

무선 메쉬 네트워크 구축 및 보안 기술 현황

이 용*, 이 구 연**

요 약

미래의 광대역 무선망은 고주파수의 대역을 사용하여 신호의 감쇠가 높고, 높은 multi-path fading 효과를 가지므로 전력 제어가 필요하고 사용자에게 넓은 대역폭을 제공할 것으로 예측한다. 이를 위해 셀의 크기가 줄게 되고 BS의 수가 증가하여 네트워크 설치비용도 증가하게 될 것이다. 무선 메쉬 네트워크는 이런 문제를 해결하여 망구축과 운영을 쉽게 하고 영역 확장과 용량 확장을 유연하게 하며 저비용의 무선 backhaul로 높은 신뢰성을 제공하는 특성을 가진다. 무선 메쉬 네트워크는 노드와 노드간의 무선 멀티-홉 통신을 이용하여 끊임없는 연속적인 연결을 제공하는 네트워크 기술이다. 이 기술은 메쉬 라우터와 메쉬 클라이언트라는 노드로 구성되며 각 노드는 라우터인 동시에 호스트로 동작할 수 있다. 앞서 언급한 바와 같이 자가 구성, 자가 복구의 능력을 가지고 저비용으로 신뢰성 있는 네트워크 구축을 제공하기 때문에 무선랜이나 WiMAX, WPAN 등에서 채택되고 있다. 이 논문에서는 메쉬 네트워크의 구조와 특징을 자세히 설명하고 IEEE 802.11s와 IEEE 802.16j에서 진행되는 무선 메쉬 네트워크 관련 표준화를 살펴본 후 관련업체에서의 메쉬 네트워크 관련 개발 현황과 실제 구축 현황을 설명하고자 한다. 또한 무선 메쉬 네트워크에서 발생하는 여러 가지 보안 문제와 적용기술들을 짚어 보고자 한다.

1. 서 론

무선랜 기술은 유선망과는 독립적으로 다양한 광대역 네트워크 구성을 특징으로 하여, 디지털 가전이나, 개인용 컴퓨터, 이동 단말 등을 포함하여 다양한 단말로 구성되는 미래 유비쿼터스 네트워크를 위한 기본 기술로서 주목을 받아왔다.

무선 메쉬 네트워크(Wireless Mesh Network) 기술은 새로운 방법으로 기본 RF(Radio frequency)을 사용하여 무선 커버리지 문제와 처리속도, 비용 등의 문제를 해결하고 무선 이동성을 제공하는 4세대 기술로 인정받고 있다. 메쉬 네트워킹은 다양한 장소에서 저비용으로 무선 액세스를 제공하여 기존의 무선 데이터나 음성 통신을 그래도 사용자에게 제공할 수 있는 새로운 모델을 제공한다. 또한 무선 메쉬 네트워크는 어떤 어려운 환경에서도 설치가 용이하고 높은 전송률을 보장하여 군대와 같이 응급 서비스가 필요한 경우에 메쉬 네트워크를 재빨리 구성하여 municipal 무선 광대역 네트워크를 구축할 수 있도록 한다^{[1][2][3]}.

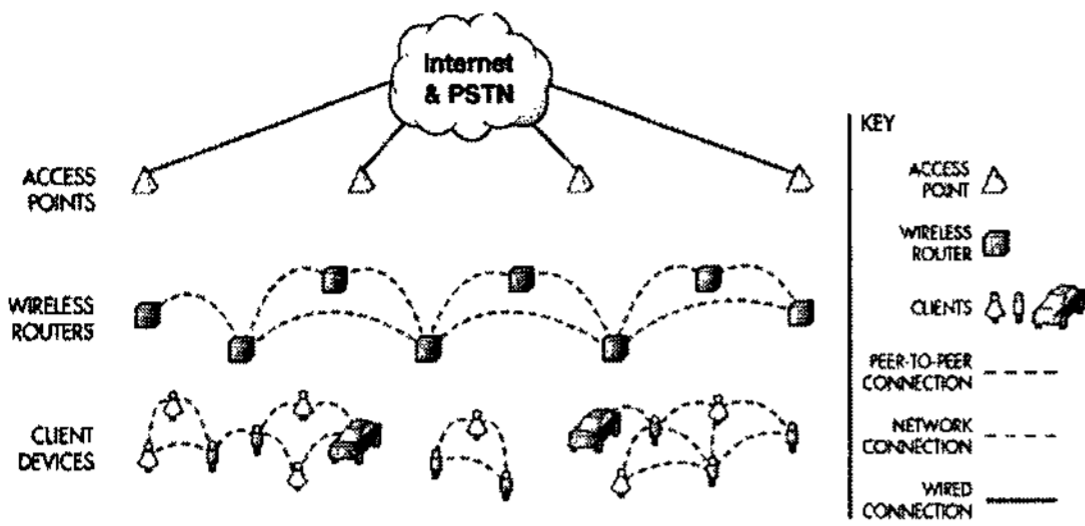
무선랜 기반의 메쉬 네트워크에 대한 다양한 상상력이 동원되어 기업의 무선랜 네트워크의 커버 영역을 확장하고 애드혹 네트워크를 구성하기 위해 홈 네트워크 구축에도 적용되고 있다. 무선랜 메쉬 네트워크는 베이스 스테이션과 같은 중앙 집중화된 제어 장치의 도움 없이 무선 연결의 수단만으로 이웃하는 단말들을 서로 직접 연결하여 구성된다. 이런 종류의 네트워크에서 단말이 전송한 데이터는 멀티-홉 무선 네트워크 구성을 통하여 여러 무선 단말들을 거쳐서 목적지에 도착한다.

무선랜 기술은 광대역 무선 통신을 가능하게 하는 수단으로 널리 사용되고 있으며 QoS 기술과 무선 고속 전송 기술에 있어서 많은 발전을 이루고 있다. 무선 메쉬 네트워크는 짧은 통신 거리로 인한 고속의 데이터 전송 속도와 주파수 재사용으로 인하여 네트워크의 전송 용량 확대, 자동화된 네트워크 구성, 경로 복구 메커니즘으로 인한 네트워크 유지의 안전성 등의 특징을 갖는다[그림 1].

그러나 멀티-홉 무선 네트워크가 기본적으로 가지는 문제점을 무선 메쉬 네트워크도 그대로 유지하여 처리율 감소의 원인이 되는 히든 단말의 문제점이나 노출

* 충주대학교 전기전자및정보공학부 전자통신공학전공 (yleehyun@cjnu.ac.kr)

** 강원대학교 컴퓨터학부 컴퓨터정보통신전공 (leegyeon@kangwon.ac.kr)



(그림 1) 무선 메쉬 네트워크 개념(6,8)

단말의 문제점이나 네트워크 혼잡 등의 문제점을 가지게 된다.

무선 메쉬 네트워크는 필요한 구성요소들이 애드혹 네트워크 라우팅 프로토콜, IEEE 802.11 MAC 프로토콜에 따라 이루어지므로 설치도 어렵지 않다. 이미 여러 회사들이 이미 이 기술을 개발하여 메쉬 네트워킹 제품을 출시하고 있다. 그러나 무선 메쉬 네트워크에 적용될 MAC과 라우팅 프로토콜의 확장성이 충분하지 않거나 흡을 거치면서 처리율이 감소하는 등 무선 메쉬 네트워크는 아직도 연구되어야 할 부분이 많이 있는데 그 중에서도 특히 메쉬 구조가 무선으로 자가 조직됨에 따라 메쉬 노드들간의 인증이나 애드혹 라우팅 프로토콜을 적용함에 따라 발생하는 제어 정보의 보안과 같은 네트워크 보안에 대한 문제점이 중요한 이슈이다. 모바일 애드 혹 네트워크와 유사하게 무선 메쉬 네트워크는 채널이나 노드가 취약하고 기반시설의 부재, 네트워크 토폴로지의 동적인 변화 등으로 인해 효율적이고 확장성 있는 보안 방법이 필요하다. 공격자는 라우팅 정보를 공격할 수도 있고 패킷 포워딩을 지연하는 등의 공격을 할 수도 있다. 혹은 네트워크에 합법적인 노드임을 가장하고 침입하여 네트워크 구성을 위해 수행해야 할 과정들을 따르지 않는 등 네트워크 운영에 문제가 될 수도 있다^{[11][7]}.

