www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.3.107

무선센서네트워크 환경에서 생체기반의 개선된 사용자 인증 프로토콜

A Robust Biometric-based User Authentication Protocol in Wireless Sensor Network Environment

신광철(Kwang-Cheul Shin)*

초 록

무선센서 네트워크 환경에서 센서노드들에 대한 식별자 노출을 억제함으로써 익명성을 보장하고 실시간 인증, 인증의 경량화, 동기화 등이 요구되고 있다. 특히 무선 채널상에서 이루어지는 통신은 제3자에 의한 위치정보가 노출되거나 프라이버시 침해 및 보안상의 취약점이 존재한다. 익명성은 유·무선 네트워크 환경에서 중요한 문제로 폭넓게 연구되어왔다. 센서 노드는 노드간의 무선망 구성을 기본으로 하여 계산능력의 제한과 저장장치의 제한, 전력 장치의 소형화가 강조되고 있다. 본 논문에서는 생체기반의 D. He scheme을 개선하여 네트워크 성능 향상과 익명성을 보장하며 URSC(Unique Random Sequence Code)와 가변식별자(variable identifier)를 이용한 실시간 인증 프로토콜을 제안한다.

ABSTRACT

In a wireless sensor network environment, it is required to ensure anonymity by keeping sensor nodes' identifiers not being revealed and to support real-time authentication, light-weight authentication and synchronization. In particular, there exist possibilities of location information leakage by others, privacy interference and security vulnerability when it comes to wireless telecommunications. Anonymity has been an importance issue in wired and wireless network environment, so that it has been studied in wide range. The sensor nodes are interconnected among them based on wireless network. In terms of the sensor node, the researchers have been emphasizing on its calculating performance limit, storage device limit, and smaller power source. To improve of biometric-based D. He scheme, this study proposes a real-time authentication protocol using Unique Random Sequence Code(URSC) and variable identifier for enhancing network performance and retaining anonymity provision.

키워드 : 무선센서 네트워크, 유일랜덤순차코드, 상호인증, 익명성 가변식별자
Wireless Sensor Network, URSC, Mutual Authentication, Anonymity, Variable Identifier

* Professor in Dept. of Industrial Management Engineering, Sungkyul University(skcskc12@sungkyul.edu)
2013년 06월 05일 접수, 2013년 07월 11일 심사완료 후 2013년 07월 29일 게재확정.

1. 서 론

기존 무선센서 네트워크는 비밀성과 인증, 무결성 등에 대한 많은 연구가 있었지만 최근 들어 강력하면서도 초경량화한 인증과 센서노드의 익명성을 보장하는 문제에 관심이 고조되고 있다[3]. 센서 네트워크에서의 익명성은 주요 개체들의 식별자 및 추적요소들을 통신선 상에서 노출되는 것을 제 3자로부터 보호하는 것이다. 제 3자는 센서노드에 의해 송수신되는 메시지를 도청하더라도 송수신자의 식별자를 결정할 수 없어야 한다[10]. 무선센서 네트워크의 상호인증은 센서노드와 게이트웨이 간 최소한의 정보를 전달하여 인증하는 것이다. 공개키를 이용한 전자서명을 통해 인증하는 경우 일반적으로 많은 메모리 공간과 복잡한 계산을 필요로 하는데 전력이나 메모리, 프로세서와 같은 자원의 제약이 있는 무선 환경에서 적용하기 어려운 것이 현실이다[7]. 그러므로 대칭형 암호 시스템이나 속도가 빠른 해시함수를 사용하여 네트워크 성능을 유지하면서 경량화된 보안시스템이 필요하다. 무선센서네트워크에서 일반적으로 스킴들은 패스워드를 기반으로 한 인증 기술이었다[13]. 그러나 패스워드는 낮은 엔트로피로 인해 사전공격에 쉽게 취약하다. 이러한 문제를 해결하기 위해 암호키를 사용하게 되는데 암호키는 매우 길고 랜덤하여 기억하는데 어려움이 있다. 더구나 패스워드와 암호키는 분실하거나 다른 사람과 공유할 때 부인방지를 제공할 수 없다. 따라서 지문과 같은 사람의 생체나 행동특성에 기반을 둔 인증기법이 제안되고 있다[2]. 2010년, Yuan et al.[16]은 무선센서 네트워크환경을 위한 생체기반의 사용자 인증스킴을 제안했다. 그들의 스킴은 해시함수만을 사용하므로 매우 효율적으로 평가했다. 그러나 2011년, Yoon et al.[15]는 Yuan et al.[16] 스킴이 내부자 공격과 게이트웨이 위장공격, 센서노드 위장공격, 사용자 위장공격에 취약함을 지적하고 보안이 향상된 스킴을 제안하였다. 2012년, D. He는 Yuan et al.'s 스킴이 센서노드 위장공격에 취약함을 지적하고 개선된 새로운 스킴을 제안하였다. 하지만 D. He 스킴은 사용자의 식별자를 노출시킴으로써 익명성을 보장받지 못하며 스마트카드 도난 또는 분실했을 때[8]에 의해 생체정보인 Bi를 위장할 수 있으며 password 추측공격으로 인해 사용자 위장공격과 센서노드 위장공격에 취약한 구조적인 결점을 가지고 있다[14]. 본 논문에서는 D. He 스킴을 분석하고 개선된 사용자 인증스킴을 평가하기 위한 10가지의 요구사항을 제시하고 분석한다.

Req1 : 노드간 상호인증
Req2 : 위치추적 방지
Req3 : 익명성 유지
Req4 : 재전송공격방지
Req5 : 위장공격방지
Req6 : 중간자공격 방지,
도청공격(Eavesdropping Attack) 방지
Req7 : 전송실패 최소화
Req8 : 패턴과 동기화
Req9 : 사용자의 패스워드 선택 및 갱신
Req10 : 스마트카드 도난 및 분실로부터 안전

따라서 본 논문에서는 성능향상과 보안레벨 강화를 위해 센서노드와 게이트웨이 간 암호알고리즘을 사용하는 대신 유일순차코드(Unique Sequence Code)인 URSC[4, 11]와 가변식별자

를 이용하여 강한 익명성의 보장과 도청, 위치 추적, 센서노출 등 취약성에 대비한 경량화된 상호인증 프로토콜을 제안하고 분석하였다.

2. D. He 인증 스킴 검토

He[1] scheme은 등록, 로긴 및 인증의 3단계로 구성되며 주요 표기는 다음과 같다.

U_i	사용자 i
ID_i, pw_i, B_i	사용자 i의 식별자, 패스워드, 생체정보
GW-node	게이트웨이 노드
x, y	게이트웨이 노드의 마스터 키
S_j	j번째 센서노드
SID_j	S_j의 식별자
d()	대칭 매개변수 함수
τ	생체검증을 위한 소정의 임계값
Ek[]	대칭키 k로 암호화함수
Dk[]	대칭키 k로 복호화함수
h()	단 방향 함수
⊕	XOR 연산
‖	연접

D. He 스킴은 게이트웨이를 신뢰된 노드로 가정하고 충분한 크기의 두 개의 마스터키 x와 y를 보유한다. 시스템이 운용되기 전에 센서노드 S_j에 비밀키 $h(SID_j \| y)$를 생성하여 저장한다.

2.1 등록단계

합법적 사용자가 처음 등록을 원할 때 다음과 같은 절차에 따른다.

