논문 2007-44TC-10-15

IEEE 802.16j기반의 모바일 멀티 홉 릴레이에서의 혼합형 인증 기법에 대한 연구

(Hybrid Authentication Scheme for Mobile Multi-hop Relay in IEEE 802.16j)

이 용*, 이 구 연**

(Yong Lee and Goo Yeon Lee)

요 약

모바일 멀티 홉 릴레이는 self-organizing 등의 특성으로 인하여 설치가 용이하며 관리하기 편한 장점이 있지만, 반면에 무선으로 설치되어 자치적으로 운영되는 릴레이 스테이션을 신뢰하기 어려운 보안상 문제점이 있다. 특히 IEEE 802.16j 기반의 무선 멀티 홉 네트워크에서는 일반적인 모바일 멀티 홉 네트워크에서의 보안상 문제점뿐만 아니라, 기존의 IEEE 802.16에서의 특성을 유지해야 하는 요건으로 인하여 발생하는 추가적인 문제점도 존재한다. 본 논문에서는 IEEE 802.16j 기반에서의 모바일 멀티 홉 릴레이에서 가지는 보안상의 문제점들을 해결하기 위하여 혼합형 인증 방법을 제안한다. 제안된 혼합형 인증방법은 중앙 집중 인증방법과 분산형 인증방법에 대한 혼합형 방법으로서, 멀티 홉 구조를 갖는 릴레이 스테이션의 네트워크 진입 시의 초기 인증 문제, 릴레이 스테이션 간의 홉 간 인증 문제 등의 절차를 포함한다. 또한 혼합형 방식의 효과에 대하여 분석함으로서 모바일 멀티 홉 릴레이 네트워크에 제안된 방식이 효율적으로 적용될 수 있음을 보인다. 제안하는 혼합형 인증방식은 IEEE 802.16j 기반의 모바일 멀티 홉 릴레이 네트워크뿐만 아니라 모바일 멀티 홉 구조를 갖는 다른 네트워크에도 적용될 수 있으며, 무선으로 연결되어 자치적으로 운영되는 네트워크에서의 필수적인 보안 문제점인 인증문제를 해결하는데 기여할 것으로 기대된다.

Abstract

It is easy to install and maintain a mobile multi-hop wireless network due to its self-organizing characteristics. However, it has security weakness of the authentication of mobile multi-hop relay stations. Specially, the mobile multi-hop relay network in the IEEE 802.16j has the additional security weakness caused by the requirement of backward compatibility for mobile stations of the conventional IEEE 802.16 system. In this paper, we propose a novel mutual authentication scheme applicable to IEEE 802.16j-based mobile multi-hop relay network architecture. The scheme is able to 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 have been considered to be deployed in the wireless ad-hoc network and the wireless network connected to wired authentication servers, respectively. Also, we analyze the effectiveness of the proposed hybrid authentication method.

Keywords: IEEE 802.16j, 상호 인증, 멀티 홉 릴레이, 모바일 무선 네트워크, 혼합형 인증

I. 서 론

최근 네트워크 설치의 용이성, 확장성 등을 이유로 모바일 멀티 홉 무선 네트워크에 대한 관심이 증가하고 있다[1~5]. 광대역 휴대 인터넷 관련 기술인 WiMAX (WiBro)도 기존의 IEEE 802.16e에서의 노메딕한 이동

* 정회원, 충주대학교 전자통신공학전공
(Dept. of Electron. and Comm., ChungJu National University)
** 정회원-교신저자, 강원대학교 컴퓨터학부
(Dept. of Computer Eng. Kangwon National University)
※ 이 논문은 2007년도 충주대학교 교내학술연구비의 지원을 받아 수행한 연구임
접수일자: 2007년8월27일, 수정완료일: 2007년10월18일

성을 지원하는 내용을 넘어서 IEEE 802.16j에서의 모바일 멀티 홉 릴레이(mobile multi-hop relay : MMR)를 도입하여 영역 확대와 데이터 처리율 향상을 목표로 하고 있다[5]. 이러한 모바일 멀티 홉 네트워크에서는 네트워크 구성을 용이하게 하고자 모바일 멀티 홉 노드들이 무선으로 설치되므로 설치가 용이하고, self-organizing과 self-healing 의 특성을 가지므로 관리가 용이하다. 또한 저비용의 무선 백본을 제공하며, 유연한 영역확장과 용량확장 기능을 제공하는 등의 장점 등이 있다[1, 3~5]. 그러나 이런 모바일 멀티 홉 무선 네트워크에서는 self-organizing으로 네트워크가 구성되는 특성 상 모바일 멀티 홉 노드들의 초기 네트워크 진입시에 BS(base station)와 멀티 홉 노드 간, 혹은 모바일 멀티 홉 노드와 모바일 멀티 홉 노드간의 신뢰를 확보하기 위한 상호 인증이 필요하다[1, 6]. 본 논문에서는 IEEE 802.16j에서 지원하는 모바일 멀티 홉 릴레이 환경에서 발생하는 이러한 보안 기술들에 대해 연구한다.

IEEE 802.16j 기반의 모바일 멀티 홉 릴레이에서는 영역 확장과 수율 향상을 목적으로 모바일 멀티-홉 릴레이 스테이션을 정의하는 등의 표준화가 진행 중이다[5]. 여기서는 모바일 멀티-홉 릴레이 기능이 릴레이 스테이션(relay station : RS)에 구현되며, 모바일 스테이션(MS)은 중간에 위치한 RS를 통하여 BS와 통신할 수 있도록 하고 있다. BS가 이러한 기능을 지원하도록 하기 위하여, IEEE 802.16e의 BS의 기능을 보완한 MMR-BS (mobile multi-hop base station)를 정의하였으며, 또한 RS의 종류를 위치가 고정된 고정 릴레이 스테이션(fixed relay station : FRS), 일정 시간동안만 한 위치에 고정된 노메딕 릴레이 스테이션(nomadic relay station : NRS) 그리고 이동성을 가진 모바일 릴레이 스테이션(mobile relay station : MRS)로 나누어 정의하고 있다. 이러한 새로운 정의에서 MS는 기존 기능의 변경 없이, BS는 약간의 수정만으로 모바일 멀티 홉 릴레이 네트워크의 향상된 인프라스트럭처에서 동작할 수 있어야 한다[5].

