센서 네트워크 보안 프로토콜 소개와 향후 과제

한국전산원 서운석 · 신순자 · 김유정 · 신상철

1. 서 론

유비쿼터스 컴퓨팅 (Ubiquitous Computing)은 새로운 IT 패러다임으로, 1988년 미국 제록스 팰로앨토 연구소의 마크 와이저(Mark Weiser)가 제안한 개념이다. 이는 일상생활과 컴퓨팅이 접목된 지능화된 환경을 통해 제한 없이 접속하고 쉽게 서비스를 제공받을 수 있도록 발전되었으며, 기술의 비약적 발전을 통해 실현 가능성을 높여가고 있다.

유비쿼터스 컴퓨팅은 메인프레임, PC에 이은 제3의 정보혁명의 물결로 여겨지며, 새로운 지식정보국가 건설과 자국의 정보산업 경쟁력 강화를 위한 핵심 과제라는 인식하에 미국, 일본, 유럽의 정부뿐만 아니라 기업 및 연구소 등에서도 앞 다투어 유비쿼터스 관련 기술개발에 심혈을 기울이고 있다.

유비쿼터스 컴퓨팅을 실현하는 핵심기술 중의 하나는 유비쿼터스 센서 네트워크이다. USN(Ubiquitous Sensor Network)이란 "필요한 모든 것(곳)에 전자태그를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 환경정보(온도, 습도, 오염정보, 균열정보 등)까지 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것"을 말하는 것으로 궁극적으로 모든 사물에 컴퓨팅 및 커뮤니케이션 기능을 부여하여 Anytime, Anywhere, Anything 통신이 가능한 환경을 구현하기 위한 것이다. USN은 먼저 인식정보를 제공하는 전자태그를 중심으로 발전하고 이에 센싱 기능이 추가되고 이들간의 네트워크가 구축되는 형태로 발전할 것이다[13].

무선 센서 네트워크는 가까운 미래에 널리 사용되어질 수 있는 기술로서 실 세계를 대상으로 한 무선 센서 네트워크 서비스 구성에 대한 연구, 개발이 주류를 이루었으며 보안에 대한 연구는 상대적으로 적은 관심을 보여 왔다.

점차 센서 네트워크 기반의 서비스에 대한 기술이 구체화되어지면서 센서 네트워크상에서 보안에 대한 필요성이 대두되어지고 이에 대한 보안 기술에 대한 연구가 활발해지고 있다. 일반적으로 센서 네트워크는 일반 PC 컴퓨팅 환경과 비교해서 제한된 CPU, 저장 공간, 대여폭, 전원 등의 제약 사항을 갖는다. 그러나 보안 요구사항은 일반적인 인터넷 환경에서 요구되는 수준을 만족해야하므로 이에 적합한 연구가 이루어져야 한다. 센서 네트워크의 활용 사례는 다음과 같으며, 그 적용 범위의 확장성을 짐작할 때, 보안 기능을 충족해야 하는 당위성을 파악할 수 있다.[1][2][5]

- 비상 대응 정보 분야 : 센서 네트워크는 건물, 사람, 수송 경로에 대한 상태 정보를 취할 수 있다. 이렇게 수집된 센서 정보는 안전하게 비상 대응 담당자에게 안전하고 신속하게 전송되어야 한다.
- 에너지 관리 분야 : 에너지 관리는 원격으로 이루어질 경우 보다 효과적일 수 있다. 즉, 주위 환경의 기온과 순간 전력 등에 따른 전선에 부과되는 전력 소모량을 원격으로 감지할 수 있으며 이로 인한 자동적 전력 부하 분산 관리를 통해 전력 과부하에 따른 단전 사고 등을 미연에 방지할 수 있다.
- 의료 모니터링 분야 : 가까운 미래에는 각 사람의 신체 정보 상태를 센서 네트워크를 통해 원격으로 모니터링을 할 수 있고 이를 통해 의료 시스템과 연계함으로써 의료 서비스의 획기적인 변화를 가능케 할 수 있다.
- 군수 물류, 재고 관리 분야 : 상품이 과잉 생산된 곳에서 공급이 부족한 지역으로 신속하게 이동할 수 있는 메커니즘을 센서 네트워크를 통해 실현 가능하다. 이 영역은 전 세계를 시장으로 하며 물류에 대한 신속, 정확한 정보의 현황을 파악하는데 많은 기여를 할 수 있다.
- 전투지역 관리 분야 : 전투 지역의 무기, 전투 차량, 군인에 대한 정확한 정보를 실시간적으로 수집, 관리함으로 전투 현황에 대한 정보의 혼란을 최소화할 수 있다.