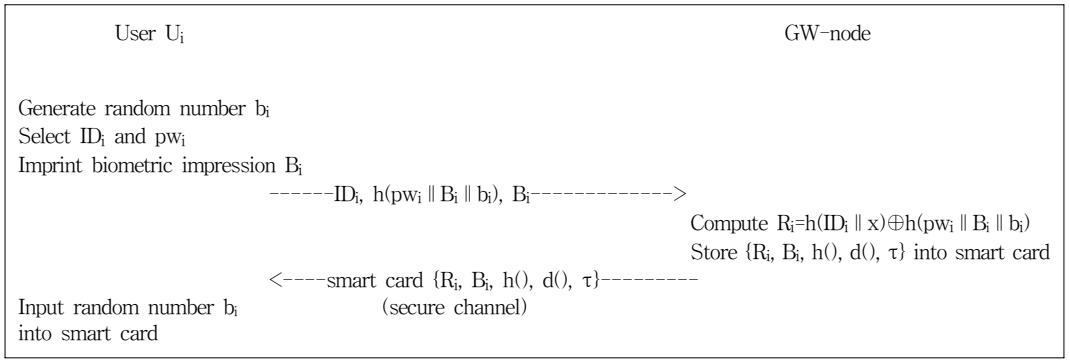
step 1 : U_i는 무작위 수 bi를 생성하고 자신의 ID_i와 pw_i를 선택한 다음 생체정보 B_i를 생성한다. 이어서 안전한 채널을 통해 GW-node에게 ID_i, $h(pw_i \| B_i \| b_i)$, B_i를 전송한다.

step 2 : 등록요청을 수신한 GW-node는 자신의 비밀키 x를 사용하여 R_i를 연산하고 스마트카드에 R_i, B_i, h(), d(), τ를 저장하여 안전한 채널로 U_i에게 발급한다.

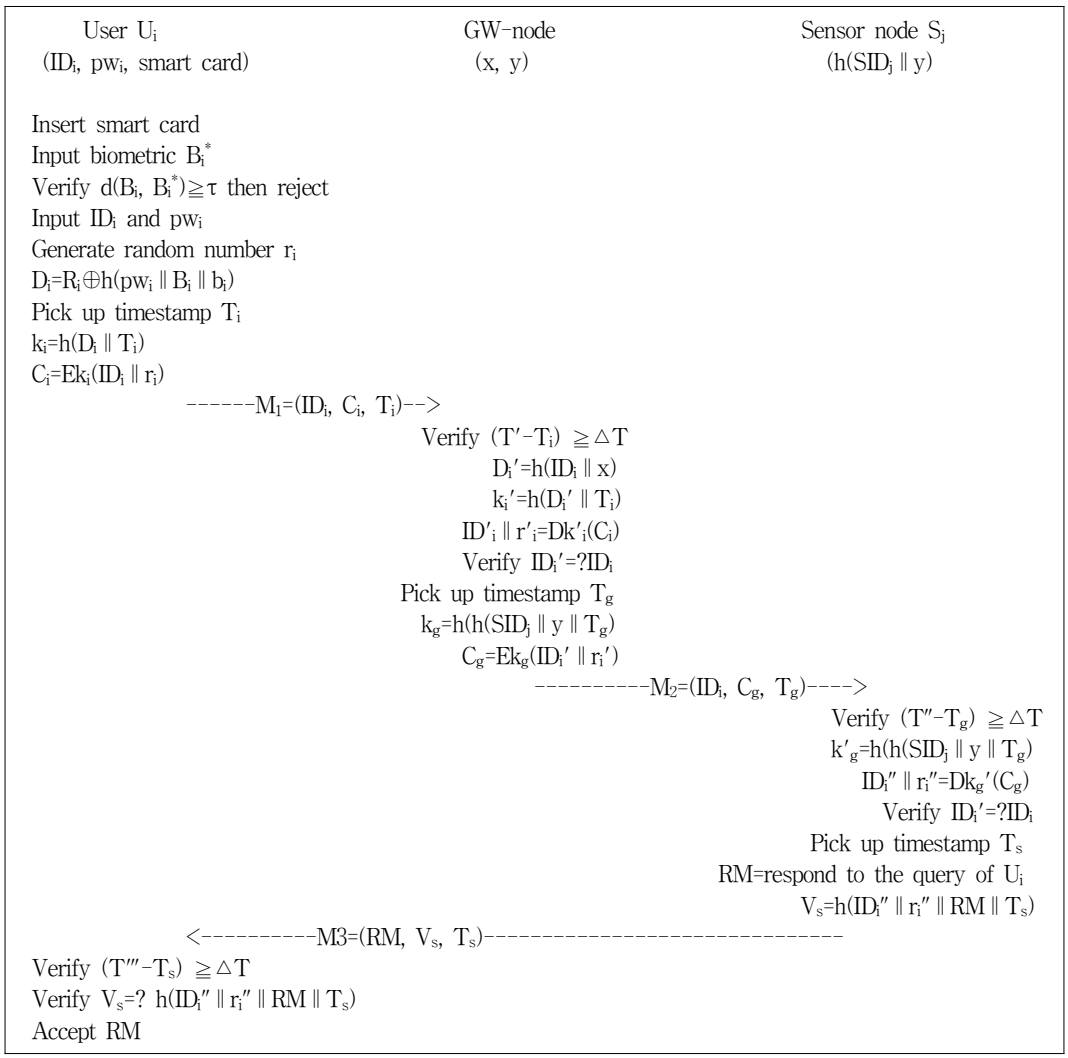
step 3 : 스마트카드를 수신한 U_i는 무작위 수 b_i를 입력하여 등록을 마친다.

2.2 로그인 단계

U_i가 데이터에 접근하기를 원할 때 다음과 같은 단계<Figure 2>로 수행한다.



〈Figure 1〉 Registration Phase of D. He Scheme



〈Figure 2〉 Login and Authentication Phase of D. He Scheme

step 1 : U_i는 스마트카드를 삽입하고 생체정보 B_i를 입력하여 정확성 여부를 체크($d(B_i, B_i^*) \geq \tau$, $d(B_i, B_i^*) < \tau$)하게 되며 미리 정의된 소정의 임계값($d(B_i, B_i^*) < \tau$)을 만족하게 되면 승인이 되어 그 다음 절차로 ID_i와 pw_i를 입력한다. 그 때 스마트카드는 무작위 수 r_i를 생성하고 타임스템프 T_i를 추출하여 D_i와 k_i를 연산한 후 암호문 C_i를 생성한다.

step 2 : U_i는 로긴메시지 M_1을 GW-node로 전송한다.

2.3 인증 단계

T'시간에 로긴 메시지 M_1을 수신한 GW-node는 U_i를 인증하기 위해 다음을 수행한다.

step 1 : GW-node는 T_i의 유효성를 체크하고 D'_i, k'_i, $ID'_i \| r'_i$를 연산한다. ID_i와 ID_i'가 일치하면 게이트웨이의 타임스탬프 T_g를 추출하여 k_g, C_g를 연산한 후 M_2를 센서노드 S_j로 전송한다.

step 2 : S_j는 M_2를 수신하여 센서노드의 타임스탬프 T''를 이용하여 $(T''-T_g) \geq \triangle T$의 유효성이 만족하면 k'_g와 $ID''_i \| r''_i = Dk'_g(C_g)$를 연산한다. 연산결과 ID'_i와 ID_i가 일치하면 S_j는 타임스탬프 T_g를 추출하여 $V_s = h(ID''_i \| r''_i \| RM \| T_s)$를 연산하고 $M_3(RM, V_s, T_s)$를 U_i로 전송한다.

step 3 : M_3를 수신한 U_i는 $(T'''-T_s) \geq \triangle T$의 유효성을 체크하고 V_s와 $h(ID''_i \| r''_i \| RM \| T_s)$가 동일한지 체크하여 승인한다.

