A-09

센서 네트워크 환경에서 Safe Korea 실현을 위한 보안 정책

김선호
서울소방방재본부 전산개발팀

Security Policy for Safe Korea on the Sensor Network

Seonho Kim
Seoul Fire & Disaster Management Department

1. 서론

최근 유비쿼터스 관련 기술의 급속한 발전과 함께 유비쿼터스 라이프 실현에 대한 기대가 한층 높아지고 있다. 유비쿼터스 컴퓨팅 환경은 모든 사물에 컴퓨팅 기능을 부여하여 사물이 인간과 같이 다른 사물을 인식하고 주변 환경을 감지하게 하여, 네트워크를 통해서 언제, 어느 곳에서든 정보를 확인하고 활용할 수 있도록 하는 것이다. 이러한 기술은 생산, 유통, 물류, 의료서비스, 복지서비스, 환경감시시스템, 재난관리시스템 등 다양한 분야에 적용되어 인류의 삶을 더욱 편리하고 윤택하게 만들어 줄 수 있을 것이다.

유비쿼터스 컴퓨팅의 특징은 크게 내재화(Embedded)와 휴대성(Mobility)을 들 수 있는데 내재화를 강화함으로써 자연스러운 컴퓨팅의 구현을 가능케하며 사람들이 인식하지 못하는 상태에서 컴퓨팅 기능이 수행되고 또한 휴대성을 개선하여 언제 어디서나 상시적으로 들고 다닐 수 있을 정도의 소형 단말기를 이용함으로써 유비쿼터스 환경이 구현되는 것이다.

이러한 유비쿼터스 컴퓨팅을 가능케 하기 위한 기본기술 중에 하나가 센서 네트워크이다. 정보통신부는 유비쿼터스 센서 네트워크의 개념에 대해 △필요한 모든 것(곳)에 전자태그를 부착하고(Ubiquitous) △이를 통하여 기본적인 사물의 인식정보는 물론, 주변의 환경정보(온도, 습도, 오염정보, 균열정보 등)까지 탐지하여(Sensor) △이를 실시간으로 네트워크에 연결하고 그 정보를 관리하는 것(Network)으로 정의하고 있다. 유비쿼터스 환경은 정보가 유·무선 상에서 자유롭게 유통되고 사람이나 물건의 상황, 그 주변 환경 등을 센싱하여 대량의 데이터를 수집하고 상황에 맞는 적절한 정보를 제공하는 서비스가 보편화됨에 따라 편리성과 함께 정보의 노출 및 위협의 가능성은 더욱 증가하게 된다. 또한 무선 액세스를 기반으로 하는 센서 네트워크에 대한 요구가 늘어나면서 통신망 보호 기술 및 보호 대상이 보다 복잡하고 중요하게 되었다[1].

개인의 사적인 정보들과 공적인 정보들이 무선 센서 네트워크를 통하여 유통될 환경

하에서 이러한 정보들에 대한 보호 대책은 그 무엇보다 중요한 요소가 될 것이다. 센서 네트워크는 소방방재 분야에 있어서도 많은 편재한 기기들을 활용하여 원격 감시 및 통제를 하는 유비쿼터스 방재시스템이 안전한 삶을 도와줄 수 있지만 반면 이러한 안전 시스템의 침해에 따른 오동작이나 파괴는 인간의 생명을 좌우하는 파괴적인 양상을 보일수도 있다. 그러므로 소방안전 점검에 있어서 이러한 기기와 정보에 대한 검사는 유비쿼터스 환경에서 매우 필수적인 요소라고 할 수 있다.

그러므로 본 연구에서는 센서 네트워크 환경에서 고려해야 할 보안사항을 검토해 보고 그에 적합한 새로운 보안정책 및 안전대책을 제안하고자 한다.

2. Safe Korea 비전

정보통신부는 IT 산업의 미래 청사진으로 유비쿼터스 컴퓨팅(Ubiquitous Computing) 기술을 기반으로 국가의 모든 자원을 지능화·네트워크화 하고, 이를 바탕으로 국가사회 시스템 혁신과 국민 삶의 질 향상, 국가경제 발전을 추구하는 'u-Korea 비전'을 제시하였다. 정보통신부는 'u-Korea' 프로젝트가 기존의 IT성과를 재도약시켜 새로운 고부가가치를 창출해 신성장의 계기를 마련할 것으로 보고 IT839를 통해 [그림 1]에서 보듯이 초고속망, 방송망, 이동망 등의 통합된 인프라를 기반으로 언제 어디서나 어떤 서비스라도 받을 수 있는 'u-Korea'를 실현하고자 하는 전략을 갖고 있다. 이때 방재시스템에 있어서도 유비쿼터스 환경 하에서 원격호출 및 제어, 점검 등을 통해 편리하고 안전한 삶을 추구한다는 전략이다.