무선 메쉬 네트워크가 적용되는 네트워크는 WiFi, 애드혹 네트워크, 무선 센서 네트워크 등 여러 가지 경우가 있고 이에 대한 표준으로는 IEEE 802.11의 표준 기반의 무선랜 기술들이 주로 적용되며 최근 IEEE 802.16과 같은 WiMAX나 IEEE 802.15.4의 WPAN (Wireless Personal Area Network)에서도 메쉬 네트워크 구조를 적용하고 있다.

이 논문에서는 2장에서 무선 메쉬 네트워크의 구조를 설명하고 3장에서 무선 메쉬 네트워크 관련 표준화 동향을 살펴본다. 4장에서는 메쉬 네트워크 관련 업체 현황 및 구축 현황을 설명하고 5장에서 무선 메쉬 네트

워크에서의 보안 기술을 자세히 다루고 마지막으로 6장에서 결론을 맺는다.

II. 무선 메쉬 네트워크의 구조

2.1. 배경

무선 메쉬 네트워크가 등장하게 된 배경은 네트워크에서의 주파수 영역과 데이터 처리 속도의 문제를 해결하기 위해서였다. 광대역 무선 통신의 물리적인 특성은 전송 파워에 대한 데이터 처리 속도와 주파수 영역 간의 문제로 설명될 수 있다. 즉, 특정 전송 파워에 대해, 이용가능한 데이터 속도(처리율)는 전송자로부터 거리가 멀어질수록 감소한다. 이런 특성은 적용 프로토콜이나 주파수 영역을 불문하고 발생한다. 일단 주파수가 최대 허용 전력에 도달하면 전송거리에 따라 데이터 속도는 감소하게 된다. 전송 파워는 각 사용자 장치의 이용 전력에도 영향을 받는다^{[11][6]}.

메쉬 네트워크는 중간 노드의 홉핑의 도움으로 거리가 먼 양단간에 대하여도 주파수 영역을 제공하고 높은 데이터 속도를 보장한다. 각 노드 사이의 거리(한 홉거리)는 양쪽 송신단과 수신단 사이의 거리보다 짧고 각 홉에서의 전송은 송/수신단 사이의 직접적인 전송보다 데이터 속도도 훨씬 빠르다. 이런 특징으로 메쉬 네트워킹은 거리가 매우 먼 양단간에도 고속의 다운로드와 업링크를 제공할 수 있게 된다.

또한 무선 메쉬 네트워크에서 각 노드들은 중간 노드의 홉핑의 도움으로 통신하므로 바로 이웃 노드까지 짧은 거리의 통신만 하면 되고 이런 방식으로 매우 낮은 전송 파워 수준만을 사용할 수 있도록 한다. 따라서 이런 방식은 시스템 간의 간섭을 줄이고 스펙트럼이 고밀도로 재사용될 수 있도록 해준다.

마지막으로 무선 메쉬 네트워킹은 non-line of sight의 문제와 혼잡 제어의 문제를 해결해 준다. 중간 노드를 통한 홉핑은 메쉬 네트워크에서 라우팅이 장애 지역을 피해갈 수 있도록 해주며 지역적인 네트워크 혼잡을 피할 수 있도록 한다.

메쉬 네트워크의 이런 특징은 다양한 프로토콜의 무선 메쉬 네트워크가 등장할 수 있도록 한다.

2.2. 무선 메쉬 네트워크의 구조

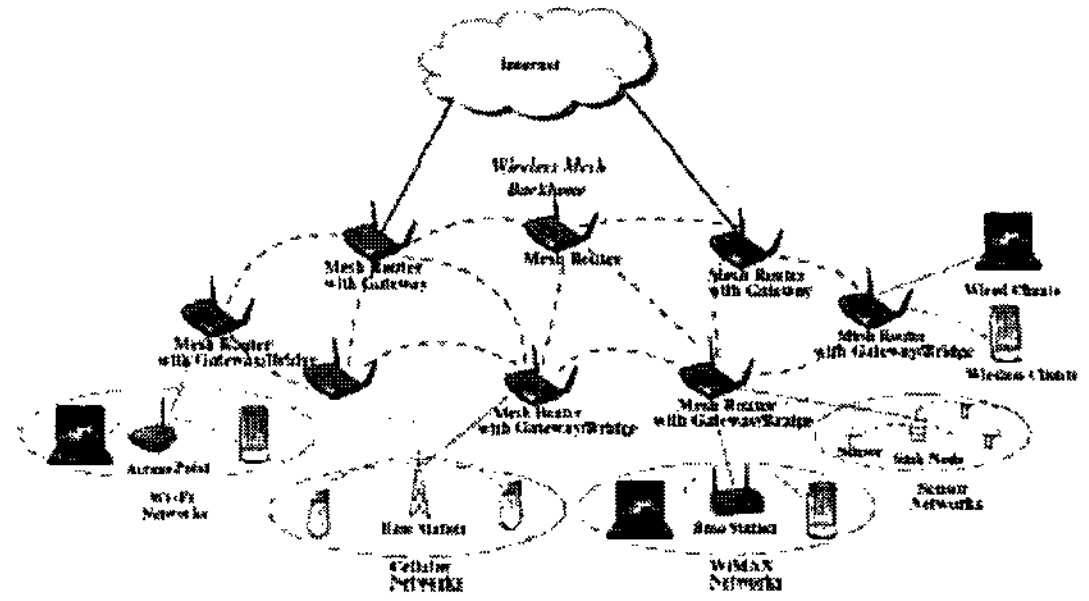
다양한 종류의 무선망들이 더 나은 서비스를 제공하기

위해 다음 세대로 진화함에 따라, 최근에는 주요 기술의 하나인 무선 메쉬 네트워크가 등장하였다. 무선 메쉬 네트워크는, 노드들이 메쉬 라우터와 메쉬 클라이언트를 구성하고 각 노드들은 호스트로서 동작하면서 동시에 라우터로서도 동작하여 목적지 노드가 소스 노드의 직접적인 무선 전송 범위 내에 있지 않은 경우에도 패킷을 전달할 수 있도록 중간 노드들이 패킷을 전달해 주는 역할을 한다. 무선 메쉬 네트워크는 동적으로 자가 조직되고 자가 구성되어 애드혹 네트워크를 구성하는 것처럼 네트워크 내의 노드들이 서로 자발적으로 메쉬 연결을 설정하여 관리한다. 이러한 특징은 무선 메쉬 네트워크에 저비용으로 간단하게 네트워크를 설치, 관리하고 신뢰성 있는 서비스를 제공하는 등의 많은 이점을 제공한다^{[1][2][4]}.