센서 네트워크를 위한 센서 디바이스의 프로토타입은

미국 버클리 대학교 Center for Information Technology Research in the Interest of Society (CITRIS)의 구성요소인 SmartDustProgram에 의해 정의되었다[8][12]. 센서 네트워크의 제약 사항은 다음과 같이 요약될 수 있다[7].

표 1 센서 네트워크 제약사항[6]

항목	사양
CPU	8-bit, 4MHz
Storage	8 Kbytes instruction flash 512 bytes RAM 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10Kbps
Operation System	Tiny OS
OS Code space	3,500 bytes
Available Code space	4,500 bytes

Security Protocols for Sensor Networks (SPINS)에서 제시되는 프로토타입은 소규모의 전력으로 구동되는 노드와 보다 강력한 자원을 갖고 있는 Base Station으로 구성된다. SPINS의 대안적 기술로는 LEAP[11], Deng et al.[3], Undercoffer et al.[9] 등이 있다.

본 고에서는 앞서 언급한 유비쿼터스 컴퓨팅을 실현하기 위한 제안 기술들 중의 하나인 SPINS와 향후 과제를 살펴보고자 한다.

2. Sensor Network에서의 보안

센서 노드는 공개 키 암호화 알고리즘을 위한 다양한 정보 및 성능을 제공하기 어렵다. 또한 Gennaro & Rohatgi에 의해 제시되는 대칭 키 방식은 패킷 당 필요 인증 정보가 1Kbyte로서 센서 네트워크에 적용하기에는 부적절하며 앞서 제시된 TESLA는 일반 인터넷에 적합한 기술로서 센서 네트워크에는 부적합한 기술이다[4]. 이에 새로운 μTESLA 기술이 제안되었다.

2.1 시스템 전제 조건

보안 요구사항과 보안 인프라를 제시하기 전에 실제적인 요구사항과 시스템 구성도를 정의해야 한다. 이러한 정의는 일반적인 센서 네트워크 상에서 일반적인 보안 요구사항을 충족하기 위한 목적을 갖는다.

2.1.1 통신 방식

일반적으로 무선망을 이용한 센서 노드 통신 방법은 Broadcasting 방식이다. 이것은 센서 네트워크 서비스 특성상 최소한의 자원 소모에 적절한 보안적 요구사항을 만족하기 위한 보안 수준을 제공하는 것이다. 전형적인 SmartDust 센서 네트워크는 외부 망과의 연계를 위해 하나 이상의 base station을 갖는다. 이러한 base station은 충분한 자원을 갖고 있으며 많은 sensor node와의 통신, 관리의 중심적 역할을 수행한다. 일반적인 센서 네트워크에서의 통신 방식은 다음과 같다.

- node to base station 통신
- base station to node 통신
- base station to all nodes 통신

이러한 환경에서 보안 요구사항은 node간 보안, node broadcasting 등에 대한 안전성을 보장하는 것이다[6].

