디지털산업정보학회 논문지 제15권 제4호-2019년 12월
http://dx.doi.org/10.17662/ksdim.2019.15.4.071

무선 센서 네트워크 환경을 위한 보안성이 향상된 프라이버시 보호형 two-factor 인증 프로토콜

최 윤 성* · 장 범 환**

Security enhanced privacy-aware two-factor authentication protocol for wireless sensor networks

Choi Younsung · Chang Beom-Hwan

〈Abstract〉

Various researchers conducted the research on two-factor authentication suitable for wireless sensor networks (WSNs) after Das first proposed two-factor authentication combining the smart card and password. After then, To improve the security of user authentication, elliptic curve cryptography(ECC)-based authentication protocols have been proposed. Jiang et al. proposed a privacy-aware two-factor authentication protocol based on ECC for WSM for resolving various problems of ECC-based authentication protocols. However, Jiang et al.'s protocol has the vulnerabilities on a lack of mutual authentication, a risk of SID modification and a lack of sensor anonymity, and user's ID exposed on sensor node Therefore, this paper proposed security enhanced privacy-aware two-factor authentication protocol for wireless sensor networks to solve the problem of Jiang et al.'s protocol, and security analysis was conducted for the proposed protocol.

Key Words : Two-Factor Authentication, Security Analysis, Wireless Sensor Networks

Ⅰ. 서론

무선 센서 네트워크 (WSNs)은 다양한 환경에서 실시간 모니터링을 수행할 수 있으며, 화산의 활동 감지 및 유해 가스 검출과 같이 사람이 접근하기 어려운 환경에도 네트워크 센서를 배치하여 정보를 수집할 수 있다.

무선 네트워크 환경에서 사용되는 게이트 노드는 CPU와 메모리와 같은 컴퓨팅 능력이 뛰어나고 전력 공급이 안정적인 반면에, 센서 노드의 경우에는 파워, 컴퓨팅 능력, 저장공간 등 대부분의 자원이 한정적이다. 실질적으로 다양한 정보를 수집하는 센서의 상황을 고려해보면, 사용자 인증 프로토콜을 구상할 때 컴퓨팅 능력 및계산 비용의 측면에서 효율적이어야 한다[1-3].

* 호원대학교 컴퓨터학부 사이버보안전공 조교수
** 호원대학교 컴퓨터학부 사이버보안전공 부교수
Corresponding Author : Beom-Hwan Chang (bchang@howon.ac.kr)

2009년에 DAS가 무선 네트워크 환경에서 사용하기 위해 스마트 카드와 패스워드를 활용한 Two-Factor 인증 프로토콜을 제안하였다[4]. 그 이후, Yeh 등은 Chen 등이 제안한 elliptic curve cryptography (ECC) 기반 사용자 인증 프로토콜이 내부자 공격과 패스워드 업데이트 공격에 취약하다는 것을 알아내고 이를 해결할 수 있는 프로토콜을 제안하였다. 하지만, Yeh 등이 제안한 프로토콜이 사용자와 센서 간의 상호인증을 제공하지 않는 다는 것을 Shi 등이 밝혀내고 ECC 기반의 인증 프로토콜을 제안하였다. 하지만, Choi 등은 Shi 등이 제안한 프로토콜이 unknown key share, stolen smart card, and sensor energy exhausting attack 등에 취약하다는 것을 알아내고 보다 안전한 프로토콜을 제안하였으나, Jiang 등은 Choi 등의 프로토콜이 익명성과 추적불가성을 제공하지 못한다는 것을 알아냈다. 그리고 Jiang 등을 프라이버시를 향상시킨 인증 프로토콜을 제안하였다. 본 논문에서는 Jiang 등이 제안한 프로토콜이 상호인증 및 센서 익명성 및 ID 익명성을 적절히 제공하지 못한다는 것과 SID 변조 공격에 취약하다는 점을 제시하고 이를 해결하기 위한 인증 프로토콜을 제공하고자 한다[5-11].

