산업기술연구(강원대학교 산업기술연구소 논문집), 제27권 B호, 2007.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 27 B, 2007.

무선 모바일 멀티 홉 네트워크에서의 인증 기법 고찰 및 개선

Authentication Scheme in Wireless Mobile Multi-hop Networks

이 용* 이 구 연**
Lee, Yong Lee, Goo Yeon

Abstract

In mobile multi-hop wireless networks, the authentication between a base station and a mobile multi-hop node, between multi-hop nodes, and between user a station and a multi-hop node is needed for the reliable and secure network operation. In this paper, we survey various authentication schemes which can be considered to be adopted in mobile multi-hop wireless networks and propose a concept of novel mutual authentication scheme applicable to mobile multi-hop network architecture. The scheme should resolve the initial trust gain problem of a multi-hop node at its entry to the network, the problem of rogue mobile multi-hop node and the problem of hop-by-hop authentication between multi-hop nodes. Effectively, the scheme is a hybrid scheme of the distributed authentication method and the centralized authentication method which are considered to be deployed in the wireless ad-hoc network and the wireless network connected to wired authentication servers, respectively.

키워드 : *상호 인증, 멀티 홉, 모바일, 무선, 메쉬*
Keywords : *mutual authentication, multi-hop, mobile, wireless, mesh*

1. 서론

모바일 애드 혹 네트워크와 기존의 infrastructure 기반의 네트워크를 통합한 멀티 홉 무선 네트워크에서 모바일 멀티 홉 노드 간의 인증 기술에 관한 연구의 필요성이 대두되고 있다.

모바일 멀티 홉 무선 네트워크는 게이트웨이와 같은 포털을 이용하여 유선망으로 연결되며, 노드들 간에는 멀티 홉 구조로서 연결된다. 그림 1은 이와 같은 구조를 보여주고 있다[1]. 그림 1은 802.11s에서 제시되고 있는 모바일 멀티 홉 네트워크 구조이다. 그림 1에서 MP(mesh point)는 포털로서 유선망에 연결되는 통로가 되며, 이는 물리적인 접속측면에서 보면 기지국(base station : BS)과 동일하다. MAP(Mesh Access Point)는 라우팅 기능이 있는 모바일 노드로서 802.16j에서의 MMR (mobile multi-hop relay) 또는 릴레이와 동일하다. STA(station)은 라우팅 기능이 없는 단말(mobile station : MS)을 의미한다.

이러한 기술을 적용한 실제 활용 예로는 무선 메쉬 네트워크과 모바일 WiMAX, 무선 센서 네트워크등이 있다. 이러한 네트워크에서는 네트워크 구성을 용이하게 하고자 모바일 멀티 홉 노드들이 무선으로 설치되므로 설치가 용이 하며, self-organizing과 self-healing 의 특성을 가지므로 관리가 용이하다. 또한 저비용의 무선 백본을 제공하며, 유연한 영역확장과 용량확장 기능을 제공하는

* 충주대학교 전자통신공학과 교수, 공학박사
** 강원대학교 컴퓨터정보통신공학전공 교수, 공학박사

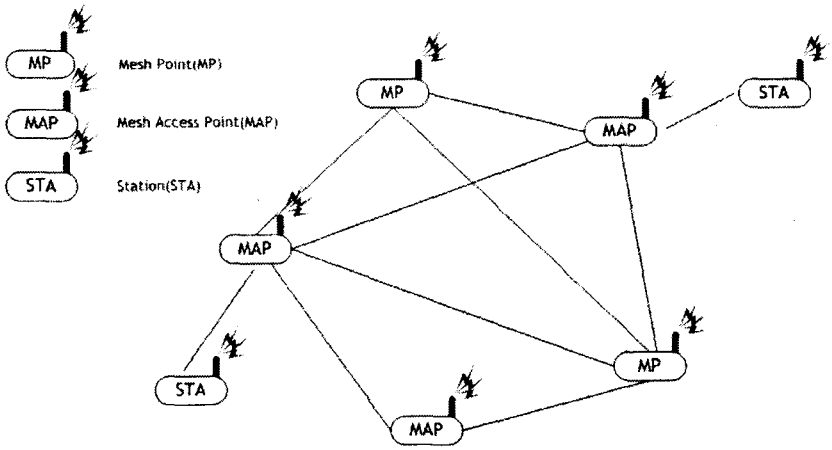

그림 1 모바일 멀티 홉 네트워크 구조 (출처 : IEEE 802.11s D0.01)