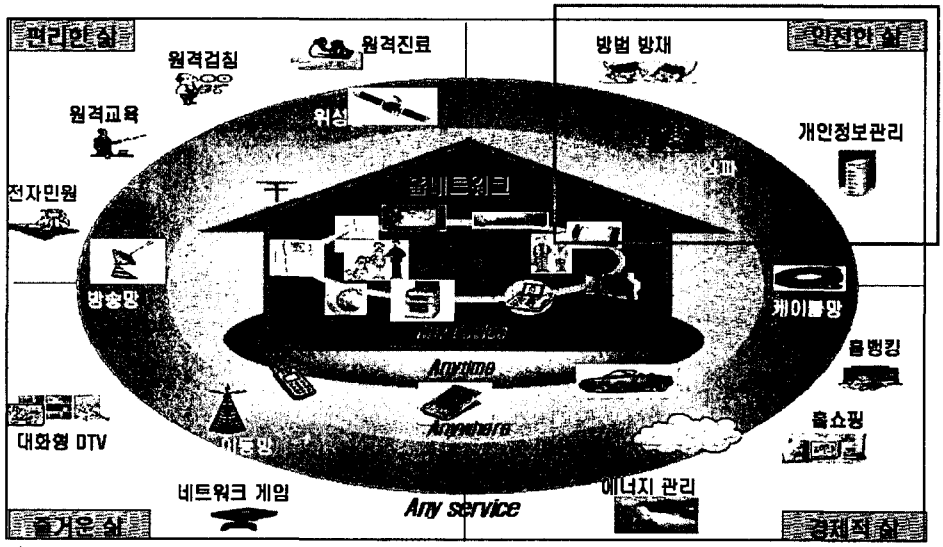

그림 1. u-Korea 비전

소방방재청은 각종 재난으로부터 국토를 보존하고 국민의 생명, 신체 및 재산을 보호하기 위하여 2004년 6월 개청되어 국가 및 지방 자치단체의 재난 및 안전관리체제 확립

을 제언하였다. 우리나라는 지난 10년간 자연재난으로 인해 연평균 137명의 인명피해, 1조 7000억원의 재산피해, 2조 6000억원의 복구비용 등의 피해를 보았으며, 피해 규모가 갈수록 커지고 있다. 지구 온난화에 따른 이상기후로 태풍·지진해일 등 재난 유형이 매우 다양해지고 있어 대응하기가 더욱 어려워지고 있다[2].

이런 환경에서 IT 기술을 재난 예방 및 사후 복구를 위해 활용한다면 보다 효과적인 방재가 가능할 것이다. 현재 전국적으로 실시되고 있는 휴대폰 긴급재난 문자서비스가 실시되고 있고 IT 미디어를 통한 재난방송도 점차 강화되는 추세다. 이동 통신망, 또는 디지털멀티미디어방송(DMB), 휴대인터넷 등의 새로운 정보통신 인프라와 유비쿼터스 기술을 활용한 재난예방 및 관리는 보다 효율적인 재난방재 정책이 될 것이다. 그 일환으로 정보기술을 활용한 효과적인 방재시스템으로 안전한 한국을 건설한다는 이념으로 'Safe-Korea 2010'을 착수하여 국가 재난관리 지리정보시스템(GIS)과 통합방재 DB 고도화를 이행하고 있으며 국가 재난 시 무선통신망을 이용한 통합 재난관리를 위하여 통합 지휘통신망 구축사업을 추진하고 있다

3. 유비쿼터스 센서 네트워크와 보안

유비쿼터스 센서 네트워크(Ubiquitous Sensor Network: 이하 USN으로 통칭)는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 하나의 네트워크로 연결되어 있는 수많은 센서들이 필드(Field)의 지리적, 환경적 변화를 감지하여 베이스 스테이션으로 그 정보를 전달한 후 센서 네트워크 서버를 통해 사용자에게 전달되는 방식으로 정보 수집이 이루어진다[3].