2.1.2 센서 노드 신뢰성

일반적으로 센서 네트워크를 위해 운영되는 센서 노드는 안전하지 않은 위치에 설치된다. 따라서 각 노드에 대한 신뢰성을 보장 받을 수 없기 때문에 한 노드의 보안 노출이 다른 노드에 영향력을 미치지 않도록 보안 사고의 최소화가 절대적으로 필요하다. 각 노드에게 broadcasting 하는 것은 안전하지 않은 무선 망에서 공격자(Adversary)의 도청이 언제든지 가능하며 메시지의 재사용 공격에 매우 취약하게 된다. 그러나 base station은 외부 망과의 gateway 및 센서 네트워크의 중심에 있으므로 언제나 안전해야 하며 각 노드는 이러한 base station과의 통신을 위해 초기 설치 시 마스터 키 값을 할당받는다. 각 노드에 설치된 마스터 키는 base station과 공유되는 대칭 키로서 향후 사용되는 모든 키 생성을 위한 SEED로 사용된다.

2.2 센서 네트워크 보안 요구사항

2.2.1 데이터 비밀성

센서 네트워크 환경의 많은 응용에서는 민감한 데이터 교류가 노드간에 빈번하게 이루어진다. 따라서 허가된 노드 이외에 민감한 정보를 볼 수 없도록 해야 하며 이것은 비밀 키로 데이터를 암호화한 상태에서 데이터 교환이 이루어져야 한다. 즉 데이터의 비밀성을 보장해야 한다.

2.2.2 데이터 인증

메시지 인증은 센서 네트워크에서 많은 응용에서 중요한 보안 요구사항이다. 공격자는 쉽게 메시지를 삽입할 수 있기 때문에 수신자는 정책방향 결정 과정에서 사용되는 데이터가 원래 작성자로부터 온 것인지를 확인해야 한다.

양단간 통신인 경우 데이터 인증은 순수한 대칭 키 메커니즘을 통해 이루어질 수 있다. 송신자와 수신자는 모든 데이터 통신에 대한 메시지 인증 코드(Message

Authentication Code : MAC) 값을 생성하기 위한 비밀 키를 공유한다. 정확한 MAC 값이 수신되어질 경우 수신자는 송신자에 의해 보내진 메시지의 진위를 검증하게 된다. 그러나 Broadcasting 통신 방법에서 공유되는 비밀 키는 모든 수신자들과 송신자간에 공유되어야 하며 수신자들 중 악의적인 수신자는 공유 키를 알고 있기 때문에 송신자를 가장해서 MAC 값을 생성할 수 있는 단점을 갖는다. 따라서 일반적으로 공개 키 방식을 통한 Broadcasting 통신을 해야 한다. 그러나 공개 키 방식은 실제적인 컴퓨팅 파워나 자원 소요가 크므로 이러한 문제점을 해결하기 위한 방식으로 지연된 키 노출과 단 방향 함수 키 chain이 제안된다.

2.2.3 데이터 무결성

통신 상에서 데이터 무결성은 수신자가 수신한 데이터의 위·변조 여부를 확인하는 것으로 SPINS에서는 데이터 인증을 통한 데이터 무결성을 보장한다.

2.2.4 데이터 신선성(Freshness)

데이터 신선성은 예전에 보낸 데이터에 대한 재 사용을 방지하기 위한 기술로서 가장 최근에 보낸 데이터임을 보장하는 보안 서비스이다. 일반적으로 2종류의 타입이 있다[10].

- weak freshness
  - counter를 통해 partial message ordering (sending order) 제공
  - 수신된 메시지를 통해 해당 송신자가 보낸 것을 확인 가능
  - 용도 : sensor로 측정 시
- strong freshness
  - 임의의 난수 값인 nonce를 통해 request-response pair에서 total ordering 제공
  - 수신된 메시지가 이전에 수신자가 보낸 요청메시지에 대한 응답인지 확인 가능
  - delay estimation 제공
  - 용도 : 네트워크 상의 time synchronization

3. Security Protocols for Sensor Networks(SPINS)

3.1 SPINS의 구성

SPINS 기술은 다음 두 가지 항목으로 구성된다.