데스크탑, 랩탑, PDA, 포켓PC, 전화기와 같은 전통적인 노드들에 무선 네트워크 인터페이스 카드(NIC)가 장착된 경우, 이들은 무선 메쉬 라우터에 직접 연결될 수 있다. 무선 NIC 카드가 없는 경우는 이더넷을 통해 무선 메쉬 라우터에 연결되어 무선 메쉬 네트워크에 접속할 수 있다. 그러므로 무선 메쉬 네트워크는 사용자들이 언제든지 네트워크에 접속할 수 있게 하는 좋은 방법이 된다. 또한 메쉬 라우터에 포함된 게이트웨이/브릿지 기능은 무선 메쉬 네트워크가 다양한 기존의 네트워크(셀룰러망, WiMAX 등)들과 연동되는 것을 가능하게 한다. 따라서 무선 메쉬 네트워크와의 연동은 기존의 네트워크의 사용자들에게 기존의 네트워크만으로는 제공할 수 없었던 더 풍부한 네트워크 서비스를 제공할 수 있게 한다^{[1][2][3]}.

무선 메쉬 네트워크는 광대역 홈 네트워킹, 커뮤니티 네트워킹, 기업 네트워킹, 빌딩 자동화 등 많은 응용을 가능하게 하는 기술이며 인터넷 서비스 제공자(ISP)나 전송 서비스 사업자들에게 저비용의 투자로 신뢰성 있는 무선 광대역 서비스를 제공할 수 있도록 하는 기술이 된다. 무선 메쉬 네트워크가 가지는 자가 조직, 자가 구성의 특징은 무선 메쉬 네트워크가 필요에 따라 노드 확장 등이 손쉽게 이루어 질 수 있도록 하며 노드가 추가될 때마다 사용자에게 대하여 네트워크 운영의 신뢰성에 문제없이 연결성 제공도 함께 증가하게 된다.

무선 메쉬 네트워크는 메쉬 라우터와 메쉬 클라이언트의 두 가지 종류의 노드로 구성됨에 따라 전통적인 무선 라우터로서 게이트웨이/라우터를 위한 라우팅 기능보다 무선 메쉬 라우터는 메쉬 네트워크를 지원하는 부가적인 라우팅 기능을 가진다. 메쉬 네트워킹의 융통성을 향상시키기 위해서 메쉬 라우터는 다양한 종류의



[그림 2] 무선 메쉬 네트워크의 구조⁽¹⁾

무선 액세스 기술을 지원하기 위해 여러 무선 인터페이스가 장착된다. 기존의 무선 라우터와 비교하여 무선 메쉬 라우터는 멀티-홉 통신을 통해서 낮은 전송 파워로도 동등한 커버리지를 갖는다. 더불어 메쉬 라우터에서 medium access control(MAC) 프로토콜은 멀티-홉 메쉬 환경에서 더 나은 확장성을 보여준다. 이런 차이에도 불구하고 메쉬 라우터와 기존의 무선 라우터는 유사한 하드웨어 플랫폼을 기반으로 제작된다. 메쉬 라우터는 전용의 컴퓨터 시스템을 기반으로 구성되며 메쉬 클라이언트는 메쉬 네트워킹에 필요한 기능을 포함하며 라우터로서도 동작할 수 있다. 또한 메쉬 클라이언트는 하나의 무선 인터페이스만을 가지므로 메쉬 클라이언트에 대한 하드웨어 플랫폼이나 소프트웨어 구조는 메쉬 라우터 보다 훨씬 단순하다. 다양한 장치가 메쉬 클라이언트가 될 수 있어서 노트북 컴퓨터나 데스크탑 PC, PDA, IP phone, RFID 리더기, 빌딩 자동화 제어 시스템 등 많은 장치가 가능하다. 무선 메쉬 네트워크의 구조는 [그림 2]에 보여준다.

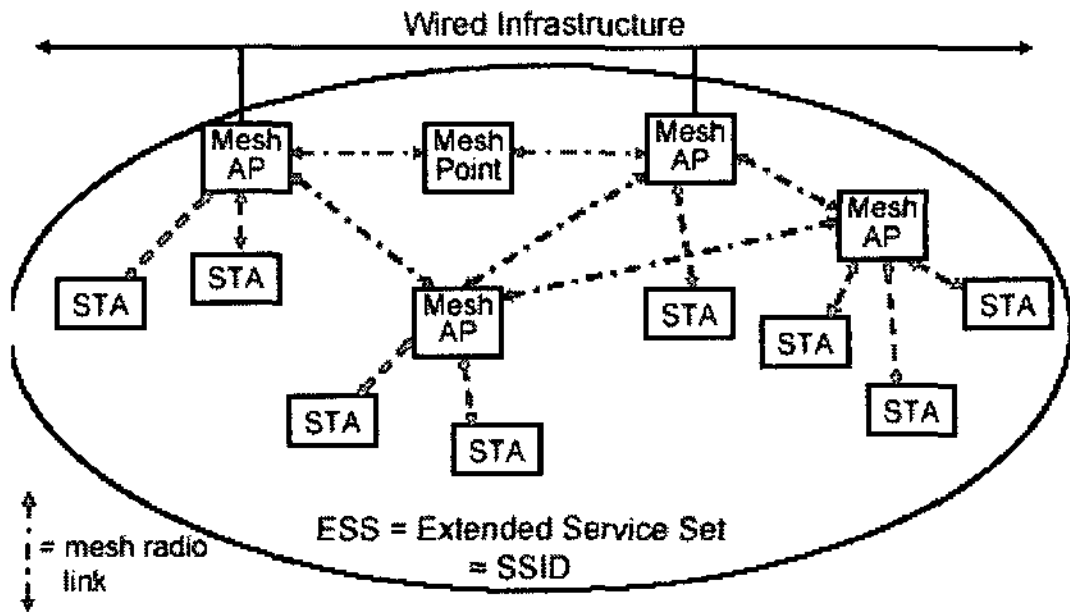
메쉬 네트워크의 장점은 다음과 같다.

- 신속한 네트워크 설치와 저비용의 backhaul
- 라인 설치가 어려운 지역에 대한 손쉬운 영역확장
- Self-healing, resilient, extensible
- 멀티-홉 전송으로 인한 영역 확장
- 고속의 대역폭 제공
- 저전력 전송으로 인한 전력사용의 효율성

III. 무선 메쉬 네트워크 관련 표준화 동향

3.1. 무선랜 기반의 무선 메쉬 네트워크 표준 (IEEE 802.11s)

IEEE 802.11s는 2003년 9월 IEEE 802.11의 스터디



(그림 3) IEEE 802.11s의 무선 메쉬 네트워크 구조⁽⁴⁾⁽⁵⁾

그룹으로 시작되어 2004년 7월에 태스크 그룹이 되었다. 2005년 7월부터 15개의 제안에 대한 검토를 거쳐 “SEE-MESH”와 “Wi-Mesh”의 두 가지 제안이 2006년 1월에 통합안으로 채택되었으며 2006년 3월에 표준의 초안으로 발표되었다. 이 초안은 Draft D1.0으로 2006년 11월 Letter Ballot 단계에 들어갔으나 75% 이상의 승인을 얻는데 실패하였다. 태스크 그룹은 이전의 Letter Ballot에서 지적된 의견을 수용하여 2007년 7월 초안 D1.06을 발표하였다⁽⁴⁾⁽⁵⁾⁽⁷⁾.

IEEE 802.11s mesh network에서 장치는 Mesh Point(MP)로 명명된다. MP들은 서로 메쉬 링크를 구성하고 라우팅 프로토콜을 사용하여 메쉬 경로를 생성한다. IEEE 802.11s에서는 기본 라우팅 프로토콜로 Hybrid Wireless Mesh Protocol(HWMP)를 적용하며, HWMP는 AODV와 트리 기반의 라우팅은 OLSR의 조합으로 이루어진 라우팅 프로토콜이다⁽⁴⁾⁽⁵⁾⁽⁷⁾.

