USN 환경에서 센서노드 데이터 인증 설계 및 구현

김원영* · 이영석*

*군산대학교 전자정보공학부

Design and Implementation of Sensor node data Authentication in USN Environment

Won-young Kim* · Young-seok Lee*

*School of Electronic and Information Engineering, Kunsan National University

E-mail : kimwin02@hotmail.com, leeys@kunsan.ac.kr

요 약

언제, 어디서나, 누구라도 컴퓨터와 네트워크를 통해 손쉽고, 편리하게 서비스를 제공 받을 수 있도록 컴퓨터를 실생활 환경 속에 편재시키는 유비쿼터스 컴퓨팅(Ubiquitous Computing)은 차세대 컴퓨팅을 주도할 개념으로 급부상하고 있다. 이러한 환경 속에서 안전하게 서비스를 이용할 수 있는 환경은 매우 중요하다. 그러나 유비쿼터스 환경을 구축하는 대부분의 센서 노드들은 초소형, 초경량의 제한된 자원을 가지고 있어, 기존의 무선 네트워크에서 사용된 기술을 그대로 사용할 수 없다. 따라서 최소한의 자원을 사용하는 보안 기술개발이 필요하다.

본 논문에서는 기존의 SHA1알고리즘을 센서 네트워크에서 사용할 수 있도록 경량화하여 적용해 보았다. 각 노드에서 센서 값을 취득하여 디지털로 변환하고 무선 통신으로 전송하기 전에 인증 알고리즘을 거쳐서 생성된 인증값을 보내려는 데이터에 추가하여 전송한다. 이 데이터를 받은 노드에서는 동일한 알고리즘으로 인증 값을 생성하고 받은 인증값과 비교하여 데이터의 인증 절차를 수행한다. 이렇게 함으로써 데이터의 정확성이나 무결성을 보장할 수 있다.

키워드

유비쿼터스 센서 네트워크, 인증, SHA1

Ⅰ. 서 론

유비쿼터스 센서 네트워크란 기존 인간과 컴퓨터 간의 커뮤니케이션에 일상 생활 속에 산재된 사물과 물리적 대상을 추가시켜 협력 네트워크를 구성하는 것으로, 필요로 하는 모든 곳에 수많은 센서 노드들을 부착하여 자율적으로 정보를 수집, 관리 및 제어하는 시스템이다. 즉 물리 공간에 빛, 소리, 온도, 움직임 같은 물리적 데이터를 센서 노드에서 감지하고 측정하여 중앙의 기본 노드로 전달하는 구조를 가진 네트워크이다. 따라서 향후 유비쿼터스 센서네트워크 환경에 대한 의존성과 그에 대한 영향력이 급속하게 증가하게 될 것이다.

그러나 이러한 유비쿼터스 컴퓨팅의 특성은 데이터의 보안이 취약할 경우 기존 컴퓨팅 환경보다 더 큰 문제를 발생시킬 수 있다. 또한 수집된 데이터가 유출 및 변조될 경우 사용자에게 심각한 피해를 줄 것이다.

이러한 문제는 실제 유비쿼터스 컴퓨팅이 현실화되는데 있어 때 가장 큰 걸림돌로 작용할 수 있다.

본 논문은 2장에서 초경량, 저전력 암호기술 및 보안 프로토콜에 대해 기술하고, 3장에서 SHA1알고리즘을 이용하여 데이터 인증을 메커니즘을 설계한다. 4장에서는 실험환경을 구축하여 실제 데이터를 인증을 실험하고, 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

유비쿼터스 센서 네트워크에서 센서노드의 전원은 주로 배터리를 사용하고, 주변 환경을 센싱할 수 있는 센서들로 구성된다. 또한 센서노드들은 작은 사이즈의 메모리와 낮은 데이터 처리 능력을 가지며, 전원의 제약으로 단거리 무선 통신이 가능하다.

유비쿼터스 환경에서 센서 네트워크의 응용분야가 넓어지면서 센서노드의 보안성은 매우 중요한 요소가 되었다. 그러나 센서노드의 한정된

자원으로 인하여 기존 네트워크 환경에서 사용하고 있는 메커니즘을 그대로 사용할 수 없다.

따라서 센서 네트워크에서 사용할 수 있는 경량의 보안 메커니즘과 에너지 소비를 줄이는 방안은 중한 과제이다.