IEEE 802.16j의 경우 앞에서 언급한 일반적인 모바일 멀티 홉 네트워크에서 가지는 보안상의 문제점을 그대로 가질 뿐만 아니라, 기존의 IEEE 802.16에서의 기능을 유지하여야 하는 특징으로 인하여 발생하는 고유의 문제점들이 추가로 존재한다. 앞에서 언급한 바와 같이 IEEE 802.16j에서는 MS가 기존의 방식과 기능을 그대로 사용하고 새로 추가되는 기능이 없는 것을 요구사항으로 가지므로, RS에 MS와 같은 사용자 단말기가 접속할 때에도 MS에게 RS의 존재를 투명하게 하여 직접 BS에 접속할 때와 달라지는 점이 없도록 하는 것이 필요하다. 만약 모바일 멀티 홉 릴레이 기술을 적용하여 달라지는 점이 발생할 경우, MS에 현재 적용중인 방식을 수정하여 재구성해야 하는 복잡한 문제가 발생하기 때문이다. 또한 기존에는 MS와 BS가 TEK(traffic encryption key)를 공유하여 MS가 전송하는 메시지 인증을 BS에서 수행하였는데, MS가 모바일 멀티 홉 릴레이를 통하여 접속할 경우 RS가 이를 대신할 수 있어야 한다[5]. 또한 기존의 라우팅이 BS를 통해 이루어지던 것과 달리 네트워크의 효율을 높이기 위해 RS가 BS를 거치지 않고, 다른 RS와 직접 라우팅을 수행하여 MS의 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 적용하고 있으며, 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 노드들 간에 상호 인증을 수행하여 서로 신뢰하여야 한다는 점에서 모바일 애드 혹 네트워크에서의 분산 인증 방식이 적절할 수 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. 그러나 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. 따라서 이러한 문제점들을 해결하기 위한 필수조건으로 모바일 멀티 홉 무선 네트워크에서는 모바일 멀티 홉 노드가 초기 네트워크 진입시의 초기 인증 과정과 주변 이웃노드들과의 지속적인 제어 정보 교환을 위한 홉 간 인증을 수행하는 것이 무엇보다 필요하다.

따라서 본 논문에서는 모바일 멀티 홉 릴레이 네트워크가 모바일 멀티 홉 무선 네트워크의 특성으로 인하여 가지는 보안상의 문제점과 IEEE 802.16j에서 MMR을 도입함에 따라 기존의 IEEE 802.16에서의 보안 기술을 유지하기 위해 발생하는 문제점들을 연구한다. 모바일 멀티 홉 네트워크에서의 보안은 네트워크에 참여하는 노드들 간의 인증을 기반으로 하므로 본 논문에서는 노드에 해당하는 모바일 멀티 홉 릴레이 스테이션 간의 인증 기술에 중점을 둔 혼합형 인증 기술을 제안하여 제안하는 방법이 앞에서 언급한 문제들을 어떻게 해결하는 지에 대해 분석한다.

본 논문의 구성은 Ⅱ장에서 모바일 멀티 홉 무선 네트워크에서의 보안 관련 기술들에 대하여 알아보고 그 문제점들을 분석하며, Ⅲ장에서는 IEEE 802.16j에서 모바일 멀티 홉 릴레이를 적용함에 따라 발생하는 보안상의 문제점들과 요구사항을 분석한다. Ⅳ장에서는 이러한 문제점들을 해결하는 인증 알고리즘을 제안하고 그 메커니즘을 상세히 살펴본다. Ⅴ장에서는 제안하는 알고리즘이 Ⅲ장에서 언급한 요구사항들을 어떻게 만족하는지를 분석하고 Ⅵ장에서 결론을 맺는다.

Ⅱ. 관 련 연 구

모바일 멀티 홉 무선 네트워크 분야에서의 보안 기술은 주로 모바일 애드 혹 네트워크를 중심으로 연구되어 왔다. 애드 혹 네트워크의 경우 기존의 인프라스트럭처의 도움 없이 노드들이 애드 혹으로 네트워크를 구성하므로 인증 서버(authentication server : AS)로부터 인증 과정을 수행하는 기존의 중앙 집중 인증 기술을 사용할 수가 없다. 또한 무선 멀티 홉으로 네트워크 노드들이 네트워크를 구성하므로 단순히 네트워크 사용자를 인증하는 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 노드들 간에 공유하는 기술이나[6~8], PGP(pretty good privacy) 방법을 응용하여 노드들이 이동할 때마다 상대노드에 대한 인증을 수행하여 그 리스트를 관리하고 공유하는 기술 등이 주로 연구되고 있다[9]. 이러한 방법들은 인프라스트럭처가 없이 구성되는 애드 혹 노드들이 어떻게 초기 인증에 필요한 정보를 효율적으로 공유할 것인가에 초점을 맞추고 있으므로 그 특성상 우리의 주제에 적용하기에는 적합하지가 않다.

무선 LAN 기반의 무선 메쉬 네트워크에 대한 표준인 IEEE 802.11s 에서는 메쉬 노드들의 인증을 위하여 메쉬 노드가 접촉하는 주변 메쉬 노드와 홉 간 인증을 수행하도록 정의하고 있다[3]. IEEE 802.11s에서 제안된 메쉬 노드들 간에 인증방법으로는 분산 인증 방식과 중앙 집중 인증 방식이 있다[3, 10]. 중앙 집중 인증 방식의 경우 홉 간 인증을 수행하기 위해 메쉬 노드들 간에 서로 인증할 때, AS로 상대노드에 대한 인증을 요청하면 AS는 인증 검증을 수행한 후에 결과는 알려준다. 이 경우 인증에 참가하는 두 개의 메쉬 노드는 각각 한번씩, 인증자가 되어 상대 노드를 인증하고 또한 자신이 인증 요청자가 되어 상대 노드로부터 인증을 받는다. 즉 AS는 이 두 번의 인증 검증 과정을 거쳐 결과를 알려준다. 분산 인증 방식의 경우 메쉬 노드들 간에 직접 홉 간 인증을 수행한다. 분산 인증 방식을 적용하기 위해서는 메쉬 노드들 간에 미리 인증에 필요한 정보를 공유하고 있어야 하는 문제점이 있으며 주변 노드들의 공모에 의한 악의적 노드의 문제를 해결하기 어렵다.