미래의 센서기술은 세 가지 단계를 거쳐 발전할 것으로 전망된다. 첫번째 단계는 센서가 생활공간에 확산되는 단계다. 정보가전을 비롯해 소파와 침대 그리고 도로 곳곳에 작고 저렴하며 소비전력이 낮은 센서들이 내장된다. 이들은 독립된 센서로서 고유의 기능을 수행한다. 두번째 단계는 이들 센서가 서로 연결되는 단계다. 기존의 전력선과 전화선을 활용한 네트워킹이 가속화되고 무선화가 보편화될수록 정보기기 속에 숨어 있던 센서들은 단일 네트워크로 통합된다. 마지막으로 네트워크 속에 편입된 센서들은 각자의 정보를 주고받게 될 것이며 기존의 무선통신망과 유기적으로 결합됨으로써 정보가 종합화될 것으로 예상된다[4].

USN 환경에서 센서 노드들이 사용 가능한 자원은 제한적이기 때문에 센서 노드들 사이에 안전한 통신 서비스를 제공하는 보안 프로토콜의 설계가 쉽지 않고, 무선 통신으로 데이터를 교환하기 때문에 공격자들에게 다양한 공격을 시도할 수 있는 기회를 제공한다. 현재까지의 보안 프로토콜들은 제한된 자원들 사이의 절충을 통해 설계되고는 있지만 아직까지는 기존 네트워크에서의 보안 서비스만큼 안전성을 제공하지 못하고 있다. 또한 공격자들이 쉽게 물리적으로 접근하여 센서 노드를 획득할 수 있기 때문에 기존의 네트워크에서 고려하지 않았던 추가적인 보안 요구사항도 필요로 한다.

정보시스템은 하드웨어, 소프트웨어, 데이터 등으로 구성되어 있다. 정보시스템에 손실

이나 해악을 끼칠 수 있는 가능성을 가진 환경을 위협(threat)이라고 하는데 정보시스템에 대한 위협으로는 중단(interruption), 도청(interception), 변조(modification), 위조(fabrication) 등이 있다. 보안은 이러한 위협으로부터 정보시스템을 보호하는 것이으로 보안은 비밀성(confidentiality), 무결성(integrity), 그리고 가용성(availability)을 유지하는 것이다. 비밀성은 오직 허가받은 자만이 정보시스템에 대한 접근을 허용해야 함을 의미한다. 무결성은 개체와 메시지를 주고 받을 때 내용이 변조되지 않고 원본 메시지 그대로임을 보장해야 하는 것을 의미하며 가용성은 허가받은 자가 정보시스템에 정당한 방식으로 접근하는 것을 방해받지 않아야 한다는 것을 말한다[5].

USN 환경에서는 다양한 분야에서 다양한 장치들을 통해 개인에 관련된 정보들이 디지털 형태로 데이터베이스에 저장된다. 이때 이런 정보들이 개인이나 회사, 정부의 이익을 위해 악용된다면 개인의 프라이버시를 침해하는 결과를 낳게 된다. USN이 구축된 장소에서 센서 노드들로부터 개인의 위치와 같은 민감한 정보들이 감지될 경우 이런 정보들이 개인의 의사와는 상관없이 저장되고 다른 목적으로 악용될 수 있는 것이다. 앞으로 USN은 많은 응용분야에서 사용될 전망이며 이에 따른 개인 프라이버시 등 보안 문제를 해결하기 위해서 개인의 정보가 어떻게 이용되는지에 대해 개인이 인지하도록 해야 하며 수집된 정보들에 대해 허가된 사람들만이 접근할 수 있도록 규제를 하는 등 사회적인 규범, 새로운 법, 기술적인 대응을 종합하여 접근할 필요가 있다.

제한적인 환경을 가지고 있는 USN에서의 보안은 통신, 에너지, 메모리 등의 요구 조건을 전체적으로 고려해서 선택하여야 한다. 특히, 물리적으로 노출되어 있는 환경에서 발생할 수 있는 다양한 공격 가능성을 예측한 대응도 필요하다. USN 보안에 대한 연구는 아직 초기단계로 일반 네트워크에서 보여주는 보안 수준을 제공하지는 못하고 있으며 표준화된 기술도 없다. 하지만 USN은 정보통신부의 IT839 추진과 더불어 앞으로 u-City 등 사회 여러 분야에서 각광받게 될 것이다. 따라서 USN이 적용되는 다양한 환경에 따라 가능한 여러 가지 공격들을 분석한 후 이에 따른 개별적인 보안 방법의 연구가 필요하다.

