GPS 시간 정보를 이용한 불법 침입 탐지시스템 구현

김관형* ·성기택**

*동명대학교 컴퓨터공학과

**동명대학교 정보보호학과

Implementation of Illegal IDS(Intrusion detection system) Using GPS Time Information

*Gwan-Hyung Kim, **Ki-Taek Seong

*Dept. of Computer Eng., Tongmyung Univ.

**Dept. of Information Security, Tongmyung Univ.

E-mail : kimgh69@nate.com

요 약

본 논문에서는 무선 센서네트워크 환경에 적용할 수 있는 불법 침입자를 감지하는 시스템으로 GPS의 위성시간과 단말기 노드 내부의 암호화 동기 시간 설정 알고리즘을 혼합하여 시간 중심의 암호화 인증시스템을 설계하여 불법적인 외부노드의 침입을 탐지하는 방법을 제안하고자 한다.

본 논문에서는 GPS의 시간 정보와 RTC(Real Time Clock) 칩과 동기화 하여 시간 정보를 실내에서도 사용할 수 있으며, 마이크로프로세서 내부 타이머 설정 시간 등을 고려하여 다중화된 시간 정보를 이용하여 보다 높은 수준의 침입 감지 시스템을 개발하여 효율성을 제시하고자 한다.

키워드

USN security, GPS, RTC, Intrusion Detection System

Ⅰ. 서 론

ZigBee는 저전력, 초소형, 저가격, 사용의 편리성을 가진 근거리 무선 센서네트워크의 대표적인 기술로 유비쿼터스(ubiquitous) 컴퓨팅 기술의 하나로 IEEE 802.15.4 표준의 PHY/MAC 층을 기반으로 상위 프로토콜(protocol)과 응용(application)을 표준화한 기술이다.

ZigBee 기술의 적용은 근거리에서 속도가 빠르지 않고, 네트워크의 사용이 그리 많지 않은 시스템에 가장 최적화된 시스템이다. 이러한 ZigBee 기술은 지능형 홈네트워크, 유비쿼터스 센서 네트워크(USN), 물류, 환경 모니터링, 헬스케어, 군사 등 다양한 유비쿼터스 컴퓨터 환경에 성공적으로 적용되고 있다.[1]

그러나 무선 센서네트워크가 갖는 근본적인 보안의 문제를 가지고 있다. 이러한 외부의 접근을 감지하기 위하여 ZigBee 내부의 PHY/MAC 층을 통하여 보안의 문제를 해결하거나 기타 어플리케이션 영역에서 보안 문제를 해결하고 있다.[2][3]

본 논문에서는 내부의 PHY/MAC 영역을 사용하는 대신 최종단의 어플리케이션 영역에서 GPS 시간을 활용하여 ZigBee 네트워크 내부의 모든 코디네이트, 라우터 및 엔드 디바이스의 GPS의 절대시간을 맞추어 동작하도록 하여 시간에 대한 정보를 보안의 키로 사용할 수 있음을 제시하고자 한다. 또한, GPS의 절대 시간은 다시 단말기 내부 시간 소자인 RTC(Real Time Clock) 칩과 동기화 시켜 실내에서도 시간 기반으로 보안을 적용시킬 수 있는 시스템을 제안하고자 한다.

Ⅱ. 시간기반의 보안 시스템 구성

ZigBee 네트워크 상의 모든 단말기는 GPS 모듈을 탑재하여 모든 디바이스에 절대시간을 디바이스 내부에 달라스 맥심사의 RTC DS1302 칩에 절대시간을 설정하도록 한다. 설정된 내부의 절대시간은 ZigBee 내부 네트워크 상의 모든 디바이스는 주기적으로 시간 정보를 갱신하여 동기화

하도록 설정하여 네트워크 관리자인 코디네이트나 라우터로 디바이스의 동기화된 시간을 전송하도록 한다. 이렇게 내부 ZigBee 네트워크의 시간 정보를 수신하여 주기적으로 다르게 동기화된 시간을 이용하므로 불법 침입에 대한 디바이스를 판단할 수 있게 된다.

이러한 시스템의 침입 검출 알고리즘에 대한 흐름도를 그림 1에 제시하였다.