Fujitsu에서는 주 인증자(master authenticator)를 별도로 운영하여 인증 서버의 기능을 제공하는 중앙 집중 인증 방식으로 멀티 홉 무선 액세스 네트워크에서의 보안 문제를 해결하고자 하였으나, 노드들의 주변 노드들에 대한 홉 간 인증은 다루고 있지 않다[11].

Ⅲ. 기존 방법의 문제점 및 IEEE 802.16j에서의 보안(security) 요구사항

1. 모바일 멀티 홉 무선 네트워크의 보안 문제점

앞 장에서 기술한 중앙 집중 방식 인증의 경우, 멀티 홉 노드는 인증 서버에 항상 연결이 가능해야 한다. 또한 네트워크의 모든 노드들 간의 상호 인증을 수행하기 위해서는 인증 서버의 로드가 많아지는 문제가 있다. 멀티 홉 노드의 입장에서도 인증을 위해 매번 인증 서버에 접속해야 하므로 인증 과정에 시간이 많이 걸리는 문제가 발생한다. 이러한 방식은 이동성을 가지고 수시로 여러 노드들과 인증을 해야 하는 모바일 멀티 홉 네트워크에서는 적절하지 않은 방법이다. 그리고 모바일 멀티 홉 노드들의 이동에 따른 핸드오프 발생 시에도 인증을 수행하기 위하여 인증 서버에 접속해야 하기 때문에, 이 과정에서 발생하는 인증 지연은 바로 핸드오프의 지연으로 나타나게 된다[1].

모바일 애드 혹 네트워크에서 주로 사용되는 분산 인

증 방식에서는 노드들 간의 인증에 필요한 비밀정보를 나눠서 공유해야 하기 때문에, 이를 위한 복잡한 알고리즘들이 사용되었다[6, 9, 11]. 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 노드 문제가 발생하거나 네트워크 내부 노드들의 공모에 의한 내부 공격 등의 문제가 발생할 수 있다. 그리고 노드들의 증가로 인한 확장성 문제도 가지게 된다.

위와 같은 보안상의 문제점들이 해결되지 않는다면, 노드 간 인증을 확보할 수 없게 되며, 따라서 라우팅 정보 등 자치적으로 운영되는 네트워크 관리의 중요 제어 정보 및 사용자의 데이터를 안전하고 신뢰성 있게 노드들 간에 전달되는 것을 보장할 수 없게 된다.

2. IEEE 802.16j에서의 보안 요구사항

가. 기존의 IEEE 802.16에서의 보안 특징

IEEE 802.16(또는 WiMAX)에서는 망이 사용자들에게 광대역 휴대 인터넷의 사용 권한을 주기 위한 MS에 대한 인증 기술만을 다루고 있다. 네트워크의 모든 시스템들이 유선으로 연결되어 망 관리자의 감독 하에 있으므로 모바일 멀티 홉 구조로 인한 문제점이 없다고 볼 수 있다. 여기서는 BS가 인증자 역할을 수행하여 MS에 대한 인증을 수행한다. AS는 MS를 인증한 후에 향후 사용될 키 생성에 필요한 PMK(primary master key)를 만들어 BS가 접속한 ACR(access control router) 및 MS에 나눠준다. ACR과 MS는 각각 인증키(authentication key)를 생성하여 서로를 인증하고, BS와 MS는 TEK를 공유하게 된다. 이후 MS가 보내는 모든 메시지들은 TEK로 암호화하여 BS를 통하여 전송되므로 TEK를 공유한 BS는 MS가 전송하는 메시지에 대한 메시지 인증을 수행하게 된다[12~15].

나. IEEE 802.16j 기반의 모바일 멀티 홉 릴레이에서의 보안(security) 요구사항

IEEE 802.16j 기반의 모바일 멀티 홉 릴레이에서는 다음과 같은 보안 기능이 요구되어진다. 그러나 이러한 기능에 대한 연구는 아직까지 이루어지고 있지 않다.

RS들의 홉 간 인증을 수행하기 위한 인증 메커니즘이 필요하다 - 모바일 멀티 홉 릴레이(MMR)에서는 네트워크의 영역 확장과 처리율 향상을 위해 RS들이 무선 멀티 홉으로 연결된다. 또한 MRS와 같이 이동성을 갖는 RS들이 존재하며, MRS는 이동함에 따라 다른 RS들과 접속하게 된다. 이 경우 RS들은 self-organizing 방식으로 무선 네트워크를 구성하므로 RS들 간의 홉 간 인증은 필수적이다.

BS 대신에 RS가 MS에 대한 인증을 수행하여야 한다 - 모바일 멀티 홉 릴레이(MMR)에서는 멀티 홉으로 구성된 RS들을 통하여 BS로 연결되므로 이전에 MS가 BS를 통해 네트워크에 접속하던 것과는 달리 RS를 통해 네트워크에 접속할 수가 있게 된다. 따라서 기존에 BS가 수행하던 인증자 역할을 RS가 수행할 수 있어야 하며, 또한 RS와 MS는 TEK를 공유하여야 한다.

모바일 멀티 홉 릴레이(MMR)에서의 MS의 기능을 변경하지 않아야 한다는 요구사항을 만족하기 위해 RS의 존재는 MS에게 투명 해야 한다

RS 간의 로컬 라우팅에 따른 메시지 인증을 수행할 수 있어야 한다 - 기존의 IEEE 802.16에서는 모든 호가 BS를 통해 라우팅 되었으나, 모바일 멀티 홉 릴레이(MMR)에서는 BS를 거치지 않고 RS와 RS 간에 직접 라우팅이 될 수 있다. 이 때 BS가 수행하던 MS의 메시지 인증을 RS가 대행할 수 있어야 한다.

본 논문에서는 위의 요구사항을 만족시키기 위하여, 혼합형 인증 방식을 제안하며 또한 제안된 방식이 위의 요구사항을 어떻게 만족하는지를 보여주고자 한다.

IV. 혼합형 인증 방법

모바일 멀티 홉 릴레이 네트워크 환경은 기존의 네트워크 환경에서 사용되는 중앙 집중 인증 방식과 애드 혹 네트워크에서 사용되는 분산 인증 방식이 모두 사용될 수 있는 환경이다. 중앙 집중 인증 방식만을 적용할 경우 멀티 홉 노드들 간의 상호 인증이 AS로 위탁되고 인증 지연이 증가하는 문제가 있으며 분산 인증 방식이 적용될 경우 노드 상호 간의 인증에 필요한 인증 검증 정보의 최초 공유 문제, 멀티 홉 노드들의 공모로 인한 내부 공격문제, 악의적 노드 등의 문제를 가지게 된다.

