안전한 센서 네트워크 관리에 관한 연구

서대희*, 이임영
* 순천향 대학교 정보기술공학부
e-mail : 1636711@hitel.net

A Study on Secure Seonor Network Management Scheme

Dae-Hee Seo° Im-Yeong Lee
Soonchunhyang Univ. Division of Information Technology Eng.

요약

최근 새로운 형태의 네트워크 환경인 유비쿼터스 컴퓨팅에 대한 연구가 활발하게 진행되고 있다. 특히 유비쿼터스 컴퓨팅에서 중요한 요소중의 하나는 센서 네트워크로써, 저전력 Ad-hoc 네트워크에 기반한 센서와 센서 노드들로 구성되며, 실제의 환경과 유비쿼터스 컴퓨팅과의 매개 역할을 한다. 따라서 본 논문에서는 센서 네트워크의 일반적인 개요 및 보안에 관해서 알아보고 취약점을 분석한 뒤 이를 바탕으로 안전하고 효율적인 센서 네트워크의 관리 구조를 제안하고자 한다.

1. 서 론

유비쿼터스 네트워크 환경의 특징이 사용자 중심으로서 그가 처한 상황이나 환경을 네트워크가 지능적으로 파악하여 사용자의 네트워크 환경을 최적화시켜 그가 어디에서나 네트워크에 편리하게 연결케하는 것이다. 그리고 PC, PDA, 핸드폰, 가전기기, 기타 모든 장소에 존재하는 물체가 모두 단말의 기능을 갖게 된다. 아울러 컨텐츠 사용이 자유롭고, 안전하게 사용할 수 있는 네트워크가 마련되는 것을 특징으로 하고 있다. 유비쿼터스 네트워크를 구성하는 기술로는 유비쿼터스 플렉시블 광대역, 유비쿼터스 텔레포테이션, 유비쿼터스 에이전트, 컨텐츠, 어프라이언스, 유비쿼터스 플랫폼 및 유비쿼터스 센서망 등이 있다. 이중 유비쿼터스 센서망은 사용자 주변의 주변기기가 통신을 하게 됨으로써 자율적으로 정보를 수집하고 관리하는 구성요소이다[1].

따라서 본 논문의 2장에서는 유비쿼터스의 센서 네트워크에 대한 일반적인 개요를 살펴보고 3장에서는 유비쿼터스에서 센서 네트워크가 형성되었을 경우 발생할 수 있는 보안적인 요구사항을 제시하고. 4장에서는 3장에서 제시한 보안 요구사항을 만족할 수 있는 안전하고 효율적인 센서 네트워크 관리 구조를 제안하고, 5장에서는 제안 방식을 분석한 뒤 마지막으로 6장에서는 결론을 맺도록 한다.

2. 센서 네트워크 개요

센서 네트워크는 물리공간의 빛, 소리, 온도 그리고 물체의 움직임과 같은 아날로그 데이터를 공간상에 다양하게 분포한 센서 노드에서 측정하여 중앙의 기지 노드로 전달하기 위해 센서 노드를 사용해 자체적으로 구성하는 네트워크를 말한다., 각각의 센서 노드는 일반적으로 수 MHz 클럭을 사용하는 마이크로 컨트롤 수, 수 십KB 크기의 EEPROM, 수 KB 크기의 플래시 메모리, 센서 소자(온도, 소리, 빛, 물체의 가속도, 자기장), 출력소자(LED, 스피커), 그리고 통신 모듈(라디오 주파수)로 구성된다.

센서 네트워크는 물리공간에서 측정한 아날로그 데이터를 디지털 신호로 변환해 인터넷과 같은 전자공간에 연결된 기지 노드로 전달하는 입력 시스템이다.[2-3]

3. 센서 네트워크의 보안 사항

3.1 센서 네트워크에서 보안의 필요성

유비쿼터스의 실현을 위한 센서 네트워크는 사용자의 프라이버시 뿐만 아니라 비즈니스, 나아가 사회 전반을 변화 시킬 수 있는 가장 큰 핵심 요소 기술이다.