등의 장점이 있다[2]. 그러나 이런 모바일 멀티 홉 네트워크에서는 모바일 멀티 홉 노드들의 초기 네트워크 진입시에 BS와 멀티 홉 노드 간, 혹은 모바일 멀티 홉 노드와 모바일 멀티 홉 노드간에 신뢰를 확보하기 위한 상호 인증이 필요하다. 또한 멀티 홉 노드에 MS와 같은 사용자 단말기가 접속할 때에도 MS에게 모바일 멀티 홉 노드의 존재를 투명하게 하여 직접 BS에 접속할 때와 달라지는 점이 없도록 하는 것이 필요하다. 만약 모바일 멀티 홉 릴레이 기술을 적용하여 달라지는 점이 발생할 경우, MS에서 현재 적용중인 방식을 수정하여 재구성해야 하는 복잡한 문제가 발생하기 때문이다. 또한 모바일 멀티 홉 노드가 BS를 거치지 않고, 다른 모바일 멀티 홉 노드와 직접 라우팅을 수행하여 호를 연결하여 주는 로컬 라우팅 기능을 제공할 경우도 BS를 대신하여 MS에 대한 인증을 수행할 수 있어야 한다.

현재까지의 인증 기술은 대칭키와 공개키 등의 암호 알고리즘에 기반한 인증 프로토콜을 적용하여, 애드 혹 네트워크에 적용되는 분산 인증 방식과 기존의 인터넷에서 사용되는 인증 서버 기반의 중앙 집중 인증 방식 위주로 발전하고 있다. 하지만 모바일 멀티 홉 무선 네트워크는 모바일 포털이 기존의 인프라스트럭처에 접속할 수 있다는 점에서 중앙 집중 인증 방식을 적용할 수 있으며, 또한 모바일 멀티 홉 노드 들간에 상호 인증 을 수행하여 서로 신뢰하여야 한다는 점에서 모바일 애드 혹 네트워크의 특성을 따른다고 볼 수 있다. 현재 인증 기술은 ID/password 방법, shared secret 기반의 대칭키(symmetry key) 알고리즘과 공개키(public key) 기반의 알고리즘, challenge-response 기반의 알고리즘 등이 사용되고 있다.

모바일 멀티 홉 무선 네트워크의 경우 멀티 홉 노드들 간에 멀티 홉 네트워크 구성에 필요한 정보를 주고받으며 이러한 정보를 이용하여 멀티 홉 라우팅을 수행하도록 라우팅 정보를 모바일 멀티 홉 노드들이 공유한다. 또한 멀티 홉 노드들을 통하여 데이터 전달을 수행하므로 네트워크에 악의적인 멀티 홉 노드가 있을 경우 멀티 홉 라우팅 정보 형성이 제대로 이루어지지 않고 잘못된 라우팅 정보를 전달하여 멀티 홉 노드가 원하는 목적지 노드를 찾을 수 없게 된다. 또한 라우팅이 제대로 이루어지더라도 악의의 멀티 홉 노드가 데이터를 올바른 경로로 전달하지 않는 등의 여러 가지 보안상의 문제가 발생할 수 있다. 이러한 문제점은 모바일 애드 혹 네트워크이나 무선 메쉬 네트워크에서 동일하게 발생할 수 있다. 따라서 모바일 멀티 홉 무선 네트워크에서는 모바일 멀티 홉 노드가 처음 네트워크에 참가하는 초기 네트워크 진입시에 초기 인증 과정과 주변 이웃노드들과 지속적인 제어 정보 교환을 위하여 홉 간 인증을 수행하는 것이 필요하다. 본 논문에서는 2장에 관련연구를 제시하며, 3장에서 기존방법의 문제점 분석과 4장에서 그에 대한 개선방법으로 혼합형 인증방법에 대하여 서술한다. 5장에서는 제시된 혼합형 인증방법에 대한 효과를 분석하며 6장에서 결론을 맺는다.

2. 관련 연구

2.1 모바일 멀티 홉 무선 네트워크

대표적인 모바일 멀티-홉 무선 네트워크 기술로는 IEEE 802.11s에서 정의하는 WiFi 기반의 무선 메쉬 네트워크와 IEEE 802.16j에서 정의하는 WiMax기반의 모바일 멀티-홉 릴레이(MMR), 무선 센서 네트워크 등이 있다.

