유비쿼터스 및 Ad Hoc 네트워크 망에서의 정보보호 분석

임지형* 이병길** 김현곤*** 정교일**** 양대헌*****

IT 환경이 발달하면서 대두되고 있는 유비쿼터스 컴퓨팅 환경은 기존의 컴퓨팅 환경과는 사뭇 다른 모습을 보여주고 있다. 기존처럼 사람이 기계를 배워 사용하는 방법이 아닌 기계가 사람의 행동 패턴을 인식하여 정보를 습득하는 기술은 부합되는 여러 기술들, 즉 센서, 프로세서, 통신, 인터페이스, 보안의 발달로 이룰 수 있게 되었다. 하지만 기존에 장소에 얽매여 데이터를 주고받을 수 있는 공간 제한형 환경이 아닌 개방형 환경은 기술 사용에 대한 편리성 못지 않게 개방된 환경이기 때문에 데이터에 대한 보호 문제가 발생한다. 이러한 서로 다른 컴퓨팅 환경을 이루는 장치들이 유선과 동일한 형태의 보안을 제공해야 하는 문제점과 개인의 정보를 어디까지 제공하고 보호해야 하는지 등의 보안 문제가 발생될 수 있다. ▧

목 차

* 인하대학교 정보통신대학원/대학원생
** ETRI AAA 정보보호연구팀/선임연구원
*** ETRI AAA 정보보호연구팀/팀장
*** ETRI 정보보호기반그룹/그룹장
**** 인하대학교 정보통신대학원/교수

I. 서 론

유비쿼터스(Ubiquitous)란 '언제, 어디에서나 존재한다'라는 뜻의 라틴어로, 유비쿼터스 컴퓨팅은 다양한 종류의 컴퓨터가 우리 주위에 내재되어 있어, 사용자가 장소에 구애 받지 않고 컴퓨팅 환경을 이용할 수 있는 컴퓨팅 환경을 지칭한다. 이러한 유비쿼터스 컴퓨팅은 1988년 Xerox사의 PARC(Palo Alto Research Center)의 연구책임자 Mark Weiser가 제시한 개념이다. 유비쿼터스 컴퓨팅에 대한 Mark Weiser가 제시한 주요 특징은 다음과 같다.

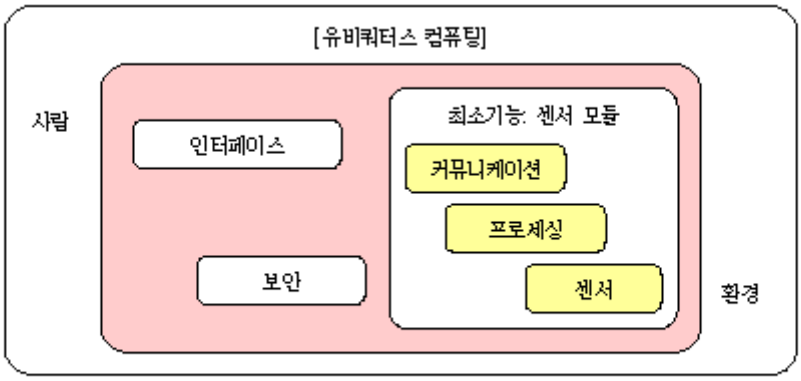
첫째, 유비쿼터스 컴퓨팅은 인간친화적인 기술이어야 하므로 사용자가 이들의 사용에 거부반응을 보이거나 방해 받지 않도록 우리 주위에 자연스럽게 파고들어야 한다는 의미로 이것을 "Invisible"이라고 한다.

둘째, 유비쿼터스 컴퓨팅은 현존하는 모든 컴퓨터뿐만 아니라 컴퓨팅 기능이 내재된 모든 컴퓨터를 연결 "Connected"해야 한다.

셋째, 사용자가 자신이 컴퓨터를 사용하는지 아닌지를 의식할 수 없는 환경을 구현하는 사용자 중심적인 환경을 구현해야 하며 이것을 "Calm"이라고 한다.

마지막으로 이러한 유비쿼터스 컴퓨팅은 가상 세계에서 이루어지는 작업이 아닌 현실 세계에서의 네트워크 연결을 의미하며, 이것은 실세계를 더욱 강화하는 의미로 "Real"을 지칭하고 있다.

이러한 환경을 구축하기 위해서는 센서, 프로세서, 커뮤니케이션, 인터페이스, 보안의 5가지 핵심 기술이 필요하다((그림 1) 참조).

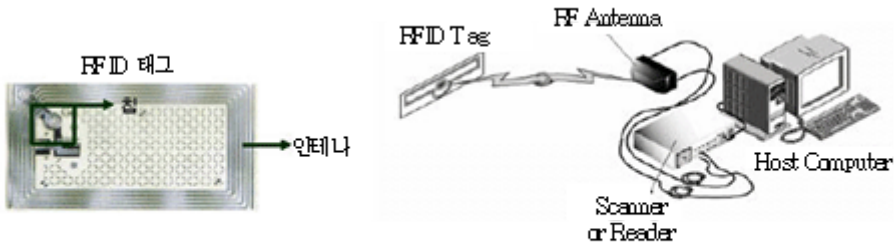


(그림 1) 유비쿼터스 컴퓨팅을 위한 기술 요소[1]

Ⅱ. 유비쿼터스 및 Ad Hoc 네트워크 기술

1. RFID

RFID(Radio Frequency IDentification)는 유비쿼터스 컴퓨팅 분야 중 센서 부분에 해당하는 기술로 일종의 능동형 센서의 역할을 담당한다. 이것은 인터넷이나 혹은 이와 유사한 환경의 네트워크를 통하여 태그가 부착된 아이템을 원거리에서 실시간 감지하는 개념이다. RFID 시스템은 태그(Tag, Transponder)와 이를 읽어 들이는 리더, 그리고 리더와 연결된 호스트 컴퓨터, 다시 이와 네트워크로서 연결된 백앤드 시스템으로 이루어져 있다((그림 2) 참조).