MP는 네트워크의 다른 장치들과 통신하기 위해 메쉬 서비스를 사용하는 기본 장치가 되며 동시에 802.11의 Access Point(AP)가 되어 다양한 모바일 클라이언트들에게 메쉬 네트워크에 대한 액세스를 제공할 수도 있다.

또한 MP들은 게이트웨이 역할을 수행하여 메쉬 포털을 통하여 802.3 네트워크로의 액세스를 제공할 수도 있다. 어떤 경우이든 IEEE 802.11s는 외부 주소를 인식하는 end-point로서 비메쉬 기반의 802 장치에 대해 addressing을 제공하는 프록시 기능을 제공할 수도 있다. 더불어 IEEE 802.11s에서는 혼잡 제어와 전력 제어에 필요한 메커니즘도 포함하고 있다.

3.2. IEEE 802.16j에서의 메쉬 네트워크

IEEE 802.16j(Mobile multi-hop relay, MMR) 표준

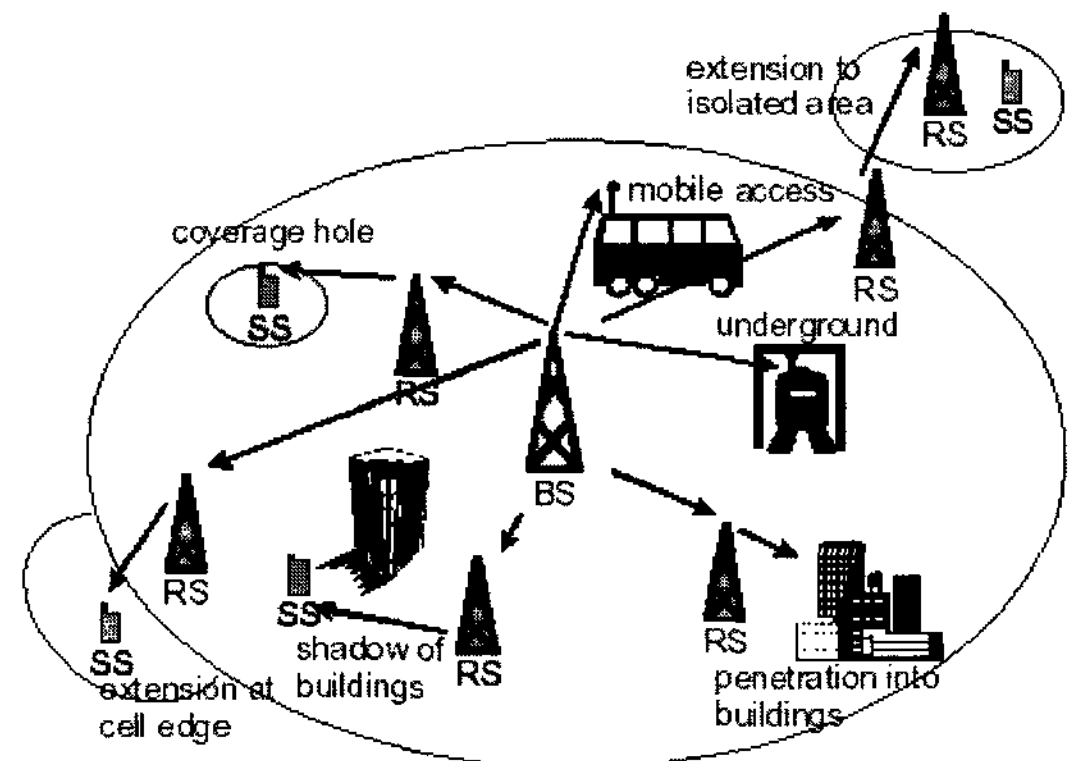
은 RS(Relay Station)을 도입하여 기존의 802.16-2005 제품의 성능을 향상시키기 위하여 등장하였다. 이 표준의 기본 목표는 다음과 같다⁽⁶⁾⁽⁷⁾⁽⁸⁾.

- 커버리지 영역의 확장
- 전송 처리율과 시스템 용량 확대
- 가입자 단말(SS)의 전력수명 연장
- RS의 복잡도 최소화

이 표준은 또한 IEEE 802.16-2004과 IEEE 802.11e와의 호환을 고려하고 있으며 이전의 802.16 SS 단말들이 MMR이 RS가 추가된 인프라에도 동작할 수 있도록 하는 것을 목표로 한다. 반면에 BS(Base Station)에서는 약간의 수정을 허용하여 RS와 통신이 가능하도록 하며, 여러 RS로부터 수신되는 트래픽을 수집할 수 있도록 한다⁽⁶⁾⁽⁷⁾⁽⁸⁾.

네트워크가 최고의 성능을 제공하기 위해서는 RS의 성능이 좋아야 하며 RS가 놓이는 위치도 잘 선택되어야 한다. 이 표준에서 정의하는 RS는 고정형, 노매딕형, 이동형의 세 가지 종류가 있다. 고정형 RS는 말그대로 정해진 위치에 영구적으로 설치된다. 노매딕형 RS는 사용자의 세션이 유지될 수 있는 시간동안 정해진 위치에 고정되어 그 기능을 제공한다. 이동형 RS는 예를 들면 버스나 기차 같은 차량에 설치되어 이동성을 가지는 것을 말한다. 경우에 따라 SS도 릴레이 스테이션으로 동작할 수도 있다⁽⁶⁾⁽⁷⁾⁽⁸⁾.

이 표준의 링크의 무선 인터페이스는 OFDMA PHY를 기반으로 하며 MAC(Medium Access Control) 계층은 BS-RS간이나 RS-RS간의 멀티-홉 통신을 지원하는데 필요한 기능들이 추가된다. 다음 [그림 4]는 모바일



(그림 4) 802.16j 사용 시나리오⁽⁶⁾⁽⁷⁾⁽⁸⁾

멀티홉 릴레이 스테이션의 예상 시나리오를 보여준다. [그림 4]에서 커버리지 영역 밖에 있는 SS나 빌딩으로 인해 커버리지가 가려져서 path loss가 발생하여 제대로 동작하지 않는 단말이 RS의 도움으로 제대로 기능을 동작할 수 있는 경우가 보여진다^{[6][7][8]}.