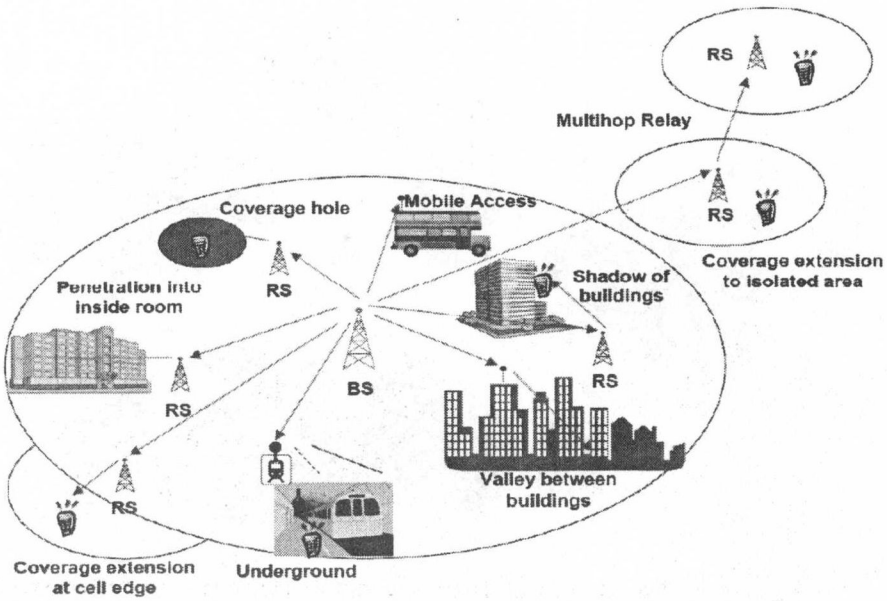

그림 2 IEEE 802.16j 개념도(출처 : IEEE 802,16j MMR TG)

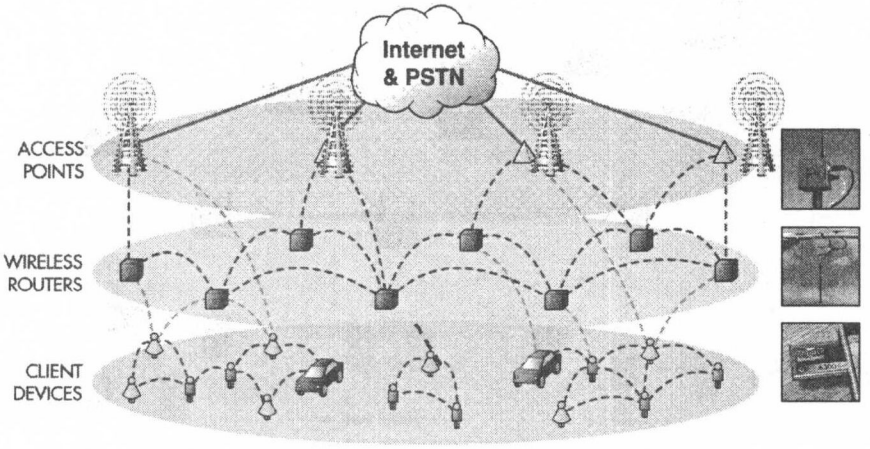

그림 3 무선 메쉬 네트워크 구조 (출처 : Mesh Networking Workshop '04)

IEEE 802.16j에서는 coverage 확장과 수율 향상을 목적으로 모바일 멀티-홉 릴레이 스테이션을 정의하여 그림 2와 같은 구조를 목표로 표준화가 진행 중이다[3]. 여기서는 모바일 스테이션이 중간에 위치한 릴레이 스테이션(relay station : RS)을 통하여 BS와 통신할 수 있도록 하는 모바일 멀티-홉 릴레이가 존재하며, 또한 BS가 이를 지원하도록 IEEE 802.16e에서의 기능을 보완한 MMR-BS (mobile multi-hop base station)를 정의하였으며, RS의 종류를 위치가 고정된 고정 릴레이 스테이션(fixed relay station : FRS)과 일정 시간동안만 한 위치에 고정된 노메딕 릴레이 스테이션(nomadic relay station : NRS), 이동성을 가진 모바일 릴레이 스테이션(mobile relay station : MRS)로 나누어 정의하고 있다. 이러한 새로운 정의에서 모바일 스테이션의 기능을 변경하지 않고 MMR에서의 향상된 인프라스트럭처에서도 동작할 수 있어야 한다. 반면에 BS는 약간의 수정으로 RS와 통신할

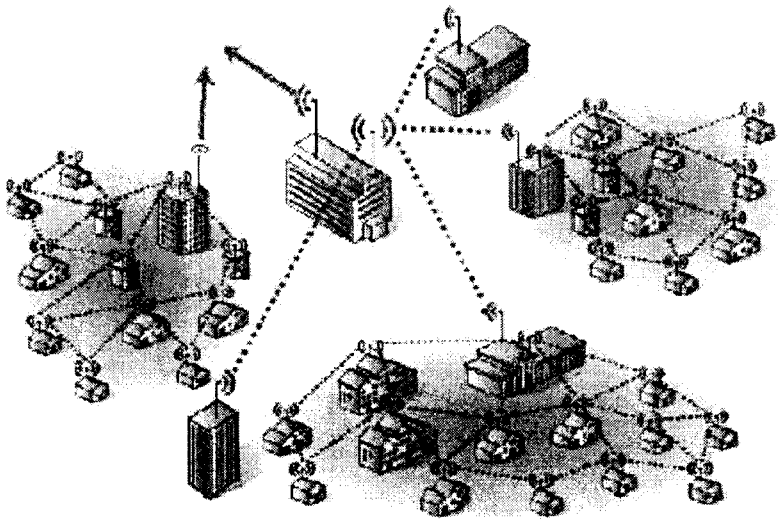

그림 4 WINNER에서의 멀티 홉 릴레이 네트워크의 개념도(출처 : WINNER Project)