본 논문의 구성은 다음과 같다. 먼저 2장에서 Jiang 등이 제안한 프로토콜의 동작과정을 분석한 후, 3장에서는 Jiang 등의 프로토콜의 취약점 분석을 하고 4장에서는 이러한 문제를 해결하기 위해 본 논문에서 제안하는 인증 프로토콜의 동작과정을 설명한다. 그리고 5장에서 제안한 프로토콜의 안전성을 분석하여 Jiang 등이 제안한 프로토콜에서 발견되었던 보안상의 취약점이 해결되었다는 것을 증명하고 추가적인 안전성 분석을 진행한다. 6장 결론에서 본 논문의 결론을 짓는다.

II. Jiang 등의 인증 프로토콜 분석

2.1 등록 과정

본 논문에서 사용한 용어정보는 <표 1>과 같다. 사용자의 등록과정은 다음과 같다.

<표 1> 용어에 대한 설명

용어	설명
U_i	사용자
S_j	센서 노드
$H(\cdot)$	해쉬 함수
PW_i	사용자 i 의 패스워드
SK_{ij}	공유 세션키
DID_i, DID_{GWN}	사용자와 게이트웨이 노드의 동적 ID
TE_i	제한 시간
||	연접 연산자
GWN	게이트웨이 노드
SID_j	센서 노드의 ID
ID_i	사용자 ID
TS	타임 스탬프 정보
PTC_i	사용자 i의 보호받는 임시 자격 증명
TC_i, TC_j	사용자 i와 서버 j의 임시 자격 증명
$K_{GWN\text{-}U}$, $K_{GWN\text{-}S}$	게이트웨이 노드가 소유한 마스터 키

본격적인 인증과정 전에 GWN은 타원 곡선에서 유한 필드 F_p에 대해 큰 소수 n을 갖는 점 P에 의해 생성된 유한 순환 그룹 G를 선택한다. 이때 타원 곡선 방정식은 유한 소수체 F_p 상에서 $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod p$, $b \in F_p$, $4a^3 + 27b^2 \neq 0 \pmod p$)로 정의된다. 그리고 다음 GWN은 임의의 숫자 x를 개인 키로 임의로 선택하고 해당 공개 키 $y = xP$를 계산하고 두 개의 마스터 비밀 키 $K_{GWN\text{-}U}$ 및 $K_{GWN\text{-}S}$를 생성한다. 그 후 GWN은 x를 저장하고 시스템 매개변수 { $E(F_p)$, G, P, y }를 생성한 후 등록과정을 시작한다[2, 12].

(R1-U) 용자 U_i 가 GWN 에 등록하기 위해서, U_i 는 자신의 ID_i 와 PW_i 를 설정하고 랜덤한 숫자 r_i를 선택한다. 그리고 U_i 는 $HPW_i = H(PW_i || ID_i || r_i)$를 계산하고 게이트웨이 노드 GWN 에게 { ID_i, HPW_i }를 전송한다.

(R2-U) GWN 는 ID_i의 적법성을 검사하고 $TC_i = H(K_{GWN\text{-}U} || ID_i || T_{Ei})$ 와 $PTC_i = TC_i \oplus HPW_i$를 계산한다. GWN은 (ID_i, TE_i)을 검증테이블에 저장한다. 그리고 GWN는 $\{H(\cdot), y, TE_i, PTC_i\}$가 저장된 카드를 U_i 에게 전달한다.

(R3-U) U_i 는 $HPW'_i = H(h(ID_i || PW_i || r_i) \bmod m)$를 계산하며, 이때 m은 $28 \le m \le 216$ 의 사이 값이다. < ID_i , PW_i >은 오프라인 패스워드 공격을 막기 위한 것이며, 사용자는 r_i 와 HPW_i 를 스마트 카드에 저장한다.