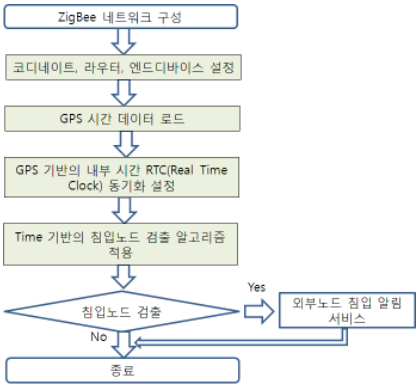

그림 1. 침입 탐지 흐름도

III. 기간 기반의 침입 탐지시스템 설계

본 연구의 알고리즘과 실험을 위하여 MaxStream사의 지그비 모듈(XBee Series) 3개와 Atmel 사의 Atxmega128A1 칩을 탑제한 CPU 모듈 3개를 이용하여 시스템을 구성하였다. GPS 모듈은 UIGGUB02-R001을 이용하여 GPS의 세계협정시간(UTC;Universal Time Coordinated)을 이용하여 각 지역의 지역시간을 설정한다.

이러한 지역시간은 다시 ZigBee 내부의 네트워크 시간으로 다시 동기화 하여 로컬 네트워크 내부의 암호화 동기화 시간으로 사용하였다. 또한, GPS 데이터가 수신 불가능한 실내에서도 시간 데이터를 사용할 수 있도록 Atxmega128A1 모듈과 RTC DS1302 칩의 입 출력 3핀(CE, I/O, SCLK)을 사용하여 인터페이스 하여 GPS 시간과 디바이스 내부 시간과 동기화 하였다.

이러한 시스템의 구성은 그림 2와 같이 구성하였다.

그림 2. GPS와 XBee 기반의 노드 구성

IV. 실험 및 고찰

GPS 데이터는 NMEA-0183 프로토콜 규약을 따르고 있다. GPS 데이터에서 시간 데이터를 추출하기 위한 센턴스(sentense)는 $GPGGA의 센텐스를 이용하여 시간, 위도, 경도 값을 추출하여야 한다. $GPGGA 필드의 내부 데이터들은 $로 시작하여 콤마(,)로 구분되어 있으며, 이러한 GPS의 "$GPGGA,075001.00,3700.00005,N,12659.99991,E,1,09,0.89,80.5,M,18.8,M,,*62" 데이터를 Xmega128에서 위도, 경고 좌표와 세계협정시간을 파싱(parsing)하여 사용하였다. 추출된 시간은 네트워크 내부의 시간 동기화 암호를 위하여 ZigBee 네트워크 내부에서 주지적으로 네트워크 내부의 동기화 시간을 재설정하여 보안의 수준을 높일 수 있도록 프로그램 하여 실험하였다.

코디네이트로 들어온 각 노드의 내부 기간 데이터는 호스트 PC의 LabView 프로그램을 이용하여 모니터링 하여 불법 침입 디바이스를 확인할 수 있었다.

그림 3. 침입 탐지시스템 모니터링 화면

V. 결 론

본 논문에서는 ZigBee 기반의 내부 센서 네트워크 환경에서 GPS의 시간 정보 및 RTC 시간 정보를 바탕으로 내부 네트워크의 주기적으로 변경되는 내부 동기화 시간과 일치하지 않는 디바이스의 접근을 감지하는 시스템을 제시하였다. 또한, GPS 데이터의 수신이 불가능한 실내에서는 디바이스 내부의 RTC를 이용하여 시간의 동기화를 맞출수 있어 실내에서도 접근 탐지가 가능한 시스템으로 그 활용도가 높다고 할 수 있다.

참고문헌

[1] 성기택, 김관형, "무선 센서 네트워크에서 MAC 주소 기반의 불법 노드 침입탐지시스템 구현", 한국해양정보통신 종합학술대회논문집, 제 15권 1호, p.727-730, 2011

[2] 김호원, 이석준, 오경희, "센서 네트워크 보안 기술 개발 동향", 정보보호학회지 제 18권 제 2호, 2008.4

[3] (주)한백전자 기술연구소, "유니쿼터스 센서네트워크 시스템", p.426-443, 2005