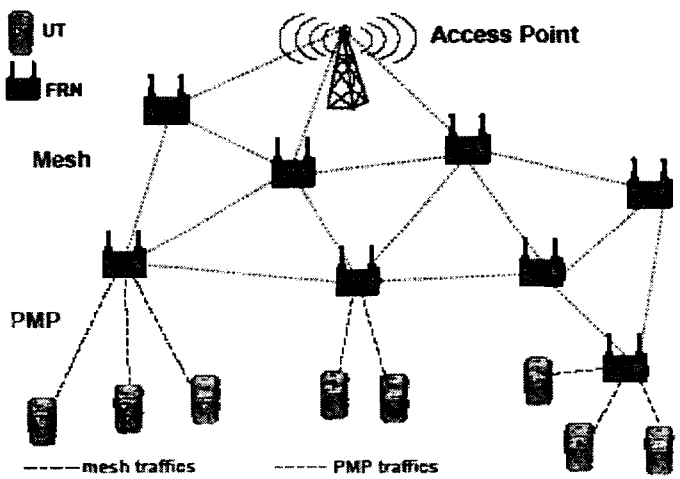

그림 5 WINNER에서의 예(출처 : WINNER Project)

수 있어야 하며 다른 RS와의 트래픽도 처리할 수 있어야 한다.

무선 메쉬 네트워크은 애드 혹 네트워크의 단점을 해결하고 성능을 개선하는 것을 목적으로 하며 릴레이 보다는 모바일 스테이션이 라우팅 기능을 수행하여 통신이 이루어지도록 하는 구조이다. 그림 3은 이러한 메쉬 네트워크 구조를 보여준다. 그림 3에서 노드들은 메쉬 라우터와 메쉬 클라이언트로 구성되며 라우팅은 BS뿐 아니라 MS를 통해서도 이루어지고 각 노드는 다른 노드를 거쳐서 직접적인 전송거리에 포함되지 않은 목적지 노드로도 패킷을 전송 할 수 있다.

IEEE 802.11s에 기반한 네트워크 토폴로지는 비관리형 메쉬 네트워크을 목적으로 하고 있다. 이러한 종류의 네트워크는 서비스 제공자에 의해 네트워크가 완전히 구성되는 것이 아니라 self-configuring 메카니즘으로 구성된다. 이 표준의 목적은 range와 coverage를 확장하고 신뢰성 있는 성능을 보장하고 이음새 없는 보안 기능(seamless security)를 제공하는 것이다. 대부분의

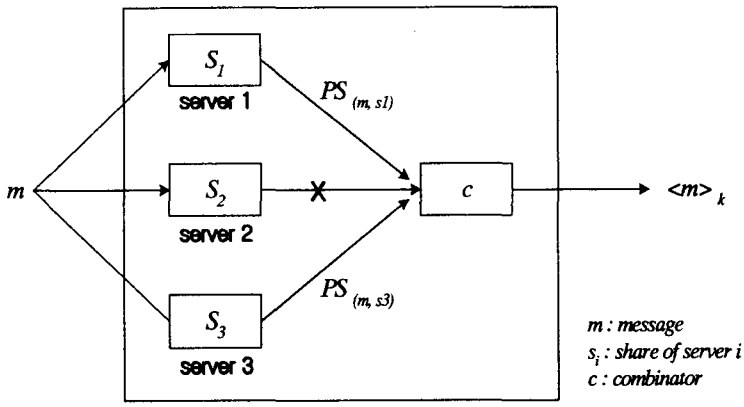

그림 6 Threshold cryptography 개념 (출처:Ref[7])

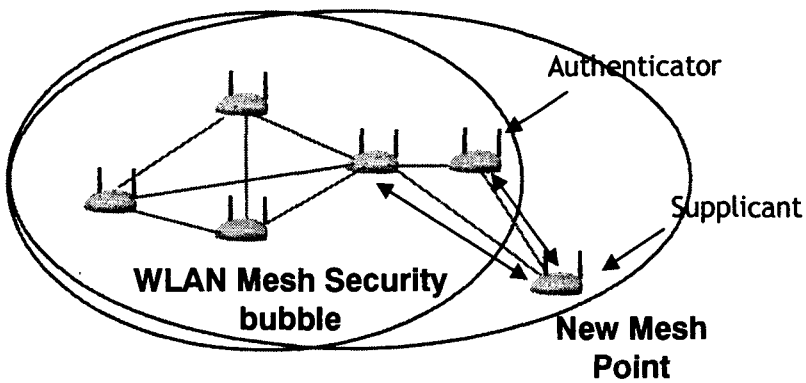

그림 7 무선 메쉬 네트워크에서 메쉬 노드들의 상호 인증 (출처 : IEEE 802.11s)