이와 같은 두 가지 방법의 단점을 해소하기 위하여 본 논문에서 제안하는 방법은 중앙 집중 인증 방식과 분산 인증 방식을 혼합한 혼합형 인증방식이다. 즉 모바일 멀티 홉 릴레이로 구성된 네트워크에서 RS의 네트워크 진입에 따른 최초의 상호 인증은 중앙 집중 인

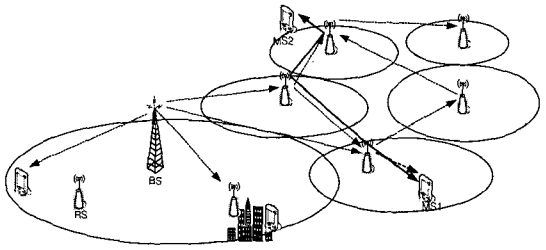

그림 1. 모바일 멀티 홉 릴레이의 한 예
Fig. 1. An example of multi-hop relay network.

증 방식을 사용하고, 이를 통하여 RS들 간의 홉 간 인증에 필요한 공유키를 획득한 후에 RS들 간에 분산 인증을 수행하도록 하는 방식이다.

이러한 방법에서는 RS가 AS와 중앙 집중 인증 방식을 수행한 후에, 기존에 존재하는 주변 RS들과 분산 인증을 수행하는 절차에 대한 연구가 필요하며, 이러한 절차는 RS의 이동으로 핸드오프가 발생할 경우의 빠른 인증을 수행할 때도 활용될 수 있다. 또한 위의 인증방법의 연장선에서 RS에 접속한 MS가 BS를 거치지 않고 다른 RS에 접속한 MS로 연결하는 로컬 라우팅을 지원하기 위하여 RS가 직접 MS에 대한 인증을 수행하는 절차에 대한 연구도 필요하다. 그러면 MS에 적용된 기존의 기능을 수정하지 않고 RS가 효율적으로 MS에게 서비스를 제공할 수 있게 될 것이다.

본 절에서는 이와 같은 RS의 초기 중앙 집중 인증 절차 및 이후의 RS간 분산 인증 절차에 대하여 다루며, 또한 RS의 MS에 대한 인증 절차 및 로컬 라우팅 과정에서의 메시지 인증절차에 대하여 다룬다.

그림 1은 제안하는 혼합형 인증 방식의 동작을 설명하기 위한 모바일 멀티 홉 릴레이 네트워크의 한 예를 보여준다. 그림에서 RS들은 BS로부터 멀티 홉으로 서로 연결된다. 또한 사용자 단말인 MS_1과 MS_2는 BS를 통하지 않고 RS만을 거쳐서 연결되며, 이 때 MS들에 대한 인증은 RS가 수행하게 된다.

1. 네트워크 진입에 따른 인증 절차

RS는 새로이 멀티 홉 릴레이 네트워크에 참가할 때 먼저 자신이 참가하는 네트워크가 정당한 네트워크인지를 검증해야 한다. 멀티 홉 릴레이 네트워크에서도 네트워크에 새로 참가하는 RS가 정당한 노드인지를 검증해야 한다. 이러한 과정은 RS가 AS와의 상호 인증을 통해 이루어지고, 이 때 얻은 공유키 정보를 이용하여 RS가 이웃 RS들과의 상호 인증을 수행한다.

따라서 새로 네트워크에 참가하는 RS는 적절한 알고

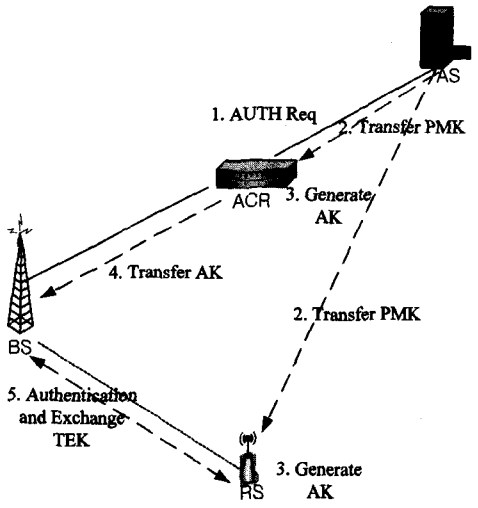

그림 2. 중앙 집중 인증을 이용한 RS의 BS를 통한 초기 네트워크 진입 시의 인증 과정
Fig. 2. The centralized RS authentication through BS at its entry to network.

리즘으로 선택된 이웃 RS 또는 BS (예를 들면 제일 먼저 발견된, 혹은 신호의 강도가 제일 좋은 이웃 RS 또는 BS)에 초기 인증을 요청한다. 선택된 이웃 RS 또는 BS는 이미 멀티 홉 릴레이에 참가하고 있으므로 AS로의 라우팅 정보를 가지고 있다. 따라서 선택된 이웃 RS 또는 BS는 모바일 멀티 홉 릴레이 네트워크에서의 안전한 연결을 통해 새로운 RS의 초기 인증 요청을 AS로 전송한다.

가. RS가 BS를 통해 네트워크 진입을 수행하는 경우

그림 2는 RS가 모바일 멀티 홉 릴레이 네트워크에 진입할 때의 인증 과정을 보여준다. 그림에서 RS는 처음 BS를 통하여 네트워크 진입을 수행하고, AS와 중앙 집중 인증 과정을 수행한다(step 1). 이 때 사용되는 인증 알고리즘은 기존에 인증에 사용되는 알고리즘을 무엇이든지 적용할 수 있다. AS와 RS간에 상호 인증이 완료되면 AS는 RS에 대한 credential을 가지게 되고 PMK를 생성하여 ACR과 RS에 전송한다(step 2). ACR과 RS는 PMK로부터 인증키를 생성하고(step 3) 이 AK를 이용하여 BS와 RS는 인증 과정을 수행한 후 TEK를 공유하게 된다(step 5).(이러한 과정은 기존의 802.16 또는 WiMAX의 인증 과정을 그대로 적용한 것이다.)