- ㅇSNEP(Sensor Network Encryption Protocol) : 데이터 비밀성, 양단간 데이터 인증, 재사용 방지, 신선성, 무결성 등 제공
- ㅇμTESLA : 데이터 Broadcasting에서의 인증

3.2 SNEP(Secure Network Encryption Protocol)

SNEP 기술은 다음과 같은 보안 기능을 제공한다.

- ㅇData Confidentiality : 의도된 수신자만이 데이터를 소유할 수 있도록 데이터를 비밀키로 암호화하며 제 3자가 암호 메시지에서 원래 메시지를 추론할 수 없는 보안 기능(semantic security)을 보장한다. 암호화를 위해서는 Counter Mode를 적용하여 비밀성을 보장한다.
  - Counter mode(CTR)의 block cipher를 위해 송수신자가 공유하는 2개의 counters를 사용〈 counter : initialization vector(IV) 〉
  - 각 메시지 전송 후에 각각의 counter를 증가시킴
  - 같은 메시지가 매번 다르게 암호화됨
  - Base station은 모든 노드에 대한 현재 counter를 가지고 있음
  - 메시지와 함께 전송할 필요 없음
- ㅇ양단간 데이터 인증 : 의도된 송신자가 정말로 해당 데이터를 보냈는지 검증하기 위해서 공유된 키를 기반으로 MAC을 사용한다.
- ㅇ재사용 방지 : MAC에 counter값을 포함하여 공격자에 의해 재사용 공격이 이루어질 경우 counter 정보로 판별한다.
- ㅇdata freshness : 해당 데이터가 가장 최근의 버전임을 의미하는 것으로 최근 데이터임을 검증하기 위한 기능이다.
- ㅇ낮은 통신 부하 : Counter 상태는 각 end point에 유지되며, 각 메시지에 담아 전송될 필요가 없다.

3.2.1 일반적인 SNEP

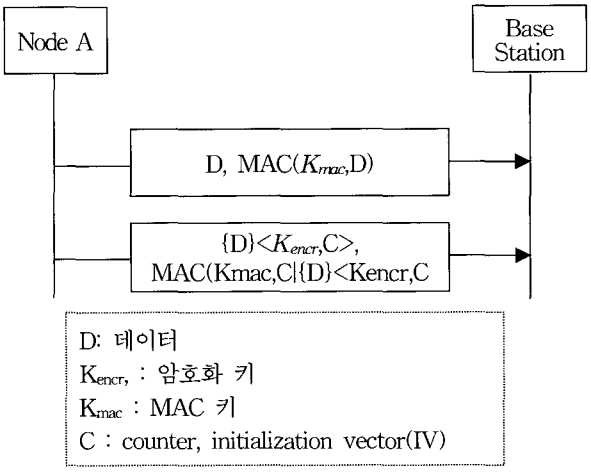


그림 1 일반적인 SNEP 구조

- 첫 번째 경우: 데이터 인증만 보장
- 두 번째 경우: 데이터 인증과 Data Confidentiality보장

3.2.2 nonce를 사용하는 SNEP

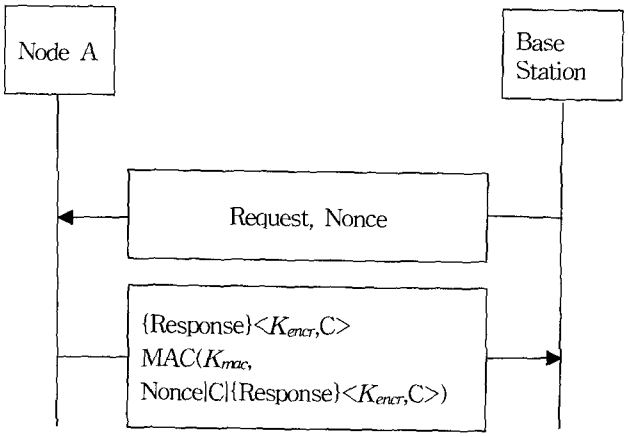


그림 2 nonce를 사용하는 SNEP

- Nonce는 random하게 생성됨
- A의 Response가 Base station이 보낸 메시지에 대한 응답임을 확인가능 (strong freshness 보장)

3.3.2 보안 서비스

가. Key Setup

일반적인 구현에서 RC5 대칭 키 암호화 알고리즘을 이용하여 다양한 목적의 키 값을 유추한다. Master 키를 기반으로 암호화를 위한 암호화 키, MAC 값 생성을 위한 키 값, 랜덤 키 값 등을 생성한다.