유비쿼터스의 특성상 모든 컴퓨터와 사물이 하나로 연결된 센서 네트워크 환경이라면 누구든지 사용자의 정보에 접근할 수 있다. 이와 같이 고도화된 네트워크 환경의 다른 취약점은 고의적인 제 3자의 공격자로부터 정보 도용을 통한 사이버 범죄로 이어질 수 있으며, 시스템의 작은 버그가 엄청난 혼란을 야기할 가능성이 크다는 것이다. 또한 크래킹에 의한 정보 유출, 바이러스 유포, 각종 컴퓨터 범죄, 프라이버시 침해, 저작권 침해 등 가상세계에서 벌어지는 각종 부작용도 간과할 수 없다.

3.2 센서 네트워크의 보안 요구사항 분석

유비쿼터스의 센서 네트워크가 사용자 중심으로 구성될 경우 사용자의 프라이버시 정보를 이용한 통신을 수행할 수 있으며, 다음과 같은 요구사항이 필요하다.

- 상호 인증 : 사용자 중심으로 이루어지는 센서 네트워크의 경우 이동 단말과 인증 서버 혹은 게이트웨이와의 상호 인증을 통해 안전성을 유지할 수 이어야 한다.
- 기밀성과 무결성 : 사용자의 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하여 전송 데이터에 대한 안전성을 유지할 수 있어야 한다.
- 상태 획득 기술 : 센서들 간에 상황이 변경됨에 따라 통신이 설정될 수 있는지를 결정하는 기술로써 다른 센서들과의 안전한 정보 전송을 기반으로 정보를 획득하는 기술을 제공해야 한다.
- 자동 서비스 생성 방안 : 일정한 통신량 이상(서비스 이용 빈도)이 높을 경우 안전한 형태의 그룹으로의 변환

이 가능해야 하며, 일정한 통신량 이하의 서비스 빈도가 나타날 경우 자동적인 그룹 해체 과정을 제공할 수 있어야 한다.

- 효율성 : 센서의 특성상 높은 연산의 계산량을 최소화하여 센서의 효율을 극대화 시킴으로써 전체 센서 네트워크의 효율성을 높이는 방안이 필요하다.

4. 안전하고 효율적인 센서 네트워크 관리 구조 방식 제안

본 논문에서는 홈 네트워크를 기반으로 구성된 센서 네트워크에서의 안전하고 효율적인 관리 구조를 제안하고자 한다. 제안 방식은 다음과 같은 가정 사항을 기반으로 한다.

- 수 Mbps 엑세스 링크를 지원하며, 옥내외에서 끊김없는 네트워크 접속이 가능하다.
- 모든 모바일 디바이스는 User Agent(UA)를 보유하고 있다. (UA는 Service Element(SE)이다.)

4.1 시스템 계수

(센서 : s, 인증서버 : A)

n : 공개 계수($n = pq$, p : 소수, q : $q|p-1$)

m_i : 서버가 제공할 수 있는 서비스의 고유 번호로써 서버에서 이미 정의 내려져 있는 값

$E()$, $D()$: 암호화, 복호화 함수

r, α : 랜덤 수

ID_S : 인증 서버의 공개 ID

4.2 제안방식 프로토콜

특수한 무선 환경이 제공되지 않는 홈 네트워크 상태에서 다수의 모바일 디바이스가 보편적인 단말기일 경우 이를 이용해 전자상거래 혹은 웹 서비스를 받고자 하는 홈 네트워크의 센서 네트워크 환경에서의 안전하고 효율적인 관리 구조를 위해 다음과 같은 흐름을 갖는다.

[Step 1] SE의 서비스 등록 단계

인증 서버는 센서들의 SE를 이용하여 센서들의 서비스 형태를 등록하는 과정을 수행한다.

① 인증 서버는 랜덤하게 선택된 $\alpha \in {}_UZ_q$를 생성하여 c_i를 계산한 후 이를 센서에게 브로드캐스팅한다.