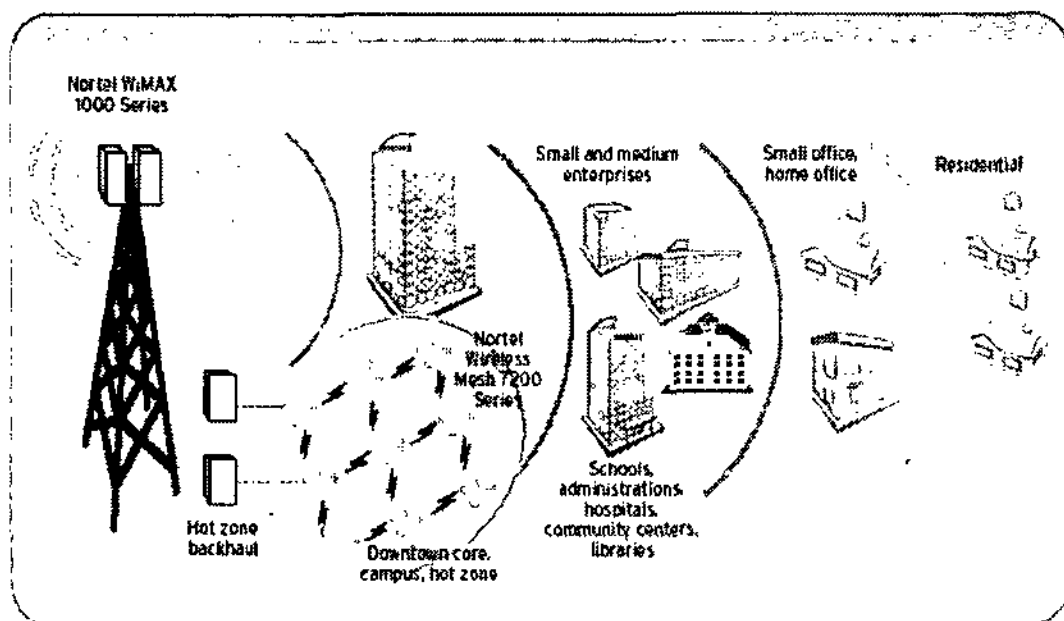
릴레이 기술은 셀 경계나 고립된 영역의 커버리지를 확장하는 경우에도 사용될 수 있으며 주파수가 미치지 않는 실내에 서비스를 제공하는 데에도 사용될 수 있다. 이외에도 버스나 기차, 페리 같은 이동 수단에도 고정 액세스나 이동 액세스를 제공할 경우에도 사용될 수 있다.

이 표준은 라우팅이나 스케줄링, 라디오 자원 관리, 전력 제어, QoS, 주파수 사용, 미래 안테나 기술의 사용, 네트워크 관리, RS들 간의 보안 문제 등, 아직도 많은 기술들이 추가로 연구되어야 한다.

IV. 메쉬 네트워크 관련 업체 현황 및 구축 현황

이 장에서는 메쉬 네트워크 기술 개발 관련 업체와 구축 현황에 대하여 살펴볼 것이다.

무선 광대역 통신에서의 메쉬 네트워크에 대한 개발은 Tropos, Strix, Skypilot, 시스코, 모토롤라, 노텔 등의 기업이 WiFi 기반의 Mesh 제품을 개발하여 Municipal Wireless(도시 전 지역에서 WiFi 접속이 가능한 무선망) 시장에서 각축 중이며, 삼성, 모토롤라, 노텔, 인텔, 알카텔, KDDI 등의 기업이 IEEE 802.16j 표준화에 적극 참여중이다. 또한 Belair는 WiMAX를 backhaul하여 WiFi mesh를 결합한 제품을 발표하였다. 홈 메쉬 네트워크 영역에서도 Sonos가 최근 WiFi mesh 기반의 멀티룸 디지털 오디오 전송 시스템을 출시하였으며, 애플과 Buffalo가 WiFi AP에 무선 메쉬네트워크의 초기 형태인 무선 분배 시스템 기능을 탑재하여 발표하였다.

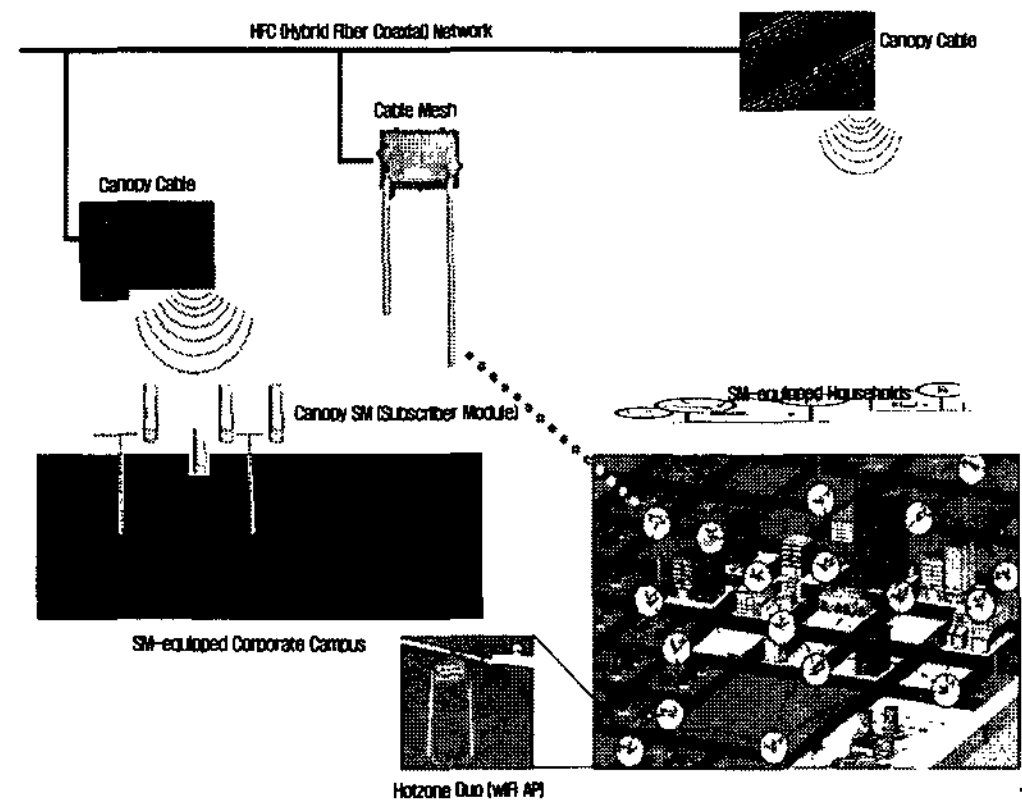


(그림 5) Nortel의 Municipal Wireless network 구성^[17]

4.1. 메쉬 네트워크 관련 업체 현황

4.1.1 모토롤라의 케이블 무선 네트워크 구성

모토롤라는 케노피를 이용하여 [그림 6]과 같은 케이블 무선 네트워크를 구성하여 municipal network를 제공하고 있다. 모토롤라의 네트워크는 500kpbs의 속도로 고정/노매딕/휴대용 WiFi 액세스를 제공하는 것을 목표로 한다. 케노피는 점대점 연결의 경우 OFDM으로 30/60/150/300 Mbps의 속도로 200km까지의 LOS(Line of Sight)와 10km의 NLOS(Non-Line of Sight)를 제공하며 점대다 연결의 경우에는 TDMA/TDD를 사용하여 20Mbps의 속도로 3.2km의 LOS를 제공한다^[16].

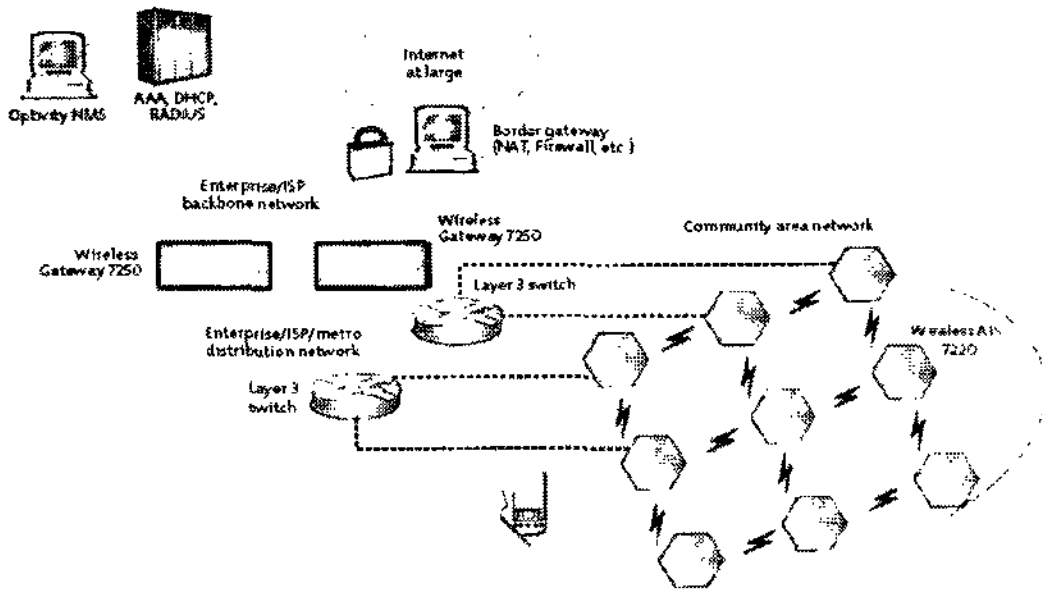


(그림 6) 모토롤라의 케이블 무선 네트워크^[16]