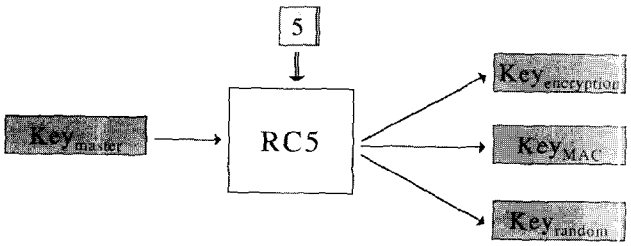


그림 3 키 생성 메커니즘

나. 암호화

암호화는 전 단계에서 생성한 암호화 키를 Counter Mode로 암호화 하여 Chain으로 연결하는 구조이다. E(En_Key, Counter) (P) = C를 이용해 암호화 루틴을 반복 수행한다.

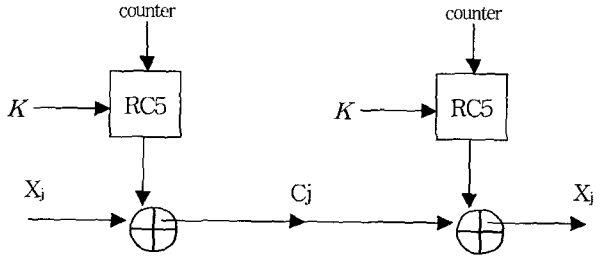


그림 4 SNEP의 암호화 과정

다. MAC 생성 메커니즘

MAC 생성은 MAC 생성 키를 이용하여 암호화된 메시지에 대한 메시지 인증 코드를 생성한다. 다음은 MAC 생성 과정이다.

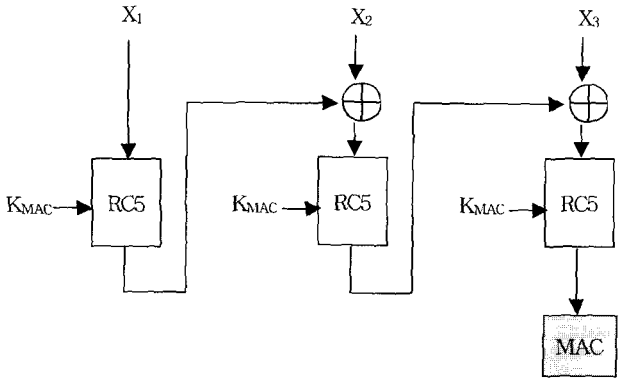


그림 5 SNEP의 MAC 생성 메커니즘

3.3 μTESLA(the "micro" version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)

Sensor network상에서 TESLA의 문제점과 μTESLA에서의 해결방법은 다음과 같다[7].

- TESLA 기술은 초기 패킷에 전자서명을 포함하여 인증하는 방식으로 시스템의 부하를 가중. μTESLA에서는 symmetric mechanism만 사용하여 인증
- TESLA 기술은 키를 각 packet에 담아 노출하여 송수신에 지나치게 많은 energy 소모 발생. μTESLA에서는 주기 당 1회 키를 노출
- TESLA 기술은 one-way key chain을 sensor node에 저장, 관리함으로 고 비용이 소요. μTESLA에서는 인증된 sender의 수를 제한함으로 효과적인 관리 가능

3.3.1 개요

Authenticated broadcasting은 asymmetric mechanism을 통해서 처리되어야 안전성을 보장할 수 있다. 그러나 컴퓨팅 파워, 통신 부하, 저장 공간 등의 문제점으로 인해서 센서 네트워크에 적용하기는 어렵다. 따라서 시간 지연 메커니즘을 통해 MAC을 생성하기 위해 사용되는 대칭 키들의 집합인 키 Chain을 생성하는 기술을 적용하여 안전한 인증이 이루어지도록 해야 한다. 대칭 키 시간 지연 메커니즘은 단 방향 함수 key chain을 통해 공개 키 기술에서 제공되는 인증 효과를 제공한다. 단, 필요조건은 base station(BS)과 node 사이에 시간적인 동기가 이루어져야 한다는 것이다. 개

략적인 절차는 다음과 같다.