(그림 2) RFID 시스템의 구성[1]

이러한 RFID의 경우 태그와 리더기 관련 표준화가 진행 중에 있으며, ISO(국제표준화기구)/ IEC(국제전기표준회의)가 공동으로 표준화를 진행하고 있다. 그러나 국별 주파수가 다르고 표준부재에 따른 문제점이 노출되면서 주파수 대역에 관한 표준화가 문제의 표면으로 노출되어 있다.

RFID 시스템에서 사용하는 주파수의 경우 크게 세 가지 정도로 나눌 수 있다. 각각의 용도에 따라 100~500kHz, 10~15MHz, 850~950MHz/2.4~5.8GHz로 나눌 수 있는데 그 중 일찍부터 관심을 끌었던 주파수는 125kHz, 13.56MHz, 2.45GHz이다. 그러나 ITU-R에 의해 전 세계는 그 쓰임에 따라 유럽 및 아프리카(지역 1), 북남 아메리카(지역 2), 극동 및 오스트리아(지역 3)의 세 지역으로 나누었지만 사용하는 RFID의 주요 관심 분야라든지 요구사항이 다른 관계로 특정한 주파수를 할당하는데 어려움이 있다. 그런 이유로 현재 전세계에서는 8개의 주파수를 사용하고 있다. 특히 13.56MHz의 경우, 주요 RFID 제조회사들이 자신들의 태그에 이를 채택하고 있고 ISO15693에 지정되어 있는 등 전세계적으로 표준화가 진행 중에 있어 더욱 널리 쓰일 것으로 예상된다.

저대역에 속하는 100~500kHz의 경우 그 용도가 접근 제어(Access Control), 생물 인식(Animal Identification) 등에 주로 사용할 수 있으며 중간대역에 속하는 10~15MHz의 경우 액세스 콘트롤이나 스마트 카드 등에 이용할 수 있다. 고주파 대역인 2.4~5.8GHz는 사용 거리가 길고, 읽는 속도가 빠르다는 점을 이용하여 도로 위에 자동차를 모니터링하거나 고속도로 톨게이트의 하이 패스 시스템에 사용할 수 있다.

2. Ad Hoc Network

가. Ad Hoc 네트워크의 특징

Ad Hoc 네트워크는 기존의 네트워크와 같이 네트워크 인프라가 구축된 상태에서 통신을 수행하는 것이 아닌 인프라가 존재하지 않은 상태에서 각 단말들 상호간의 라우팅으로 데이터 송・수신 등의 통신 기능을 수행할 수 있는 형태의 네트워크를 말한다. 따라서 네트워크에 참여하는 각 단말들은 기지국이나 AP의 도움없이 자신들이 라우터, 서버의 역할 등을 모두 수행할 수 있어야 한다.

이러한 Mobile Ad Hoc 네트워크(MANET)의 특징은 다음과 같이 요약된다.

우선 MANET의 가장 큰 특징은 네트워크에 참여하는 노드들이 가지는 이동성을 들 수 있다. 이러한 노드들은 네트워크내에서 컴퓨팅 기능을 가지고 있는 호스트이며, 또한 다른 네트워크와 통신을 하기 위한 라우팅 기능을 가진 라우터로서 작동하여야 한다.

두 번째로, MANET은 동적인 네트워크 토폴로지를 가지게 된다. 이것은 이동성이라는 특징을 가지는 Ad Hoc 네트워크내의 노드들이 네트워크에서의 진입과 이탈이 자유롭기 때문에 발생하는 문제로 네트워크는 이러한 현상이 발생하더라도 항상 네트워크가 붕괴되지 않고 통신할 수 있는 상태를 유지하여야 한다.

세 번째로 MANET의 경우, 하나의 노드가 많은 기능을 선점하고 있는 것이 아닌, 여러 노드들이 제공하는 서비스를 분배하고 협력하여 제공하는 구조를 지녀야 한다.

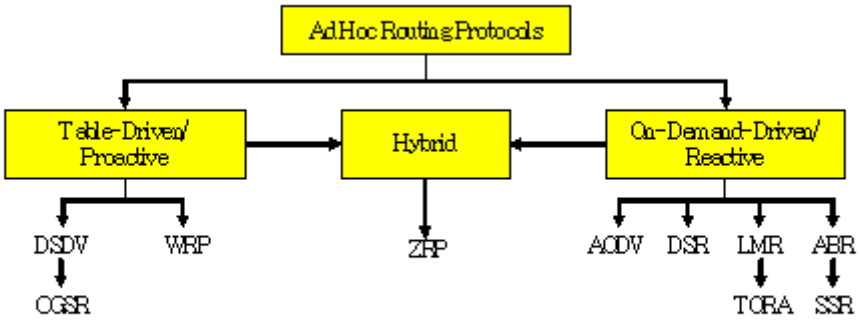
마지막으로 MANET은 불안정한 링크 특성을 가지게 된다. 이것은 무선을 사용함으로써 생기는 문제로, 데이터에 대한 전송거리와 전송대역폭에 제약을 받고, 전파간섭/다중링크로 인한 보안 문제를 야기한다는 의미가 된다.

이러한 특징을 가지는 MANET의 경우 인프라의 구성없이도 통신을 할 수 있다는 특성에 힘입어 주로 상용 시스템이 아닌 군사용 통신체계로의 연구가 이루어져 왔다. 군사용 통신망은 신속히 전개되는 기반구조이며, 제한되고 선택적인 접근만을 허용하기 때문에 이러한 형태에 적합하다.

현재 MANET은 IETF내의 MANET Working Group 내에서 이루어지고 있으며, 현재 그 특성상 주로 라우팅 프로토콜에 관련되어 표준화와 그 연구가 이루어지고 있다. 이것은 이동 단말이 가지는 특성에 힘입어 라우팅을 수행하기 위한 시간에 대부분의 노력을 들이기 때문이다.

나. Ad Hoc 라우팅 프로토콜

Ad Hoc 네트워크에서 사용되는 라우팅 프로토콜은 크게 3가지 형태로 구분될 수 있다((그림 3) 참조).