2.1 초경량 , 저 전력 암호화 기술

국내외적으로 센서노드의 한정된 전력을 고려한 초경량, 저 전력 암호화 기술들이 많이 연구되고 있다. [1][2]의 논문은 대표적인 초경량 저 전력 암호 기술들 중에 하나로 다양한 하드웨어 플랫폼에서의 암호 알고리즘들의 수행속도를 평가한 논문들이다. 이 방법들은 암호 알고리즘들 중 보다 빠른 암호 알고리즘을 사용하여 저 전력 문제를 해결하고자 하였다. [1],[2]는 대칭키 방식으로 통신에서 사용될 비밀키를 노드가 미리 가지고 있는 방식이다. 그러나 이방식의 문제점은 임의의 한 노드에서 비밀 키가 누출된다면 더 이상 이 비밀 키를 가진 노드와는 안전한 통신은 할 수 없다.

[3]의 논문에서는 경량(lightweight) 센서노드에 탑재 가능한 저 전력 공개키 암호로(Rabin Ntru)를 구현하였다. Robin Scheme은 인수분해 문제의 어려움에 기반한 RSA의 특별한 하나의 형태로 1976년 Rabin이 제안하였다.

2.2 보안 프로토콜

센서 네트에서의 안전성을 고려한 보안 프로토콜로는 UC 버클리에서 개발한 SPINS(Security Protocols for Sensor Networks)이 있다. SPINS는 리소스가 제한된 무선통신 환경에서의 두개의 기본구조인 uTESLA와 SNEP로 구성된다. 하나의 대칭적인 암호화 함수로 암호화, 인증코드, 랜덤 수 생성 등을 제공하며 MAC을 위한 8byte의 메시지를 할당하기 때문에 낮은 통신 오버헤드를 갖는다. SPINS는 데이터의 비밀성, 인증, 무결성을 보장하기 위한 SNEP라는 프로토콜과 데이터를 브로드케스트(broadcast)하는 것에 대한 인증을 위한 uTESLA라는 프로토콜을 제안하여 자원 제한적인 센서 네트워크에서의 안전한 통신에 대한 방법을 제시하였다. 또한 데이터 알고리즘의 효율성에 초점을 두고 설계되었고 센서노드에 마스터키가 저장된 상태로 센서노드가 발급된다. SPINS의 uTESLA는 일방향 해쉬 체인을 사용하고 MAC 키 생성을 시간대로 분할하여 브로드케스트 한다. 브로드케스트 할 때 시간간격이 너무 작으면 해쉬 체인이 빨리 소모되므로 시간간격을 고려해야 한다. SPINS에서는 특성상 시간대를 분할하는 것은 전체 네트워크의 전력소모를 가져올 수 있다는 문제점을 가지고 있다. 또한 비밀통신을 위해 마스터키를 노드에 저장한 상태로 노드가 발급되기 때문에 안전성 측면에 문제가 있고 센서노드 메모리에도 부담이 된다[4].

III. 인증 메커니즘 설계 및 구현

3.1 인증 메커니즘 동작

해쉬 함수는 임의의 길이의 메시지를 일정 길이(128bits, 160bit 등)의 출력으로 변환하는 함수이다.

해쉬 함수는 주어진 출력에 대하여 입력 값을 구하는 것이 계산상 불가능(일반향성)하고 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능(충돌 회피성)하다는 특성을 갖고 있다.

이러한 특성에 따라 해쉬 함수는 주로 메시지의 기밀성(Confidentiality)보다는 주로 정확성(Accuracy)이나 무결성(Integrity)을 중요시 하는 업무에 사용된다.

이러한 특성을 가지고 있는 해쉬 함수인 SHA1 알고리즘 사용하여 임의의 길이 평문 메시지 M에 대하여 일정 길이(20bit)의 메시지 인증 코드(H[M])로 만들어 낸다. 이때 사전에 분배된 암호화 Key를 사용한다. 평문 메시지와 메시지 인증코드를 안정성이 보장되지 않는 통신로를 통해 수신자에게 전송하면 수신자는 사전에 분배된 암호화키 Key와 동일한 SHA1 알고리즘을 이용하여 전송받은 평문 메시에 대한 메시지 인증 코드를 만들어 낸다. 수신자는 이때 전송받은 메시지 인증 코드와 생성된 메시지 인증코드와 비교하여 타당한 문장이라면 메시지를 인증하는 것이다.

다음 [그림 1]은 인증 메커니즘의 동작에 대한 일반적인 그림으로 표현한 것이다.