4.1.2 Nortel의 WiFi 메쉬 네트워크

Nortel의 무선 메쉬 네트워크 솔루션은 유선망에 대하여 무선으로 데이터에 대한 backhaul을 제공하기 위하여 peer-to-peer 기반구조를 사용한다[그림 7]. Nortel의 무선 메쉬 네트워크는 무선 access points, 무선 게이트웨이, 무선 메쉬 관리 플랫폼의 세가지 요소로 구성된다. 무선 AP는 클라이언트 액세스와 트래픽 분배의 기능을 수행한다. 클라이언트 액세스는 2.4GHz 스펙트럼의 802.11b/g 접속을 제공하고 5GHz 대역의 802.11a에 걸쳐서 전송이 수행된다^[17].

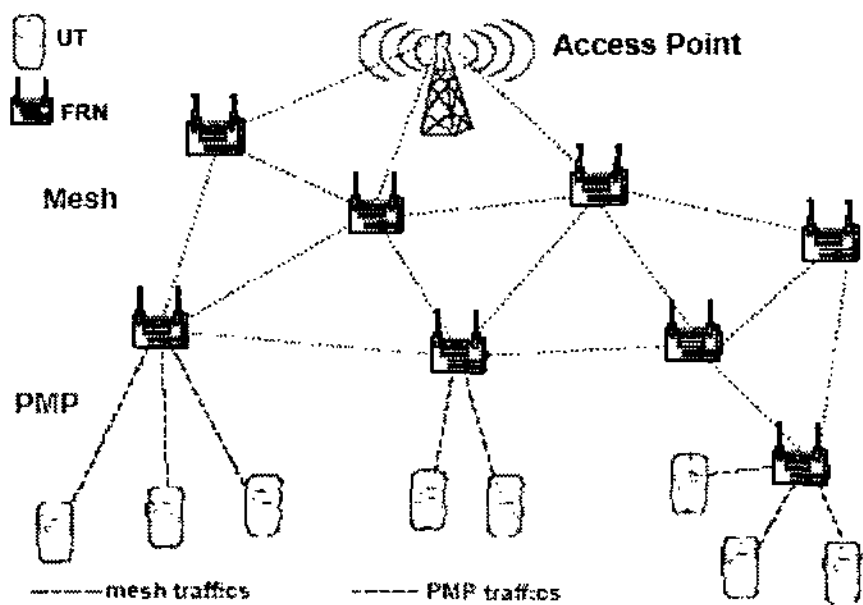
무선 게이트웨이는 기업의 유선망이나 망사업자에게 메쉬 네트워크를 통한 IP 서브넷을 제공하며 이를 위한 라우팅, 메쉬 전송 링크의 보안, firewall, 무선 사용자의 이동성 제공 기능을 수행한다.



(그림 7) Nortel의 무선 메쉬 네트워크 구성⁽¹⁷⁾

4.1.3. WINNER의 무선 멀티홉 메쉬 네트워크

WINNER에서는 2005년 4G 환경에서 메쉬 릴레이 기점에 대한 연구를 시작하여 2006년 말 개념을 확정하고 2009년까지 스펙을 확정하고 평가를 완료할 예정이다. WINNER에서 제안하는 무선 메쉬 네트워크의 개념은 다음 [그림 8]과 같다⁽⁹⁾.

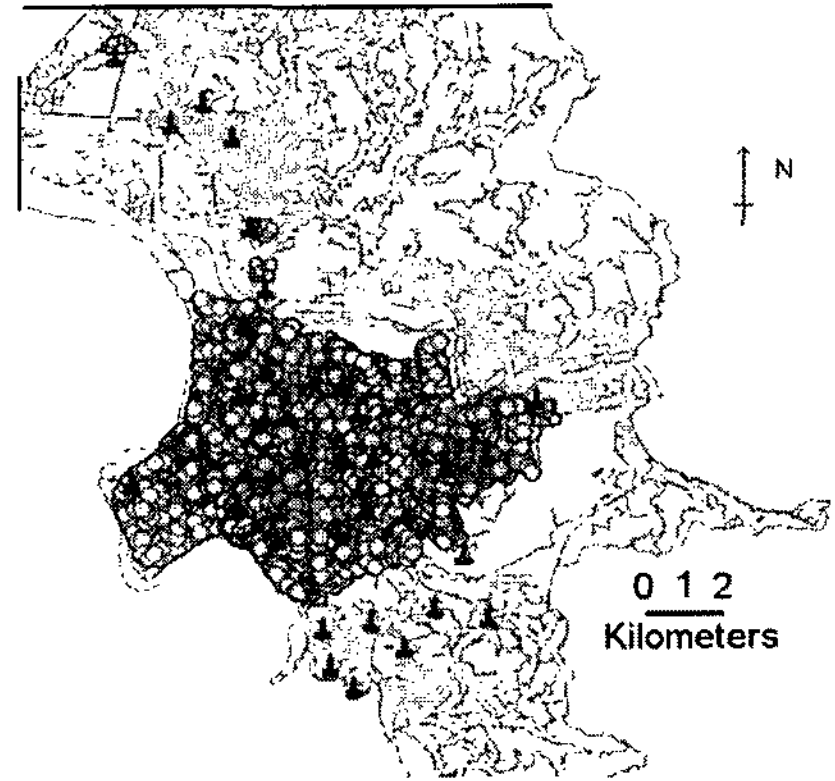


(그림 8) WINNER의 무선 멀티홉 메쉬 네트워크⁽⁹⁾

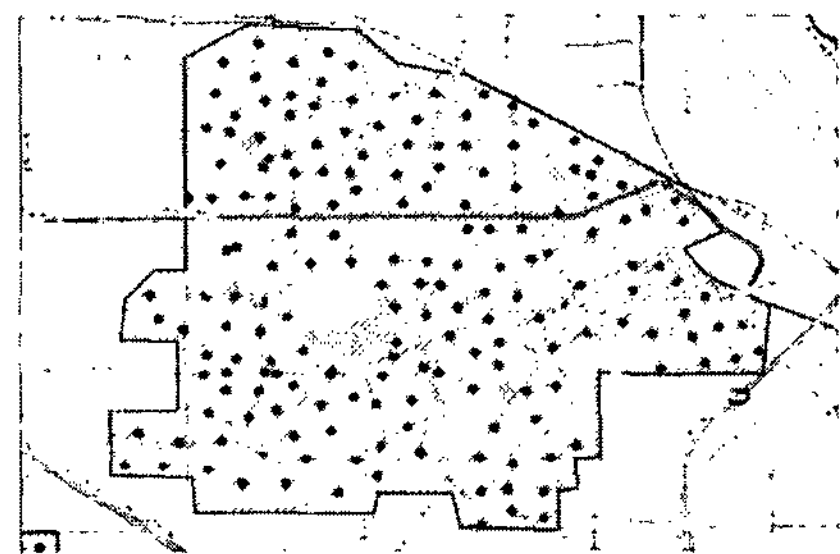
4.2. 메쉬 네트워크 구축 현황

Nortel에서는 [그림 9]와 같은 타이페이시에 도시 규모의 광대역 무선랜을 2005년 12월 구축하였다. 규모는 28.2 km²에 2,300개의 AP를 설치하고 50%의 도시 인구를 커버하며 월 13달러정도의 사용료를 지불하도록 한다⁽¹⁷⁾.