(그림 3) Ad Hoc Network Routing Protocol 형태[4]

Ad Hoc 네트워크에서 사용되는 라우팅 프로토콜은 미리 라우팅 정보를 수집해 두어 사용하는 테이블 관리 방식(Table-Driven 혹은 Proactive)과 라우팅 정보를 필요한 시기에 수집하는 요구 기반 방식(On-demand 혹은 Reactive), 마지막으로 테이블 관리 방식과 요구 기반 방식을 혼합한 하이브리드 방식으로 크게 나눌 수 있다.

테이블 관리 방식의 경우 일정 주기 동안 혹은 네트워크의 토폴로지가 변화할 때 라우팅 정보를 브로드캐스팅 함으로써 모든 노드가 네트워크의 정보를 유지하게 하는 방식으로, 주기적으로 제어 메시지의 broadcast를 수행해야 한다는 점과 라우팅 테이블을 관리해야 한다는 단점을 가지고는 있지만 서비스 요구시 빠른 응답을 해 줄 수 있다는 장점을 가지고 있다.

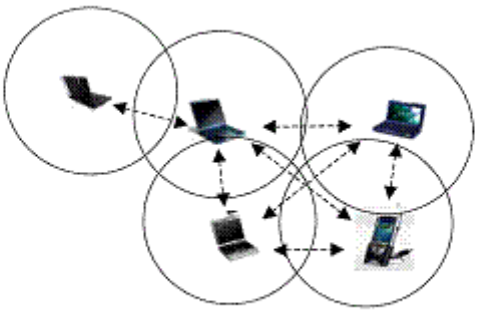
요구 기반 방식의 경우 필요한 경우에 해당 경로를 찾는 방식으로 원하는 경로에 대한 요청이 있을 경우에만 트래픽을 발생하는 방식으로, 테이블 관리 방식의 경우처럼 주기적인 제어 메시지가 브로드캐스팅 되는 형태가 아니라 필요한 경우에만 제어 메시지가 발생되므로 제어 메시지를 줄일 수 있다는 장점을 가지지만 서비스 요청시 초기 경로 탐색에 대한 서비스 지연이 발생한다는 단점을 가지고 있다.

현재 IETF내의 MANET 워킹그룹에서는 이러한 Routing Protocol에 대한 표준화 작업을 수행하고 있다.

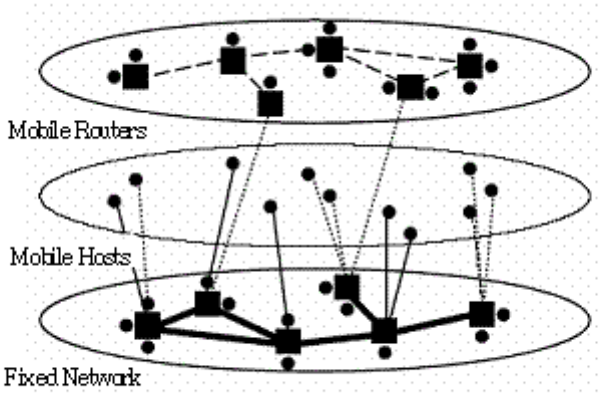
현재 DSR(The Dynamic Source Routing Protocol, Internet-Drafts)의 경우 Internet-Drafts로 제안되어져 있고[10], AODV(Ad Hoc On-demand Distance Vector, RFC 3561)[11], OLSR(Optimized Link State Routing Protocol, RFC 3626)[12], TBRPF(Topology Dissemination Based on Reverse-Path Forwarding, RFC 3684)가 현재 RFC 문서로 채택되어 있는 상태이다.

다. Ad Hoc 네트워크의 형태

Ad Hoc 네트워크의 경우, 이동 단말들로만 구성된 단일 형태의 독립적인 망 구성이 가능할 뿐만 아니라 기존의 인터넷 망 등과의 연동 역시 가능하다. 이러한 기존 망과의 연동을 통해서 Ad Hoc 네트워크는 임시적 망을 구축하여 상호간의 통신을 할 수 있다는 장점을 지니고 기존 망과의 연동을 통한 데이터의 송수신이 가능해지므로 기존 망에서 제공되는 서비스와 콘텐츠 서비스를 그대로 물려 받을 수 있으며, 여러 곳에 분산된 장비를 이용하여 데이터를 가공/처리하여 정보의 가치를 높을 수 있다는 장점을 가지게 될 수 있는 것이다.



(그림 4) 단일 Mobile Ad Hoc Network 구성[4]



(그림 5) Ad Hoc 네트워크와 기존 망의 연동[5]

3. 블루투스

유비쿼터스 환경에서 사용자와 주변과 상호 작용을 하거나 혹은 여러 이기종의 디바이스들과의 상호 작용을 지원하기 위해서 필요한 기술들 중 하나가 근거리 무선통신 기술 중 하나인 블루투스(Bluetooth)이다. 이것은 기존에 각 장치를 연결하던 유선상의 케이블을 제거하기 위해서 개발된 것으로 저가격, 저전력, 단거리의 무선 기술이다. 이러한 블루투스의 일반적인 주요 특징은 다음과 같다.

첫 번째로, 이 단말을 운용하기 위해서 사용되는 주파수 대역은 전세계적으로 사용이 가능해야 하며, 별도의 허가가 필요하지 않아야 하기 때문에 ISM(Industrial-Scientific-Medical) 대역에서 운용되어야 하므로 무선 송수신 장치가 2.4~2.5GHz 대역에서 운용되어야 한다.

두 번째로, ISM 대역이 누구에게나 개방되어 있는 환경이기 때문에 동일 대역에서 사용되는 다른 신호에 대한 간섭을 견디어야 되므로 FH(Frequency Hopping) 대역 확산 방식을 사용하여야 한다.