센서 노드의 등록과정은 다음과 같다.

(R1-S) 센서 노드 S_j는 자신의 ID_i인 SID_j을 GWN 에게 비밀채널을 통해서 전달한다.

(R2-S) GWN 는 $TC_j = H(K_{GWN\text{-}S} || SID_j)$를 계산하여 센서노드 S_j 에게 { TC_j }를 전송한다.

(R3-S) 이후 센서 노드 S_j 는 TC_j 를 저정해둔다.

2.2 로그인 과정

(L1) U_i 가 S_j 에 접속하고자 할때 , U_i 는 스마트카드를 터미널에 넣고 ID_i, PW_i를 입력한다.

(L2) 스마트 카드는 $HPW'_i = H(H(ID_i || PW_i || r_i) \bmod m)$ 를 계산하고 HPW^*_i ? = HPW'_i 인지 확인한다. 같이 같으면 $TC_i = PTC_i \oplus H(PW_i || ID_i || r_i)$ 를 계산한다.

2.3 인증 과정

(A1) U_i 는 랜덤수 $a \in Z^*p\text{-}1$를 선택하고 $A_i = aP$, $D_i = ay = axP$, $DID_i = ID_i \oplus H(A_i || D_i)$, $C_i = H(ID_i || TS_1 || D_i || A_i || TC_i)$을 계산하며 이때 TS_1 는 현재의 타임 스탬프이다. 그리고 마지막으로 사용자 U_i 는 DID_i, A_i, TS_1, C_i }를 GWN 에게 전달한다.

(A2) GWN은 U_i에게 메시지 { DID_i, A_i, TS_1, C_i }를 받은 후, GWN 는 TS_1의 검증하고 조건을 만족하며, GWN 는 $D_i = xA = xaP$, $ID_i = DID_i \oplus H(A_i || D_i)$, $TC_i = H(K_{GWN\text{-}U} || ID_i || TE_i)$를 계산한다. 그리고 $H(ID_i || TS_1 || D_i || A_i || TC_i)$를 계산하여 C_i 값과 비교한다. 두 값이 같으면, GWN 는 센서노드 S_j 를 고르고, $TC_j = H(K_{GWN\text{-}S} || SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i || TC_j || TS_5)$, $C_{GWN} = H(ID_i || TC_j || A_i || TS_2)$를 계산한다.이때 $TS2$는 최신 타임스탬프이이며, GWN 는 { TS_2 , DID_i , DID_{GWN} , C_{GWN} , A_i} 를 S_j 에게 전달한다.

(A3) { TS_2 , DID_i, DID_{GWN} , C_{GWN} , A_i }를 받은 후 S_j 는 TS_2 를 체크한다. TS_2 값이 최신 값이면, S_j는 $ID_i = DID_{GWN} \oplus H(DID_i || TC_j || TS_2)$를 계산하여 $H(ID_i || TC_j || A_i || TS_2)$ 값과 C_{GWN} 이 동일한지 검증한다. 값이 같으며 S_j 는 랜덤값 $b \in Z^*P\text{-}1$를 생성하고, $B_j = bP$, $SK_{ij} = H(bA_i) = H(abP)$, $C_j = H(TC_j || ID_i || SID_j || B_j || TS_3)$을 계산한다. 이때 TS_3 는 최신 타임스탬프이며 S_j 는 GWN 에게 { SID_j, TS_3, C_j, B_j }를 전달한다.

(A4) GWN 은 TS_3 의 최신성을 검증한 후, $H(TC_j || ID_i || SID_j || B_j || TS_3)$를 계산하고 C_j 값이 같은지 확인한다. 값이 같으면, GWN 는 S_j 를 인증하게 된다. 그리고 GWN 는 $E_{GWN} = H(ID_i || TC_i || D_i || B_j || TS_4)$를 계산한다. TS_4 는 최신 타임스탬프이며 GWN 은 { SID_j, TS_4, B_j, E_{GWN} }을 사용자 U_i에게 전달한다.