- (BS) authenticated packet 전송을 위해 base station은 그 시점에서의 비밀키를 사용하여 그 패킷에 대한 MAC값 생성
- (BS->node) 패킷 전송
- (node) BS만이 MAC키를 전송함을 확신하므로 전송 중인 패킷이 변경될 수 없었음을 확신함
- (node) 수신된 패킷을 버퍼에 저장
- (BS->all nodes) 키 노출 시점에서 검증키를 broadcasting
- (node) 키가 검증되면 버퍼에 저장된 패킷 인증에 사용
- 각 MAC 키는 one-way function에 의해 생성된 key chain의 key 중 하나임
- 키 노출은 패킷 broadcasting에 독립적이며, time intervals에 의존함

3.3.2 세부 절차

가. Sender Setup : 비밀 키의 sequence 생성

- n 길이의 키 체인 생성을 위해 sender는 마지막 키 Kn을 랜덤하게 선택.
- 나머지 키 생성(one-way function 사용)
  Kn->Kn-1->Kn-2->...->K0
  Kj=F(Kj+1)

나. Broadcasting authenticated packets

- 시간을 time interval로 나누고, 키 체인의 키와 매핑시킴 : interval i에 생성되는 MAC의 생성 알고리즘 입력키로 Ki를 사용
- interval i가 경과한 후부터 δ interval 후에 Ki를 노출시킴

다. Bootstrapping a new receiver

- 각 receiver는 one-way key chain의 인증키 하나가 필요
- sender와 receiver는 loosely time synchronized
- receiver는 one-way key chain의 키 노출 스케줄을 알고 있음(δ : 노출 delay)
- MAC : 데이터 인증에 사용
- nonce : freshness 검증용

라. Authenticating broadcast packets

- 수신된 패킷이 보안조건을 만족하면 수신자는 그 packet을 저장하고 만약 만족하지 못하면 해당 packet을 무시. 보안 조건이란 수신한 패킷에 대응되는 키가 송신자에 의해 아직 노출되지 않았음을 보장하는 조건임. 이것은 수신자가 모든 수신된 패킷을 체크할 때 사용
- 송신자가 Ki 노출
- 수신자는 one-way function을 이용해, 가지고 있던 Kv와 Ki를 다음 조건을 갖고 매핑
  one-way function F : Kv= Fi-v(Ki)
  만약 매핑이 되면 interval v ~ i 동안 보내졌던 모든 packet이 인증되고 Kv를 Ki로 대체

마. Nodes broadcast authenticated data

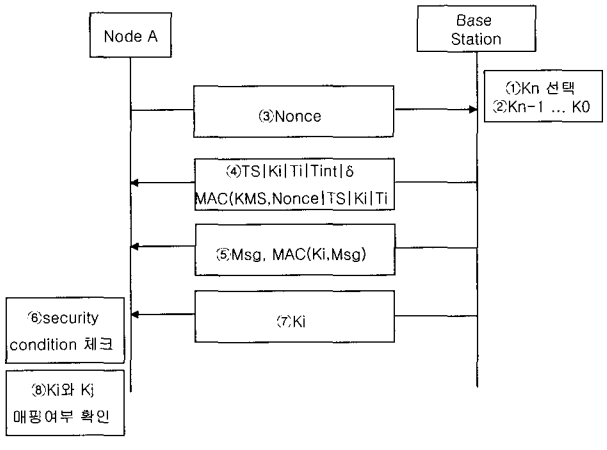
한 노드가 authenticated data를 broadcasting하는 데는 다음과 같은 문제점이 존재한다.

