USN 응용을 위한 보안 시스템 개발

이석철*, 정명균**, 김창수*
*부경대학교 정보보호학협동과정
**부경대학교 정보시스템협동과정

e-mail:{host2000,cskim}@pknu.ac.kr, 체3325@empal.com

Development of Information Security Support System for USN Application

Seok-Cheol Lee*, Myung-Kyun Jeong**, Chang-Soo Kim*
*Interdisciplinary Program of Information Security, Pukyong Nat'l University
**Interdisciplinary Program of Information System, Pukyong Nat'l University

요 약

유비쿼터스 환경 구축을 위한 무선 센서 네트워크 기술은 센서에 의한 원격 모니터링과 같은 어플리케이션에 많은 분야에 적용되고 있다. 무선 센서 네트워크는 제한된 컴퓨팅능력으로 인해 기존의 보안 프로토콜을 적용하기 어렵고 무선 매체의 특성상 보안의 취약성을 내재하고 있다. USN 응용은 주로 센서 노드 간의 통신을 위한 센서 필드, 데이터를 수집하고 가공하는 미들웨어, 서비스를 위한 웹 서비스로 구분할 수 있는데, 각 단계에서 정보보호를 위한 보안 정책이 수반되어야 한다. 본 논문에서는 USN 응용을 위한 모니터링 시스템을 대상으로 각 단계별 정보보호 플랫폼과 보안 정책에 관한 내용을 기술한다.

1. 서론

무선 센서 네트워크(Wireless Sensor Network)는 RFID와 더불어 유비쿼터스 센서 네트워크 (USNs)를 구성하는 핵심 기술로 평가 받고 있다. 무선 센서 네트워크는 IP주소와 같은 글로벌 주소 체계를 가지지 않고, 최대 65,535개의 자체 주소 체계를 부여하는 방식으로 설계되었다. 이는 무선 센서 노드의 제한된 컴퓨팅 능력과 기존 IPv4 주소 체계의 한계로 기인한 문제로 풀이된다. USN 응용은 센서에 의한 실시간 정보 수집 기능, 데이터의 체계적인 관리가 용이한 장점으로 많은 연구 개발이 진행되고 있으며, 이에 따른 무선 센서 네트워크 기술 역시 지속적인 연구 개발이 진행되어 오고 있다.

USN응용은 현재 각종 시범사업을 통한 유비쿼터스 정보화 사업에 널리 적용되고 있으며, 물류, 교통, 공장 등에 적용되고 있으며, 지속적인 확장이 진행되고 있다.

그러나 가장 큰 문제점은 대부분 보안 정책은 고려하고 있지 않다는 점이다. 실제로 패킷 스니퍼 장비와 같은 도구를 이용하여 무선 패킷의 전송 상황이 노출될 우려가 있으며, 이는 쉽게 도청 공격과 같은 상황에 노출됨을 의미한다.

본 논문은 2008년 중소기업청 중소기업기술혁신개발사업(위탁연구)에 의해 지원되었음

또한 노드의 신원 위장에 의한 오류 정보의 전송, 특정 노드로의 DoS(Denial of Service)공격으로 인한 노드 자원의 고갈 등에도 쉽게 공격 당할 우려가 있다. 또한 싱크 노드에서 미들웨어 서버로의 전송 단계에서 발생할 수 있는 보안의 취약성, 사용자 서비스를 위한 정보의 무결성과 가용성을 고려한 보안 정책이 반드시 필요하다.

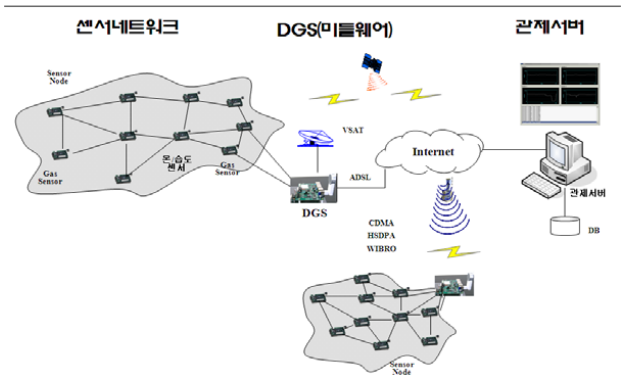
본 논문에서는 USN 응용의 전형적인 모델을 기반으로 각 단계에서 발생할 수 있는 공격 가능성과 보안 취약성을 고찰하고, 이에 적합한 보안 플랫폼을 제시한다.