4. 공격 패러다임의 변화

최근 컴퓨터와 네트워크의 보안을 위협하는 요소들은 날로 다양해지고 지능화되고 있다. 컴퓨터를 공격하는 유형에는 크게 해킹과 악성코드를 들 수 있다. 해킹은 해커가 인터넷을 통해 특정 컴퓨터에 침입하여 자료를 훔쳐보거나 변형, 파괴를 하는 행위를 말하며 악성코드는 컴퓨터에서 사용자가 원하지 않는 행위를 몰래하는 소프트웨어를 총체적으로 일컫는다. 해킹과 악성코드의 차이는 첫째, 해킹은 1:1의 특성이 있어 한명의 해커가 한 번에 한 대의 컴퓨터를 공격하는 것이 기본적인 반면 악성코드는 1:n (n>1) 의 특성이 있어 하나의 컴퓨터 바이러스나 웜이 스스로 증식하여 여러 대의 파일이나 컴퓨터를 동시에 공격한다. 둘째, 해킹은 해커가 어떤 의도를 가지고 특정한 컴퓨터를 침입하는 것으로 구체적인 공격목표가 있지만 악성코드는 자기 스스로 감염 또는 침입할 수 있

는 곳을 찾아서 퍼져 나가기 때문에 불특정 다수를 공격하게 된다. 셋째, 해킹은 해커가 직접 컴퓨터에서 컴퓨터로 공격을 하기 때문에 흔적이 남을 수 있고 그럼으로 그에 따라 추적이 가능할 수 있으나 악성코드는 자기 스스로 감염 또는 침입할 수 있는 곳을 찾아서 퍼져 나가기 때문에 추적이 불가능하며 어디를 통해서 왔는지 경로조차 추적하기 힘들다[6].

그런데 최근의 패러다임은 컴퓨터 바이러스 기술과 해킹 기술이 결합되어 활동한다는 것이다. 예전에는 컴퓨터 바이러스는 스스로 증식하는 프로그램으로 개인용 컴퓨터가 주 공격 대상이고 해킹은 해커가 여러 가지 기법을 사용하여 취약점이 있는 서버나 대형 컴퓨터에 침투하는 형태였다. 그리하여 컴퓨터 바이러스는 백신 프로그램으로 막을 수 있었고 해킹은 네트워크 보안 솔루션으로 막을 수 있었다. 하지만 컴퓨터 바이러스의 복제 기술과 해킹의 침투 기술이 결합함으로써 해킹 기술을 이용하여 네트워크에 연결된 컴퓨터들에 스스로 능동적으로 침입하고 증식할 수 있게 되었으며 공격당한 컴퓨터를 근거지로 하여 다시 다른 컴퓨터들을 공격하게 되어 전 세계로 급속하게 퍼져나갈 수 있는 엄청난 파괴력을 가지게 되었다. 그러므로 한 컴퓨터만이라도 제대로 보안 관리가 되어 있지 않아 공격을 당하게 되면 그곳을 기지로 다른 컴퓨터로 급속히 퍼져 모두 피해를 입게 되는 것이다. 즉 전체 중 가장 취약한 컴퓨터이나 사람이 그 조직 전체의 정보보호 수준을 결정하는 상황이다.

또한 향후 센서 네트워크 환경 하에서 해킹은 각 센서 노드들에 대한 공격과 전파 방해, 배터리 소진 등으로 확대될 것이다.

5. 안전을 위한 보안대책

단 한번의 완전한 보안장치는 없다. 오늘의 완전한 장치가 내일의 새로운 공격에 의해 무너질 수 있기 때문이다. 그러므로 보안에 있어서는 전담조직에 의한 꾸준한 점검 및 대응이 필요하다. 소방방재 업무에서도 최대한 예방에 집중해야 하지만 일단 재난이 발생하면 신속하고 면밀한 대응이 중요한 것처럼 방재관련 시스템의 공격에 대한 보안에 있어서도 예방을 위한 작업, 그리고 침해 발생시 신속한 대응을 위한 준비가 병행되어 마련되어 있어야 하는 것이다.

그러므로 예방과 대응을 위한 기술적, 법적 대안을 몇 가지 제시하고자 한다.

- 센서 네트워크 기술의 근간을 이루게 될 RFID 태그의 활용은 그 안에 저장된 정보의 보호 문제를 얼마나 안정적으로 제공할 수 있는가에 달려있다고 볼 수 있다. 그러므로 RFID 등 USN과 관련된 기술에 대한 중요 정보의 보호를 위하여 개인정보 수집, 활용 및 폐기에 관한 법과 제도가 마련되어야 한다.
- 무선 센서 네트워크 환경에서 이동 단말의 제한된 리소스로 인하여 기존의 보안기능을 그대로 적용하는 것은 불가능 하다. 그러므로 네트워크 장비와 단말 장비에 보안 기능을 직접 탑재하는 임베디드 보안 형태가 되어야 한다.
- 각 보안 단말과 보안시스템들을 상호 연계하여 종합적인 네트워크 보안 서비스를

할 수 있는 통합 보안관리 시스템의 구축이 필요하다.

