센서 네트워크 기반의 홈네트워크에서 안전한 지불 방식 제안

서대희*, 강서일*, 이임영*, 강성우**
*순천향대학교 정보기술공학부
**한국정보보호진흥원 암호인증기술팀

A Study on Secure Payment scheme in Home Network based on Sensor Network

Dae-Hee Seo*, Seo-Il Kang*, Im-Yeong Lee*, Sung-Woo Kang**
* Division of Information Technology Engineering. SoonChunHyang University
**Electronic Transaction Security Technical Team, Korea Information Security Agency

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 홈네트워크에 센서 네트워크가 구성되어 사용자가 센서 네트워크 기반의 지불 서비스를 제공받고자 할 경우 안전한 무선 지불 방식을 제안한다. 제안방식은 센서 네트워크의 특성인 자동 서비스 등록 과정을 거쳐 사용자의 프라이버시 정보에 대한 안전성을 유지하면서도 다양한 서비스의 등록이 가능한 확장성을 제공한다.

1. 서 론

유비쿼터스 네트워크 환경의 특징이 사용자 중심의 상황이나 환경을 네트워크가 지능적으로 파악하여 네트워크 환경을 최적화시켜 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. 이들 중 유비쿼터스 센서망은 사용자 주변의 주변기기가 통신을 하게 됨으로써 자율적으로 정보를 수집하고 관리하는 구성요소이다. 현재 사용하고 있는 단말기는 PC, PDA, 핸드폰 등은 제한된 정보 단말기나 앞으로 최소형 칩으로 된 센서가 모든 환경에서 분산 존재할 경우 각종 정보를 취득/저장하여 이용자의 요구에 따라 자유롭게 분배하여 이용할 수 있게 하는 것이다. 센서 네트워크는 최소형 칩의 활용으로 바코드 등을 이용한 관리 시스템에서 상세한 정보를 최소형 칩에 의한 무선 전자태그로 네트워크 내부를 관리할 수 있게 한다. 이와 같이 필요에 따라 자율적으로 정보를 수집하고 관리하는 체계를 형성하는 망이다[1].

이에 본 논문에서는 센서 네트워크 기반의 홈네트워크가 형성 후 사용자 지불 서비스를 위한 안전하면서 확장성을 제공하는 방식을 제안하고자 한다.

본 논문의 2장에서는 센서 네트워크의 개요에 대해 논의하고, 3장에서는 센서 네트워크 보안의 필요성과 보안 요구사항을 제시하고자 한다. 4장에서는 센서 네트워크 기반의 홈네트워크에서 안전하고 확장성이 가능한 지불 방식을 제안하고 5장에서는 이를 분석한 뒤 6장에서 결론을 맺고자 한다.

2. 센서 네트워크의 개요

센서 네트워크는 물리공간에서 측정한 아날로그 데이터를 디지털 신호로 변환해 인터넷과 같은 전자공간에 연결된 기지 노드로 전달하는 입력 시스템이다. 센서 네트워크에서의 센서는 에이전트와 같은 형식으로 데이터를 전송하게 된다. 따라서 센서들은 자동 분산 개체로써 그룹을 형성하거나 사용자에게 서비스를 제공할 수 있으며, 전자상거래와 같은 환경에 적용 되었을 경우 각각의 센서는

본 연구는 한국정보보호진흥원에서 지원하는 위탁과제로 수행하였습니다.(과제번호2003-S-054)

고정되지 않고 상황에 따라 변경이 가능하며, 통신이 설정될 수 있는지를 결정하기 위해 다른 센서들간에 정보를 획득하는 기술이 필요하다. 또한, 센서들이 일정한 통신량 이상이 높은 경우 그룹 형태로 구성할 수 있다. 따라서 유비쿼터스에 이용될 수 있는 센서는 하드웨어적인 기술의 고도화와 더불어 최소형화를 통한 용이한 칩의 구현등을 들 수 있다. 그러나 사용자 주변으로 형성된 센서 네트워크 경우 사용자의 프라이버스와 매우 밀접한 관계가 있으며, 이에 따라 보안적인 요소가 반드시 요구되는 연구이다[2][3].

3. 센서 네트워크의 보안 사항

3장에서는 센서 네트워크의 보안의 필요성과 요구되는 보안 사항에 대해 분석하고자 한다.

3.1 센서 네트워크 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 가상 세계에서 벌어지는 각종 부작용도 간과할 수 없다[3].

뿐만 아니라 유비쿼터스 세계에서의 불법적으로 수정된 정보의 위협성도 내포하고 있다. 특히, 개인의 정보가 개인의 의사와 무관하게 불법적으로 사용된다면, 새로운 네트워크 환경에서의 안전성을 보장할 수 없다.

따라서 본 논문에서는 유비쿼터스와 같은 새로운 환경에서는 기술적인 효율성과 더불어 안전성에 대한 문제가 선행되어 연구되지 않는다면 여러 가지 사회 문제로 양산될 수 있다.