2. 관련 연구

2.1 무선센서네트워크

무선 센서 네트워크는 빛, 소리, 온도, 움직임 등의 물리적인 데이터를 센서 노드에서 감지하고 측정하여, 중앙의 기본 노드(base-station or SINK Node)로 전달하는 센서 노드들로 구성되는 네트워크이다[1][2][3][7]. 센서 네트워크가 기존의 네트워크와 구분되는 점은 상호간의 정보 전달 보다는 자동화된 원격 수집에 있다는 점을 들 수 있다[1][2][3]. 즉, 각 센서 노드가 특정 목적을 위해 필요한 주변의 이벤트를 센싱하고, 센싱된 정보를 센서 노드간의 Ad-hoc 네트워크를 이용하여, 전달하고, 사용자는 원격으

로 취합된 정보를 활용할 수 있다는 것이다. 이러한 센서 네트워크는 무선 센서 필드 개념을 중심으로, 불특정 공간에 배포된 센서로부터 수집된 정보를 일괄적으로 활용하는 것을 의미한다[2]. 최근 유비쿼터스 컴퓨팅 분야에서 이러한 센서 네트워크가 대표적으로 부상하고 있는데, 이는 센서 네트워크 노드가 독자적으로 네트워크를 구성하는 구성의 용이성 때문에 기반기술로 운용할 수 있는 장점이 있다. WSN은 미국 버클리 대학의 MOTE 센서 노드 플랫폼을 기준으로 TinyOS 운영체제를 기반으로 하는 플랫폼이 주류를 이루고 있다. 그러나 대부분의 TinyOS를 기반으로 하는 응용에서는 보안 정책은 고려하고 있지 않으며, TinySec 이라는 별도의 보안 소프트웨어를 내장하여 사용하여야 한다. USN 응용의 큰 흐름은 센서 노드에 의해 구성되는 센서 네트워크 필드(WSN Fields), 수집되는 센서 데이터 관리를 위한 미들웨어(Middleware), 사용자 서비스(User Service)의 3단계로 구분하며, 각 단계에서는 유/무선 통신에 의한 데이터 전송이 이루어진다. 결국 USN응용의 보안을 위해서는 3가지의 보안 정책을 모두 수반한 개발이 이루어져야 한다.



(그림 1) USN 응용 플랫폼

2.2. WSN의 보안 취약성

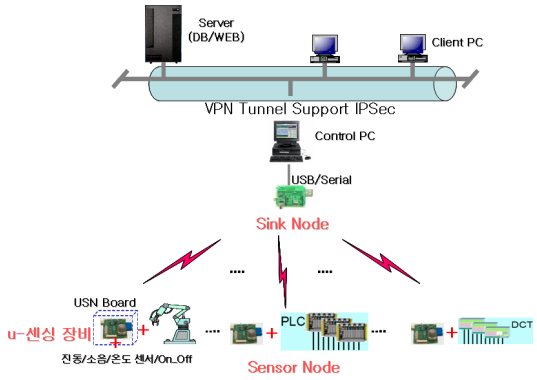
무선 센서 네트워크를 이용한 어플리케이션은 크게 세 가지의 주된 구성요소를 가지고 있다. 첫 번째로, 무선 센서 네트워크의 하드웨어는 주로 마이크로 센서와 마이크로 컨트롤러, 무선 통신을 위한 칩셋으로 구성되어 있고, 센서 노드를 제어하고, 실제 센서 네트워크를 구축하고 운용하기 위한 운영체제가 포팅되어 있다[6-7]. 여기서 무선 센서 네트워크의 보안 문제를 고려해 보면, 무선 센서 노드의 특성상 무선 매체가 가지고 있는 보안의 취약성을 그대로 가지고 있으며, ID를 위장한 위장 수법에 의한 공격, 특정 노드로의 무한 루프에 의한 패킷 전송에 의한 DoS공격과 같은 상황에 직면할 경우, 오용된 데이터의 전파, 시스템 마비와 같은 치명적인 결과를 가져올 수 있다. 이러한 공격을 대비하기 위한 방법으로는 노드 간의 통신에 있어서 공개키 알고리즘에 의한 키 교환 및 분배, 노드의 ID를 이용한 센서 노드의 신원확인과 같은 절차가 필요하다. 그러나 이러한 보안 모듈의 탑재는 제한된 모바일 컴퓨터 시스템에 있어서 부하 현상을 야기할 수 있으며, 과중한 보안의 경우 저속 통신 체계인 무선 센서 네트워크의 성능 저하에 영향을 미칠 수 있다. 두 번째로 센서 네트워크의 구성요소인 미들웨어는 보통 미들웨어를 탑재한 서버 혹은 미들웨어의 기능을 수행하는 임베디드시스템에 탑재되는 경우가 많다. 미들웨어의 주요 기능은 첫 번째로 센서가 동작하는 소스 노드로부터 전송되는 데이터를 취합하는 기능과, 이를 데이터베이스 시스템과 같은 저장소 시스템에 전송하는 기능을 수행하는 게이트웨이 기능을 가지고 있다. 게이트웨이 기능과 같은 경우 기존의 유/무선랜과 CDMA, HSDPA 와 같은 상용 이동통신 체계를 이용하는 경우가 많으며, 최근에는 원격지에서 효율적인 데이터 전송을 위한 임베디드 시스템에 CDMA와 같은 상용 이동통신망을 이용하여 전송하는 방법이 널리 쓰이고 있다[9].