$c_i = m_i^{\alpha} \bmod n$ (i는 서비스 형태를 규정짓는 고유번호, i=1,..., N)

② 센서는 서버로부터 전송된 c_i (i=1,..., N)으로부터 현재 UA에서 제공할 수 있는 서비스의 고유 번호를 선택한 후 (3개의 서비스를 선택한다면) 이것을 c_{i_1}, c_{i_2}, c_{i_3}라 정의한다. 서비스 형태를 정의내린 센서는 $\beta_0 \in {}_UZ_q^*$를 선택하여 d_{i_j}를 계산하여 서버에 전송한다.

$$d_{i_j} = c_{i_j}^{\beta_0} \bmod n \ (= m_{i_j}^{\alpha\beta_0} \bmod n) \ (i=1,2,3)$$

③ 인증 서버는 $s = \alpha^{-1} \bmod q$를 계산 한 후 다음을 계산하여 e_{i_j}를 센서에 전송한다.

$$e_{i_j} = d_{i_j}^{s} \bmod n \ (= m_{i_j}^{\beta_0} \bmod n) \ (i=1,2,3)$$

④ 센서는 $t = \beta^{-1} \bmod q$를 계산한 후 f_{i_j}를 검증함으로써 그 정당성을 확인한다.

$$f_{i_j} = e'_{i_j} \bmod n \ (= m_{i_j}) \ (i=1,2,3)$$

[Step 2] 임시 그룹 설정을 위한 센서의 초기 등록 과정

다음은 일정한 개수 이상의 센서들이 동일한 서비스를 요청할 경우 임시적으로 그룹을 형성하여 서비스와 통신의 효율성을 높이는 단계이다.

① 센서는 [Step 1]에서 설정된 3개의 서비스 c_{i_1}, c_{i_2}, c_{i_3}중 하나의 서비스를 제공받고자 할 경우(c_{i_2} 서비스를 제공 받고자할 경우) 다음을 계산하여 Z_2, T_s를 인증 서버에 전송한다.

$$C_2 = c_{i_2} \| m_{i_2} \| ID_S, \ d_2 = c_{i_1} * c_{i_3} * r_{s_1}$$

$$Z_2 = C_2^{d_2} \bmod n$$

② 인증 서버는 서버로부터 전송된 Z_2의 값을 임시 저장한 뒤 센서의 임시 비밀정보 값인 d_n, Z_a값을 다음과 계산하고, 인증 서버의 랜덤수 r_A를 선택하여 Z_A를 생성하여 Z_A, Z_a, T_a를 센서에 전송한다.

$$d_n = c_{i_1} * c_{i_2} * c_{i_3}, \ Z_a = Z_2^{d_n^{-1}} \bmod n,$$

$$Z_A = Z_a^{r_A} \bmod n$$

③ 센서는 인증서버로부터 전송되는 $Z_a \cong V_2$이면 다음을 계산한 뒤 올바른 경우 Z_2', m_{i_2}를 인증 서버에 전송한다.

$$V_2 = C_2^{c_{i_1}^{-1} * r_{s_1}} \bmod n, \ Z_2' = Z_A^{(r_{s_1})^{-1}} \bmod n$$

⑤ 인증 서버는 센서로부터 전송된 m_{i_2}의 값을 이용해 현재 센서가 요구하는 서비스에 대한 임시 비밀 정보 y_2를 저장한다

$$y_2 = Z_2'^{(r_A^{-1})} \bmod n$$

[Step 3] 임시 그룹 설정 단계

인증 서버는 [Step 3]에서 센서로부터 등록된 비밀정보 y를 등록하는 과정에서 전송되어온 m_*를 확인하여 같은 서비스를 제공 받고자 하는 센서가 일정한 개수 이상이거나, 동일한 서비스에 대한 빈도가 높을 경우이거나, 동일한 통신량이 증가할 경우 해당 센서들의 임시 그룹 설정을 위한 과정을 수행한다.