그림 3에서는 이웃한 RS들이 분산 인증을 수행하는데 필요한 AK를 획득하는 과정을 보여준다. 그림에서 RS_1과 RS_2가 BS를 통해 초기 인증을 수행한 경우, BS는 RS_1과 RS_2에 대한 AK_1과 AK_2를 가지게 된다. 이후,

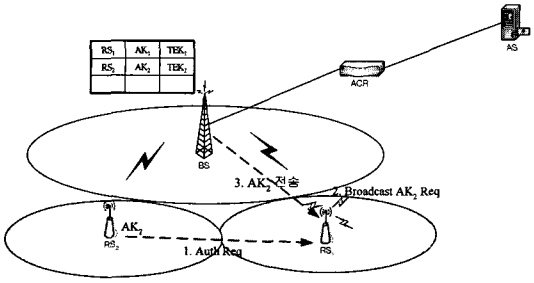

그림 3. 이웃한 RS들간에 인증 획득과정
Fig. 3. Hop-by-hop authentication of RS.

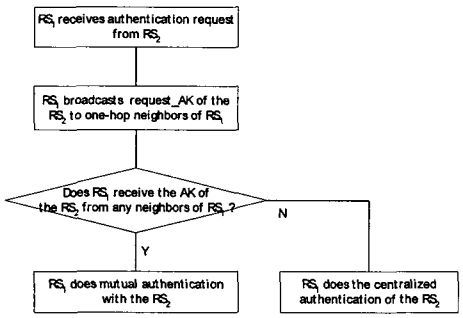

그림 4. RS가 이웃 RS와 홉 간 인증을 수행하는데 필요한 인증을 획득하는 과정
Fig. 4. Flow chart for hop-by-hop authentication of RS.

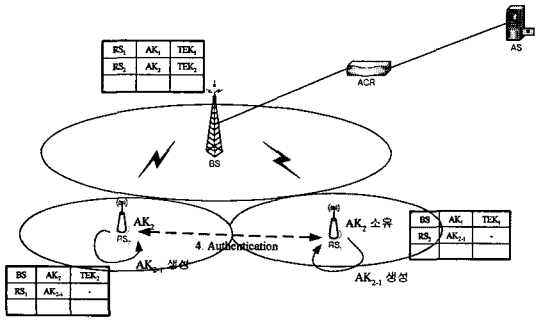

그림 5. 이웃한 RS들 간에 분산 인증 수행
Fig. 5. Distributed hop-by-hop authentication of RS.

RS_2가 RS_1과 분산 인증을 수행하려면 서로 간에 인증 정보를 공유하고 있지 않으므로 RS_1과 RS_2간의 AK가 필요하다. RS_2가 RS_1에 인증을 요청하면(step 1), RS_1은 RS_2에 대한 AK가 필요하므로 BS를 포함하여 주변 이웃 RS들에게 RS_2의 AK를 요청한다(step 2). RS_1의 주변에서 BS가 RS_2의 AK_2를 가지고 있으므로 BS는 AK_2를 RS_1에게 전송한다. 이 때 BS는 AK_2를 BS와 RS_1간의 TEK를 이용하여 암호화하여 전송한다(step 3). 이렇게 하여 RS_1과 RS_2는 분산 인증을 수행하는 필요한 AK_2를 공유하게 된다. BS와 RS_2는 RS_1이 AK_2를 알게된 후에, 키 리프레쉬를 수행하여 AK_2값을 재생성 할 수 있다.

RS_1이 RS_2의 AK를 획득하는 과정의 흐름을 나타내면 그림 4와 같다.

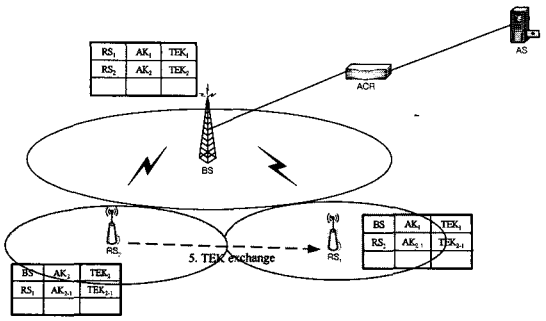

그림 6. 이웃한 RS들이 분산 인증을 수행한 후 TEK를 공유하는 과정
Fig. 6. TEK sharing between neighbored RSs.

RS_1과 RS_2는 AK_2를 이용하여 분산 인증 방식을 수행하며, 인증 후 두 RS사이에 별도의 독립적인 AK를 공유하기 위하여 AK_{2-1}를 만든다. 이러한 과정은 그림 5에 보여준다.

그림 6에서는 RS_1과 RS_2가 상호 인증을 수행한 후 TEK를 공유하는 상황으로 각 RS의 표에서 확인할 수 있다.

나. RS가 다른 RS를 통해 네트워크 진입을 수행하는 경우

그림 7에서는 RS가 다른 RS를 통하여 네트워크 진입을 수행할 때 인증 과정을 보여준다. 그림에서는 RS_3가 네트워크에 참여하면서 RS_2를 통하여 인증 요구를 보내는 경우이다(step 1). 이 때 RS_2는 RS_3의 요청을 단순히 AS로 릴레이만 하며, 이는 그림 2에서의 BS의 역할과 같다. AS는 RS_3를 인증하고 PMK를 생성하여 RS_2와 RS_3에 전송한다(step 2). RS_2와 RS_3은 PMK를 이용하여 AK를 생성한 후에 분산 인증을 수행한다(step 3). 인증을 수행한 후에, RS_2와 RS_3사이에 TEK

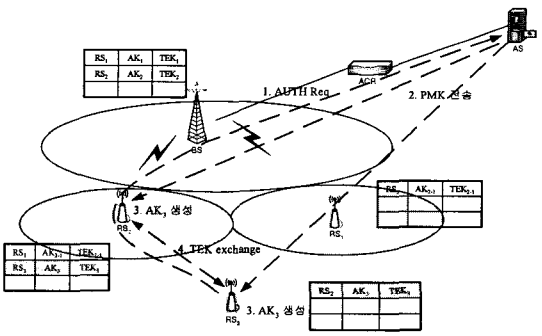

그림 7. RS가 다른 RS를 통하여 네트워크 진입을 수행하는 경우 인증 과정
Fig. 7. Authentication of a RS when it enters network through other RS.