3.2 센서 네트워크의 보안 요구사항 분석

- 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.
- 자동 서비스 생성 방안 : 일정한 통신량 이상(서비스 이용 빈도)이 높을 경우 안전한 형태의 그룹으로의 변환이 가능해야 하며, 일정한 통신량 이하의 서비스 빈도가 나타날 경우 자동적인 그룹 해체 과정을 제공할 수 있어야 한다.
- 확장성 : 센서의 특성상 하나의 서비스만을 제공할 경우 센서의 개수에 대한 비효율성이 취약점이 된다. 따라서 하나의 센서로 다양한 서비스가 제공하기 위한 확장성을 제공해야 한다.

4. 센서 네트워크 기반의 홈 네트워크에서 안전한 지불 방식 제안

본 논문에서는 센서 네트워크를 기반으로 구성된 홈 네트워크에서 안전한 지불 방식을 제안하고자 한다. 제안방식은 다음과 같은 2개의 구성 객체로 이루어진다.

- 사용자 : 사용자는 UA(User Agent)가 내장된 보편적인 무선 단말기를 소유하고 있으며, 인증 서버와 상호 인증을 수행한 후 서비스를 생성 및 상태를 획득하는 개체(SE : Service Element)이다.
- 인증 서버 :사용자 주변의 센서와 상호 인증 과정을 수행하는 객체로써 센서가 생성한 서비스를 제공하기 위해 게이트웨이와 연동되어 있는 센서 네트워크상의 객체이다.

4.1 시스템 계수

다음은 센서 네트워크 기반의 홈 네트워크에서 안전한 지불 방식 제안을 위한 시스템 계수를 기술한다.

* (s: 센서, a:인증서버, PG:지불 게이트웨이)

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

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

P_*, Q_* : 각 객체의 공개키, 개인키 쌍
$E()$, $D()$: 암호화, 복호화 함수
$^-$, r, □ : 랜덤 수
ID_S : 인증 서버의 공개 ID
PM : 지불 메시지(Payment Message)
PD : 지불 데이터(Payment Data)
PI : 사용자 프라이버시 정보(Personal Information)

4.2 제안 방식 프로토콜

특수한 무선 환경이 제공되지 않는 홈 네트워크 상태에서 다수의 모바일 디바이스가 보편적인 단말기일 경우 이를 이용해 전자상거래 혹은 웹 서비스에 대한 지불 서비스를 제공 받고자 할 경우 안전하고 효율적인 지불 방식 프로토콜은 다음과 같은 사전 전제 사항을 기반으로 이루어진다.

- 사용자는 PG와 인증서버에 안전하게 PI를 전송하고 인증서버와 PG는 이를 안전하게 저장한다.

[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 $\beta \in {}_UZ_q^*$를 선택하여 d_{i_j}를 계산하여 서버에 전송한다.

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

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

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

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

$f_{i_j} = e_{i_j}^{t} \bmod n (= m_{i_j})$ (i=1,2,3)

[Step 2] 센서 네트워크 기반의 지불 서비스를 위한 센서 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.

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

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

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.

$$d_n = c_{i_1} * c_{i_2} * c_{i_3}$$

$$Z_a = Z_2^{d_n^{-1}} \ mod \ n,\ Z_A = Z_a^{r_A} \ mod \ n$$

③ 센서는 인증서버로부터 전송되는 $Z_a \cong V_2$이면 계산한 뒤 올바른 경우 Z_20, m_{i_2}를 인증 서버에 전송한다.

$$V_2 = C_2^{c_{i_2}^{-1} * r_{s_1}} \ mod \ n$$

$$Z_20 = Z_A^{(r_{s_1})^{-1}} \ mod \ n$$

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

$$y_2 = Z_20^{(r_A^{-1})} \ mod \ n$$

[Step 3] 지불 프로토콜

지불 프로토콜은 [Step 2]에서 인증 서버에 저장된 센서의 고유 비밀값을 기반으로 한 안전한 지불 방식이 이루어지는 단계이다.

① 홈네트워크의 사용자가 지불 서비스를 제공받고자 할 경우 사용자가 보편화된 디바이스에 PIN을 입력한 뒤 PM, PD를 이용해 다음을 계산하여 V_{d_a}, T_d, *Service Connection*를 홈 네트워크 인증 서버에 이를 전송한다.

$$V_{d\_a} = E_{P_a}(PM||PD||c_{i_2})$$

② 인증서버는 센서로부터 전송되어온 *Service Connection*을 확인하고 V_{d_a}를 개인키로 복호화한 뒤 y_0를 계산하여 [Step 2]에서 저장된 비밀 정보 y_2의 검증을 통해 센서 인증 및 서비스 인증을 수행하고 다음을 계산한 뒤 인증서버와 연결되어 있는 PG에 SIG_{a_PG}, T_a를 이를 전송한다.