(A5) U_i 는 TS_4 의 최신성을 확인하고 $H(ID_i || TC_i || D_i || B_j || TS_4)$를 계산한 후 E_{GWN} 와 같은지 확인한다. 같으면 U_i는 S_j와 GWN 를 인증하게 된다. 끝으로 U_i 는 공유 세션키 $SK_{ij} = H(aB_j) = H(abP)$ 를 계산한다.

User U_i | GWN | Sensor node S_j

$\langle ID_i, PW_i \rangle$ | $\langle K_{GWN-U}, K_{GWN-S} \rangle$ | $\langle TC_j \rangle$

inputs ID_i and PW_i ;
$TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$;
Generates $a \in Z^*_{P-1}$;
$A_i = aP$;
$D_i = ay = axP$;
$DID_i = ID_i \oplus H(A_i \| D_i)$;
$C_i = H(ID_i \| TS_1 \| D_i \| A_i \| TC_i)$;

$M_1 = \langle DID_i, A_i, TS_1, C_i \rangle$ →

Check TS_1 ;
$D_i = xA = xaP$;
$ID_i = DID_i \oplus H(A_i \| D_i)$;
Check ID_i and Retrieve TE_i ;
$TC_i = H(K_{GWN-U} \| ID_i) \| TE_i)$;
Check $H(ID_i \| TS_1 \| D_i \| A_i \| TS_2)$;
$TC_j = H(K_{GWN-S} \| SID_j)$;
$DID_{GWN} = ID_i \oplus H(DID_i \| TC_j \| TS_2)$;
$C_{GWN} = H(ID_i \| TC_j \| A_i \| TS_2)$;

$M_2 = \langle TS_2, DID_i, DID_{GWN}, C_{GWN}, A_i \rangle$ →

Checks TS_2 ;
$ID_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_2)$;
Check $C_{GWN} \stackrel{?}{=} H(ID_i \| TC_j \| A_i \| TS_2)$;
Generate $b \in Z^*_{P-1}$;
$B_j = bP$;
$SK_{ij} = H(bA_i) = H(abP)$;
$C_j = H(TC_j \| ID_i \| SID_j \| B_j \| TS_3)$

$M_3 = \langle SID_j, TS_3, C_j, B_j \rangle$ ←

Checks TS_3;
Check $C_j \stackrel{?}{=} H(TC_j \| ID_i \| SID_j \| B_j \| TS_3)$;
$E_{GWN} = H(ID_i \| TC_i \| D_i \| B_j \| TS_4)$;

$M_4 = \langle SID_j, TS_4, B_j, E_{GWN} \rangle$ ←

Check TS_4 ;
Check $E_{GWN} \stackrel{?}{=} H(ID_i \| TC_i \| D_i \| B_j \| TS_4)$;
$SK_{ij} = H(aB_j) = H(abP)$;

<그림 1> Jiang 등이 제안하는 인증 프로토콜

2.4 패스워드 변경 과정

(PC1) U_i 가 패스워드를 변경하고자 할 때 자신의 스마트 카드를 넣고 ID_i와 PW_i를 입력한다.

(PC2) 스마트카드는 $HPW^*_i = H(h(ID_i || PW_i || r_i)$ mod m을 계산하여 저장되어 있는 HPW'_i 와 비교한다. 값이 같으면, U_i 는 새로운 패스워드를 입력하고 $PTC_i = TC_i \oplus RPW_i \oplus H(r || PW_i)$ 계산하고 PTC_i를 PTC_i로 대체한다.

