포함할 경우, IP_{MN}은 사용하지 않아도 된다.
- Replay attack은 nonce에 의해 방지된다.
- MN이 서명된 메시지를 보냄으로서 부인방지를 해결한다.
- 메시지 (3)은 MN에 의해 서명되었으므로 공격자는 CoA_{MN}을 변조할 수 없으며 HA_1은 서명된 CoA를 이용하여 MN의 현재 주소를 확인할 수 있다.

MN에 대하여 인증한 후에 HA_1는 세션키를 생성하고 다음과 같이 Binding Acknowledgement (BA)를 MN에 보낸다.

$HA_1 \rightarrow MN$: $BA \mid E[sign_{HA_1}[nonce]]_{session_{HA_1\text{-}MN}} \mid [E[session_{HA_1\text{-}MN}] PK_{MN} \mid Cert_{HA_1}$ (4)

- HA_1은 (3)에서 $Cert_{MN}$로부터 PK_{MN}을 얻는다.
- MN은 $Cert_{HA_1}$과 $sign_{HA_1}[nonce]$를 통해 이 메시지가 HA_1에 의해 보내진 것임을 확인할 수 있으며 nonce에 의해 이 메시지가 (3)에 대한 응답임을 알 수 있다.
- HA_1가 MN의 공개키인 PK_{MN}를 이용하여 세션키를 암호화하므로 MN만이 공개키에 대응하는 비밀키를 이용하여 세션키를 복호화할 수 있다.

이제부터 MN은 HA_1으로 보내는 BU는 세션키를 이용하여 암호화할 수 있게 되므로 공개키 연산으로 인한 복잡한 연산을 피할 수 있게 된다. 각 객체에서 공개키 연산과 인증서 검증은 한번만 수행됨을 알 수 있다.

3. 이동 노드들 간의 인증 프로토콜

다음은 HA_1에 위치한 MN과 HA_2에 위치한 CN이 서로 통신할 때의 인증 메커니즘에 대하여 설명한다.

$MN \rightarrow HA_2$: $Auth_{req}(sign_{MN}[IP_{MN}|IP_{CN}|nonce]) \mid Cert_{MN}$ (5)

- 이 메시지에서는, HA_2가 CN의 홈 IP 주소로 보내는 MN의 패킷을 가로채고, MN의 서명을 검증하여 MN을 인증한 후에 이를 CN으로 전달한다. 그러나 HA_2에서의 MN에 대한 인증은 선택적이며 HA_2는 아무런 조치없이 이 메시지를 그대로 CN에게 전송할 수 있다. 여기서 MN이 방문망이 있다면 메시지 (5)에 IP_{MN}대신에 CoA_{MN}를 넣는다.

$HA_2 \rightarrow CN$: 메시지 (5)를 그대로 전송

- CN은 이전의 단계에서처럼 MN을 인증한 후에, 메시지의 무결성을 확인하고, 정보를 분석한다.
- CN과 HA_2사이의 메시지들은 IV장의 2절에서와 동일한 방법으로 공유한 $session_{CN\text{-}HA_2}$를 이용하여 암호화된다.

$CN \rightarrow MN : Auth_{res}(sign_{CN}[IP_{CN}|IP_{MN}|hash(nonce)|E[session_{CN-MN}]_{PK_{MN}}])|Cert_{CN}$ (6)

- CN은 MN과의 통신을 위해 세션키 $session_{CN-MN}$을 생성하여 이를 MN의 공개키를 이용하여 암호화한 후에 전달한다.
- MN은 hash(nonce)를 통해 이 메시지의 연속성을 확인한다.
- MN은 $sign_{CN}[]$과 $Cert_{CN}$을 이용하여 CN을 인증하고, 메시지 (6)이 CN으로부터 온 것임을 확인한다.
- MN은 메시지 (6)에서 세션키 $session_{CN-MN}$을 복호화하여 이후에 CN과의 통신에 사용한다.

다음은 MN이 방문망에 위치하는 동안, 어떻게 CN과 MN이 서로 인증하는 지에 대하여 설명한다.