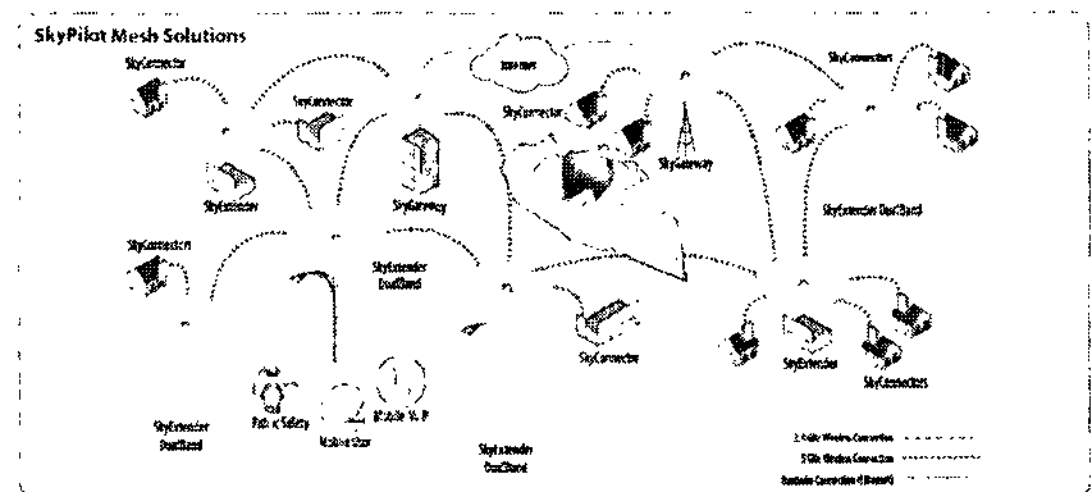
Skypilot은 미국 캘리포니아의 Cupertino와 Santa Clara지역에 무선 메쉬 네트워크를 구축하여 20mile² 넓이의 지역에 300개의 노드를 설치하였다[그림 10]. 이 네트워크는 하향링크로 1Mbps, 상향 링크로 256kbps를 보장하며 월 19.95달러의 사용료를 지불한다.



(그림 9) 타이페이시의 메쉬 네트워크 구축현황⁽¹⁷⁾



(그림 10) 캘리포니아 지역의 메쉬네트워크 구축현황⁽¹⁸⁾



(그림 11) Skypilot의 메쉬 네트워크 솔루션⁽¹⁸⁾

V. 메쉬 네트워크에서의 보안 기술

5.1. 무선 메쉬 네트워크에서의 보안 이슈

무선 메쉬 네트워크를 구축하고 관리하는 데 있어서 보안은 중요한 이슈가 된다. 무선랜의 경우 AAA (Authentication, Authorization, and accounting)와 같은 중앙 관리 시스템을 이용하여 인증 등의 보안 관리가 가능하지만, 무선 메쉬 네트워크에서는 중앙 집중식 시스템의 적용이 확장성의 문제로 인하여 적합하지 않다. 모바일 애드혹 네트워크와 유사하게, 무선 메쉬 네트워크에서는 무선 MAC에서의 채널과 노드의 취약성

과 중앙집중식 관리 시스템의 부재, 네트워크 토폴로지의 동적 형성 등으로 인하여 네트워크가 공격당하게 쉬운 구조이며 효율적이고 확장성 있는 보안 시스템의 적용이 취약한 상황이다. 공격자는 라우팅 정보를 공격할 수 있고, 라우팅 경로 설정에 참여하면서도 라우팅 테이블을 의도적으로 제때에 갱신하지 않아서 패킷의 전송을 방해할 수도 있다. 또한 공격자가 네트워크에 침입하여 합법적인 노드인 척 가장하여 라우팅 프로토콜에 따르는 요구사항을 수행하지 않을 수도 있다. 악의적인 노드가 보안 구멍을 만들어서 합법적인 노드들 사이의 원활한 흐름을 방해할 수도 있다^{[1][10][12][13]}.

또한 무선 메쉬 네트워크에는 기반구조가 존재하지 않으므로 신뢰 정점을 형성할 수가 없으므로 노드 상호간에 신뢰를 구축하는 과정이 중요하다. 키 관리도 네트워크 보안의 중요 요소인데, 무선 메쉬 네트워크 환경에서는 키 관리가 매우 어렵다. 그 이유는 비밀키를 관리할 서버나 신뢰 구조가 없기 때문이다. 따라서 무선 메쉬 네트워크에서는 분산된 방법을 적용한 키관리 메커니즘이 필요하다. 자가 조직으로 네트워크가 구성되는 방법에서 노드들 사이에 비밀키를 분배하고 관리하는 방법이 많이 연구되고 있어서 인증서를 사용하거나 인증서 체인을 통하여 상호 신뢰 관계를 구축하는 방법들이 제안되고 있다^{[1][10][12][13]}.

무선 메쉬 네트워크의 보안 기능을 강화하기 위하여 보안기반의 라우팅이나 MAC 프로토콜을 네트워크 프로토콜 내에 탑재하거나, 공격을 모니터하고 재빨리 대응하기 위하여 위한 보안감지 및 대응 시스템을 개발하는 것이 필요하다. 무선 메쉬 네트워크에서의 공격은 여러 프로토콜에 걸쳐서 동시에 수행되므로 멀티-프로토콜에 걸친 보안 방법의 개발이 필요하다.

Cross-layer 프레임워크에 걸친 보안 모니터링 시스템 개발도 필요하다. 실질적인 보안 감지 시스템을 어떻게 설계하고 개발할 것인지 하는 것은 향후의 과제이다.

5.2. 802.11s에서의 보안 이슈

이 절에서는 IEEE 802.11s에서 논의되고 있는 보안 주제에 대하여 다루고자 한다.

현재 IEEE 802.11s에서는 기본적인 IEEE 802.11i 기반의 보안 메커니즘이나 그 확장을 적용하는 것을 정의하고 있다. 그러나 802.11i의 경우 링크 보안에 대한 내용을 주로 다루고 있으므로 무선 메쉬 네트워크가 직

면하는 다양한 보안 문제를 모두 커버할 수 없는 상황이다. 따라서 다음과 같은 기능이 추가로 필요하다^{[4][5]}.

- 이웃하는 mesh point(MP)와 mesh AP 사이에 association와 인증에 대한 메커니즘
 - MP가 안전한 무선 메쉬 네트워크에 참가할 수 있어야 함
 - 디바이스가 무선 메쉬 네트워크에 존재하는 다른 노드들을 인증하는 방법 (rogue MP의 문제)
 - 무선 메쉬 네트워크에 있는 노드들이 새로 참가하는 MP를 인증하는 방법
- MP와 mesh AP 사이에 교환되는 제어 메시지와 메쉬 관리 메시지(라우팅과 토폴로지 정보 등)를 보호하는 메커니즘
 - 안전한 패킷 전달을 위한 키공유와 키 분배 메커니즘

802.11s에서 논의되고 있는 보안 모델은 현재 802.11i의 기술을 재사용하는 것을 목표로 하며 인증된 MP만이 무선랜 메쉬 서비스에 참가하여 신뢰 기반을 마련하고자 하며 분산 인증 방식이나 중앙 집중식 인증 방식의 적용하고자 하는데, 이 때 각 MP는 이웃에 대하여 인증자나 피인증자가 될 수 있다^{[4][5]}.