- 단일 기능으로는 지능적인 침입을 막기 어렵다. 그러므로 사용자의 접근제한, 침입방지, 침입탐지 등 단계별 보안이 필요하며 운영체제부터 응용단계까지의 보안 아키텍춰의 구축이 필요하다.
- 국내외 표준화 기구를 중심으로 초경량 암호 및 인증 기술을 개발해야 한다.
- 단말 노드간 정보교환을 위해서는 임베디드 기술을 통한 보안 S/W 기술개발 및 보안기능 탑재가 필요하며 DRM 요소기술 및 기반구조 개발과 적용을 통하여 안전하게 콘텐츠 정보를 유통할 수 있는 환경 구축이 선행되어야 한다.
- 센서 네트워크 환경에서는 객체들 각각이 모두 보안 체계를 갖추는 환경이 만들어져야 하며 보안의 적용도 사용자가 느끼지 못하도록 인간화(calm)되어 있어야 한다. 또한 전달될 정보가 항상 동일한 수준의 보안을 요구하는 경우보다는 상황에 따라 보안의 수준이 변할 수 있으므로 다양한 강도의 암호화 방법들이 상황에 적응해 적용될 수 있어야 한다.
- 소방방재에 도입될 대규모의 다양한 시스템에 대한 보안 및 안전 점검을 위한 규정 및 지침이 마련되어야 한다.
- 시스템의 보안대책 수립 및 안전점검을 담당할 보안안전 전담팀이 구성되어야 한다. 조직의 특성에 적합한 보안 안전체계를 구축하고 지속적인 점검 및 관리가 이루어져야 한다.
- 소방방재 관계자, 관련 기술자, 전 국민을 대상으로 유비쿼터스 기술에 의한 생활의 편리성과 함께 고려해야 할 정보 보호에 대한 마인드 제고 및 인터넷 범죄 예방을 위한 체계적인 안전, 보안에 대한 지식 및 의식 교육을 해야 한다.
- 범국가적으로 안전문화에 대한 방재환경 변화 및 안전에 관한 홍보를 시행하고 방재교육 및 정보시스템 안전점검을 위한 전문가의 육성 및 확보를 위한 체계를 마련해야 한다.
- 정보시스템에 의한 보안도 중요하지만 무엇보다 가장 중요한 것은 정보를 사용하는 각 개인이 정보 유출에 대해 보안시스템에만 의지하지 말고 보안에 대한 인식을 제고하고 스스로 보호하는 노력을 다해야한다.

6. 결 론

유비쿼터스 센서 네트워크를 바탕으로 하는 개인의 안전하고 편리한 u-life 실현을 위해서는 전체 시스템과 개인정보에 대한 안전한 보안환경도 함께 마련되어 가야한다. 센서를 이용한 소방 및 방재 시스템은 정보시스템에 매우 의존적이기 때문에 정보시스템의 물리적, 논리적 파괴나 침해는 국가 전체의 재난 위험을 초래할 수 있다. 그러므로 안전점검에 있어서 소방 대상물 등의 점검 뿐 아니라 방재관련 정보시스템의 안전 점검이 실시되어야 하며 이를 위한 법 규정 및 지침이 마련되어야 한다.

기본적으로 보안의 대상은 정보이며 보안의 목적은 해당 서비스를 지속적으로 유지하

는 것이다. 그렇다면 소방방재에 있어서도 관련 정보가 어떤 환경 속에서도 기밀성, 무결성, 가용성을 유지할 수 있도록 관련 법규 및 시스템을 확보하고 지속적으로 관리 및 교육을 실시해야 한다. 유비쿼터스 센서 네트워크 시대로 진전되면서 안전한 보안환경 구축은 진정한 의미의 안전하고 편리한 유비쿼터스 Safe Korea 실현을 가능케 할 것이다.

참고문헌

1. 정보통신부, "u-센서 네트워크 구축 기본계획", 2004.
2. 소방방재청, http://www.nema.go.kr
3. 이동훈, "USN 정보보호 기술동향", IITA기술정책정보단, 2005. 9.
4. 이종옥, "유비쿼터스의 개요와 동향", 전파지 5·6, 2005.
5. William Stallings, "Network Security Essentials", Prentice Hall, 2001.
6. 정진성, "최근의 보안 패러다임의 변화와 2004년 악성코드 동향", 정보과학회지, 23권 제1호 통권 제188호, 2005.