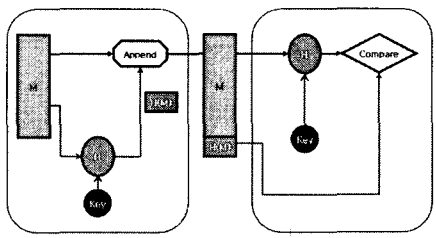

그림 1. 해시절차

3.2 ZigbeX모트 인증 컴포넌트 연결 구성도

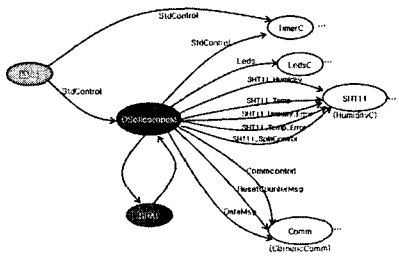

그림 2. 수신 노드 컴포넌트 연결 구성도

[그림 2]는 전송 노드에서 습도를 측정하기 위한 컴포넌트 연결 구성도로 프로그램을 시작하기 위한 Main 컴포넌트와 125ms 마다 Timer.fired()함수를 호출하기 위한 TimerC 컴포넌트, LED를 제어하기위한 LedsC 컴포넌트, 온·습도의 측정값을 얻을 수 있는 HumidityC 컴포넌트 그리고 무선 통신을 위한 GenericComm 컴포넌트가 선언되어 있다. 여기서 HumidityC 컴포넌트와 GenericComm 컴포넌트는 각각 SHT11과 Comm이라는 이름으로 선언되어 사용된다.

OscilloscopeM에서 우선 필요한 변수를 선언하고, 실제 구현 부분에서 사용할 여러 컴포넌트의 인터페이스들을 기술한다.

처음 호출되는 StdControl.init() 함수는 여러 컴포넌트들 및 변수들의 초기화와 관련된 일을 처리한다. 그 다음 호출되는 StdControl.start() 함수에서는 125ms 시간마다 반복해서 signal을 발생시키는 Timer 컴포넌트 및 시리얼 통신 부분을 담당하는 CommControl 컴포넌트 그리고 SHT11 컴포넌트와 관련있는 Splitcontrol 컴포넌트를 활성화 시킨다.

StdControl.start()에서 설정된 Timer 컴포넌트에 의해 125ms 마다 Timer.fired() 함수가 호출되고, 이 함수에서는 SHT11_Humidity.getData() 함수를 통해 SHT11 칩에게 습도 또는 온도 값을 요청한다. HumidityC 컴포넌트는 SHT11 센서로부터 요청한 결과 값을 받은 후, event 형태로 SHT11_humidity.dataReady(uinit16_t) 함수를 통해 상위 컴포넌트에게 센싱값을 전달한다.

그 후, 상위 컴포넌트에서는 전달 받은 값을 SHA1 컴포넌트를 사용하여 인증값을 생성하고, 생성된 메시지 인증코드를 센싱한 값과함께 Comm 컴포넌트의 SendMsg.send[uini8_t](...) 함수를 통해 수신 노드로 전송하게 된다.

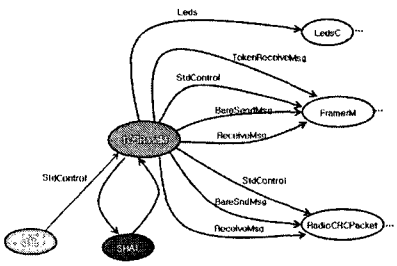

그림 3. 수신 노드 컴포넌트 연결 구성도

[그림 3]은 수신 노드의 컴포넌트 연결 구성도로 수신되는 메시지가 있을 때, 시그널이 발생해서 그 메시지를 받고 그 안에 있는 데이터 값을 가져와서 LED와 SHA1 컴포넌트로 보낸다.

SHA1 컴포넌트에서 전송받은 데이터 값에 대한 메시지 인증코드를 생성하고, 함께 전송받은 메시지 인증코드와 비교하여 전송받은 데이터를 인증한다. 인증에 성공하면 UART 컴포넌트를 사용하여 데이터를 Serial로 Base Station에게 보낸다.

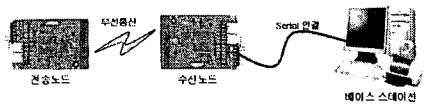

그림 4. 센서 노드 구성도

[그림 4]는 전송 노드 및 수신 노드, Base Station의 전체 구성도를 나타낸다.

전송 노드에서 센싱한 데이터를 인증값과 함께 무선통신으로 전송하면 수신노드에서는 전송받은 데이터를 동일한 알고리즘으로 인증값을 생성하고 데이터값과 함께 전송된 인증값과 비교하여 동일하면 Base Station에게 Serial로 전송한다.

3.3 인증 컴포넌트의 전송 메시지 형식

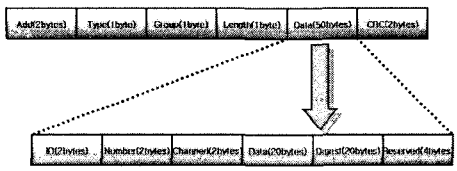

그림 5. 전송 메시지 형식

[그림 5]는 전송 노드에서 무선으로 데이터를 전송시 메시지 형식으로 그 구성은 특별한 메시지 형식과 Data로 이루어 졌다. 특별한 메시지 형식에는 주소(2byte), 타입(2byte), 그룹아이디(2byte) 및 전송하는 데이터를 크기(2byte)와 오류를 검사하기 위한 CRC(2barre)로 구성되어 있다.