무선 LAN 네트워크에서 액세스 포인트(access point : AP)와 같은 인프라스트럭처 기기와 클라이언트 기기에게 서비스를 제공하고 있듯이 IEEE 802.11s에서도 MP와 MAP가 메쉬 스테이션에게 AP 서비스를 제공한다.

또한 유럽의 4G 연구기관인 WINNER (wireless world initiative new radio)에서도 모바일 멀티-홉 무선 네트워크을 그림 4 와 그림 5와 같이 정의하고 있다[6].

2.2 무선 보안 기술 동향

애드 혹 네트워크의 경우 기존의 infrastructure의 도움없이 노드들이 애드 혹으로 네트워크를 구성하므로 인증 서버(AS)로부터 인증 과정을 수행하는 기존의 중앙 집중 인증 기술을 사용할 수가 없다. 또한 단순히 네트워크 사용자를 인증 하는 문제가 아니라 네트워크 구성에 참가하는 노드들 간의 상호 신뢰를 위하여 서로를 인증해야 하는 문제가 발생한다. 애드 혹 네트워크에서 인증에 사용되는 기술은 threshold cryptography 방법을 이용하여 인증서 검증에 필요한 검증키를 노드들간에 공유하는 기술(그림 6 참조)이나[7], PGP(pretty good privacy) 방법을 응용하여 노드들이 이동할 때마다, 상대노드에 대한 인증 을 수행하여 그 리스트를 관리하고 공유하는 기술 등이 주로 연구되고 있다[8].

무선 LAN 기반의 무선 메쉬 네트워크에 대한 표준인 IEEE 802.11s 에서는 메쉬 노드들의 인증을 위하여 그림 7과 같이 메쉬 노드가 접촉하는 주변 메쉬 노드와 홉 간 인증을 수행하도록 정의하고 있다[1].

Fujitu에서 2005년에 등록한 특허(apparatus, method, and medium for self-organizing multi-hop wireless access networks)의 경우도 주 인증자(master authenticator)가 인증 서버의 기능을 제공하는 중앙 집중 인증 방식이다[9].

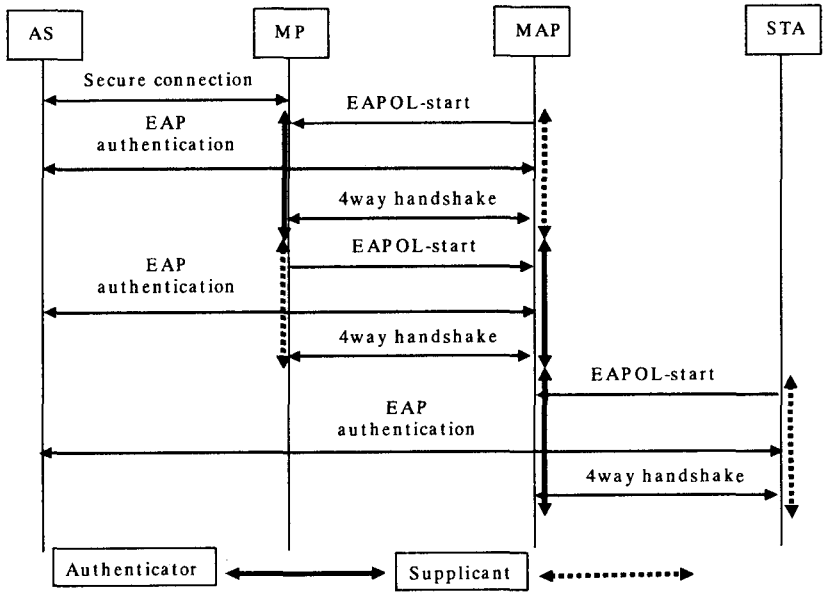

그림 8 EAP 를 이용한 중앙 집중 인증 방식 예 (출처 : IEEE 802.11s)