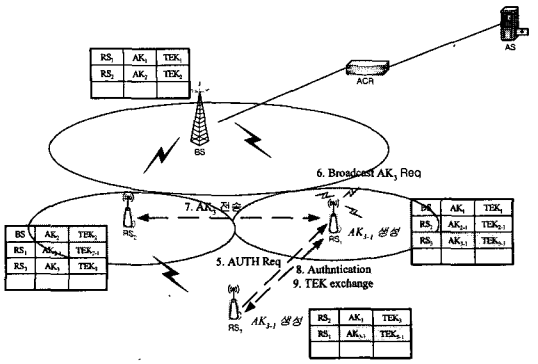

그림 8. RS간에 분산 인증을 이용하여 홉 간 인증을 수행하는 과정

Fig. 8. Distributed hop-by-hop authentication of RS.

를 공유하게 된다(step 4).

그림 8에서는 RS가 중앙 집중 인증을 이용하여 네트워크 진입시의 상호 인증을 수행한 후에, 분산 인증을 이용하여 인접한 이웃 RS들과 홉 간 인증을 수행하는 과정이다. RS_3는 인접한 RS_1에게 인증 요구를 보내면(step 5), RS_1은 RS_3와의 인증에 필요한 AK 정보를 이웃 RS들에게 방송을 통해 요청한다(step 6). RS_1의 이웃 노드들 중에서 RS_2가 RS_3에 대한 AK_3를 가지고 있으므로, RS_2가 RS_1의 요청에 대한 응답으로 AK_3를 전송한다. 이 때, RS_1과 RS_2는 이미 TEK를 공유하고 있으므로 RS_3를 인증하는데 필요한 AK_3는 이 TEK를 이용하여 암호화해서 전달하여 중간에 노출될 염려가 없도록 한다. RS_1은 AK_3를 이용하여 RS_3와의 인증을 수행하고 TEK를 생성한다. 마찬가지로 이 경우에도 RS_1과 RS_3은 별도의 독립적인 AK를 공유하기 위하여 AK_{3-1}을 만든다.

다. MS가 RS를 통해 네트워크에 접속하는 경우

그림 9에서는 MS가 RS를 통하여 네트워크 진입을 수행할 때에 중앙 집중 인증을 수행하는 과정을 보여준다. 이 과정은 RS가 네트워크 진입을 수행할 때의 인증 과정과 동일하게 이루어진다. 그림에서 RS_1이 MS에 대한 인증을 수행한다. 기존의 IEEE 802.16(또는 WiMAX)의 경우 MS가 보내는 메시지에 대한 인증을 BS가 수행하는 데, 이 방법에서는 RS가 MS와 TEK를 공유하게 되고, BS를 대신하여 메시지 인증을 수행하게 된다.

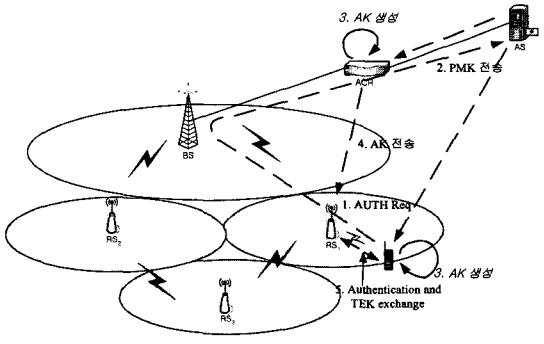

그림 9. MS가 RS를 통하여 네트워크 진입을 수행할 때의 인증 과정

Fig. 9. Authentication of MS when it enters network through RS.

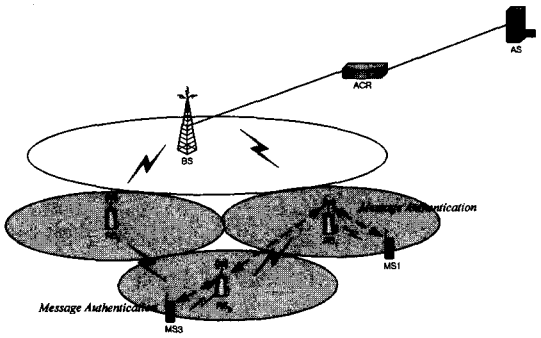

그림 10. 로컬 라우팅의 예

Fig. 10. An example of local routing.

2. 로컬 라우팅 문제

로컬 라우팅은 MS간의 호를 연결할 때에 BS를 거치지 않고, RS와 RS간에 라우팅을 통하여 이루어지는 것을 말한다. MS가 BS를 통해 접속할 경우에는 BS가 MS의 메시지를 인증하고 이를 전송해준다. 로컬 라우팅이 이루어질 경우, MS와 TEK를 공유하고 있는 RS는 BS의 도움없이 MS의 메시지를 인증하여 바로 목적지 RS로 라우팅할 수 있다. 그림 10에서는 RS_1이 BS를 거치지 않고 RS_3와 연결되는 경우이다. RS_1에 접속한 MS_1과 RS_3에 접속한 MS_3와 통신이 이루어 질 때, MS_1이 MS_3로 보내는 메시지는 RS_1이 메시지 인증을 수행

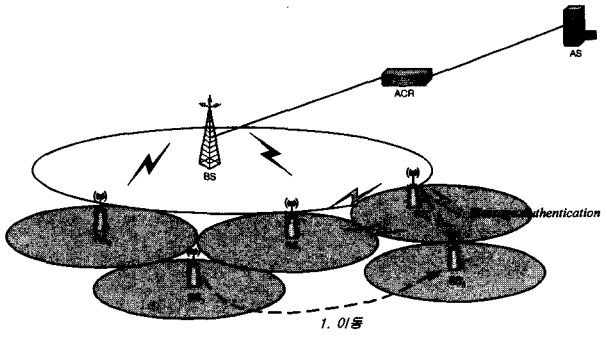

그림 11. RS가 이동하여 다른 RS와 핸드오프를 수행하는 과정에서의 인증

Fig. 11. Authentication at RS handoff.

하고 RS_3로 전송한다. 이 때 MS_1과 MS_3간의 종단간 보안기능을 별도로 수행할 수 있다.