① 인증 서버는 동일한 서비스를 제공 받고자 하는 센서들의 비밀정보 $(y_1,\ldots,y_n)$으로 정의하고 각각의 y_*에 대한 D_*를 대응 생성하여 이를 임시 보관한다. 또한 임시 그룹 설정(ID_A, ID_B, ID_C를 임시 그룹으로 설정할 경우)을 위해 센서 ID_A에 s_A, T_A를 전송한다.

$$D_A = H(c_{i_2} \| y_A), \ s_A = g^{D_A} \bmod n$$

② 센서 ID_A는 인증 서버로부터 전송되어온 s_A를 이용해 세션키 $K_{G_{temp}}$를 생성한다. 생성된 세션키 $K_{G_{temp}}$를 이용해 암호 통신이 필요한 어플리케이션

서비스 메시지 M_C를 $K_{G_{temp}}$로 암호화하여 V_A를 인증 서버에 전송한다.

$K_{G_{temp}} = s_A^{(y_A^{-1})} \ mod \ n$, $V_A = E_{K_{G_{temp}}} M_C \ mod \ n$

③ 인증 서버는 전송되어온 V_A의 검증을 수행하기 위해 $K_{G_{temp}}$를 생성한 뒤 V_A를 복호화한 뒤 암호 통신이 필요한 어플리케이션 서비스 확인한다.

$$K_{G_{Temp}} = (s_A)^{y_A^{-1}} \ mod \ n$$

서비스 확인을 마친 인증 서버는 $K_{G_{temp}}$를 임시 그룹원들과의 세션키로 정의하고 $K_{G_{temp}}$리스트를 안전하게 보관한다.

[Step 4] 임시 그룹 SE의 서비스 요청단계

다음은 서비스 등록이 완료된 센서들이 동일한 형태의 서비스를 제공 받기 위해 그룹을 형성하였을 경우 그룹의 대표 센서는 1-out-2 분실 통신을 이용하여 서버에 서비스를 요청하는 단계이다.

- 1-out-2 분실 통신을 수행하는 것은 전송되는 정보가 소실되거나 전송 실패 되었을 경우를 최소화하여 센서의 전력 효율을 높이기 위함이다.

① 센서는 랜덤값 r_0, r_1을 서버에 브로드 캐스팅 한다.

② 서버는 센서로부터 수신된 r_0, r_1을 임시 저장하고 랜덤하게 β_1과 x ($\beta_1 = U(0, 1)$, $x \in {}_UZ_n$)를 선택하고 다음과 같이 Q를 계산하여 센서에 전송한다.

$$Q = E_{K_{G_{temp}}}(x) + r_{\beta_1} \bmod n$$

③ 센서는 $y = D_{K_{G_{temp}}}(Q - r_i \bmod n)(i = 0, 1)$을 계산하여 c_0와 c_1를 다음과 같이 계산하여 서버에 전송한다. (m_0, m_1은 암호 통신이 필요한 서비스 요청 메시지)

$$c_0 = m_0 + y_0 \bmod n, \ c_1 = m_1 + y_1 \bmod n$$

④ 서버는 $m_{\beta_1} = c_{\beta_1} - x \bmod n$을 획득한다.

[Step 5] 임시 그룹의 삭제

임시 그룹으로 형성된 센서들이 임의의 개수 이하가 될 경우 현재 형성된 임시 그룹을 삭제하는 과정을 인증서버는 수행한다.

① 인증서버는 임시 그룹 형성을 위해 센서들의 임시 저장한 비밀정보($y_1, \ldots, y_n$)과 비밀정보를 기반으로 생성된 D 리스트를 임시 저장정보에서 추출한다.

② 인증 서버는 추출된 값에서 $s_{DEL} = (ID_A, D_1, \ldots, ID_{DEL} * D_k)$값을 센서 네트워크 전체에 브로드 캐스팅 한다.

③ 브로드캐스팅된 정보를 수신한 센서는 자신이 포함된 임시 그룹의 상태를 확인하고, 임시 그룹 삭제를 수신한다.