각 MP는 브로드캐스트와 멀티캐스트를 수행하기 위해 그룹에 대한 세션키를 소유하여야 하며 유니캐스트를 위해 상대노드와 한 쌍의 세션키를 소유하여야 한다.

이 표준에서 고려하는 메쉬 네트워크의 보안은 트랜스포트 계층에서의 보안 기능이며 내부 라우팅이나 외부 라우팅에서의 보안과 패킷 전송에서의 보안은 다루지 않는다. 메쉬 네트워크의 트랜스포트 계층과 메쉬 구성에서의 보안을 강화하는 것은 권한을 갖지 않는 디바이스가 메쉬 구조를 통해 데이터를 보내거나 받는 것을 방지하여, 이웃한 MP들 사이에 데이터 전송을 안전하게 하는 것을 의미한다. 메쉬 기반의 안전한 트랜스포트를 설정하기 위해 필요한 메쉬 구성에서의 기능은 다음과 같다^{[4][5]}.

- 이웃한 MP들 사이에 상호 인증
- 세션키와 브로드캐스트키를 생성, 관리
- 링크를 통해 전송되는 메시지 위조와 재전송 공격을 감지
- 링크에 걸쳐서 데이터의 무결성 보장

이 과정에서 필요한 인증과 초기 키 관리는 기본적으로 802.11i와 802.1X를 재사용하여 안전한 비밀키 분

배(PMK) 메커니즘을 제공하고자 한다. 메쉬에서 PMK는 메쉬 네트워크에 참가하는 MP에게 권한을 부여할 토큰을 다루는 내용을 포함한다. 우선 메쉬 네트워크에 참가하기 위해 이용가능한 메쉬를 찾아야 하며 이 과정에서 이용가능한 인증키 관리 프로토콜을 파악할 수 있어야 한다. 그 결과에 따라 peer link를 사용하여 보안에서의 역할과 정책에 대한 협상을 수행하여야 한다. 키 관리 메커니즘의 목표는 세션키 갱신이 이루어져야 하며 상대 PMK 소유자가 생존해 있음을 증명할 수 있어야 한다. 또한 세션키를 대응하는 MP와 연결할 수 있어야 하고 세션키의 사용을 동기화하고 그룹키를 분배할 수 있어야 한다.

VI. 결 론

다양한 종류의 무선망들이 더 나은 서비스를 제공하기 위해 다음 세대로 진화함에 따라, 최근에는 주요 기술의 하나인 무선 메쉬 네트워크가 등장하였다. 무선 메쉬 네트워크는 메쉬 라우터와 메쉬 클라이언트로 구성되며 저비용의 네트워크 설치와 용이한 네트워크 운영과 관리로 높은 신뢰성 제공, 용량 확장과 영역 확장의 편이성, 자가 구성 및 자가 복구 능력의 특징을 가진다. 이러한 특징으로 인하여 무선 메쉬 네트워크는 최근 무선랜 기반의 무선 메쉬 네트워크 구성, WiMAX에서의 모바일 무선 멀티-홉 릴레이 구조, 홈네트워크 구성 등에서 채택되고 있으며 IEEE 802.11s, IEEE 802.16j, IEEE 802.15.4 기반의 WPAN등에서 이에 대한 표준화를 진행 중이다.

많은 장점에도 불구하고 무선 메쉬 네트워크는 아직 QoS를 보장하기 위해 멀티-홉 처리로 인해 발생하면 지연시간 문제와 추가되는 네트워크 장비의 비용, 네트워크 설계와 관리 비용의 증가, 라우팅 기능과 시그널링을 지원에 따른 비용추가, 라이선스 주파수 대역에서의 간섭 회피를 위한 프레임 구조의 필요성과 메쉬 네트워크 진입 부분에서의 대용량의 필요성 문제 및 MP간의 시간 동기화의 문제 등이 향후 과제로 남아 있다. 이와 같은 문제의 해결은 무선 메쉬 네트워크의 성능을 향상시키고 무선 메쉬 네트워크의 진화와 시장 점령을 촉진하는 요인이 될 것이다.

참고문헌

[1] I. F. Akyildia, X. Wang and W. Wang, "Wireless

mesh networks: a survey", *Computer Networks*, Vol. 47. pp. 445-487, Jan. 2006.

[2] Jain, R. : *Wireless Mesh and Multi-Hop Relay network*, 2006

[3] H. Aoki, H. Takeda, K. Yagyu and A. Yamada, "IEEE 802.11s Wireless LAN Mesh Network Technology", *NTT DocoMo Technical Journal*, Vol. 8. No.2

[4] W. Steven Conner, J. Kruys, K. Kim and J. C. Zuniga, *IEEE 802.11s Tutorial*, Nov. 2006

[5] IEEE 802.11 WG, *IEEE 802.11s/D0.01*, March 2006. <http://www.802wirelessworld.com>

[6] IEEE 802.16 Mobile Multihop Relay Study Group : *Recommendations for the Scope and Purpose of the Mobile Multihop Relay Task Group*, Nov. 2005

[7] P. Mach, R. Bestak, "Wireless Mesh and Relay Network", *Fireworks*, 2006

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

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

[10] N. B. Salem and J. P. Habaux, "Securing Wireless Mesh Network", *IEEE Wireless Communications*, Apr. 2006. pp. 50-55

[11] J. D. Camp and E. W. Knightly, "The IEEE 802.11s Extended Service Set Mesh Networking Standard"

[12] W. Choi, T.S. Shon, H.H. Choi and Y. Lee, "Designing a Novel Unlicensed Monadic Access Relay Station in IEEE 802.16-based Wireless Access Networks," *IEEE VTC 2007*.

[13] 이용, 이구연, "IEEE 802.16j 기반의 모바일 멀티 홉 릴레이에서의 혼합형 인증 기법 대한 연구," *대한전자공학회 논문지 제44권 TC편 제10호*, 2007년 10월 pp 127 - 136

[14] www.belainetworks.com

[15] www.strixsystems.com

[16] www.motorolar.com

[17] www.nortel.com

[18] www.skypilo

〈著者紹介〉

**이 용 (Lee Yong)**

정회원

1997 : 연세대학교 컴퓨터과학과
(석사)2001 : 연세대학교 컴퓨터과학과
(박사)

1993-1994 : 디지털정보통신연구소

2001 ~ 2003 : 한국정보보호진흥
원 선임연구원2004 ~ 2005 : 코벨대학교 방문연
구원2005 ~ 2007 : 삼성전자 통신연구
소 책임연구원2007 ~ 현재 : 충주대학교 전자통
신공학전공 조교수<관심분야> Mobile and Wireless
Security, Ubiquitous Sensor Net-
work, Wireless Mesh Network,
Mobile Ad hoc network**이 구 연 (Lee Goo Yeon)**

정회원

1988 : KAIST 전기및전자공학과
(석사)1993 : KAIST 전기및전자공학과
(박사)

1993-1996 : 디지털정보통신연구소

1996 : 삼성전자

1997-현재 : 강원대학교 컴퓨터학
부 교수<관심분야> 이동통신, 네트워크보
안, 초고속통신망, ad-hoc 네트워크