3. 핸드 오프시의 인증

모바일 멀티 홉 릴레이 네트워크에서 RS의 핸드오프는 일반적으로 자신의 영역 내의 MS들과 함께 이동할 경우가 일반적이다. 그림 11에서는 RS가 이동하여 다른 RS와 핸드오프를 수행하는 과정을 보여준다. RS_3이 이동하여 RS_4의 새로운 이웃이 된 경우, RS_3과 RS_4는 상대를 신뢰하기 위한 상호 인증을 수행한 후에 핸드오프를 수행하여야 한다. 상호 인증시에, RS_4는 RS_3에 대한 AK가 필요한 데, 이 키를 얻기 위하여 초기 네트워크 진입 때의 홉 간 인증 과정과 마찬가지로, 주변의 이웃 RS들에게 RS_3에 대한 AK를 요청하여 획득한다. 이러한 과정은 RS_3이 이동하면서 거쳐 온 RS들이 RS_4의 이웃 RS일 가능성이 높기 때문에 가능하다. 또한 좀 더 빠른 인증이 가능하도록, RS_3이 RS_4로 이동하기 전에 접속한 이웃 노드가 RS_3이 핸드오프를 수행하여야 함을 인지했을 때에 미리 자신의 주변 노드들에게 RS_3의 AK를 TEK를 사용하여 암호화한 후에 전송하여 RS_3이 이동할 경우 RS_4가 미리 RS_3의 AK를 확보하여 인증이 신속하게 이루어지도록 할 수 있다.

이 경우 RS에 접속하여 RS와 같이 이동하는 MS들은 접속되어 있는 RS가 인증된 후에 그 RS를 통하여 통신을 계속 유지할 수 있다.

V. 혼합형 인증 방법 효과 분석

이 장에서는 본 논문에서 제안하고 있는 혼합형 인증 방법이 Ⅲ장에서 언급한 요구사항들을 어떻게 만족하는지를 분석한다.

1. RS들 간의 홉 간 인증 수행

본 논문에서 제안하는 혼합형 인증 방법은 중앙 집중 인증 방식과 분산 인증 방식을 혼합하여 RS가 모바일 멀티 홉 릴레이 네트워크에 초기 진입할 때에, 초기 인증은 AS를 통하여 중앙 집중 인증 방식으로 수행하고, 이웃한 RS들과의 홉 간 인증은 분산 인증 방식을 적용하여 수행한다. 이웃한 RS들과의 홉 간 인증에 필요한 인증 키는 먼저 인증 과정을 수행한 RS로부터 암호화하여 획득할 수 있다.

가. RS의 최초 신뢰 획득

모바일 애드 혹 네트워크에서 적용하는 분산 인증방식에서는 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 데 비하여, 제안하는 인증 기술은 인증 서버를 통해 최초의 신뢰를 획득하므로 이러한 문제를 해결할 수 있다.

나. 모바일 멀티 홉 노드간의 홉 간 인증

이웃한 RS들 간에 상호 인증을 할 경우, 중앙 집중 인증 방식을 수행하게 되면, 인증 서버가 각각 RS들을 인증한 후에 각 RS에게 상대 RS가 인증되었음을 알려주는 trust transitive의 문제가 발생하게 된다. 또한 한 RS의 주변에 n개의 이웃한 RS가 존재할 경우 이 RS는 인증 서버와 $2n$번의 인증 과정을 수행하여야만 모든 이웃 RS들과 상호 인증을 완료할 수 있으며 이것은 모바일 멀티 홉 릴레이 네트워크에 상당한 부담이 된다. 그러나 혼합형 인증 기술을 적용할 경우 RS들 간에 공유키를 이용하여 직접 상대 RS를 인증할 수 있게 된다.

2. MS에 대한 요구사항

본 논문에서 제안하는 혼합형 인증 방법에서는 MS에 대한 인증 과정을 수행할 때 RS가 BS와 동일하게 인증자 역할을 수행하도록 하며, MS는 기존의 기능변화 없이 모바일 멀티 홉 릴레이 네트워크에의 접속에 필요한 인증 과정을 수행할 수 있도록 한다. 즉 RS는 BS가 원래 수행하던 역할을 그대로 수행하므로, MS는 RS의 존재에 대하여 특별히 인식하지 못하고, 마치 BS에 접속되어 있는 것으로 생각하게 된다.

3. 로컬 라우팅 제공

기존의 IEEE 802.16 또는 WiMAX의 경우, BS와 MS는 인증 후에 TEK를 공유하며, BS는 이 키를 이용하여 MS가 보내는 메시지에 대한 인증을 수행한다. 본 혼합형 인증 방법에서는 MS가 접속하는 RS나 BS가 MS와의 상호 인증을 수행하고 TEK를 공유하게 된다. 만약 MS가 RS 및 BS를 통하여 다른 MS와 연결을 할 경우, MS와 TEK를 공유하는 RS가 메시지 인증을 검증하고, 이 결과를 BS에 전달하게 된다. BS와 RS는 이미 상호 인증을 통하여 서로를 인증하고 신뢰하므로 이 결과를 신뢰하게 된다.

MS가 BS를 거치지 않고 RS만을 거쳐서 다른 RS에

접속한 MS와 연결이 될 경우 RS와 MS간의 상호 인증을 기반으로 MS에 대한 메시지 인증을 RS가 수행하고 데이터를 포워딩할 수 있게 된다.

4. 기타의 문제점에 대한 효과 분석

가. 악의적 노드 문제

모바일 애드 혹 네트워크나 무선 LAN과 같은 무선 네트워크에서는 악의적 노드(또는 악의적 AP) 문제가 발생할 가능성이 아주 많다. 특히 모바일 멀티 홉 네트워크 환경에서 분산 인증을 사용할 경우 RS들 간의 공모에 의한 악의적 노드 문제는 네트워크 운영을 어렵게 만들 수 있다. 이러한 문제는 RS들에 대한 신뢰의 기반이 중앙 집중 서버에 의한 것이 아니라 RS들끼리 상대의 신뢰도를 검증하므로 발생한다. 그러나 혼합형 인증 방식에서는 RS가 모바일 멀티 홉 릴레이 네트워크에 참가하고자 할 경우, 인증 서버와 초기 인증이 수행하여야 하므로, 인증서버는 초기 인증에 필요한 검증 정보를 소유할 수 있게 한다. 그러므로 RS들 간의 공모에 의하여 검증키를 위조하는 등의 불법적인 행위로 악의적인 노드가 네트워크에 참가하는 것이 불가능하게 된다. 또한 RS가 자신이 참가하려고 하는 멀티 홉 릴레이 네트워크가 정상적인 네트워크인지를 검증하고자 할 경우, 분산인증만이 사용된다면, 주변 RS들이 공모하여 검증 정보를 위조하여 인증과정을 수행할 수 있는 데 이 때 네트워크에 새로 참가하는 RS는 이를 알 수 없게 된다. 그러나 혼합형 인증 방식을 적용할 경우 사업자의 관리 하에 있는 인증 서버가 인증 정보를 관리하므로 RS들의 공모에 의한 거짓 정보의 전달이 가능하지 않게 된다.