- node : 메모리 한계로써 one-way key chain의 키 목록을 저장할 수 없음
- 초기 생성키 Kn으로부터 각각의 키들을 재계산하는 것에는 고 비용이 소요
- 노드는 각 수신자와 키를 공유하고 있지 않을 수 있으므로 key chain의 공유는 고비용의 node-to-node key agreement를 수반함
- 노출된 키를 모든 수신자들에게 broadcasting하는 것도 노드 측면에서는 고 비용이 발생

이의 해결 방안은 다음과 같은 방법을 통해 서비스가 이루어지도록 하는 것이다.

- Node는 base station을 통하여 데이터를 broadcast한다. Node는 base station에게 인증된 방법으로 데이터를 전송하기 위해 SNEP을 사용하며, 그 후에 base station이 broadcasting
- 노드가 데이터를 broadcasting 하되 base station이 one-way key chain을 유지하며, 필요시 broadcasting node에게 키를 전송한다. 또한, broadcasting node의 에너지 절약을 위해 base station이 노출된 키를 broadcasting하고, 새로운 수신자들에 대한 initial bootstrapping 절차를 수행 가능

3.3.3 주요 흐름도



TS : 현재 시간
Ki : interval i 에 사용된 key
Ti : i 의 시작 시간
Tint : time interval
δ : 노출 delay

그림 6 μTESLA 프로토콜 개요

4. 결 론

본 고에서 센서 네트워크의 보안기술 중의 하나인 SPINS를 고찰하였다. SPINS의 개요, 시스템 전제 조건, 보안 요구사항을 설명하고, 요소기술인 SNEP과 TESLA의 문제점을 개선한 μTESLA의 기능과 프로토콜을 개략적으로 제시하였다. 앞서 언급한 바와 같이 SPINS 이후에 대안적인 기술이 연구되어 발표되었다. 각 기술의 장·단점 분석과 개선을 통한 선택적인 적용이 요구될 것이다.

2004년이 되면서 우리나라는 정부를 중심으로 센서 네트워크 구축을 위한 정책 수립과 기술 개발이 본격적으로 이루어지고 있다. 센서 네트워크에 대한 일반적인 요구조건은 Fault tolerance, scalability, 가격 등이며, 각 응용별로 적용 여부 및 정도가 달라지는 요구조건으로는 실시간성, reliability, 데이터양, 주기성, 저전력, 이동성 등을 들 수 있다. 보안 및 인증은 상대적으로 일반적인 요구조건으로 고려되어야 하며, 구축 초기부터 설계에 반영되어야만 안전하고, 비용 효과적인 시스템 및 네트워크를 구축할 수 있다. 이때, 무선 센서 네트워크를 통하여 다양한 정보 및 제어 서비스를 안전하게 제공하기 위해서는 센서 네트워크를 구성하는 요소들과 이와 연동되는 유선 네트워크의 보안과 인증이 통합적으로 이루어져야 한다.

센서 네트워크는 유비쿼터스 컴퓨팅 환경의 구축에 중요한 역할을 하는 기반 기술임에 틀림없다. 따라서, 센서 네트워크의 구축과 병행하여 이의 안전성을 제고하는 보안 및 인증 기술의 적용이 구축 초기인 지금부터 고려될 때 효과적인 정보화가 이루어질 것이다.

결론적으로, 유비쿼터스 환경에서의 보안 인증은 유비쿼터스 모델 및 서비스가 구체화되어질 경우 적절한 기술 사항이 도출될 것이다. 그러나, 현재의 유비쿼터스는 특정 기술에 종속적이지 않고 현재 연구, 개발되는 다양한 기술의 조합으로서 발전되고 있다. 따라서 현 수준에서의 유비쿼터스 환경에 적합한 보안 인증 기술을 위해서 신 개념의 기술을 연구, 개발하는 것보다 유비쿼터스 환경을 구축하기 위해 적용된 기반 기술에 대해 개별적인 보안 인증 기술을 효과적으로 조합할 수 있는 연구, 개발이 요구될 것이다.