3. D. He 인증 스킴의 취약성

제3자는 유선구간인 U_i와 GW-node, 무선구간인 GW-node와 sensor node S_j간의 통신채널을 모두 통제할 수 있다고 가정한다. Messerges et al.[8]연구에 의하면 스마트카드에 저장된 비밀정보는 전력소비를 분석하고 모니터링하여 추출할 수 있는 취약성이 있다.

3.1 생체정보 및 패스워드의 취약성

Messerges et al.[8]에 기반을 두고 전력분석 공격을 이용하여 사용자의 스마트카드에 저장된 비밀정보 R_i, B_i를 획득한 후 일치하는 패스워드 pw_i를 얻기 위해 오프라인 패스워드 추측공격을 수행한다. 문제는 생체정보 B_i가 스마트카드 내에 저장되어 제 3자에게 노출되었다는데 있다. B_i가 추출되면 D. He 스킴의 로그인 단계에서 $d(B_i, B_i^*) < \tau$를 쉽게 통과할 수 있다. 이어서 패스워드를 추측하기 위해 제 3자는 로그인 메시지 M_1을 가로채기 한다. 다음 pw_i의 추측과 D_i*를 얻기 위해 $R_i \oplus h(pw_i \| B_i \| b_i)$를 연산하여 D_i*를 구하고 D_i*를 이용하여 k_i* = $h(D_i \| T_i)$를 얻게 된다. 키 k_i^*로 $C_i = Dk_i^*(ID_i \| r_i)$을 복호화하여 $ID_i^* \| r_i^*$를 얻는다. $ID_i^* = ID_i$가 성립하면 $pw_i^* = pw_i$, $D_i^* = D_i$가 올바르게 추측되었다고 판단한다. 결국 제3자는 올바른 $D_i = h(ID_i \| x)$를 얻게 되고 정당한 사용자로 위장할 수 있다.

3.2 위치추적에 의한 익명성 문제

익명성이란 사용자가 자신의 신원을 노출시키지 않고 서비스나 자원을 이용하는 것을 말한다. He[1] 스킴에서는 $M_1 = (ID_i, C_i, T_i)$과 $M_2 = (ID_i, C_g, T_g)$ 메시지에서 ID_i를 비보호 채널에 공개함으로써 신원을 노출할 뿐 아니라 위치추적에 취약함을 보이고 있다. 특히 위치추적 공격은 공격자가 센서노드의 위치변화를 감지하고 센서노드 소유자의 이동경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 센서노드로부터 매 세션마다 동일한 정보가 나오는 무선센서 시스템은 위치추적이 가능하다.

3.3 사용자 위장공격

He[1] scheme은 사용자 U_i 위장공격에 취약하다. 제3자는 서로 다른 전력분석 공격[8]을 통해서 패스워드를 획득하여 $D_i = R_i \oplus h(pw_i \|$

$B_i \| b_i$)을 연산하고 비밀 값 $D_i = h(ID_i \| x)$를 획득한다. 그때 제 3자는 $k_i = h(D_i \| T_a)$와 $C_a = Ek_i(ID_i \| r_a)$를 연산하여 사용자 U_i의 로긴 메시지 M_1을 위조한다. T_a는 제 3자의 타임스탬프이고 r_a는 제 3자에 의해 생성된 무작위 수이다. 제 3자는 GW-node에게 위조된 메시지 $M_1 = (ID_i, C_a, T_a)$를 전송한다. 이때 GW-node는 자신의 비밀 키 x와 ID_i로 비밀 값 $D_i = h(ID_i \| x)$를 연산할 수 있기 때문에 위조된 메시지는 GW-node의 검증을 쉽게 통과한다. 그러므로 D. He scheme은 사용자 U_i 위장공격에 취약하다.

4. 제안 스킴

본 절에서는 사용자 U_i의 생체정보와 아이디, 패스워드, GW-node의 비밀키를 사용하여 상호간 인증을 수행하며 D. He 스킴에서는 생체정보 B_i를 직접 스마트카드에 저장하여 제공하였으나 제안스킴에서는 식으로 유도하였다. 또한 패스워드의 입력을 3회로 제한하여 그 이상 입력이 진행될 때 승인이 거부되며 패스워드의 입력이 정확한지의 여부를 검사한다. GW-node와 센서노드 간에는 URSC와 가변식별자를 사용하여 메시지 암호화 기능을 없애 속도를 향상시키고 경량화에 중점을 두고 있다.

4.1 표기

g : 순환군 z_p의 생성자
p : 1024 bit 소수
GW_i : GW-node i의 식별자
SID_j^0 : 센서노드 S_j의 초기식별자
G() : 다음 식별자를 생성하는 해시함수
$SID_j^q{}_{(SN/GW)} = G(SID_j^0)$: 센서노드/게이트웨이 노드가 Generator G에 의해 생성된 센서노드의 다음 식별자
$SID_j^{q+1}{}_{(SN/GW)} = G(SID_j^q)$: 센서노드/게이트웨이 노드가 Generator G에 의해 생성된 센서노드의 그 다음 식별자

4.2 초기화

GW-node는 센서노드에게 로긴 메시지를 전송할 때마다 센서노드의 식별자를 generator(G)을 통해 다음 식별자인 $SID_j^q(GW) = G(SID_j^0)$로 바꾸어 저장한다. 센서노드는 자신의 초기 식별자인 SID_j^0와 GW의 식별자인 GW_i를 저장하며 인증 메시지를 전송한 후 다음 식별자(SID_j^q)를 바꾸어 저장한다. GW-node는 센서노드의 다음 식별자를 저장하고 있어야 이 식별자를 통해 어느 센서노드로부터 온 메시지인지 확인할 수 있다.

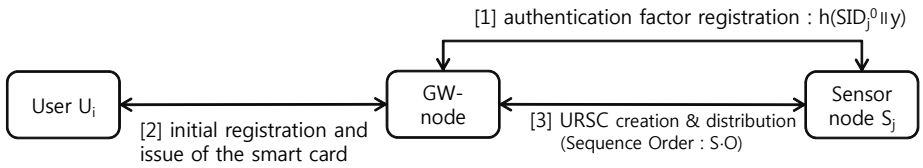
4.2.1 등록 I
(게이트웨이 GW-node와 센서노드 S_j)

GW-node는 신뢰하는 노드로 충분한 크기의 두 개의 마스터키 x와 y를 보유한다고 가정한다. 시스템이 운용되기 전에 센서노드 S_j에 비밀키 $h(SID_j \| y)$를 생성하여 저장한다<Figure 3>.

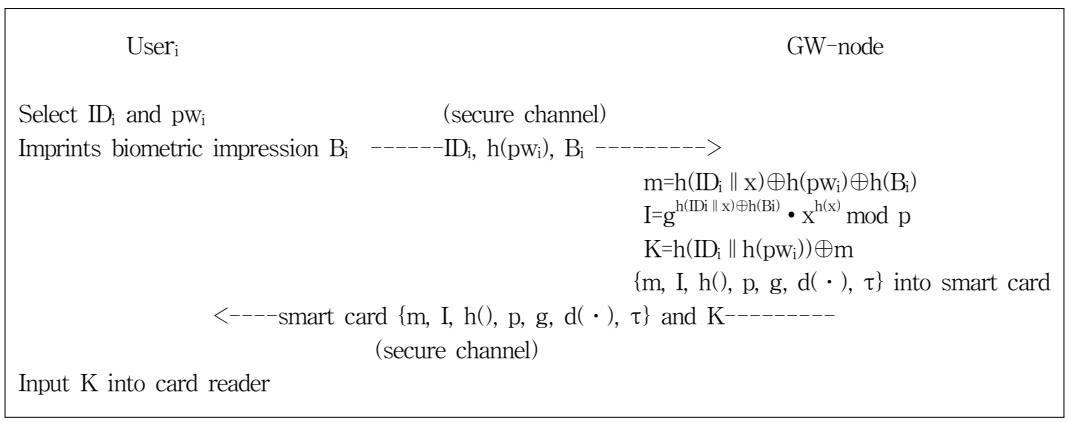
4.2.2 등록 II(사용자 U_i와 GW-node)

합법적인 사용자 U_i가 등록을 원할 때 수행하는 프로세스는 <Figure 4>와 같다.