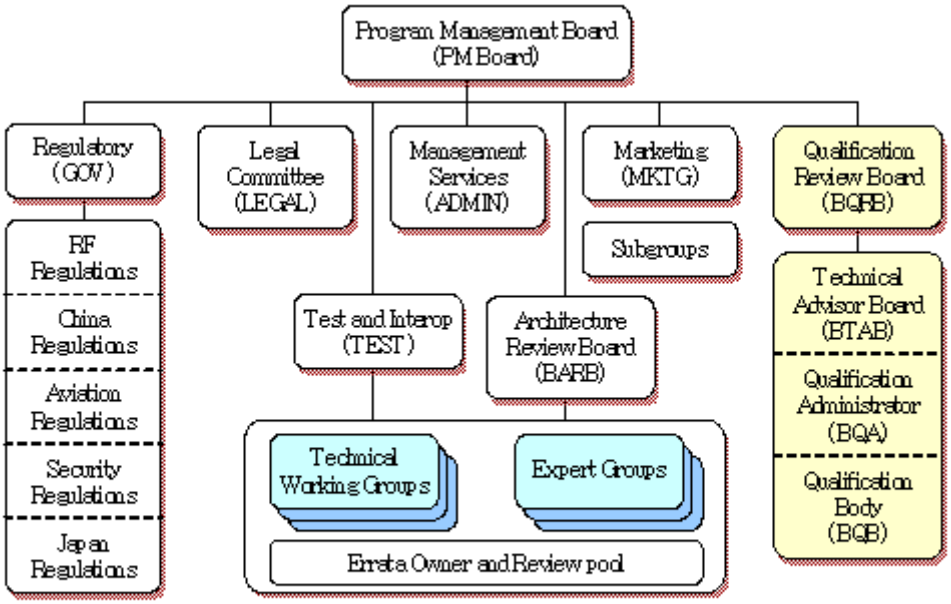
세 번째로, 무선 네트워크를 사용하는 등의 이유로 이 시스템에 대한 기밀성, 인증, 인가와 같은 기본 보안 사항이 적용된다.

네 번째로 동기식 연결 지향형 링크(Synchronized connection oriented link)와 비동기식 비연결형 링크(Asynchronous connectionless link)를 정의하여 음성/데이터 통신 지원이 가능하다.

마지막으로 블루투스 채널은 FH/TDD 기법을 사용하게 되므로, 두 개 이상의 장치가 채널을 공유하게 된다.

이러한 특징을 가지는 블루투스에서 사용되는 표준은 블루투스의 기술 개발, 시장 형성을 위해 구성된 통신, 컴퓨터, 네트워크 관련 유수 회사들의 협력체 SIG(블루투스 Special Interest Group)에 의해 사실상 표준안이 마련되었다.

블루투스 SIG는 1998년 2월에 창립되었고 Ericsson Mobile Communications AB., Intel Corp., IBM Corp., Toshiba Corp., Nokia Mobike Phones., 등의 주요 프로모터로 구성되어졌다. 이후 1999년 12월 4개의 회사 Microsoft, Lucent, 3Com, Motorola를 추가로 영입함으로써 SIG 그룹을 확대하게 되었다. 이러한 SIG는 다음과 같이 구성된다((그림 6) 참조).



(그림 6) SIG 조직 구성도[13]

또한, 공식적인 국제표준 단체로는 IEEE 802.15 워킹그룹이 있어 블루투스 규격에 근거한 국제표준의 제정을 위해 노력하고 있다. 이들은 SIG와 긴밀히 협력하며, 각 구성원이 연구해야 하는 분야에 대한 논의와 ISM 밴드 영역을 사용하기 때문에 이 대역에서 사용하는 무선 네트워크가 공존할 수 있는 방법에 대한 논의, 차세대 고속 블루투스 표준에 대한 논의 등을 하고 있다.

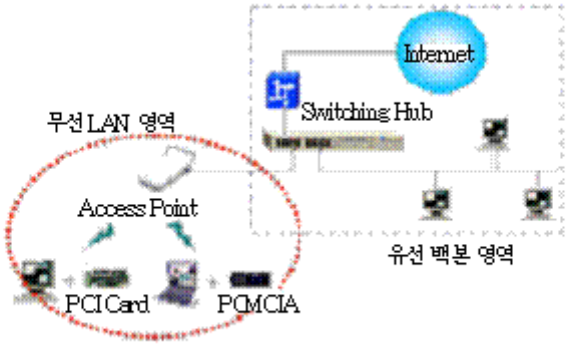
4. 무선랜

무선랜(Wireless Local Area Network: WLAN)이란 기존의 유선랜(Wired LAN)을 대체, 또는 확장한 유연한 데이터 통신 시스템으로 무선주파수(Radio Frequency) 기술을 이용하여 유선망 없이도 데이터를 주고받을 수 있는 기능을 제공한다. 즉, 유선망에 구속됨이 없이 이더넷(Ethernet)이나 토큰링(Tokenring)과 같은 전통적인 랜 기술의 모든 이점과 기능을 그대로 제공한다.

다른 무선 기술과 차별화되는 무선랜 시스템의 특징으로는 일반 이동전화 단말기가 발산하는 전력보다 낮은 저전력(Low Power) 사용, 전세계적으로 인정된 비허가 주파수 대역인 2.4GHz인 ISM밴드를 사용, 신호간섭이 존재하는 곳에서도 매우 수신강도가 강한 속성(Very Resilient Reception Attributes)을 가지는 대역확산 기술(Spread Spectrum Techniques)의 이용 등을 들 수 있겠다[14].

무선랜 분야의 표준은 2.4GHz 대역에서 최대 11Mbps의 속도를 제공하는 IEEE 802.11b가 상용화 제품을 대거 출시하며 시장을 주도하고 있는 가운데, 5GHz대역에서 최대 54Mbps의 속도를 제공하는IEEE 802.11 a와 HIPERLAN/2 가 제품 상용화를 목표로 시장 진입을 추진하고 있다.

무선랜과 관련된 표준안은 크게 IEEE 802.11 규격, 유럽 ETSI BRAN위원회(ETSI's Committee on Broadband Radio Access Networks)의 하이퍼랜(High Performance Radio LAN, HIPERLAN) 규격, 일본 MMAC-PC(Multimedia Mobile Access Communication Systems-Promotion Council) 규격으로 분류된다. 이중 IEEE의 표준안에는 인가없이 사용할 수 있는 ISM(Industrial, Scientific and Medical) 밴드의 2.4GHz를 사용하여 2Mbps까지 전송할 수 있는 802.11, 기존 802.11 변복조 기술을 일부 변경하여, 전송속도를 11Mbps까지 고속화한 802.11b, 5GHz대역에서 6~54Mbps의 전송속도를 제공하는 OFDM(Orthogonal Frequency Division Multiplexing) 방식의 IEEE 802.11a 규격이 있다. 한편, 고속 무선랜의 표준안인 IEEE 802.11a와 HiperLAN/2에서는 2.4GHz에 비해 상대적으로 주파수 대역폭이 넓은 5GHz대의 무선 주파수를 사용하고 고속의 데이터 전송에 적합하며 주파수 효율이 높은 OFDM 변복조 방식을 공통적으로 사용한다.