$CN \rightarrow HA_1 : Auth_{req}(sign_{CN}[IP_{CN}|IP_{MN}|nonce])|Cert_{CN}$ (7)

- 이 메시지의 구조와 검증과정은 메시지 (5)와 동일하다.

$HA_1 \rightarrow MN : Auth_{req}(E[IP_{CN}|CoA_{MN}|nonce]_{session_{HA1-MN}} | message(7))$ (8)

- MN은 이미 HA_1과 세션키를 공유하고 있으므로 $session_{HA_1-MN}$을 이용하여 이 메시지를 복호화하고 그 진위를 확인할 수 있다. 그 후에 메시지 (7)에 포함된 서명을 통하여 CN을 인증한다.

$MN \rightarrow CN : Auth_{res}(sign_{MN}[CoA | IP_{CN} | hash(nonce) | E[session_{MN-CN}]_{PK_{CN}}])|Cert_{MN}$ (9)

- MN은 CN과의 세션키 $session_{MN-CN}$을 생성하여 CN의 공개키를 이용하여 암호화한후 메시지 (9)에 포함하여 CN에게 전달한다.

위의 두 프로토콜이 완료된 후에는 공통적으로 MN의 BU는 세션키 $session_{MN-CN}$을 이용하여 수행되고, 공개키 알고리즘과 인증서 검증은 더 이상 수행되지 않는다.

V. 제안하는 프로토콜의 안전성 검증

이 장에서는 제안하는 프로토콜이 어떻게 III장에서 언급하였던 Mobile IP 프로토콜의 요구사항을 만족하는지에 대하여 설명할 것이다.

1. CoA 획득

메시지 (1)의 Advertisement에 포함된 서명과 인증서를 통하여 MN이 FN으로부터 CoA를 획득하기 전에, MN은 먼저 메시지들이 정말로 FN으로부터 오는 것인지를 확인하고 메시지의 무결성을 확인할 수 있다. 또한 FN은 메시지 (2)의 MN으로부터 오는 Advertisement Acknowledgement (ACK)에 포함된 MN의 인증서를 사용하여 MN의 identity를 확인할 수 있다. 서명 검증을 통하여 FN은 ACK가 정말로 MN으로부터 오는지에 대한 진위와 ACK 메시지의 무결성을 검증할 수 있다. 만일 공격자가 이 ACK를 가로채고 MN이 다른 방문망으로 이동한다며, 공격자는 MN의 현재 위치에 대한 혼란을 주기 위하여 혹은 FN으로부터 CoA를 얻기 위하여 가로챈 ACK를 이용하여 replay attack를 할 수가 있다. 그러나 이 ACK는 Advertisement에서와 동일한 nonce를 포함하고 있기 때문에, FN은 replay attack을 감지하고 공격자의 CoA 요청을 거절할 수 있다. CoA 사용에 대한 과금이 중요한 경우에, ACK에 포함된 MN의 서명은 MN의 CoA 사용에 대하여 부인하지 못하도록 하는 데 이용될 수 있다.

2. 이동 노드의 등록 프로토콜

메시지 (3)에서 HA_1은 인증서를 이용하여 MN의 identity를 인증한 후에, MN의 서명을 사용하여 BU 메시지가 MN으로부터 온 것인지를 검증할 수 있다. 만약에 공격자가 MN의 identity를 사용하여 MN의 주소가 아닌 다른 노드의 주소를 가진 BU를 보낸다면, HA_1은 첨부된 인증서와 서명을 통하여 MN의 identity의 진위를 검사할 수 있다. 그리고 공격자가 BU 메시지에 대한 replay attack를 수행하여 앞에서 언급한 것과 같이 MN의 현재 위치에 대한 혼란을 야기하고자 하더라도 HA_1은 nonce를 이용하여 replay attack을 감지할 수 있다. BU 메시지는 MN의 서명을 포함하므로 MN은 이 메시지의 전송을 부인할 수가 없다. MN은 또한 BA가

메시지 (3)에 대한 응답임을 BA에 포함된 sign[nonce]를 통하여 검증할 수 있고 SK_{MN}를 이용하여 PK_{MN}으로 암호화된 세션키를 복호화할 수 있다. MN만이 공개키에 대응하는 비밀키를 가지므로 이 세션키를 복호화할 수 있게 된다. MN은 진짜 HA_1이 BU 요청을 받았음을 메시지 (4)에 포함된 서명과 인증서를 이용하여 확인할 수 있다. 그 후에 MN은 $session_{HA_1\text{-}MN}$을 이용하여 HA_1으로 BU를 보낼 수 있다.