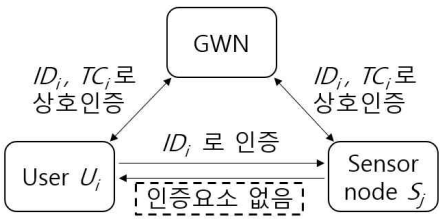
III. Jiang 등의 프로토콜의 취약성 분석

이번 장에서는 Jiang 등이 제안한 프로토콜에 취약점 분석을 진행하여 상호인증 및 센서 익명성 및 ID 익명성을 적절히 제공하지 못한다는 것과 SID 변조

공격에 취약하다는 것을 알아내고자 한다.

3.1 상호인증 미충족

상호인증이란 2 혹은 3 구성요소들이 서로 인증을 하는 것을 뜻한다. 사용자, 게이트웨이 노드 및 센서 노드들은 각각의 ID를 이용하고 있다. 사용자와 게이트웨이 노드 간에는 ID_i 와 TC_i 를 이용하여 상호간의 인증을 하고 있으며, 게이트웨이 노드와 센서 노드는 TC_j and C_{GWN} 를 이용하여 인증을 제공한다. 하지만 사용자와 센서 노드 간에는 상호 인증을 하지 않는다. 센서는 게이트웨이 노드를 중개자로 하여 사용자를 인증하고 있지만, 사용자는 센서노드에 대한 인증을 제공하지 못한다. 그래서 사용자는 센서 노드가 전송해오는 SID_j 값이 정상적인 값인지를 확인할 수 없는 문제가 있다.



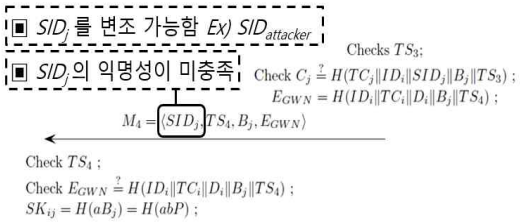
<그림 2> Jiang 등의 프로토콜의 상호인증 미충족

3.2 SID 변조 공격

사용자는 게이트웨이로부터{ SID_j, TS_4, B_j, E_{GWN} }를 전송받아 메시지의 정확성과 최신성을 확인하고 있다. 하지만 SID_j 이외에 메시지 TS_4, B_j, E_{GWN} 에는 SID_j 에 대한 정보가 없어서, 공격자가 SID_j 값을 변조하더라도 사용자가 알아낼 수가 없게 된다. 예를 들어, 공격자가 { SID_j, TS_4, B_j, E_{GWN} }에 있는 SID_j를 공격자의 $SID_{attacker}$로 변경하더라도 사용자는 변화를 확인할 수 없다. 그래서 사용자는 SK_{ij}를 계산하더라도 정상적인 센서 노드와 추가적인 통신을 할 수 가 없다. 사용자가 생성한 세션키 SK_{ij} 는 $SID_{attacker}$ 와의 통신을 위한 것이기 때문이다. 그래서 센서 노드 SID_j 가 추후에 사용자에게 통신을 하고자 하더라도 센서의 ID 와 센서 공유키는 간에는 연간관계가 없기 때문에 센서 노드가 특정이 되지 않아서 정상적인 암호 통신을 진행할 수 없게 된다.

3.3 센서 익명성 미충족

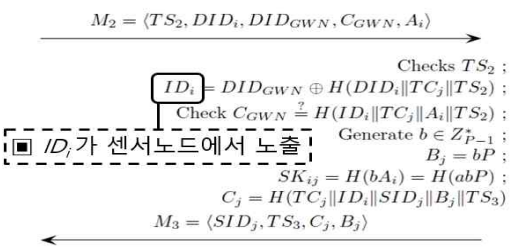
익명성은 프로토콜에서 효과적인 보안기능으로 로그인 및 인증과정에서 사용된다. Jiang 등이 제안한 인증 프로토콜에서는 사용자의 익명성을 보호하기 위해서 동적 ID인 DID_i를 사용한다. 그리고 이 프로토콜은 게이트웨이 노드의 ID를 보호하기 위해서 DID_{GWN}를 사용하고 있으나 센서 노드의 ID 를 위한 익명성 보장기법은 제공하지 않고 있다. 그래서 본 프로토콜에서는 센서 노드가 사용자와 통신을 하는 경우 공격자는 통신 중인 센서 노드를 특정할 수 있다. 더욱이 공격자는 센서 노드의 SID_j를 쉽게 할 수 있기 때문에, 센서 노드의 ID 를 활용하여 다양한 공격을 시도할 수 있게 된다. 그러므로 이러한 센서 노드의 ID 의 오남용을 막기 위해서, 프로토콜 설계과정에서 SID_j의 익명성을 보호하는 기능을 제공하여야 한다.