2.3 USN 응용을 위한 보안 정책

u-방재 시스템을 위한 보안 정책의 도입과 운용은 중요한 사항으로 지적된다. 먼저 무선 센서 네트워크에서의 보안 취약성의 대표적인 문제는 노드의 신원 위장에 의한 공격이 있을 수 있다. 가령 센서의 고유한 이름과 같은 노드 ID를 위장하여 거짓된 정보를 보내는 등의 신원 위장 공격 하에서는 전체 시스템의 교란으로 이어질 수 있다. 예를 들면, 정상적인 ID 번호 X번의 센서 디바이스를 단절시키고, 거짓 정보를 보내기 위하여 프로그래밍 된 센서 디바이스를 설치하여 네트워크 상에 동작하게 할 경우, 거짓된 위험 정보를 미들웨어가 수신하고, 위험 상황으로 판단하여 각 기관에 거짓된 정보를 보낼 수 있다. 이 경우 실제 위험 상황이 발생하지 않았음에도 불구하고, 각 기관에서는 대응을 위한 조치, 시민들의 대피 상황과 같은 혼란이 발생할 가능성은 자명하다. 이를 위해서는 정상적인 네트워크 구성을 위해 가입 노드의 신원 인증을 위한 인증체계, 공개키 기반의 암호화 알고리즘의 적용 등이 필요하다. 두 번째 센서 데이터를 처리하는 미들웨어의 보안 문제를 들 수 있다. 미들웨어는 센서 네트워크의 우두머리격인 Sink 노드로부터 센서 데이터를 수신받아 이를 가공하여 처리하는 기능을 담당하고 있는데, 보통 Sink 노드로부터 미들웨어 서버까지의 전송로는 공중망, RS-232C 시리얼 인터페이스와 같은 물리적인 접속, 위성, 전화 망 등 다양한 형태의 경로로 구성 할수 있다. 물리적인 접속을 제외한 공중망 사용 역시 위장 공격에 취약할 수 밖에 없다. 인터넷을 비롯한 공중 통신망은 개방형 인터페이스로 모든 패킷이 방송 형태로 전송되는 형태를 가지고 있으며, 이 경우 해킹 등의 사이버 테러에 노출 될 우려가 높다. 이를 보완하기 위한 방법으로 전용의 전송로를 구성하고, 전송되는 데이터의 암호화 및 복호화 작업이 따라야 한다.

3. USN 응용을 위한 보안 플랫폼 설계

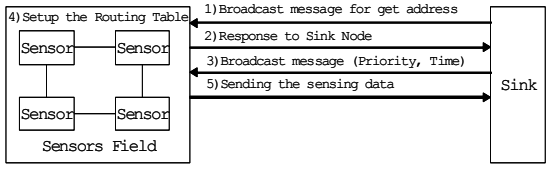
본 논문에서 제안하는 전체 시스템은 센서 필드, 미들웨어, 사용자 서비스의 세 부분에 보안 정책을 적용한다. [그림 1]은 시스템 구성도를 나타낸다.