(그림 7) 무선랜의 구성[14]

가. IEEE 802.11

IEEE 802.11 Working Group은 1990년대 초 2.4GHz와 5GHz 대역에서 운용되는 무선 LAN 표준 개발을 시작하여, 1997년에 3개의 물리 계층과 매체접근제어 계층에 대한 기술적 요구사항이 포함된 IEEE 802.11 표준을 확정하였다. 1999년에는 동 기술을 확장하여 2.4GHz 대역에서 최대 11Mbps까지 전송할 수 있는 802.11b와 5GHz 대역에서 최대 54Mbps까지 전송 가능한 802.11a 물리계층 표준을 추가하였고, 2.4GHz 대역에서 54Mbps의 속도로 데이터를 전송할 수 있는 802.11g가 표준화되었다[5].

나. IEEE 802.11b

802.11b는 DSSS(Direct Sequence Spread Spectrum) 방식에 따라 11Mbps의 속도를 제공한다. 이에 기반한 제품은 1M 또는 2M의 속도를 제공하는 802.11 DSSS 표준에 기반한 기존 제품들과 상호 운영성을 갖는다. 802.11b 표준은 IEEE에 의하여 설계되었으며, WECA (Wireless Ethernet Compatibility Alliance)에 의하여 채택되었다. WECA는 전술하였듯이, 여러 업체의 출시 제품이 802.11b 표준과 호환되는지 여부를 테스트하고 인증하는 역할을 수행하며, 아울러 테스트 통과 업체에게 WiFi 라벨을 부여한다[19].

다. IEEE 802.11a

기존 IEEE 802.11 규격에 따르는 무선랜 제품은 2.4GHz 대역에서 최대11Mbps의 전송속도를 내는 것이 대부분이어서 최근 증가하고 있는 인터넷과 멀티미디어 서비스 요구를 수용하는 데는 한계가 있다. 이에 지난 1999년 9월, 고속 무선랜의 표준안으로서 5GHz 대역에서 6~54Mbps의 전송속도를 갖는 OFDM 방식의 IEEE 802.11a가 최종 확정되었다. IEEE 802.11a는 유럽의 표준화기구인 ETSI BRAN의 하이퍼랜(HIPERLAN/2)과 일본의 MMAC-PC 등에서 고속 무선랜의 공통된 물리 계층 표준안으로 채택되었다. 최근 고속 무선랜의 표준안으로IEEE 802.11a가 확정되고 이 표준안에 따르는 고속 무선랜을 사용하여 공중망과 연동하여 광대역 무선 서비스를 제공하려는 계획이 발표됨에 따라, 많은 국제 표준화 기구와 국내외 기업, 연구소에서 이에 대한 연구 및 개발을 21세기 핵심 기반사업으로 수행하고 있다[19].

라. IEEE 802.11g

802.11g 표준은 IEEE 전체 802.11 Working Group의 승인을 받아 2003년 6월에 통과되었고, 2.4GHz 대역에서 802.11와 호환성을 제공할 수 있어 기존 망과 상호 운용이 가능하다는 장점이 있다. 기존의 2.4GHz 대역에서 OFDM 변조 방식을 이용하여 전송속도를54Mbps까지 지원하며, 이론적으로는 802.11a와 동등한 수준의 전송속도를 제공할 수 있으나, Wi-Fi와의 하위 호환성을 위한 Wi-Fi 오버헤드를 끌어안는 부담 때문에 802.11a와 동일한 전송속도를 얻기는 어려울 것으로 보인다[20].

마. HIPERLAN/2

광대역 무선 액세스 네트워크의 망 구성을 위해 유럽의 표준화기구(ETSI)는 2000년 4월 5GHz대역에서 6~54Mbps의 전송속도를 갖는 OFDM 방식의 고속 무선랜의 표준안으로서 HIPERLAN/2를 확정하였다. IEEE 802.11과 HIPERLAN/2의 가장 큰 차이점은 매체접근 제어 계층에 있다. IEEE 802.11에서는 CSMA/CA를 사용하는 반면, HIPERLAN2에서는 무선 ATM에 기반을 둔 중앙집중 방식의 CSMA/TDD를 사용하여 ATM 및 IP 네트워크에서 요구하는 다양한 QoS (서비스 품질: Quality of Service)을 보장할 수 있도록 했으며, 또 HIPERLAN/2에서는 이동 단말과 유선 광대역망과 연동하여 사용할 계획이나 IEEE 802.11은 이더넷 기반의 네트워크에 한정되어 있다[20].

Ⅲ. 유비쿼터스 및 Ad Hoc 네트워크 보안

유비쿼터스 컴퓨팅 환경은 각종 디바이스들이 우리의 생활 속에 스며들어 사용자가 자신이 인식하지 못하고 있는 사이에 이들 디바이스들의 도움을 받으며 좀 더 편리한 생활을 추구하고자 하는 것이다. 따라서 기존의 컴퓨터 환경과 같이 자신이 유선이라는

특성에 얽매여 한 곳에서 작업을 해야 하며, 정보를 습득하기 위한 장소가 한정되는 환경이 아닌 무선의 특징에 힘입어 자신이 어디에 있든 어떠한 디바이스를 가지고 있든지간에 기존과 동일한 서비스를 받을 수 있다는 개념이다.

그러나 유비쿼터스 컴퓨팅 환경에서의 시큐리티 문제는 기기들이 무선으로 데이터를 주고 받는다는 특성과 각 기기들의 Computing Power와 전력 관리 등의 문제를 가지고 있으므로 인터넷 시대의 시큐리티 문제보다 복잡하며 이들 구성 장비에 대한 공격은 쉬운 반면 이러한 공격에 대한 방어를 수행하는 작업은 기존의 방법보다 더 어려울 것으로 예측된다.