<그림 3> SID 변조 공격과 센서 익명성 미충족

3.4 센서노드 상의 사용자 ID 노출

Jiang 등의 인증 프로토콜에서 사용자는 익명성을 보장하기 위해서 DID_i를 이용하고 있다. 그래서 공격자는 DID_i로부터 ID_i를 계산해 낼 수 없다. 그것은 공격자가 $DID_i = ID_i \oplus H(A_i || D_i)$ 중에서 $H(A_i || D_i)$ 값을 알 수 없기 때문이다. 하지만 본 프로토콜에서는 공격자가 센서 노드에 접근하게 되면 사용자의 ID_i 를 알아낼 수 있다는 문제가 발생하는데, 이를 통해 공격자는 특정한 센서 노드의 위치를 추적할 수 있게 된다. 공격자가 센서 노드에 접근하여 $ID_i = DID_{GWN} \oplus H(DID_i || TC_j || TS_2)$를 이용하여 사용자의 ID_i를 계산할 수 있다. 센서 노드에는 등록과정에서 공유된 TC_j, 정보가 저장되어 있으며, DID_{GWN} 및 DID_i, TS_2 는 메시지를 통해 전달되기 때문에 공격자가 사용자 ID를 계산해내는 것이 가능한 것이다. 그러므로 본 프로토콜에서는 센서 노드에서 사용자의 ID 값이 노출되므로 완벽한 익명성을 제공하지 못하여 프라이버시 문제도 발생할 수 있다.



<그림 4> Jiang 등의 센서노드 상의 사용자 ID 노출

IV. 보안성이 향상된 인증 프로토콜

Jiang 등이 제안했던 프로토콜의 취약점인 상호인증 미충족, SID 변조 공격, 센서 익명성 미충족, 센서 노드 상의 사용자 ID 노출을 해결하기 위해서 본 논문에서는 무선 센서 네트워크 환경을 위한 보안성이 향상된 프라이버시 보호형 two-factor 인증 프로토콜을 제안한다.

4.1 등록 과정

(R1-U) 그림 2과 같이 사용자 U_i 가 게이트웨이 노드 GWN 에 등록을 하기 위해서는, 먼저 U_i 는 자신이 향후 사용할 ID_i 와 PW_i 를 선택하고, 무작위로 생성된 숫자 r_i 를 선택한다. 그리고 U_i 는 패스워드를 보호하기 위해서 $HPW_i = H(PW_i || ID_i || r_i)$를 계산한 후, GWN 에게 메시지 { ID_i, HPW_i }를 전송하여 등록과정을 시작한다.

(R2-U) GWN 는 사용자의 ID_i 가 적법한지를 검사한 후, GWN 은 $TC_i = H(K_{GWN\text{-}U} || ID_i || T_{Ei})$ 와 $PTC_i = TC_i \oplus HPW_i$ 을 계산한다. 그리고 GWN 은 (ID_i, TE_i)을 GWN상에서 관리하고 있는 검증테이블에 저장한다. 그리고 GWN 는 { $H(\cdot)$, y, TE_i, PTC_i }를 사용자에게 전달할 스마트 카드에 저장하고 사용자 U_i에게 전달한다.