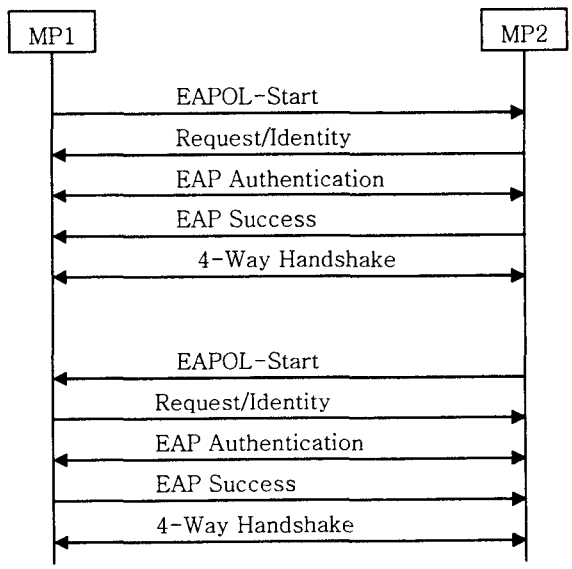

그림 9 EAP를 이용한 분산 인증 방식 예 (출처 : IEEE 802.11s)

IEEE 802.11s 무선 메쉬 네트워크에서는 메쉬 노드들 간에 상호 인증을 수행하기 위해 분산 인증 기술과 중앙 집중 인증 기술을 제안하고 있으며 자세한 내용은 각각 다음 그림 8 과 그림 9와 같다[1][10]. 중앙집중 인증의 경우 메쉬 노드들 간에 인증할 때, AS(인증 서버)로 상대노드에 대한 인증을 요청하면 AS는 인증 검증을 수행한 후에 결과는 알려준다. 이 경우 인증에 참가하는 두 개

의 메쉬 노드는 각각 한번씩, 인증자(authenticator)가 되어 상대 노드를 인증 하고 또한 자신이 인증 요청자(supplicant)가 되어 상대 노드로부터 인증을 받는다. AS는 이 두 번의 인증 검증과정을 거쳐 결과를 알려준다.

분산인증의 경우 메쉬 노드들 간에 직접 홉 간 인증을 수행한다. 이 방법을 적용하기 위해서는 메쉬 노드들간에 미리 인증에 필요한 정보를 공유하고 있어야 하나 악의적(rogue) MP의 문제가 발생할 수 있다.

3. 기존 방법의 문제점

앞에서 기술한 중앙 집중 인증기술의 경우, 멀티 홉 노드가 인증 서버에 항상 연결이 가능해야 하며, 또한 네트워크의 모든 노드들 간의 상호 인증을 수행하기 위하여서는 인증 서버의 로드가 많아지는 문제가 있다. 멀티 홉 노드의 경우도 인증을 위해 매번 인증 서버에 접속해야 하므로 인증에 시간이 많이 걸리는 문제가 발생한다. 이러한 방식은 이동성을 가지고 수시로 여러 노드들과 인증을 처리해야 하는 모바일 멀티 홉 노드에게는 적절하지 않은 방법이다. 또한 멀티 홉 노드간의 인증이 인증 서버에 위탁되는 trust transitive 의 문제가 발생한다. 모바일 멀티 홉 노드들의 이동에 따른 핸드오프 발생 시에도 인증을 수행하기 위하여 매번 인증 서버에 접속하는 인증 지연도 문제가 된다.

모바일 애드 혹 네트워크에서는 기존의 인프라스트럭처를 이용하지 않으므로 노드들 간에 인증 검증에 필요한 비밀정보를 나눠서 공유해야 하며 이를 위한 복잡한 알고리즘을 사용하게 되므로 모바일 멀티 홉 노드들의 처리 로드도 문제가 된다. 그리고 노드들이 최초에 비밀정보를 어떻게 공유할 수 있을지의 실질적인 문제를 가지게 된다. 또한 최초의 신뢰 정점이 없이 노드들 간에 분산 인증 방식을 적용할 경우, 악의적인 MP 문제가 발생하거나 네트워크 내부 노드들의 공모에 의한 내부 공격 등의 문제가 발생하며 노드들의 증가로 인한 확장성 문제도 가지게 된다.

4 혼합형 인증 방법

모바일 멀티 홉 네트워크 환경에서는 기존의 네트워크 환경에서 사용되는 중앙 집중 인증 방식과 애드 혹 네트워크에서 사용되는 분산 인증 방식이 모두 사용될 수 있다. 중앙 집중 인증 방식만을 적용할 경우 멀티 홉 노드 들 간의 상호 인증이 인증 서버로 위탁되고 인증 지연이 증가하는 문제가 있으며 분산 인증이 적용될 경우 노드 상호 간의 인증에 필요한 인증 검증 정보의 최초 공유 문제, 멀티 홉 노드들의 공모로 인한 내부 공격문제, 악의적 MP등의 문제를 가지게 된다. 그러므로 본 논문에서 제안하는 개선 방법은 중앙 집중 인증 방식과 분산 인증 방식을 혼합하여 모바일 멀티 홉 무선 네트워크에서 모바일 멀티 홉 노드와 멀티 홉 네트워크간의 최초의 상호 인증은 중앙 집중 인증 방식을 사용하고 이를 통하여 모바일 멀티 홉 노드들 간의 홉 간 인증에 필요한 공유키를 획득한 후에 이를 이용하여 노드들 간의 분산 인증을 수행하도록 하는 혼합형 인증 방법을 사용하여 모바일 멀티 홉 노드의 네트워크 진입시의 인증 문제를 해결한다.