<y_2의 검증>

$$y_2 = Z_2 0^{(c_0^{-1})} \bmod n = C_2^{c_0^{-1}} \bmod n$$

<인증서버에서 PG에 전송되는 SIG_{a_PG} >

$$SIG_{a\_PG} = (Sig_Q(E_{P_{PG}}(PD||PI||PM)))$$

③ PG는 인증서버로부터 전송되어온 서명값 SIG_{a_PG}를 인증서버의 공개키로 이를 검증하고 자신의 개인키로 암호화된 값을 복호화하여 사전 등록된 사용자의 PI와의 비교를 통해 사용자를 인증하고 사용자가 요구하는 PD에 대한 지불 서비스를 제공하고 PD, PM에 대한 응답값을 생성하여 다음을 계산한 뒤 V_{PG_a}, SIG_{PG_a}, T_{PG}를 인증 서버에 전송한다.

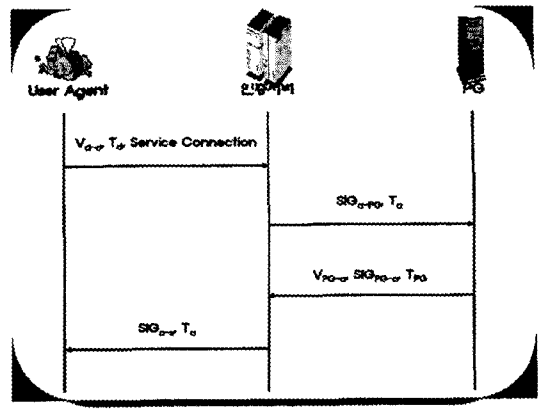
$$V_{PG\_a} = E_{P_a}(PD_{res})$$

$$SIG_{PG\_a} = Sig_{Q_{PG}}(PM_{res})$$

④ V_{PG_a}, SIG_{PG_a}, T_{PG}를 전송 받은 인증 서버는 SIG_{PG_a}에서 PM_{res}를 확인한 후 올바른 경우 V_{PG_a}에 인증서버의 개인키로 서명한 뒤 SIG_{a_s}, T_a를 센서에 전송한다.

$$SIG_{a\_s} = Sig_Q(V_{PG\_a})$$

이상의 과정을 수행하여 홈 네트워크에서 구성된 센서 네트워크를 기반으로 한 안전한 지불 프로토콜을 수행하며, 이는 그림 1과 같다.



(그림 1) 센서 네트워크 기반의 홈네트워크에서의 안전한 지불 방식

5. 제안방식 분석

본 장에서는 4장에서 제시했던 제안 방식을 3장에서 기술한 보안 요구사항을 기반으로 분석할 경우 다음과 같은 특징을 가지고 있다.

- 상호 인증 : 사용자 중심으로 이루어지는 센서 네트워크의 경우 이동 센서와 인증 서버 혹은 지불 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 선택이 필수적으로 요구된다.
- 기밀성과 무결성 : 제안 방식은 디바이스 보안과 전송 데이터에 대한 기밀성으로 구분하여 전송 데이터에 대한 기밀성과 무결성을 제공하였다.

* 디바이스 보안 - 홈 네트워크상의 개체들에 포함되어 있는 SE들은 자동 서비스 생성 개체로써 이와 연관된 비밀값을 안전하고 저장하여야 한다. SE는 UA로써 센서 네트워크상에서 이루어지는 연산 과정에서 기밀 연산을 수행함으로써 디바이스 저장 정보에 대한 무결성을 보장하였다. 제안 방식에서는

$$V_2 = C_2^{(c_{i_2}^{-1} * r_{s_1})} \bmod n = Z_2^{(a_n^{-1})} \bmod n$$

$$= C_2^{(c_{i_1} * c_{i_2} * r_{s_1}) * (c_{i_1} * c_{i_2} * c_{i_3})^{-1}} \bmod n$$

의 검증과정을 거쳐 디바이스의 비밀값 r_{s_1}를 전송하지 않고 기밀 의뢰 연산 방식을 수행하였다.

* 전송 데이터에 대한 기밀성과 무결성 : 홈 네

트워크를 기반으로 형성된 센서 네트워크 구조에서의 전송 데이이터의 기밀성은 공개키 암호 알고리즘과 안전한 해쉬 함수를 이용해 전송 데이터에 대한 기밀성을 유지하였다.

- 자동 서비스 생성 방안 : 제안 방식은 자동 서비스 생성에 대한 요구사항을 제공하기 위해 서버에서 제공할 수 있는 서비스 등록에 대한 고유 서비스 (i는 서비스 형태를 규정짓는 고유번호, i=1,..., N) f_i를 계산하여 서비스 신청의 정당성을 확보하였다.
- 확장성 : 제안방식은 하나의 센서가 다양한 서비스를 제공할 수 있는 방식을 통해 소수의 센서를 통해 여러 가지 서비스를 사용자에게 제공할 수 있는 확장성을 제공하였다.

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 센서 네트워크 기반의 홈 네트워크 상태에서 안전한 전자 지불 방식을 제안하였다.

7. 참고 문헌

[1]http://www.sktelecom.com//tlab/pdf/tr/13_1/13_1_07.pdf
[2].http://user.chollian.net/~zmnlks/paper/reliable.pdf
[3]. http://www.uk.research.att.com/
[4]. http://www.freeband.nl/ENindex.html
[5]. 이임영 "전자상거래 입문", 생능출판사, 2001.8