① 사용자 U_i는 자신의 식별자 ID_i와 패스워드 pw_i를 선택하여 $h(pw_i)$, 생체정보 B_i를 안전한 채널을 통하여 GW-node에게 ID_i, $h(pw_i)$, B_i를 전송한다.



〈Figure 3〉 Composition of sensor network



〈Figure 4〉 Registration Phase of Propose Scheme

② GW-node는 $m = h(ID_i \| x) \oplus h(pw_i) \oplus h(B_i)$와 $I = g^{h(ID_i \| x) \oplus h(B_i)} \cdot x^{h(x)} \bmod p$ 그리고 $K = h(ID_i \| h(pw_i)) + m$를 연산하여 m, I, h(), p, g를 사용자 U_i에게 안전한 채널로 전달한다. 이때 K는 스마트카드에 포함시키지 않고 값만을 전달하여 사용자측에서 카드리더기에 직접 입력하도록 한다.

③ 카드리더기에 K를 직접 입력한다.

4.2.3 URSC의 생성 및 분배 (GW-node와 센서노드 S_j)

GW-node와 센서노드들 간의 직접 상호인증을 제공하기 위해 경량화 된 URSC를 사용한다. Kim et al.[4]에서 제안한 frequency-hopping optical orthogonal code에서 공백을 제거하여 메시지 인증을 위한 필드에 적용할 수 있도록 개선하였다.

GW-node는 자신 영역의 센서노드들의 수에 따라 코드길이 L을 선택하고 시드(seed)가 되는 순차코드 생성자(Sequence Code Generator)를 찾고 순차

코드행렬을 생성한다. 이때 각 행렬의 번호를 시퀀스 오더(S.O : Sequence Order)라 정의하고 자신 영역의 센서노드들에게 순자코드 생성자와 시퀀스오더를 무작위로 배분하여 순차코드인 URSC를 생성한다. URCS 코드는 케이트웨이와 센서노드의 인증요소로써 PSC와는 다르게 URSC 생성은 노드가 자신의 S.O 이외에 순차코드 생성자를 추가로 저장하고 있어야 한다[11]. 한 영역의 GW-node에 할당된 센서노드가 5라면 임의의 소수 p = 11, L = 5인 경우 거리호핑 패턴을 임의로 D = [2, 4, 6,

sensor node	S.O	S.C	·····	sensor node	S.O	S.C
S_j	J	0 2 6 1 8	·····	S_{j+n}	J+n	4 6 10 5 1

〈Figure 5〉 Sequence Code Matrix(SCM) : S.O(Sequence Order), S.C(Sequence Code)

7, 9]를 선택했을 때 다음과 같이 되어 순차코드가 5개 생성된다.

$$M=\begin{bmatrix} 0 & 0+2 & 0+2+4 & 0+2+4+6 & 0+2+4+6+7 \\ 1 & 1+2 & 1+2+4 & 1+2+4+6 & 1+2+4+6+7 \\ 2 & 2+2 & 2+2+4 & 2+2+4+6 & 2+2+4+6+7 \\ 3 & 3+2 & 3+2+4 & 3+2+4+6 & 3+2+4+6+7 \\ 4 & 4+2 & 4+2+4 & 4+2+4+6 & 4+2+4+6+7 \end{bmatrix} \bmod 11 =$$

$$\begin{bmatrix} 0 & 2 & 6 & 1 & 8 \\ 1 & 3 & 7 & 2 & 9 \\ 2 & 4 & 8 & 3 & 10 \\ 3 & 5 & 9 & 4 & 0 \\ 4 & 6 & 10 & 5 & 1 \end{bmatrix}$$

모든 행과 열에 같은 수가 없으므로 M을 순차코드행렬로 사용하며 게이트웨이는 자신이 관리하는 영역의 센서노드들에게 비밀리에 순차코드 생성자와 시퀀스 오더를 전달, 분배한다. 각각의 센서노드들은 순차코드 생성자를 이용하여 순차코드를 생성하고 자신의 시퀀스오더에 해당하는 순차코드(URSC)를 보관한다.

센서노드는 이웃하는 센서노드들이 어떤 시퀀스 오더를 보유하고 있는지 모른다. 센서노드 S_j는 자신의 시퀀스 오더 'J'와 시퀀스 코드 '0 2 6 1 8'을 보유하게 된다.

4.3 프로토콜

<Figure 6>에서와 같이 User와 GW-node간 인증과 익명성 보장, GW-node와 센서노드 간에는 URSC를 이용한 익명성과 프라이버시 보장, 재전송공격에 대한 방어, 위치추적방지를 위한 연산이 이루어지고 동일영역의 정당한 상호인증을 해야 한다. 인증순서는 [step1] … [step 7]의 순으로 진행된다.

4.3.1 Login phase

본 단계에서는 등록이 완료된 사용자가 게이트웨이에 로그인 하는 단계이며 로그인은 사용자가 생체정보(B_i')를 입력하여 임계값 τ을 벗어($d(B_i, B_i') \geq \tau$)나면 합법적 사용자가 아니므로 거절된다[15]. 그렇지 않으면 발급받은 스마트카드를 리더기에 삽입하고 ID_i 및 pw_i를 입력한다.

[step 1]