Data(50byte)는 다시 노드의 ID(2barre), SampleNumber(2byte), Channel(2byte)과 Data(20byte), 인증코드(20byte), 예약(4byte)값으로 이루어졌다.

IV. 실험 환경 및 결과

4.1 인증 컴포넌트의 테스트 베드환경

° 한백전자 ZigbeX 모트
- CPU : Atmaga128
- OS : Tiny OS
- RF : CC2420 (Zigbee)
- PCB Antenna : outdoor(125m) indoor(50m)
- 온도, 습도, 조도 센서, 4 Led

° Base Station
- Windows XP
- Serial 젠더

° Application
- Java 응용프로그램
- Cygwin (리눅스 컴파일 환경 제공)

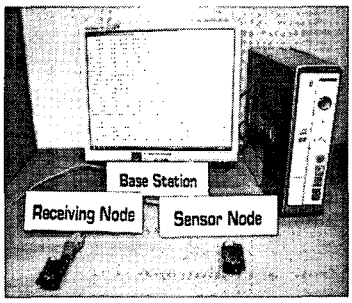

그림 6. 시험 환경

4.2 실험 결과

수신 노드에서 메시지 인증에 성공하면 데이터를 Serial로 전송한다. [그림 7]은 Base Station에서는 Java Application 프로그램을 사용하여 전송받은 데이터의 탈출 문자, 패킷 시작 바이트, 끝 바이트, 패킷의 타입, CRC 바이트를 제거하고 패킷의 내용 자체만을 보여주고 있다.

[그림 8]에서는 인증에 성공한 데이터 값을 또 다른 Java Application 프로그램을 이용하여 그래픽하게 표현하고 있다.

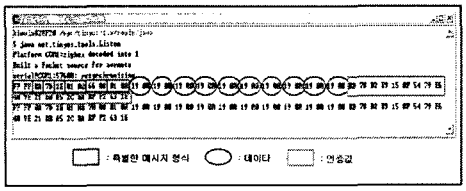

그림 7. 시험 결과 화면1

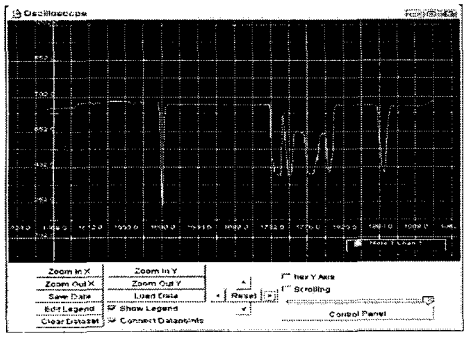

그림 8. 시험 결과 화면2

V. 결 론

본 논문에서는 센서노드에서 센싱한 데이터를 다른 노드로 전송시, 이들간에 송·수신되는 메시지의 내용에 대한 변조사실을 감지할 수 있도록 메시지 인증을 구현하였다. 이렇게 함으로써 전송한 메시지가 해커에 의해 변조된 것임을 발견할 수 있고, 이에 대한 피해를 예방할 수 있을 것이다. 이를 위해서, SHA1 알고리즘을 적용하여 메시지 무결성을 제공하였다.

향후, 보다 제한된 환경에서도 적용 가능하도록 최적화하고, 다양한 플랫폼에도 적용이 쉽도록 코드의 이식성을 높여야 할 것이다. 마지막으로 암호화 기능을 적용한 메시지 인증과 더불어서 암호화와 인증에 사용될 키 분배 방식에 대한 연구 선행되어야 할 것이다.

참고문헌

[1] Prasanth Ganesan, Ramnath Venugopalan,Pushkim Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu, "Analyzing and Modelig Encryption Overhead for Sensor Network Nodes", WSNA'03,September 19, 2003 Page(s):151-159.

[2] Karl E Persoon and D, Manivannan, "Secure Connection in BlueTooth Scatternets", System Sciences. 2003. Proeedings of the 36th Annual Hawaii International Conference on 6-9 jan, 2003 Page(s):10-19.

[3] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar. "Public Key Cryptography in Sensor Networks Revisited". European Workshop on Security in Ad_Hoc and Sensor Networks (ESAS 2004),LNCS3312. Heidelberg. Germany. august 6, 2004 Page(s)2-18

[4] 조영복, 정윤수, 김동명, 이상호. "유비쿼터스 센서 네트워크에서의 저전력 상호인증 프로토콜", 寒國 컴퓨터情報學會 硏究誌 第10號. 2005, 5. Page(s) 188-189