이와 같은 방법에서는 모바일 멀티 홉 노드가 인증 서버와 중앙 집중 인증을 수행한 후에, 주변 노드들과 분산 인증을 수행할 때, 주변 노드들이 새로 합류하는 노드와의 인증을 확보하는 방법에 대한 연구가 필요하다. 이러한 방법은 모바일 멀티 홉 노드의 이동으로 핸드오프가 발생할 때에 빠른 인증을 수행하기 위해 필요하다.

또한 이러한 인증방법을 연장하여 모바일 멀티 홉 노드에 연결된 모바일 스테이션이 BS를 거치지 않고 다른 멀티 홉 노드에 연결된 모바일 스테이션으로 연결하는 로컬 라우팅을 지원하기 위하여 모바일 멀티-홉 노드가 직접 모바일 스테이션에 대한 인증을 수행하는 절차에 대한 연구도 필요하다. 그러면 모바일 스테이션에 적용된 기존의 방식을 수정하지 않고 제안하는 알고리즘을 이용하여 모바일 멀티 홉 네트워크가 효율적으로 모바일 스테이션에게 서비스를 제공할 수 있게 될 것이다.

5 혼합형 인증 방법 효과 분석

본 논문에서 제안하고 있는 혼합형 인증방법의 효과는 다음과 같다.

5.1 모바일 멀티 홉 노드의 최초 신뢰 획득

모바일 애드 혹 네트워크에서 적용하는 분산 인증방식은 무선 센서 네트워크나 무선 메쉬 네트워크같이 산재해 있는 노드들 간의 인증에 필요한 공유 정보 (예: 인증서 검증 키, shared secret)를 미리 공유하는 것이 현실적으로 어려운 문제를 가지는 데 반해 제안하는 인증 기술은 인증 서버를 통해 최초의 신뢰를 획득하므로 최초에 노드 인증에 필요한 정보를 획득할 수 있다.

5.2 악의적 MP 문제

모바일 애드 혹 네트워크나 무선 LAN과 같은 무선 네트워크 에서는 악의적(rogue) MP가 발생할 가능성이 아주 많다. 특히 분산 인증을 사용할

경우 노드들 간의 공모에 의한 악의적 MP 문제가 발생할 수 있다. 이러한 문제는 노드들에 대한 신뢰의 기반이 중앙 집중 서버에 의한 것이 아니라 노드들끼리 상대의 신뢰도(credential)을 검증하므로 발생한다. 악의적인 노드가 모바일 멀티 홉 네트워크에 참가하고자 할 경우, 인증 서버와 초기 인증이 완료되어야만 네트워크에 참여할 수가 있게 함으로서, 초기 인증에 필요한 검증 정보를 인증 서버가 소유할 수 있게 한다. 그러므로 노드들 간의 공모에 의하여 검증키를 위조하는 등의 불법적인 행위로 네트워크에 참가하는 것이 불가능하게 된다. 다른 예로 분산 인증에서는 모바일 멀티 홉 노드가 자신이 참가하려고 하는 멀티 홉 네트워크가 정상적인 네트워크인지를 검증하고자 할 경우, 노드들이 공모하여 검증 정보를 위조하여 인증과정을 수행할 수 있는 데, 이 때 네트워크에 새로 참가하는 노드는 이를 알 수 없게 된다. 그러나 혼합형 인증 방식을 적용할 경우 사업자의 관리하에 있는 인증 서버가 인증 정보를 관리하므로 노드들의 공모에 의한 거짓 정보의 전달을 발생하지 않게 된다.

5.3 모바일 멀티 홉 노드간의 홉 간 인증

이웃한 모바일 멀티 홉 노드들 간에 상호 인증을 할 경우, 중앙 집중 인증을 수행하게 되면, 인증 서버가 각각 노드들을 인증한 후에 각각 노드에게 상대 노드가 인증되었음을 알려주는 trust transitive의 문제가 발생하게 된다. 또한 한 노드의 주변에 n개의 이웃노드가 존재할 경우 이 노드는 인증 서버와 2n번의 인증 과정을 수행하여야만 모든 이웃노드들과 상호 인증을 완료할 수 있으며 이것은 모바일 멀티 홉 네트워크에 상당한 부담이 되며 특히 하드웨어 환경에 열악한 무선 센서 네트워크의 경우 사용하기에 무리가 있다. 그러나 혼합형 인증 기술을 적용할 경우 노드들 간에 공유키를 이용하여 직접 상대 노드를 인증할 수 있게 되므로 홉 간 인증은 로컬에서 이루어지게 된다. 따라서 최대 2번의 인증 서버와의 인증과 2n번의 분산 인증 으로 구성된다.