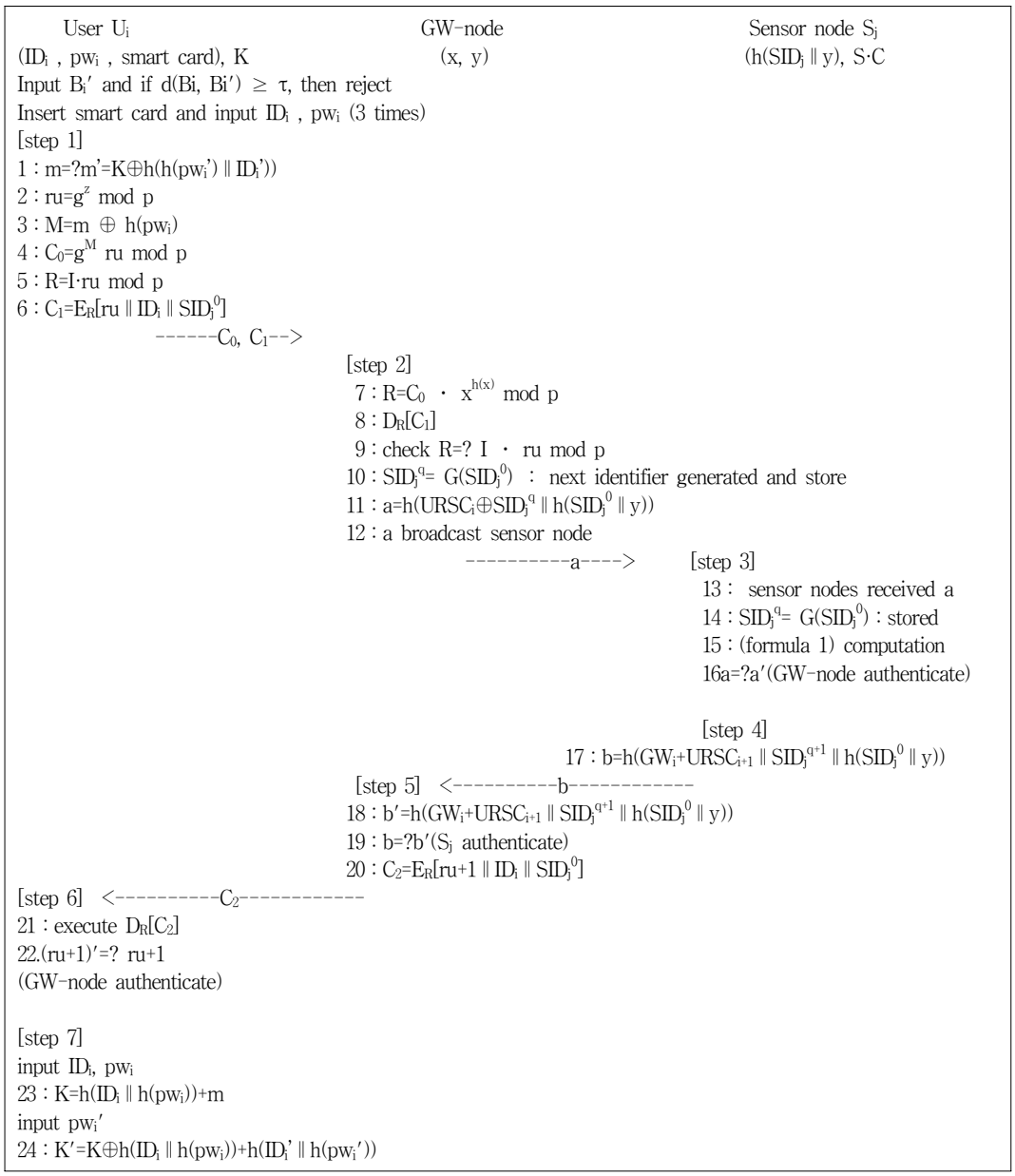
입력된 ID_i, pwi는 스마트카드 리더기 내의 K를 사용하여 m′를 생성하고 m과 비교하여 정확하게 ID_i, pw_i가 입력되었는지 검증(1 : m = ?m' = $K \oplus h(h(pw_i') \| ID_i')$)한다. 이 때 패스워드는 3회 입력의 제한을 두어 일치하지 않으면 거절한다. 이어 리더기는 임의 수 z를 선택하여 난수 ru(2 : ru = $g^z \bmod p$)를 생성한다. 그리고 M, C_0, R(step1의 3, 4, 5)을 계산한 다음 인증을 요청하는 메시지 $C_1 = E_R[ru \| IDi \| SID_j^0]$를 R로 암호화하여 C_0와 함께 GW-node로 전송한다.

4.3.2 Authentication phase

본 단계에서는 사용자의 로그인 메시지를 전송받은 GW-node에서 사용자 인증과 센서노드 S_j의 요청메시지를 작성하는 단계이다.

[step 2]

GW-node는 자신의 비밀 키 x와 수신한 C_0를 이용하여 R(7 : $R = C_0 \cdot x^{h(x)} \bmod p$)을 연산하고



〈Figure 6〉 Login and Authentication,Password Change Phase of Propose Scheme

메시지 C_1를 복호(8 : $D_R[C_1]$)화 한다. 또한 x와 ID_i를 사용하여 I를 계산한 후 R′를 계산하여 R을 비교(9 : check R = ? I · ru mod p)한다. R을 비교하여 일치하면 정당한 사용자로 인증이 되며 GW-node가 보관중인 S.O에서 무작위로 S.C의 수를 선택하여 a를 생성(11 : $a = h(URSC_i \oplus SID_j^q \| h(SID_j^0 \| y))$)하고 영역내의 센서노드들에게 브로드캐스트(broadcast)한다.

[step 3]

a를 수신한 S_j는 자신의 식별자, 그리고 게이트웨이와 공유하는 비밀정보 $h(SID_j^0 \| y)$와 URSC 코드를 사용하여 수신된 a와 일치할 때까지 반복하여 a′식 (1)을 계산하고 a와 일치하면 S_j는 게이트웨이를 인증하게 되며 그렇지 않으면 거절된다.

$$a' = \sum_{i=1}^{L} h(URSC_i \oplus SID_j^q \| h(SID_j^0 \| y)) \quad (1)$$

[step 4]

센서노드(S_j)는 식별자(SID_j^{q+1})와 다음의 URSC 코드($URSC_{i+1}$)를 선택하여 b를 생성(17 : $b = h(GW_i + URSC_{i+1} \| SID_j^{q+1} \| h(SID_j^0 \| y))$)하고 게이트웨이로 전송한다.

[step 5]

GW-node는 정당한 센서노드인지 확인을 위해 자신의 식별자로 b′를 생성(18 : $b' = h(GW_i + URSC_{i+1} \| SID_j^{q+1} \| h(SID_j^0 \| y))$)하여 수신된 b와 비교한 후 일치하면 승인하고 그렇지 않으면 거절한다. 이후 사용자에게 GW-node가 정당하다는 메시지를 ru+1를 포함하여 센서노드의 인증요소 C_2(20 : $C_2 = E_R[ru+1 \| ID_i \| SID_j^0]$)를 암호화($E_R[ru+1, ID_i, SID_j^0]$)하여 전송한다.

[step 6]

수신한 암호화 메시지($E_R[ru+1 \| ID_i \| SID_j^0]$)를 복호화($D_R[ru+1 \| ID_i \| SID_j^0]$)하여 정당한 게이트웨이를 확인((ru+1)′ = ? ru+1)하여 일치하면 승인하고 그렇지 않으면 거절한다.

4.3.3 Password change phase

사용자는 임의 pw_i'를 선택하여 게이트웨이와는 무관하게 독립적으로 스마트카드에 내장된 $h(ID_i \| h(pw_i))$의 값을 변경할 수 있다.

[step 7]

(1) 사용자는 ID_i, pw_i 입력을 통해 로그인 인증 프로세스가 정상적으로 수행된다.

(2) 현재의 pw_i와 임의 새로운 pw_i' 입력하면 $m' = K \oplus h(h(pw_i') \| ID_i'))$가 연산되어 스마트카드는 현재의 K를 K′로 변경되고 K값 대신에 $K' = K \oplus h(ID_i \| h(pw_i)) + h(ID_i' \| h(pwi'))$로 대체되어 저장된다.

5. 분석 및 평가

GW-node와 센서노드 간에는 메시지 패턴 추측이 어려운 URSC 코드를 해시값과 가변식별자, $h(SID_j^0 \| y)$를 사용하여 인증이 이루어지고 사용자와 게이트웨이 간에는 대칭키 R를 생성할 수 있는지와 비밀키 x에 의해 생성된 값 K와 U_i의 password pw_i에 의존한다. 이 과정이 진행되는 상호인증 프로토콜을 분석과 평가를 하면 다음과 같다.