(R3-U) 사용자 U_i 는 향후 로그인 및 인증과정에서 사용할 $HPW'_i = H(h(ID_i || PW_i || r_i) \bmod m$, m은 28≤m≤216 의 사이 값)를 계산한다. 이것은 공격자가 < ID_i , PW_i >을 알아내기 위해 오프라인 패스워드 공격을 진행하는 것을 막는 효과가 있다. 그리고 사용자는 < $H(\cdot)$, y, TE_i, PTC_i, r_i, HPW_i > 를 스마트 카드에 저장한다.

센서 노드 Sj가 GNW에 등록하는 과정은 다음과 같이 3 단계로 이루어지며, TC_j 의 전달이 주요한 이유이다.

(R1-S) 센서 노드 S_j는 자신의 SID_j을 GWN 에게 비밀채널을 통해서 안전하게 전달함으로써 등록을 시작한다.

(R2-S) GWN 는 향후 인증과정에 사용할 TC_j = H($K_{GWN\text{-}S}$ || SID_j)를 계산하여 S_j 에게 { TC_j }를 전송한다.

User U_i | GWN

$\langle ID_i, PW_i \rangle$ | $\langle K_{GWN-U}, K_{GWN-S} \rangle$

Chooses ID_i and PW_i ;
Generate r_i ;
$HPW_i = H(PW_i \| ID_i \| r_i)$;

$\xrightarrow{\langle ID_i, HPW_i \rangle}$

$TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$;
$PTC_i = TC_i \oplus HPW_i$;
Store $\langle ID_i, TE_i \rangle$;
Stores $\langle H(\cdot), y, TE_i, PTC_i \rangle$ into smart card ;

$\xleftarrow{\text{Smart card } \langle H(\cdot), y, TE_i, PTC_i \rangle}$

$HPW_i' = H(h(ID_i \| PW_i \| r_i) \bmod m)$;
Smart card $\langle H(\cdot), y, TE_i, PTC_i, r_i, HPW_i' \rangle$ into smart card ;

<그림 5> 제안하는 프로토콜의 등록과정

User U_i | GWN | Sensor node S_j

$\langle ID_i, PW_i \rangle$ | $\langle K_{GWN-U}, K_{GWN-S} \rangle$ | $\langle TC_j \rangle$

Inputs ID_i and PW_i ;
$TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$;
Generates $a \in Z_{p-1}^*$;
$A_i = aP$;
$D_i = ay = axP$;
$DID_i = ID_i \oplus H(A_i \| D_i)$;
$C_i = H(ID_i \| TS_1 \| D_i \| A_i \| TC_i)$;

$\xrightarrow{M_1 = \langle DID_i, A_i, TS_1, C_i \rangle}$

Checks TS_1 ;
$D_i = xA = xaP$;
$ID_i = DID_i \oplus H(A_i \| D_i)$;
Check ID_i and Retrieve TE_i ;
$TC_i = H(K_{GWN-U} \| ID_i) \| TE_i)$;
Check $H(ID_i \| TS_1 \| D_i \| A_i \| TS_2)$;
$TC_j = H(K_{GWN-S} \| SID_j)$;
$F_i = H(ID_i \| TS_2)$;
$DID_{GWN} = F_i \oplus H(DID_i \| TC_j \| TS_2)$;
$C_{GWN} = H(F_i \| TC_j \| A_i \| TS_2)$;

$\xrightarrow{M_2 = \langle TS_2, DID_i, DID_{GWN}, C_{GWN}, A_i \rangle}$

Checks TS_2 ;
$F_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_2)$;
Check $C_{GWN} \stackrel{?}{=} H(F_i \| TC_j \| A_i \| TS_2)$;
Generate $b \in Z_{p-1}^*$;
$B_j = bP$;
$SK_{ij} = H(bA_i) = H(abP)$;
$C_j = H(TC_j \| F_i \| SID_j \| B_j \| TS_3)$;
$DSID_j = SID_i \oplus F_i$;