5.4 공유키 분배방식

기존에 인증 알고리즘의 문제점은 대칭키 방식의 인증을 사용할 경우, 노드들 간의 공유키 분배의 문제를 가지며, 또한 공개키 방식을 사용할 경우 공개키 검증에 필요한 인증서 발급의 문제점이 있다. 그러나 혼합형 인증 방식을 적용할 경우 초기 인증을 인증 서버를 통해 수행하므로 인증 서버가 KDC(key distribution center)와 같은 공유키 분배의 역할을 수행할 수 있으며 인증 알고리즘 적용을 간단하게 한다.

5.5 로컬 라우팅 문제

WiMAX의 경우 BS와 MS간에 인증 후에 TEK(traffic encryption key)를 공유하고, BS가 이 키를 이용하여 MS가 보내는 메시지에 대한 인증을 수행한다. 본 혼합형 인증 환경에서는 MS가 접속하는 RS(relay station)나 BS가 MS와의 상호 인증을 수행하고 TEK를 공유하게 된다. 만약 RS가 MS와 TEK를 공유하게 될 경우, RS가 MS에 대한 메시지 인증을 검증하고, 이 결과를 BS에 전달하게 된다. BS 와 RS는 이미 상호 인증을 통하여 서로를 인증하고 신뢰하므로 이 결과를 신뢰하게 된다.

5.6 모바일 멀티-홉 노드의 이동으로 핸드 오프 발생 시에 빠른 인증 수행

혼합형 인증 환경에서는 모바일 멀티 홉 노드들 간의 인증을 분산 인증을 이용하여 홉 간 인증이 수행되도록 하므로 AS를 이용하는 경우보다 신속하게 상호 인증이 이루어진다. 또 노드들 간에 인증정보도 핸드오프를 감지하기 전에 미리 이웃 노드들로부터 획득할 수 있으므로 핸드오프 발생 후에 노드들 간에 인증 키 획득에 필요한 지연을 줄일 수 있다. 이러한 방법은 MS가 이동함에 따라 발생하는 핸드오프에도 동일한 알고리즘을 그대로 적용하여 효과를 볼 수 있다.

6. 결론

모바일 멀티 홉 무선 네트워크에서의 신뢰성 있는 데이터 전송과 안전한 네트워크 운영을 위해서 BS와 모바일 멀티 홉 노드 간, 멀티 홉 노드들 사이, 그리고 사용자 스테이션과 멀티 홉 노드간의 상호인증 과정이 필요하다. 본 논문에서는 모바일 멀티 홉 무선 네트워크에서 현재 고려되고 있는 여러 인증 방법에 대하여 고찰하였다. 그리고 그러한 인증방법의 문제점을 분석하고, 이를 해결할 수 있는 혼합형 인증방법을 제안하였다. 혼합형 인증방법은 중앙 집중 인증방법과 분산형 인증방법의 혼합형 방법으로서, 기존 방법에서의 초기 신뢰 정보 획득 문제, 악의적 모바일 멀티 홉 노드 문제 및 노드간의 홉 간 인증 문제 등을 해결 할 수 있다.

참 고 문 헌

[1] IEEE 802.11 WG, IEEE 802.11s/D0.01, March 2006. http://www.802wirelessworld.com

[2] I. F. Akyildiz, X. Wang and W. Wang, "Wireless Mesh Networks : a survey," Computer Networks, Elsevier, 2005

[3] IEEE 802.16's Relay Task Group, http://www.802wirelessworld.com
[4] IEEE Standard 802.16-2004, "Air Interface for Fixed Broadband Wireless Access Systems," IEEE, October 2004
[5] IEEE P802.16e/D7, "Air Interface for Fixed and Mobile Broadband Wireless Access Systems: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE, April 2005
[6] "D 2.4 Multi-radio Access Architecture", WWI Ambient Network Project, 2005
[7] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Mag., 1999
[8] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Transactionson Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003. pp. 52 64
[9] Lusheng Ji, Brian Feldman and Jonathan Agre, "Self-Organizing Security Scheme for Multi-hop Wireless Access Networks," 2004 IEEE Aerospace Conference, pp. 1231-1240, 2004.
[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extension Authentication Protocol(EAP)," IETF RFC 3748, June 2004
[11] P. Papadimitratos and Zygmunt J. Haas, "Securing Mobile Ad Hoc Networks," The Handbook of Ad Hoc Wireless Networks, CRC Press 2003
[12] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in Mobile Ad Hoc Networks : Challenges and Solutions," IEEE Wireless Mag., Feb. 2004