참고문헌

[1] H. Abrach, S.Bhatt, J. Carlson, H. Dui. Rose, A. Sheth, B. Shucker, J. Deng, R. Han, "MANTIS: System Support for Multimodal Network of In-Situ Sensors", In Proc. of 2nd ACM Workshop on Wireless Sensor Networks and Applications(WSNA' 03), San Diego, CA, Sep, 2003

[2] B.j.Bonfils, P. Bonnet, "Adaptive and Decentralized Operator Placement for In-Network Query Processing", IPSN'03, April, 2003, LNCS 2634

[3] J. Deng, R. Han, and S. Mishra, "Security Support for In-network Processing in Wireless Sensor Networks", 2003 ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN '03), October 31, 2003

[4] Diameter CMS Security Application, draft-ietf-aaa-diameter-cms-sec-04.txt, www.ietf.org/html.charters/aaa-charter.html

[5] H. Han, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", Appears in IEEE Symposium on Security and Privacy 2003

[6] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Cullar, K. Pister, "System architecture directions for network sensors", ASPLOS 2000, Cambridge, Nov 2002

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D.Tygar, "SPINS : Security Protocols for Sensor Networks", Wireless Networks Journal (WINET), 8(5):521-534, Sep 2002

[8] K. S. J. Pister, J. M Kahn, and B. E. Boser. Smart dust : Wireless network of millimeter-scale sensor nodes, 1999

[9] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for Sensor Networks", http://www.cs.umbc.edu/cadip/2002 Symposium/sensor-ids.pdf

[10] Y, J, Zhao, R. Govindan, and D. Estrin, "Computing Aggregates for monitoring Wireless Sensor Networks", The First IEEE International Workshop on Sensor

Network Protocols and Applications (SNPA′ 03), Anchorage, AK, USA, May 11, 2003
[11] S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", The 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., October, 2003
[12] http://www.citris.berkeley.edu/index.html
[13] 정보통신부, 'u-센서 네트워크 구축 기본계획', 2004. 2. 17.

서 운 석

1995 성균관대학교 정보공학과(공학사)
2003 성균관대학교 과학기술대학원 정보공학과(공학석사)
2003~현재 성균관대학교 대학원 컴퓨터공학과 박사 과정
1995~현재 한국전산원 인터넷기반·인증팀 선임연구원
관심분야 : 에이전트지향 지능형 시스템, 사용자 인증, ITS DB
E-mail : sws@nca.or.kr

신 순 자

1995 성균관대학교 정보공학과(공학사)
1995~현재 한국전산원 인터넷기반·인증팀 전임연구원
관심분야 : PKI, 인증, 정보보안
E-mail : ssj@nca.or.kr

김 유 정

1990 한국외국어대학교 경영학(경영정보) 석사
1999 고려대학교 경영학(경영정보) 박사
1999 부천대학교 사무자동학과 초빙교수
2001 (주) 디지트 메이트 기획이사
2002~현재 한국전산원 인터넷기반·인증팀 팀장
관심분야 : 차세대인터넷(IPv6), 모바일 전자정부, 유비쿼터스 인프라, 웹 서비스
E-mail : yjkim@nca.or.kr

신 상 철

1983. 8~1988. 7 삼성반도체통신 시스템개발 선임
1988. 8월~1993. 7 삼성전자 시스템개발 팀장
1993. 2 KAIST 전산학과 수료
1995. 9~현재 한국전산원 정보화기반구축단 단장
2004. 2~현재 한국USN센터장
2002. 3~현재 건국대학교 컴퓨터공학과 박사수료
관심분야 : 초고속통신망, IT839 3대인프라(BcN, IPv6, USN/RFID), 홈네트워크, PKI
E-mail : ssc@nca.or.kr