5. 제안방식 분석

제안 방식은 사용자 중심으로 이루어지는 센서 네트워크에서 가질 수 있는 여러 가지 보안 사항을 만족할 수 있는 안전성을 제공하면서 센서 용량을 고려한 방식을 제안하였다.

안전하고 효율적인 센서 네트워크의 관리 구조에 대한 제안 방식은 센서 네트워크가 가져야 하는 보안 요구사항을 기반으로 하여 다음과 같은 안전성을 유지할 수 있다.

- 상호 인증 : 사용자 중심으로 이루어지는 센서 네트워크의 경우 이동 단말과 인증 서버 혹은 게이트웨이와의 상호 인증을 통해 안전성을 유지할 수 이어야 한다. 따라서 본 논문에서는 Feige-Fiat-Shamir 인증 방식을 이용한 인증 방식을 활용하였다. 그러나 Feige-Fiat-Shamir 인증 방식 특성상 키의 사이즈가 매우 커지는 결점이 있다. 따라서 키의 사이즈를 고려한 키 사이즈에 대한 선택이 필수적으로 요구된다.
- 기밀성과 무결성 : 사용자의 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하여 전송 데이터에 대한 안전성을 유지할 수 있어야 한다.
- 효율성 : 센서의 특성상 높은 연산의 계산량을 최소화하여 센서의 효율을 극대화 시킴으로써 전체 센서 네트워크의 효율성을 높이는 방안이 필요하다. 따라서 본 논문에서는 통신의 효율을 높이기 위해 1-out-2 분신 통신 방식을 수행하였다. 이는 하나의 통신 메시지가 분신된다 하더라도 다른 하나는 정당히 수신될 수 있음을 의미한다. 따라서 재전송하기 위한 브로드캐스팅 메시지를 최소화 하도록 하였다.

6. 결론

최근 정보통신의 급속한 발전으로 개인 정보통신의 수요는 날로 증가하고 있다. 특히, 유비컴퓨팅에 대한 연구는 차세대 IT 기술로써 많은 각광을 받고 있는 기술이다.

유비컴퓨팅 환경 중 센서 네트워크 기술은 향후 사용자들에게 아주 많은 편리함을 제공해 줄 수 있는 신기술임에도 불구하고 보안적인 사항이 고려되지 않는다면, 악의적인 목적을 가진 사용자들에 의한 개인 프라이버시 침해와 같은 공격적 취약점을 나타낼 수 있다. 특히, 유비쿼터스 환경의 센서 네트워크은 반드시 보안이 필요하며, 기존의 보안 개념인 인증, 기밀성과 무결성을 비롯하여 새로운 형태의 서비스 제공에 따른 보안 요구사항이 필요하다. 본 논문에서는 기존의 보안 요구사항과 더불어 새로운 보안 요구사항을 제시하여 이를 만족할 수 있는 안전하고 효율적인 센서 네트워크 관리 구조를 제안하였다. 따라서 제안된 방식의 경우 유비쿼터스 상거래와 정부와 같은 유비쿼터스 기반의 환경들에게서 활용할 수 있는 구조이다. 이는 향후 추가적인 보안 요소를 정의하고 그에 따른 해결책을 제시함으로써 보다 향상된 센서 네트워크상에서의 보안 서비스를 실현하고자 한다.

참고문헌

[1]http://www.sktelecom.com//tlab/pdf/tr/13_1/13_1_07.pdf

[2]http://user.chollian.net/~zmnlks/paper/reliable.pdf

[3]김완석, 김정국, 김효기, 김창석, 구홍서, 이상범, 박태웅, 이성국, "유비쿼터스 컴퓨팅 기술과 인프라 그리고 전망", 한국정보처리학회 학회지, 제 10권 제 4호, pp23-38, 2003

[4].http://snow.icu.ac.kr/~korykang/pervasive/papers/introduction_sensornet.pdf

[5]. 이임영 "전자상거래와 보안 입문", 생능출판사, 2001.