나. 공유키 분배방식

기존에 인증 알고리즘에서는 대칭키 방식을 사용할 경우, 인증 당사자들 간의 공유키 분배의 문제점을 가지며, 또한 공개키 방식을 사용할 경우 공개키 검증에 필요한 인증서 발급의 문제점을 갖는다. 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 따라서 인증 알고리즘 적용을 간단하게 할 수 있다.

다. RS의 이동으로 핸드오프 발생 시에 빠른 인증 수행

혼합형 인증 환경에서는 RS들의 이동에 따른 핸드오프시에, 분산 인증을 통한 홉 간 인증을 수행하므로, AS를 이용하는 중앙 집중 방식의 인증보다 신속하게 이루어진다. 또 RS들 간의 인증정보도 미리 이웃 RS들로부터 획득할 수 있으므로 핸드오프 발생시에 RS들 간의 인증 키 획득에 필요한 지연을 줄일 수 있다. 이러한 방법은 MS가 이동함에 따라 발생하는 핸드오프시에도 동일하게 적용할 수 있다.

VI. 결 론

최근 모바일 멀티 홉 무선 네트워크에 대한 관심이 증가하면서 IEEE 802.16j 및 WiMAX(WiBro)에서도 영역 확장과 데이터 처리율 향상 등의 이유로 모바일 멀티 홉 릴레이를 도입하고 있다. 모바일 멀티 홉 릴레이는 self-organizing 등의 특성으로 인하여 설치가 용이하며 관리하기 편한 장점이 있지만, 반면에 무선으로 설치되어 자치적으로 운영되는 릴레이 스테이션을 신뢰하기 어려운 보안상 문제점이 있다. 특히 IEEE 802.16j 기반의 무선 멀티 홉 네트워크에서는 일반적인 모바일 멀티 홉 네트워크에서의 보안상 문제점뿐만 아니라, 기존의 IEEE 802.16에서의 특성을 유지해야 하는 요건으로 인하여 발생하는 추가적인 문제점도 존재한다.

본 논문에서는 IEEE 802.16j 기반에서의 모바일 멀티 홉 릴레이에서 가지는 위와 같은 보안상의 문제점들을 해결하기 위하여 혼합형 인증 방식을 제안하였다. 제안하는 방식에서는 RS의 네트워크 진입시 초기 인증과정은 중앙 집중 인증 방식으로 하고, RS 간의 홉 간 인증은 분산 인증 방식으로 수행하도록 하였다. 이 때 RS들 간의 분산 인증 과정에 필요한 AK는 초기 중앙 집중 인증 과정에서 안전하게 획득한 인증 정보를 이용하여 만드는 방안을 제안하여 네트워크의 효율을 높이고 분산 인증 방식에서 문제가 되는 공유키 관리의 어려움을 해결 하였다. 또한 RS가 이전에 BS가 수행하던 MS 인증 및 메시지 인증 등의 기능을 수행하도록 하여, MS가 기능 변경이 없이 모바일 멀티 홉 릴레이 구조에 적용될 수 있도록 하였다.

제안하는 혼합형 인증방식은 IEEE 802.16j 기반의 모바일 멀티 홉 릴레이 네트워크 뿐만 아니라 모바일 멀티 홉 구조를 갖는 다른 네트워크에도 적용될 수 있으며, 무선으로 연결되어 자치적으로 운영되는 네트워크에서의 필수적인 보안 문제점인 인증문제를 해결하는데 기여할 것으로 기대된다.

참 고 문 헌

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

[2] P. Baronti, P. Phllai, V.W.C. Chook, S. Chessa, A. Gotta, and Y.F. Hu, "Wireless sensor networks : A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, Elsevier, Vol. 30, Issue 7, pp. 1655-1695, May 2007

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

[4] "D 2.4 Multi-radio Access Architecture", WWI Ambient Network Project, 2005

[5] IEEE 802.16's Relay Task Group,]http:// www.802wirelessworld.com

[6] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks," *IEEE Network Mag.*, 1999

[7] Yanchao Zhang and Yuguang Gang, "ARSA : An Attck-Resilient Security Architecture for Multihop Wireless Mesh Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 10, pp. 1916-1928 Oct. 2006.

[8] R. Falk, A. Prasad, and A. Tschofenig, "Secure Access Over Multi-hop Relay Extension of Public Networks," *WPMC 2005,* Aslborg, Denmark, Sep. 2005.

[9] 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, pp. 52-64, Jan-Mar 2003

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extension Authentication Protocol(EAP)," IETF RFC 3748, June 2004

[11] 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.

[12] IEEE Standard 802.16-2004, "Air Interface for Fixed Broadband Wireless Access Systems," IEEE, October 2004

[13] 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

[14] Arkoudi-V. Aikaterini, Security of IEEE 802,16, MS thesis, Dept. of Computer and Systems Science, Royal Institute of Technology, 2006.

[15] Sen Xu, Manton Matthews and Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16," *ACM SE'06*, Florida USA. March 2006.

저 자 소 개

이 용(정회원)

1997년 연세대학교 컴퓨터과학과 (석사)

2001년 연세대학교 컴퓨터과학과 (박사)

1993년~1994년 디지콤정보통신 연구소

2001년~2003년 한국정보보호진흥원 선임연구원

2004년~2005년 코넬대학교 방문연구원

2005년~2007년 삼성전자 통신연구소 책임연구원

2007년~현재 충주대학교 전자통신공학전공 조교수

<주관심분야 : Mobile and Wireless Security, Ubiquitous Sensor Network, Wireless Mesh Network, Mobile Ad hoc network>

이 구 연(정회원)

1988년 KAIST 전기및전자공학과 (석사)

1993년 KAIST 전기및전자공학과 (박사)

1993년~1996년 디지콤정보통신 연구소

1996년 삼성전자

1997년~현재 강원대학교 컴퓨터학부 교수

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