Req1 : 노드간 상호인증 (Mutual Authentication)

제안스킴은 U_i와 GW-node, 그리고 S_j 3자간 상호인증구조를 제공한다. U_i와 GW-node 간의 상호인증은 수신메시지 C_0로부터 R을 계산해 낼 수 있는가와 R을 사용하여 C_1를 정확하게 복호화할 수 있는가에 달려 있다. 정당한 GW-node만이 비밀리에 보관중인 비밀키 x를 사용하여 R을 구하고 C_1를 복호화할 수 있다.

복호화된 메시지의 ID_i와 x를 이용하여 I를 계산한 후 ru를 사용하여 I · ru mod p의 결과와 R을 비교하여 일치하면 승인되고 그렇지 않으면 거절된다. 사용자는 GW-node에 의해 정당하게 복호화 된 메시지의 검증으로 ru+1의 값으로 인증된다. GW-node와 S_j 간의 인증은 무선환경임을 감안하여 속도에 제한을 받지 않도록 $h(SID_j^0 \| y)$와 가변식별자, URSC에 의존한다. GW-node는 U_i에서 수신한 메시지의 정보 SID_j를 사용하여 S_j에게 사전 분배하여 생성된 시퀀스코드(S · C) '0 2 6 1 8' 중 임의 코드를 선택하여 $a = h(URSC_i \oplus SID_j^q \| h(SID_j^0 \| y))$를 생성하여 전송한다. S_j는 자신의 URSC 코드(0 2 6 1 8) 중 차례로 적용하여 수신된 a와 일치하는 코드 식 (1)을 찾는다. $a = a'$가 성립되면 GW-node를 인증한다. GW-node에서는 S_j가 정확하게 다음 URSC 코드를 사용하여 식별자를 생성($b = h(GW_i+URSC_{i+1} \| SID_j^{q+1} \| h(SID_j^0 \| y))$) 했는지의 여부로 S_j를 인증한다.

Req2 : 위치추적(Location Tracking Attack) 방지

위치추적공격은 공격자가 센서노드의 위치변화를 감지하고 센서노드의 이동경로를 파악하여 사용자의 프라이버시를 침해하는 공격으로 센서노드로부터 매 세션마다 동일한 정보가 나오는 무선센서 시스템은 위치추적이 가능하다. 랜덤한 센서노드를 두고 이들을 구별해 낼 수 없으면 불구분성(indistinguishability)을 만족하며 센서노드의 위치 프라이버시를 보장받을 수 있다[11]. D. He 스킴은 제 3.2절에서 $M_1 = (ID_i, C_i, T_i)$과 $M_2 = (ID_i, C_g, T_g)$ 메시지에서 ID_i를 비보호 채널에 공개함으로써 신원을 노출할 뿐 아니라 위치추적에 취약함을 보였다. 제안 프로토콜에서는 사전 등록된 정보 $m = h(ID_i \| x) \oplus h(pw_i) \oplus h(B_i)$을 U_i와 게이트웨이가 비밀키 R을 생성할 수 있다. U_i와 게이트웨이 간의 송수신은 암호화(6 : $C_1 = E_R[ru \| ID_i \| SID_j^0]$)되어 정당한 사용자가 아니면 사용자 식별이 되지 않으며 매 세션마다 무작위로 변경되는 URSC 코드와 가변식별자에 의해 계산된 값이 계속해서 바뀌게 된다. 그러므로 이전 세션과 항상 다른 값을 전송하며 GW-node는 메시지 a를 브로드캐스트하므로 공격자는 특정한 센서노드를 식별할 수 없으므로 위치추적에 안전하다.

Req3. 익명성(Anonymity) 유지

익명성이란 사용자나 GW-node, 센서노드 자신의 식별자를 드러내지 않고 서비스나 리소스를 사용하는 것을 말한다[12]. 센서노드 장치들 간의 정보 누출은 노드의 ID 및 위치정보의 노출을 가능하게 한다. 제3자는 로그인 단계에서 사용자가 GW-node로 전송하는 메시지 C_0, C_1를 도청한다 해도 C_0로부터 R을 유추해야 하며 R에서는 I와 ru를 유추해내야 한다. 그러나 GW-node의 비밀키 x를 소유한 개체만이 유추할 수 있다. GW-node와 S_j간의 전송정보 a, b에서 모두는 해시값으로 a에는 URSC의 무작위 수와 S_j의 식별자, GW-node와 S_j의 해시값인 공유비밀정보 $h(SID_j^0 \| y)$가 포함되어 있다. b의 값 또한 GW-node의 식별자와 URSC의 다음코드로 된 해시값으로 합법적인 GW-node와 S_j외에는 계산할 수 없다.

Req4 : 재전송공격(Replay Attack)방지

데이터 신선성(Freshness)은 이전에 전송되었던 데이터가 재전송되는 것을 방지하는 기술로써 현재 통신 상대가 보낸 데이터임을 보장하는 보안 서비스로 Ui와 GW-node간에 제3자가 re-

play공격을 시도할 경우, 전송메시지 C_0와 C_1에는 각 세션마다 생성되는 무작위 난수 ru가 포함되어 있으며 GW-node와 S_i간에는 매 전송시마다 수신노드에 해당하는 순차코드 내에서 무작위로 질의 코드를 바꾸기 때문에 공격자는 응답메시지에 포함되어야 하는 다음의 응답코드 $URSC_{i+1}$를 쉽게 추측할 수 없다. 그러므로 이러한 질의-응답 코드 순서쌍이 메시지의 freshness를 제공한다. 메시지 인증에 필요한 필드를 N비트 사용해도 네트워크 성능에 영향을 미치지 않는다. $p \leq 2^N$을 만족하는 p와 L을 선택하여 L개의 순차코드를 인증에 사용할 경우 공격자가 응답메시지의 인증을 맞출 확률이 $1/2^N$이 된다. 제3자가 replay공격을 시도할 경우 GW-node에서 매 전송 시마다 센서노드에 해당하는 순차코드 내에서 무작위로 질의코드를 바꾸기 때문에 공격자는 응답코드를 쉽게 추측할 수 없으며 $1-1/2^N$의 보안성이 보장된다.

Req5 : 위장공격(Forgery Attack)방지

무선센서 네트워크 환경에서 노드간에 통신되는 메시지가 평문으로 전달되면 메시지의 위조와 변조가 가능하게 되어 공격의 대상이 된다. 제 3.1절의 생체정보와 패스워드 유추에 의한 취약성은 D. He 스킴이 위장공격(제 3.3절)에 취약함을 의미한다. 본 제안에서는 등록단계에서 사용자는 $h(pw_i)$를 사용하므로 서버의 내부자는 사용자의 패스워드를 알 수 없으며 사용자 자신이 합법적 공격자로 위장하기 위해서는 GW-node의 비밀난수 x를 구할 수 있어야 하는데 GW-node에서 제공한 m과 I로부터 $m = h(ID_i \| x) \oplus h(pw_i) \oplus h(B_i)$, $I = g^{h(IDi \| x) \oplus h(Bi)} \cdot x^{h(x)} \bmod p$를 얻을 수 없다는 안전성이 있다. 이로 인하여 공격자가 C_0의 값을 가로채더라도 비밀키 R을 찾아낼 수 없다. 공격자가 정당한 사용자로 위장하기 위해서는 로그인 단계에서 전송 메시지인 C_0, C_1이 상호인증을 위한 전송정보인 a, b, C_2를 계산할 수 있어야 한다. 따라서 제안 기법에서는 제3자는 서버나 사용자로 위장하기 위해서 필요한 비밀 값들을 구할 수 없으므로 공격자의 위장공격에 안전하다.