또한 이러한 환경에서는 각 디바이스들이 생활의 곳곳에 널리 퍼져 있기 때문에 개인 정보보호, 시스템 혼란 방지, 확장성, 보안 등이 장기적 이슈가 될 문제점을 노출하고 있다.

무선 네트워크의 특성상 개인의 정보가 쉽게 노출되며, 자동 지원 시스템이 증가할수록 개인 정보의 노출도 심각하게 된다. 그리고 센서와 상황 모델로부터 생성되는 의미있는 정보와 무의미한 정보가 구별 없이 폭주할 경우, 무의미한 정보로부터 시스템 혼란 방지를 어떻게 구현할 수 있을 것인지, 분산 환경에서의 유비쿼터스 컴퓨팅 시스템의 응용 레벨에서 하위의 통신 레벨까지 확장성은 어떻게 할 것인지, 마지막으로 네트워크화된 모든 장치나 시스템이 서로 연결된다면 인증되지 않은 소프트웨어나 하드웨어의 공격에 어떻게 대처할 수 있는지 등이 고려되고 있다.

1. RFID 보안

RFID는 그 편리함에도 불구하고 개인 정보나 보안에 대해 취약한 것이 사실이다. 바코드 시스템과 비교하여 시야가림에 대한 문제가 없어졌지만 그 시야가림의 문제로 인하여 RFID의 태그는 항상 읽혀질 준비를 하고 있는 것도 사실이다. 2005년부터 유럽중앙은행은 유럽에서 사용하는 유로 화폐에 RFID 태그를 내장한다고 밝히고 있다. 만약의 경우이긴 하지만 아무런 보안 대책을 세우지 않는다면 악의적인 사람이 길거리에 지나가는 사람들을 모니터링 할 수 있다. 예를 들어, 보이지 않지만 그 사람은 누가 현금을 더 많이 가지고 다니는지 알 수 있으며 그는 범죄의 피해자가 될 수도 있다.

다른 예로 들 수 있는 것은 개인 정보에 관한 문제이다. 만약, 옷(물론 속옷도 포함해서)에 붙인 태그가 악의적인 사람의 물음에 자신의 고유 번호를 가르쳐 준다면 이는 심각한 사회 문제가 될 것이다. 확실하지는 않지만 사람에게 RFID 태그를 부여한다고 가정해보자. RFID 태그에는 너무 많은 정보가 들어 있을 것이고 개인의 정보란 더 이상 존재하지 않을 수도 있다.

이러한 보안 문제를 고려한다면 RFID 시스템에서 태그에 부여하는 정보의 양은 충분히 고려하여 결정하여야 한다.

불행하게도 태그에는 자체적인 네트워킹 기능이 있어 신뢰할 수 있는 CA(Certificate Authority) 같은 곳에 접속하여 리더가 믿을 수 있는지 알아낼 방법이 없다. 고기능 시스템의 경우 나름대로의 인증과 암호화 시스템을 탑재할 수 있지만 그렇지 않을 경우 태그는 어떠한 리더의 요구에도 응답하게 된다.

그래서 가장 보편적인 해결 방안들은 태그와 리더가 주고받는 신호를 도청하는 것을 막아 보고자 하는 데에 있다.

가. Kill Tag

이 Kill Tag 방법은 MIT의 AutoID Center에서 제안한 방법으로 태그의 설계에 8-bit의 패스워드를 포함하고 태그가 이 패스워드와 'Kill' 명령을 받을 경우 태그가 비활성화되는 방식이다. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로서 Kill 명령을 실행하게 되는데, 이로 인해 한번 죽은 태그는 다시 살릴 수 있는 방법이 없게 된다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 아주 간단한 예로, 반품이 가능한 물건에 붙어 있는 태그의 경우 이런 Kill Tag 명령 방식을 사용할 수 없다.

물론, Read/Write로 설계된 태그의 경우 플래그(Flag) 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있을 것이다. 하지만, 이 경우 또한 여전히 태그에 사용하는 8-bit 암호에 대한 문제가 남는다. 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 128-bit 이상을 암호로 사용해야 하지만 이는 태그에 상당한 부담이 된다. 태그마다 다른 암호를 사용한다면 이를 저장하는 것도 문제이다.

나. 페러데이 우리(Faraday Cage)

무선 주파수가 침투하지 못하도록 하는 방법으로 금속성의 그물(Mesh)이나 박막(Foil)을 입히는 방법이다. 실제로 RSA 연구소는 2005년 유로화의 RFID 시스템의 도입에 대비하여 돈 봉투에 그물을 입힌 상품을 제시하였다. 그러나 이 경우도 사용 범위가 극히 제한적인 것이 문제로 생물 인식에 쓰인 태그 같은 경우 사용할 수 없다.

다. 방해 전파(Active Jamming)

리더기가 제품을 읽지 못하도록 방해 신호를 보내는 물건을 소비자가 들고 다니자는 것인데, 불법적으로 이용될 소지가 크고 오히려 방해 신호에 의해 다른 RFID 시스템이 손상될 수 있기 때문에 이를 회피하는 연구를 해야 할 상황이기도 하다.

라. 차단자 태그(Blocker Tag)

차단자 태그는 모든 질문 메시지에 대해서 '그렇다'라고 대답하는 태그를 말한다. 모든 질문 메시지에 응답하기 때문에 바이너리 트리 워킹을 사용하여 태그를 읽어 들이는 방식에서는 바이너리 트리의 모든 영역을 검색하게 되는 결과를 가져온다. 태그의 고유번호 길이가 길어지면 길어질수록 리더는 리더의 용량을 초과하는 개수의 태그를 찾기 위해 시도할 것이고 이는 리더에게 치명적인 결과를 가져올 것이다.

차단자 태그를 조금 더 유용하게 사용하는 방법은 자신이 비밀을 지키고자 의도 태그들의 비트에 맞추어 처음 비트들을 제어함으로서 비밀 구역(Privacy Zone)을 만드는 것이다. 차단자 태그와 동일한 시작 비트를 갖는 태그들은 차단자 태그가 만드는 비밀 구역 안에서 안전하게 보호될 수 있다.