3. MN과 CN 사이의 인증 프로토콜

메시지 (7)에서와 같이, CN이 방문망에 있는 MN에 패킷을 전송할 때, HA_1은 이 패킷을 가로챈 후에 MN의 CoA로 이를 전송한다. MN은 이 패킷을 받은 후에, CN과 메시지를 인증하여야 한다. 먼저, MN은 HA_1과의 세션키로 암호화된 메시지를 복호화하여 메시지 (8)에서와 같이, 이 메시지가 HA_1으로부터 온 것임을 확인한다. 그리고 MN은 CN이 보낸 인증서와 서명 검증을 통하여 CN을 인증한다. 공격자가 CN인척 가장하고 패킷을 보내더라도 공격자는 인증서에 포함된 공개키를 이용하여 검증될 서명을 위조할 수 없다.

MN이 CN에 BU 메시지를 보낼 때, CN은 서명을 통하여 이 메시지를 실제로 MN이 보냈음을 검증할 수 있다. 악의적인 노드가 엉뚱한 노드의 CoA를 삽입한 BU를 CN에 보내더라도, CN은 서명을 통하여 이를 알아차릴 수가 있게 된다. 더구나 이 프로토콜에서는 최초의 인증후에 MN과 CN이 세션키를 공유하기 때문에, BU 메시지는 이 세션키로 암호화될 수 있으며 공격자는 CoA와 같은 정보를 위조할 수 없게 된다.

MN은 nonce를 해쉬하고 세션키를 생성하여 BU를 CN에 보내므로, CN은 nonce에 의해 reaply attack을 감지할 수 있으며, 인증서와 서명을 통하여 MN과 메시지를 인증할 수 있다.

VI. 성능 분석

이 장에서는 제안하는 프로토콜의 실제 응용적인 측면을 고려하도록 한다. 제안하는 인증 프로토콜은 Mobile IPv6 고유의 등록 프로토콜의 스텝을 수정하지 않고 적용될 수 있다. 공개키 암호와 서명검증 등의 연산은 최초의 인증 때에만 계산되기 때문에 여기서는 복잡한 공개키 연산의 계산 횟수를 줄이고 최초의 인증 후에는 대칭키 알고리즘이 사용되도록 하였다. 또한 사용되는 인증서도 short-lived 인증서를 적용하여 CRL 검증등의 복잡한 인증서 검증과정을 피할 수 있도록 하고 공개키와 객체를 연결해 주는 인증서 본래의 목적을 제공할 수 있도록 하였다. 또한 최근에는 CPU의 성능 향상등으로 인하여 이동 노드에서의 공개키 연산이 어렵지 않음을 많은 연구결과가 보여주고 있다[7][11][12].

VII. 결 론

Mobile IP 프로토콜에서는 이동 노드들이 방문망으로 이동할 때에도 다른 노드들과 통신하거나 방문망의 자원들을 사용할 때에 자신의 고정 주소를 그대로 사용할 수 있도록 한다. 그러므로 이동 노드와 대응 노드, 홈망, 방문망 간에 인증은 중요한 문제이다.

이 논문에서는 공개키 알고리즘에 기반하여 Mobile IP 프로토콜에서 이동 노드들과 네트워크 간의 새로운 인증 프로토콜을 제안하였다. 공개키 암호 방식은 키 공유의 복잡한 문제를 해결하는 등 효율적이지만, 복잡한 공개키 연산을 수행해야 하는 어려움이 있다. 또한 공개키와 공개키 소유자를 연결해주는 인증서를 사용하기 때문에 복잡한 인증서 검증 과정도 필요하다.