Req6 : 도청공격(Eavesdropping Attack)에 의한 Man-in-the middle Attack 방지

도청공격은 유선구간인 U_i와 GW-node, 무선통신구간인 센서노드와 GW-node 사이에 송수신되는 내용을 도청하여 센서노드에 대한 정보를 알아내는 공격이다. 도청공격이 성공하기 위해서는 사용자의 pw_i와 GW-node의 비밀키 x를 알아내야 한다. 두 가지의 경우를 가정해 볼 수 있다. 제3자는 GW-node의 비밀키 x와 사용자의 pw_i를 알아내야 하는데 정당한 사용자가 다른 정당한 사용자를 공격할 경우는 자신의 스마트카드에 내장된 $m = h(ID_i \| x) \oplus h(pw_i) \oplus h(B_i)$에서 GW-node의 비밀키 x를 계산하는 것은 시간이 걸려도 off-line으로 가능하다. $h(ID_i \| x) \oplus h(pw_i) \oplus h(B_i)$에서 x는 n bit로 가정하고 사전파일을 만들어 $2^n!$ 반복, 대입하여 m과 일치하는 값을 찾는다. 비밀키 x를 유추한다 하더라도 다른 사용자의 pw_i, B_i를 추측하여야 한다. 물론 off-line으로 $2^n!$ 반복하면 가능하나 문제는 pw_i를 3회 입력하여 초과하면 패스워드 사용이 거절된다. pw_i의 길이가 32bit라고 가정하면 pw_i를 맞출 확률이 $(1/2^{32})/3$으로 매우 낮다. URSC는 무작위로 선택한 코드를 해시 값으로 변경했으므로 검색이 불가능하며 이로 인해 URSC와 가변식별자로 생성된 a와 b를 도출해 낼 수 없으며 따라서 제안한

프로토콜은 도청이 이루어져도 알 수 있는 정보가 없으므로 공격에 안전하다. 중간자공격은 불법적인 제3자가 Ui와 GW-node, 센서노드와 GW-node의 통신에 참여하여 두 개체를 속여 인증을 통과하거나 비밀정보를 획득하여 잘못된 정보(변조, 위조)를 전송하는 공격이다.

중간자에 의한 변조공격이 성공하기 위해서는 도청공격이 성공해야 하는데 전체구간에서 도청 이후 알아낼 수 있는 정보는 정보생성의 원천이 다르기 때문에 도청을 해도 정보를 알아낼 수가 없다는데 있다.

Req7 : 전송실패 최소화

무선환경에서는 메시지의 분실이 발생할 우려가 있다. 이 경우 각 센서노드의 식별자는 계속 변화하며 게이트웨이에 저장된 센서노드의 식별자도 변경되어 저장된다. 그러나 전송실패 등의 이유로 어느 한쪽 노드의 식별자 값이 다를 경우 식별자의 동기화가 필요하다. 게이트웨이는 저장된 센서노드의 다음식별자와 비교하여 일치여부를 판단($SID_j^{q+1}{}_{(GW)} = ?SID_j^{q+1}{}_{(SN)}$)하여 일치하지 않으면 센서노드의 값을 최소 G를 통해 k번 생성하여 동일 값이 있는지 확인한다. 동일한 값이 있으면 저장된 센서노드의 다음식별자($SID_j^{q+1}{}_{(GW)}$)와 업그레이드 한다. 센서노드로부터 GW-node로 메시지가 전송되지 않을 경우가 발생하게 된다면 이때 메시지가 전달되지 않을 확률을 p라 하고 전송할 때마다 전송에 실패할 확률이 독립적이라고 가정하자. k번 연속으로 전송에 실패할 확률은 p^k가 된다. 만약 전송실패 확률이 1/2일 경우 p가 1/2이고 저장하고 있는 식별자의 개수가 5, 즉 k가 5이면 전송 실패확률이 $(1/2)^5 = 1/32 \approx 0.031$이므로 매우 낮은 확률을 갖는다. 이와 같이 전송실패확률이 낮고 k값이 크다면 k번 연속 전송실패확률은 매우 낮게 된다. 따라서 식별자의 값이 일치하지 않을 경우에도 적은 횟수의 G연산으로 인증확률을 높일 수 있다.

Req8 : 패턴과 동기화

URSC코드는 각 코드간의 거리(distance)가 랜덤하게 정해지므로 공격자가 코드패턴을 쉽게 알 수 없다. 적어도 L(코드 길이)번 만큼 메시지 전달을 엿들어야만 코드 전체 패턴을 알 수 있는데 이것마저 해시값으로 되어 있어서 알 수 없다. 또한 GW-node와 S_i간에 동기화의 필요가 없다. GW-node는 수신노드에 해당하는 순차코드 하나를 임의로 골라서 질의코드로 사용하고 노드는 질의 코드에 대한 유일한 응답코드를 전송하면 되므로 주고받는 코드에 대해 동기화를 맞출 필요가 없다.

Req9 : 사용자의 패스워드 선택과 갱신

등록단계에서 패스워드는 서버에 의해 지정되지 않고 사용자에 의해 자유롭게 선택되고 변경될 수 있으며 패스워드는 등록할 때 $h(pw_i)$로 보호되어 서버의 관리자는 알 수 없다.

Req10 : 스마트카드 도난 및 분실로부터 보호

D. He scheme에서 스마트카드 분실 혹은 도난당했을 때[8]에 의해 생체정보인 B_i의 노출과 패스워드 추측공격에 의해 사용자와 S_j의 위장공격에 취약함을 알 수 있다. 본 스킴에서는 스마트카드에 저장된 정보는 {m, I, h(), p, g, d(・), τ}로 생체정보 B_i를 스마트카드 내에 저장하지 않기 때문에 스마트카드 도난 시 로그인 단계에서 $(d(B_i, B_i^*) < \tau)$을 통과할 수 없다. [step 1]에서 패스워드 추측을 방지하기 위해 패스워드 입력제한을 3회로 설정

〈Table 1〉 Performance Comparisons Among Different Schemes

	Req1	Req2	Req3	Req4	Req5	Req6	Req7	Req8	Req9	Req10
Yoon et al. scheme	yes	no	no	yes	no	yes	no	no	x	no
Debiao He scheme	yes	no	no	yes	yes	yes	no	no	yes	no
Proposed scheme	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

〈Table 2〉 A Comparison of Computation Costs

Computational Type	Yoon[15] scheme	Debiao He[1] scheme	Proposed scheme
User	3Th	$4Th + 1T_{sym} \approx 4Th$	$1Th + 2_{sym} \approx 3Th + 2T_{exp} + 3T_{mod}$
GW-node	4Th	$3Th + 2T_{sym} \approx 5Th$	$3Th + 1_{sym} \approx 4Th + 1T_{exp} + 2T_{mod}$
Sensor node	3Th	$2Th + 1T_{sym} \approx 3Th$	3Th

한다. 또한 K는 스마트카드에 포함되어 있지 않으므로 공격자는 스마트카드를 훔치더라고 패스워드 인증단계에서 승인이 될 수 없어서 사용할 수 없다.

6. 비 교

제 5장의 보안성분석 및 평가를 기준으로 제안된 스킴과 Yoon et al.[15]과 He[1]스킴과의 차이점에 대해 다음과 같이 <Table 1>에 비교하였다.

Req1. 노드간 상호인증; Req2. 위치추적 방지(가변식별자); Req3. 익명성 유지(가변식별자); Req4. 재전송공격방지; Req5. 위장공격방지; Req6. 중간자공격 방지, 도청공격(Eavesdropping Attack) 방지; Req7. 전송실패 최소화; Req8. 패턴과 동기화; Req9. 사용자의 패스워드선택 및 갱신; Req10. 스마트카드 도난 및 분실로부터 보호.