(그림 1) 전체 시스템 구성도

3.1 센서 노드 보안

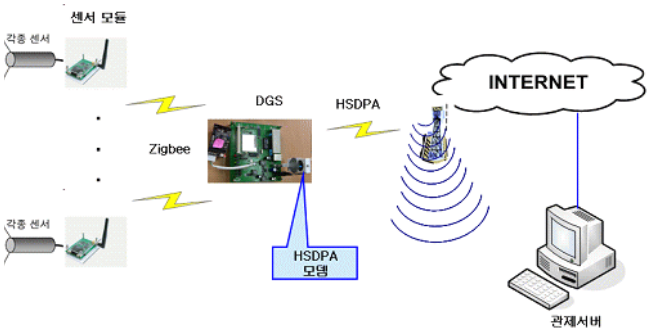
본 논문에서는 센서 네트워크 구축 시험을 위해 Telos-B기반의 센서 노드 15개에 TinyOS를 탑재하였다. 각 센서 노드는 1초 간격의 센싱 타임으로 데이터를 수집하여 전송하는 어플리케이션을 구성하였다. 실험을 위하여 노드의 개수는 싱크 노드를 포함하여 15개의 노드를 배치하여 2개의 그룹으로 배치하였다. 그리고 기본적인 데이터 보안을 위하여 CC2420칩셋에 내장된 보안 관련 API를 모두 활성화 시켜 하드웨어 레벨의 보안 체계를 구축하였다. 보안 관련 API를 사용하여 동작할 경우 기본적으로 전송 효율은 조금 떨어지나, 패킷의 무분별한 브로드 캐스트에 의한 수신측의 오작동은 쉽게 예방할 수 있다는 장점이 있다. 그리고 TinyOS에서 제공하는 TinySec을 사용하여 간단한 접근제어와 메시지, 위 변조를 막을 수 있는 무결성기능과 센서 정보의 해석을 방지하는 기밀성을 제공할 수 있도록 설계하였다. 센서 네트워크에서 센서 노드와 싱크노드 간의 데이터를 수집하고 전송하기 위한 방법은 다음의 절차를 거치도록 구성하였다. 첫 번째로 싱크노드는 센서의 정보를 획득하기 위하여 브로드캐스트 메시지를 송출한다. 싱크노드로부터 메시지가 도착하면 센서노드는 자신의 물리주소와 Application ID를 CC2420에 내장된 AES128알고리즘을 사용하여 암호화 한 후 싱크노드로 전송한다. 다음 단계로, 싱크노드는 센서노드의 우선순위를 부여한다. 이는 메시지 패킷형태로 전송되는데, 이 메시지에는 센싱주기와 센싱의 우선순위가 정해진다. [그림 2]는 센서 네트워크 운영 방법을 나타내었다.



(그림 2) 센서 네트워크 운영 방법 및 메시지 흐름도

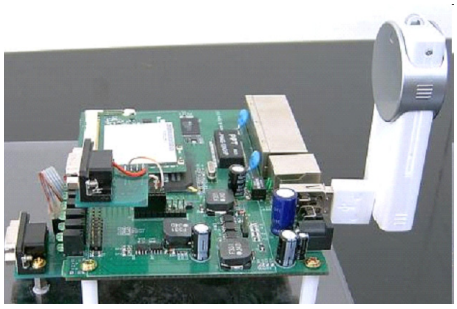
3.2 VPN 터널링에 의한 게이트웨이 보안

본 논문에서 소개하는 센서 네트워크의 게이트웨이는 (그림 3)과 같이 미들웨어 서버와의 안전한 통신을 위해 임베디드 리눅스 기반의 시스템에 VPN터널을 구축하여 설계하였다.



(그림 2) 위해요소 감지를 위한 하드웨어 플랫폼

개발 시스템은 게이트웨이 측에 설치되어 다음과 같은 기능을 수행한다. 먼저 게이트웨이는 (그림 3)과 같이 S3C4530 MCU를 사용한 게이트웨이를 구성하였다. S3C4530의 경우 ARM7TDMI Core가 내장되어 있고, 내부에는 Network를 위한 H/W를 가지고 있다. WAN 전송을 위한 인터페이스로는 HSDPA 형식의 USB 모뎀을 사용하였다. 따라서 S3C4530의 Ext I/O 영역에 매핑하여 사용이 가능하다. UART는 S3C4530내부에 2개가 존재하므로 외부에 Driver만 장착하여 사용한다. UART0는 프로그램 개발동안 콘솔 포트만 사용하고 리눅스의 포팅이 끝난 후 데이터를 관제 센터로 보내는 기능을 수행한다. 두 번째로 IPSec 암호화 기능은 vlinux를 이식한 운영체제에 freeswan 1.9 OpenSource를 포팅하여 설계하였다. 이러한 과정을 거친 후 개발 시스템과 관제 서버 앞단에 있는 VPN게이트웨이와는 서로 암호화 된 Tunnel을 형성한다.