제안하는 프로토콜은 공개키 연산을 노드들 간의 최초의 인증 시도로만 제한하고 이후에는 노드들이 세션키를 공유하도록 하여 공개키 사용의 부담을 줄였다. 또한 이 프로토콜은 원래의 Mobile IP 프로토콜 메커니즘에 영향을 주지 않고 각 메시지 뒤에 추가되어 수행될 수 있다. 우리는 또한 Mobile IP 프로토콜에서 발생할 수 있는 보안 문제점들을 지적하고 그 문제점들에 기반하여 제안하는 프로토콜의 안전성을 검증하였다. 제안하는 프로토콜은 향후, Mobile IP 등록 프로토콜 뿐 아니라 단말기 성능에 많은 제약을 갖는 이동 통신망과 모바일 애드혹 네트워크에서의 인증 프로토콜에 확장될 수 있을 것이다.

참 고 문 헌

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," RFC3775, (2004).

[2] A. Patel, K. Leung, M. Khalil and H. Akhtar, "Authentication Protocol for Mobile IPv6," Internet Draft, draft-ietf-mip6-auth-protocol-00.txt, (2004).

[3] Sufatrio and K. Y. Lam, "Mobile IP registration protocol : a security attack and new secure minimal public-key based authentication," I-SPAN'99, Fremantle, Australia, 1999, pp. 364-369

[4] S. Jacobs, "Mobile IP Public Key Based Authentication," Internet Draft, draft-jacobs-mobileip-pki-auth-00.txt, (1998).

[5] S. Kent and R. Atkinson, "IP Encapsulating Security Payload(ESP): IETF 2406", IETF Network Working Group, 1998.

[6] OMA, "Wireless Transport Layer Security," WAP-261-WTLS, Apr. 2001.

[7] J. I. Lee, Yong Lee and J. S. Song, "Wireless PKI Technology in Korea," The First International Workshop for Asian PKI(IWAP), Vol. 1, Korea, Nov. 2001.

[8] M. Shi, X. Shen and J. W. Mark, "A Light Weight Authentication Scheme for Mobile Wireless Internet Applications," IEEE WCNC series 23, 2003, pp. 2126-2131

[9] S. Salsano, L. Veltri and D. Papalilo, "SIP Security Issues : The SIP Authentication Procedures and its Processing Load," IEEE Network, Nov/Dec, 2002, pp. 38-44

[10] G. O'Shea and M. Roe, "Child-proof Authentication for MIPv6(CAM)," ACM Conference, 2000.

[11] K.Y Lam, S. L Chung, M. Gu and J. G. Sun, "Lightweight security for mobile commerce transactions," Journal of Computer Communications, Vol. 26, 2003, pp. 2052-2060

[12] M. Aydos, T. Yang and C. K. Koc, "High-speed implementation of an ECC-based wireless authentication protocol on an ARM micriprocessor," IEE Proceeding of Communication, Vol. 148, No. 5, Oct. 2001, pp. 273-279

저 자 소 개

이 용(정회원)

1997년 연세대학교 컴퓨터과학과 (석사)

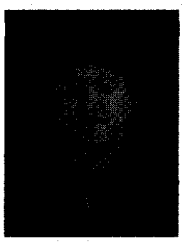
2001년 연세대학교 컴퓨터과학과 (박사)

1993년~1994년 디지콤정보통신 연구소

2001년~2003년 한국정보보호진흥원 전자서명 인증관리센터 선임연구원

2004년~현재 코넬대학교 방문연구원

<주관심분야 : 이동통신, Wireless PKI, Mobile Ad Hoc 네트워크, Mobile Ad hoc 네트워크 보안>



이 구 연(정회원)

1988년 KAIST 전기및전자공학과 (석사)

1993년 KAIST 전기및전자공학과 (박사)

1993년~1996년 디지콤정보통신 연구소

1996년 삼성전자

1997년~현재 강원대학교 전기및전자공학부 교수

<주관심분야 : 이동통신, 네트워크보안, 초고속통신망, ad-hoc 네트워크>