<Table 1>에서 req1~req10을 만족시키면 yes, 그렇지 않으면 no, 해당되지 않음은 x로 표기하였다.

Yoon et al.[15]과 He[1]스킴과 비교해 볼 때 가장 큰 차이점은 각 노드 상호간에 인증스킴을 개선하였고 사용자 ID의 암호화와 가변식별자, URSC 순차코드를 이용하기 때문에 익명성이 보장되고 이로 인해 위치추적이 어렵도록 개선되었다. 또한 URSC의 질의-응답코드로 인하여 동기화 절차가 불필요하며 스마트카드 도난 또는 분실했을 때 패스워드 검증절차를 통해서 안전하다. <Table 2>에서는 연산량을 비교하였으며 표기는 다음과 같다. 해시함수 연산은 Th로 표기하며 대칭키 암호화 및 복호화는 T_{sys}로, 지수연산과 모듈러연산은 T_{exp}과 T_{mod}로 표기하였다.

<Table 2>에서 제안된 스킴의 연산효율은 사용자, GW-node, 센서노드가 각각 $3Th + 2T_{exp} + 3T_{mod}$, $4Th + 1T_{exp} + 2T_{mod}$, 3Th로 해시연산과 대칭키 암호 연산은 동등한 연산효율

을 갖는다. 익명성보장을 위해 모듈에 추가한 지수연산과 모듈러 연산은 자원의 제약을 받는 센서노드에서 연산되지 않으므로 센서노드 측면에서 볼 때 D. He scheme과 Yoon et al. 스킴과 비교해 더욱 경량화 되었다.

7. 결 론

무선센서 네트워크는 노드간의 계산능력의 제한과 저장장치의 제한, 전력장치의 소형화가 강조되므로 인증방법의 경량화와 같은 기존 무선센서 인증방법과는 다른 접근이 필요하다.

본 논문에서는 첫째, GW-node와 S_i간에는 He[1] 스킴과 다르게 암호알고리즘을 사용하지 않고 가변식별자와 URSC 순차코드를 사용하여 매 세션마다 GW-node와의 송수신과정에서 전달되는 값이 달라지도록 하여 위치추적공격, 재전송공격 등에 대해 저항성을 가지며 노드의 익명성이 보장되는 프로토콜을 제안하였다.

둘째, 이전에 전송 되었던 데이터가 재전송되는 것을 막기 위해 URSC, 가변식별자를 이용하여 타임스탬을 대신하여 동기화된 도전-응답 메시지로 강한 신선성(Freshness)을 제공하고 있다.

셋째, 최소한의 압축된 전송메시지(C_0, C_1, C_2, a, b)는 제3자에 의한 센서노드들의 메시지 경로를 알아내지 못하며 악의적인 메시지 차단이나 통신의 문제로 두 개체사이에서 정보 불일치를 유도하는 공격에도 효율적이다.

넷째, 패스워드 검증기능을 추가하여 D. He 스킴에서 생체정보 B_i와 패스워드의 취약성을 보완하였으며 모듈러연산을 통해 비도를 향상시켰다.

다섯째, 무선 네트워크의 성능에 영향을 미치지 않고 기밀성을 제공함으로써 여러 공격 가능성을 줄일 수 있다.

따라서 본 논문에서 제시한 가변식별자를 사용한 익명성 보장의 인증기법은 무선 경비 시스템에 적용할 경우 나타날 수 있는 정보보안상의 취약점을 방지하고 향후 무인 탐지식별기능의 인증프로토콜로 여러 응용분야에 적용할 수 있다.

References

[1] He, D., “Robust biometric-based user authentication scheme for wireless sensor networks,” IACR Cryptology ePrint Archive 2012, Vol. 203, pp. 1-15, 2012.

[2] Hwang, L. C. M., “An efficient biometric-based remote authentication scheme using smart cards,” Journal of Network and Computer Applications, Vol. 33, pp. 1-5, 2010,

[3] Kim, T., Wang, K., and Cho, K., “A Secure Key Agreement Scheme in Low-energy Wireless Sensor Network,” Lecture Notes in Computer Science 4096 (EUC 2006), pp. 78-88, 2006.

[4] Kim, J., Lee, C. K., Seo, S. W., and Lee, B., “Frequency-hopping Optical Orthogonal Codes with Arbitrary Time-blank Pattern,” Applied Optics, Vol. 41, No. 20, pp. 4070-4077, 2002.

[5] Liao, I. E., Lee, C. C., and Hwang, M. S., A Password Authentication Scheme over insecure networks, Vol. 72, pp. 727-740, 2006.

[6] Manabu, Inuma, Akira Otsuka., Hideki Imai, Theoretical framework for constructing matching algorithms in biometric authentication systems, In proc. of ICB 2009, LNCS 5558, pp. 806-815, 2009.

[7] Mehta, K., Liu., D., and Wright, M., "Location Privacy in Sensor Network Against A Global Eavesdropper," in Proc. on IEEE Conference on Network Protocols (ICNP 2007), 2007.

[8] Messerges, T. S., Dabbish, E. A., and Sloan, R. H., Examining smart card security under the threat of power analysis attacks. IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, 2002.

[9] NIST, Secure hash standard, Technical report FIPS 180-1, NIST, US Department of Commerce, April 1995.

[10] Ouyang, Y., Le, Z., Xu, Y., Triandopoulos, N., Zhang, S., Ford, J., and Makedon, F., "Providing Anonymity in Wireless Sensor Network," in Proc. on 10th Conference on Parallel and Distributed Systems(ICPADS 2007), pp. 7-9, July, 2007.

[11] Shin, K. C., "A Study on Lightweight Efficient Key Agreement Mutual Authentication Protocol in Wireless Sensor Environment," Korea Institute of Information Technology, Vol. 10, No. 11, pp. 49-62, 2012.

[12] Shin, K. C., "A Robust and Secure remote User Authentication Scheme Preserving User Anonymity," Society for e-Business Studies(www.calsec.or.kr), Vol. 18, No. 2, pp. 81-93, 2013.(dx.doi.org/10.7838/jsebs.2013.18.2.081).

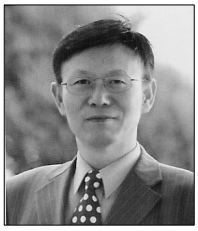
[13] Vaidya, B., Rodrigues, J. J. P. C., and Park, J. H., "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," International Journal Communications Systems, Vol. 23, pp. 1201-1222, 2010.

[14] Yoon, E. J. and Yoo, K. Y., "Comments on He et al.'s robust biometric-based user authentication scheme for WSNs," World Academy of Science, Engineering and Technology, Vol. 68, pp. 52-55, 2012.

[15] Yoon, E. and Yoo, K., A New Biometricbased User Authentication Scheme without using Password for Wireless Sensor Networks, 2011 20th IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises, pp. 279-284, 2011.

[16] Yuan, J., Jiang, C., and Jiang, Z., "A Biometric-based user authentication for wireless sensor networks," Wuhan University Journal of Natural Sciences, Vol. 15, No. 3, pp. 272-276, 2010.

저 자 소 개



Shin Kwang Cheul (E-mail : skcskc12@hanmail.net)

1985	Seoul National University of Science and Technology Computer Science
1990	Korea National Defense University Computer Science
2003	Sungkyunkwan University Dept. Information Engineering
2004~Current	Sungkyul University, Division of Industrial Management Engineering
Interest Field	Smart card security, E-Payment System, Network and RFID security