(그림 3) 보안 기능을 탑재한 센서 게이트웨이

개발 시스템 상에 동작하는 암호화 프로그램과 관제서버에서 동작하는 Tunneling 프로그램은 통신하는 대상이 모두 Tunnel 내부에 해당하므로 개발 시스템과 VPN게이트웨이 사이에서 Protocol에 의해 암호화 된다.개발 시스템은 유동 IP를 얻어서 인터넷에 접속된다. 터널과 관련된 파라미터는 웹 인터페이스를 통하여 설정할 수 있다. 터널을 형성하는 방법은 크게 네트워크 인터페이스 위에

IPSec 라는 가상의 인터페이스를 설정하는 방법과 명령어를 이용하여 터널 설정 정보를 커널에 전달하고, 터널을 생성하는 방법이 있다. 개발 시스템과 사용 VPN게이트웨이와는 터널이 연결된 상태에서 핑 테스트를 실시하고, 되돌아오지 않을 경우 터널의 문제가 발생하였다고 간주한다. 이 때 공격에 의한 터널의 파괴, 혹은 전원 단절과 같은 물리적인 에러에서도 게이트웨이와 VPN 시스템은 터널 생성을 계속 시도하여 터널을 반드시 생성한 후 데이터를 전송한다.

4. 연구 고찰

본 논문에서 기술한 개발 시스템은 첫 번째로 센서 노드에 의한 센서 네트워크 필드 환경에서의 데이터 암호화를 지원한다. 성능 시험을 위하여 Zigbee 패킷 스니퍼를 통해 전송되는 패킷을 캡처해 본 결과 정상적으로 암호화된 데이터 패킷을 수신할 수 있었다. 두 번째로 싱크노드와 미들웨어까지의 VPN게이트웨이를 이용한 터널 구축을 통한 암호화 통신은 기본적으로 개발된 VPN 터널을 사용할 경우 시스템의 전송율은 보안 모듈을 탑재하지 않은 시스템에 비교하여 떨어지지만, 전용의 암호 통신로를 확보함으로써, 감지영역의 보안 전송로를 통한 중요 정보 전송 기능을 수행할 수 있었다.

5. 결론

유비쿼터스 센서 네트워크 (USN)기술은 기존의 사람 중심의 네트워크에서 사물 중심의 네트워크 기능을 지원하고, 구축된 인프라 내에서 사람은 그 환경 속에서 어우러져 살아가는 유비쿼터스 컴퓨팅의 핵심 기술로 평가 받고 있다. 본 논문에서는 USN 응용을 위한 보안 시스템을 개발, 적용함으로써 보다 안전한 정보 전송이 가능하도록 하였다. 제안한 시스템은 센서 네트워크 필드 레벨에서의 기본적인 암호화 통신과 임베디드 시스템 기반의 보안 게이트웨이를 통한 센서 노드와 미들웨어간의 IPSec을 사용한 VPN 터널방법으로 전용 전송로를 확보할 수 있다. 개발된 시스템은 전체 센서 네트워크 영역의 미들웨어에 탑재되어 서버와의 게이트웨이 역할을 수행하면서 암호화 통신을 지원한다. 이렇게 개발된 시스템은 공장 설비관리, 원격 감시 시스템, 홈 시큐리티를 위한 게이트웨이, 기타 보안 데이터 전송이 필요한 분야에 사용 가능할 것으로 판단된다.

참고문헌

[1] K.T. Erickson et al., Reliability of SCADA Systems in Offshore Oil and Gas Platforms, Stability and Control of Dynamical Systems with Applications, Birkhauser Press, 2003, chapter 20.

[2] A. Miller and K.T. Erickson, Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity, Int'l Workshop Research and Education in Control and Signal Processing, NATO Symp. Adaptive,Defence in Unclassified Networks, 2004, pp. 13-1?13.8.

[3] D. Craigen et al., Multi-Layer Vulnerability Assessments of SCADA Networks, Proc. Ottawa, CyberSecurity Workshop, 2005

[4] US Computer Emergency Readiness Team, Control Systems Cyber Security Awareness, US-CERT, 7 July 2005

[5] A.B. Baker et al., A Scalable Systems Approach for Critical Infrastructure Security, tech. report SAND2002-0877, Sandia Nat'l Labs., Apr. 2002

[6] K.H.Jung et al, The Design and Implementation of Real-Time Environment Monitoring System Based on Wireless Sensor Networks, International Conference Computer Science and its Application , 2006, Glasgow in Scotland.

[7] 이석철, 신삼범, 김명호, 김창수, 스마트공장을 위한 무선센서 기반의 모니터링 시스템 설계 및 구현, 한국멀티미디어학회 춘계학술발표대회, 2007.05.

[8] A. Boulis, C.C. Han, and M. B. Srivastava, Design and Implementation of a Framework for Programmable and Efficient Sensor Networks, In The First International Conference on Mobile Systems, Applications, and Services (MobiSys), San Francisco, CA, 2003.

[9] 윤철환, 김희천, 나종화, 신승중, 정광호, 류대현, IPSec을 이용한 원격 감시 및 제어 시스템에 관한 연구, 제19회 한국 정보처리 학회 춘계학술발표대회 논문집 제 10권 제 1호, 2003.05