2. Ad Hoc 네트워크 보안 메커니즘

보안 문제는 유선 네트워크에서도 존재하고 있지만, 이동 Ad Hoc 네트워크는 무선 인터페이스를 사용하기 때문에 유선 네트워크에 비해 훨씬 더 많은 위험에 노출되어 있다. 그러므로, 기본적인 Ad Hoc 네트워크의 보안 요구조건은 다른 통신 네트워크에서 요구되는 것과 동일하지만, 이동Ad Hoc 네트워크에서는 노드가 신뢰받은 인증기관을 통해 인증을 받는 형식이 아니기 때문에, 멀티홉 방식에 의해 라우팅을 수행할 경우 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 특히, 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로, 암호키에 크게 의존하게 된다. 또한, MANET 환경은 모든 노드들이 분산되어 있고, 어떠한 고정된 기반구조도 없으며, 모든 노드가 공평하게 역할을 나누어 갖는다는 특징을 갖는다. 한편으로, 보안 문제가 확실히 해결되다보면, 컴퓨팅 문제가 발생되어, 노드와 네트워크 전체에 심각한 부하를 주게 되므로, 이동 Ad Hoc 네트워크에 적합하게 구현된 알고리즘, 키 분배 및 인증 프로토콜의 개발이 현실적으로 가장 필요하다. 즉, 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 이동 Ad Hoc 네트워크 전반에 분배하는 것이 주요 관심 사항이라 할 수 있다.

Ad Hoc 환경에서 중요하게 고려되는 위협은 크게 외부 위협과 내부 위협으로 구분할 수 있다. 외부 위협은 다시 잘못된 라우팅 정보의 삽입을 통한 위협과 이전의 라우팅 정보를 재생하여 악용하는 위협, 라우팅 정보를 변형하여 네트워크에 위험을 가져오는 위협 등으로 분류할 수 있다. 외부 위협을 통해 공격자는 네트워크를 분할하거나 네트워크에 극심한 트래픽을 유발하여, 전체 네트워크 시스템에 장애를 일으키는 결과를 초래할 수 있다. 이러한 위협을 막는 것은 굉장히 어려운 일인데, 그 이유는 라우팅 정보를 통해 공격자에 의해 훼손된 노드를 찾는 것이 매우 어렵기 때문이다. 다시 말해서, 라우팅 정보의 한 부분이 유효하지 않다고 발견된 경우, 그 정보가 공격자와 타협한 노드에 의해서 만들어진 것인지 아니면, 토폴로지 변화의 결과로 유효하지 않게 되는 경우인지를 구분해내는 것이 매우 어렵다는 의미이다. 이러한 위협에 대처할 수 있는 효과적인 방법은 충분한 노드를 확보하여 공격자들을 우회할 수 있는 경로를 찾는 것이다. 두 번째는 내부 위협으로, 이는 외부 위협보다 훨씬 더 심각한 위협이며, 시스템 내의 훼손된 노드들에게서 발생하는데, 이 경우 어떤 노드들은 다른 노드들에게 잘못된 정보를 제공하여 시스템에 장애를 유발한다. 이를 막기 위한 방법으로써, 올바른 노드들이 충분히 존재하기만 하면, 라우팅 프로토콜은 훼손된 노드들 주변을 우회할 수 있는 경로를 찾을 수 있을 것이다.

따라서 Ad Hoc 보안에서 중요한 연구 과제는 먼저, Ad Hoc 네트워크에서는 무선 연결을 사용하기 때문에 공격자로 하여금 가장(Impersonation), 메시지 재연(Message Replay), 메시지 변형(Distortion) 등과 같은 수동적 공격을 가능하게 하므로, 이에 대한 연구가 필요하다. 또한, Ad Hoc 환경은 상대적으로 물리적 보호에 취약하다. 즉, 노드들은 항상 공격자가 존재하는 환경에서 움직이므로, 언제든지 공격자에 의해 중요한 정보가 훼손될 가능성을 무시하면 안된다. 한편, MANET에서는 네트워크 외부에서의 공격자뿐만 아니라, 네트워크 내부의 공격자와 타협한 노드들에게서 시작되는 공격 또한 간과해서는 안된다. 그러므로, MANET에서 보다 높은 생존성을 보장하기 위해, 어떤 'Central Entities'도 없는 분산된 구조를 지녀야 한다. 그 이유는 중앙의 관리자(Authority)가 공격자와 타협하면 모든 정보가 노출되고, 다양한 공격이 가능하기 때문이다.

한편, Ad Hoc 네트워크는 토폴로지와 구성원이 수시로 변하는 동적인 구성을 갖고 있어서 어떤 노드가 훼손되었을 때, 노드들의 신뢰 관계도 변하게 되어 다른 무선 네트워크(예, Mobile IP)와는 다르게 Ad Hoc 노드들이 동적으로 관리 도메인(Administrative Domains)에 가입하고 탈퇴한다. 결론적으로, 정적 구성에서의 보안 해결책으로는 충분하지 못하며, 빈번한 변화에 즉각적으로 적응할 수 있는 시스템이 필요하다. 마지막으로, Ad Hoc 네트워크는 수백 내지 수천 개의 노드들로 구성될 수 있으므로, 보안 구조는 거대한 규모의 네트워크를 모두 포함할 수 있는 구조로 연구되어야 한다.

마지막으로 MANET의 보안 목표는 여러 가지가 존재하지만, 대체로 다섯 가지 정도로 말할 수 있다[6].

첫 번째로, 가용성(Availability) 측면인데, 이는 공격자에 의한 DOS 공격에도 불구하고, 네트워크 서비스의 붕괴가 초래하지 않아야함을 의미한다. 여기서 DOS 공격은 Ad Hoc 네트워크의 어떤 계층을 통해서도 도달할 수 있다고 보며, 물리 계층과 미디어 접근제어 계층에서 작은 Jamming을 통해 물리적인 채널을 통한 통신을 간섭할 수 있다고 가정하면, 네트워크 계층의 라우팅 프로토콜들을 붕괴시키고, 네트워크 연결을 끊을 수 있다. 상위 계층에서도 다양한 서비스들에 영향을 미칠 수 있으므로, 키 관리 서비스 측면에서 가용성은 중요한 목표가 된다.

두 번째는 노드들 간에 전달되는 데이터들은 인증되지 않은 노드들에게는 노출되지 않아야함을 보장하는 것으로 '신뢰성(Confidentiality)'이라 한다. 이는 특히 군사적인 부분에서 많이 요구된다.

세 번째는 전송된 메시지가 훼손되지 않았음을 보장하는 무결성(Integrity)이다.

네 번째는 인증(Authentication)으로서, 이는 노드로 하여금 통신에 관여하고 있는 상대 노드의 신원을 확신하게 하는 것을 의미한다.

마지막으로, 부인방지(Non-Repudiation)가 요구되는데, 이는 메시지를 보낸 곳에서 메시지를 보낸 사실을 부정하지 못하도록 하는 것이다.

이외에도 ordering, timeliness, isolation, lightweight computations, location privacy, Byzantine robustness, key management 등의 보안 목표가 있다.

3. 블루투스 보안

블루투스 무선 기술은 단거리상에서 peer-to-peer 통신을 제공한다. 보호와 정보의 기밀성을 제공하기 위해서 시스템은 application layer와 link layer 사이에서의 보안을 제공하게 된다.

이러한 보안 제공은 페어 환경에 적합하게 설계되어졌다. 이것은 각각의 단말들이 인증과 암호화 루틴을 동일하게 적용한다는 것을 의미한다. link layer에서 보안을 관리하는데 4개의 다른 개체가 사용되는데 Bluetooth device address, 두 개의 secret key, pseudo-random number가 그것이다[13].

그러나 이러한 보안이 End-to-End로 이루어지는 것이 아닌 무선 링크상에 대해서만 이루어지는 등의 문제로 그에 따른 위협 문제와 요구 사항이 필요하다.

블루투스에 내재된 보안 문제로 기밀성이 손실될 경우 상대방 장비를 도청할 수 있게 되며, 데이터에 대한 무결성이 손실될 경우 사용자 데이터의 훼손이 우려된다. 마지막으로 Dos와 DDos 공격은 네트워크와 장비에 대한 가용성을 손실을 가져올 것이다.

따라서 이러한 위험을 감소시키기 위해서는 다차원적인 부분에서 위협 요소에 대한 대책을 고려하여야 하는데 관리적 대책, 운영적 대책, 기술적 대책 등을 고려해 볼 수 있다고 한다[10].

<표 1> 인증과 암호화를 위해 사용되는 Entity[13]

Entity	Size
BD_ADDR	48bit
Private user key, authentication	128bit
Private user key, encryption Configurable length(byte-wise)	8~128bit
RAND	128bit

4. IEEE 802.11 Wireless LAN 보안 메커니즘

현재 가장 많이 사용하고 있는 802.11b 무선랜은 처음부터 보안에 큰 관심을 두지 않았다. 또한 공중망에서의 활용을 전제로 설계되지 않았던 것이 사실이다. 예를 들면, 무선랜은 브로드캐스팅 특성으로 인하여 도청 등 무선 데이터 프라이버시에 대한 취약성이 예상되었음에도 불구하고, 동적인 키 분배 방법이 없다거나, 취약한 무결성 알고리즘을 사용하여 데이터 프라이버시를 제공하지 못한다는 점이다.

IEEE 802.11i(Enhanced MAC security) Task Group은 최근 무선랜 인프라 망과 Ad Hoc 망에 적용할 수 있는 새로운 형태의 보안 아키텍처(Robust Security Network, RSN)를 제안하고 표준화를 완료했다. RSN은 다수의 액세스 포인트가 연결된 핫스팟에서 802.1x 기반 가입자 인증을 통한 네트워크 접속제어, 보안 세션 관리, 패킷당 키 관리, 그리고 새로운 암호 알고리즘 도입을 통한 무선접속 구간 보안을 강화하는데 이용된다[5].

<참 고 문 헌>

[1] 김재윤, "유비쿼터스 컴퓨팅: 비즈니스 모델과 전망," 삼성경제 연구소, 2003. 12.
[2] 연승준, 박상현, 하원규, "유비쿼터스 컴퓨팅의 시스템적 함의와 관련기술 동향," 전자통신동향분석 제19권 제2호 2004년 4월, pp1-8
[3] 김완석, "유비쿼터스 프로젝트와 IT 메가 트랜드," 2003. 10, http://justit.gigaro.net/
[4] 권혜연 외 5인, "이동 Ad Hoc 네트워크 기술 동향," 전자통신동향분석, 제 18권 2호, 2003. 4.
[5] 양대헌 외 4인, "차세대 컴퓨팅 환경에서 디바이스 인증을 위한 PKI 적용기술 연구," 한국정보보호진흥원, 2003. 12.
[5] Joseph P. Macker, M. Scott Corson, "Mobile Computing and Communications Review," Vol.2, No.4.
[6] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network 1999.
[7] C.K. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and System," Addison-Wesley
[8] Charles E. Perkins, "Ad Hoc Networking," Addison-Wesley, 2001. 6.
[9] 이정구, "BQTF 국제 시험서비스 및 블루투스 표준화 동향," TTA 저널 제 92호, 2004. 4.
[10] 윤준, "블루투스 및 휴대장비 보안," 한국정보보호진흥원, 2002. 9.
[11] http://www.ietf.org
[12] http://www.itfind.or.kr
[13] http://www.bluetooth.org
[14] 김형수, "무선랜의 기술과 시장 전망," 한국전파진흥협회, 2003. 8.
[15] 이근호 외 3 공역, "RFID HANDBOOK," 영진.com, 2004.
[16] 이근호, "무선식별 RFID 기술," TTA 저널 제 89호, 2003. 10.

[17] Stephen A. Weis, “Security and Privacy in Radio-Frequency Identification Devices,” MIT, 2003. 3.
[18] Ari Juels and Ronald L. Rivest and Michael Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,” RSA Laboratory, MIT
[19] 이상오, 무선랜 시장의 구조와 전개방향, KISDI IT FOCUS 2001년 6월호, pp. 5-33
[20] 홍승표, 정현수, 무선 LAN 기술의 개요 및 시장 동향, IT Find Mailzine, 2002. 12. 66호