;

$\xleftarrow{M_3 = \langle DSID_j, TS_3, C_j, B_j \rangle}$

Checks TS_3;
$SID_j = DSID_j \oplus F_i$;
Check $C_j \stackrel{?}{=} H(TC_j \| F_i \| SID_j \| B_j \| TS_3)$;
$E_{GWN} = H(ID_i \| TC_i \| D_i \| B_j \| TS_4 \| DSID_j)$;

$\xleftarrow{M_4 = \langle DSID_j, TS_4, B_j, E_{GWN} \rangle}$

Check TS_4 ;
Check $E_{GWN} \stackrel{?}{=} H(ID_i \| TC_i \| D_i \| B_j \| TS_4 \| DSID_j)$;
$SK_{ij} = H(aB_j) = H(abP)$;

<그림 6> 제안하는 프로토콜의 로그인 및 인증 과정

(R3-S) 센서 노드 S_j 는 TC_j를 안전하게 저장해둔다.

4.2 로그인 과정

(L1) 그림 3와 같이 사용자 U_i 가 S_j 의 정보를 얻기 위해 통신을 시도하고자 접속하고자 할때, U_i 는 스마트카드를 터미널에 넣고 자신의 ID_i ,PW_i 를 입력한다.

(L2) 사용자의 스마트 카드는 $HPW^*_i = H(H(ID_i || PW_i || r_i) \bmod m)$ 를 계산하여, 스마트 카드에 저장된 HPW''_i 와 동일한지 검사한다. 값이 다르면 로그인 과정을 중단하고, 같으면 $TC_i = PTC_i \oplus H(PW_i || ID_i || r_i)$를 계산하면서 인증과정을 시작하게 된다.

4.3 인증 과정

(A1) 그림 와 같이 사용자 U_i 는 랜덤한 값인 $a \in Z^*_{p-1}$ 를 선택하고 $A_i = aP$, $D_i = ay = axP$ 를 계산한다. 그리고 메시지 전송때 사용할 동적 ID인 $DID_i = ID_i \oplus H(A_i || D_i)$와 $C_i = H(ID_i || TS_1 || D_i || A_i || TC_i)$을 계산한다. 이때 TS_1 는 현재시점의 사용자 타임스탬프이다. 그리고 마지막으로 사용자 U_i 는 메시지 $M_1 = \{DID_i, A_i, TS_1, C_i\}$를 생성하여 인증을 위하여 GWN 에게 전달한다.

(A2) GWN 은 U_i 에게 메시지 $M_1 = \{DID_i, A_i, TS_1, C_i\}$ 를 전송받으면, 우선 타임 스태프인 TS_1 을 최신성을 검증하여 조건을 만족하지 않으면 인증과정를 중단한다. 최신성을 만족하면, GWN 는 $D_i = xA = xaP$ 를 계산하고 이를 이용하여 $ID_i = DID_i \oplus H(A_i || D_i)$를 통해 ID_i 을 알아내고, 이를 이용하여 $TC_i = H(K_{GWN\text{-}U} || ID_i || TE_i)$를 계산한다. 그리고 앞에서 계산한 값들을 이용하여 $H(ID_i || TS_1 || D_i || A_i || TC_i)$를 계산하여, 메시지 M1을 통해 전송된 C_i 값과 비교한다. 두 값이 다르면 인증과정을 중단하게 되고, 같으면 GWN 는 센서노드 S_j 를 선택하여, $TC_j = H(K_{GWN\text{-}S} || SID_j)$를 계산한다. 그리고 센서노드 상의 IDi의 익명성을 보장하기 위한 $F_i = H(ID_i || TS_2)$를 계산하고, F_i 를 $DID_{GWN} = F_i \oplus H(DID_i || TC_j || TS_5)$와 $C_{GWN} = H(F_i || TC_j || A_i || TS_2)$를 계산에 활용한다. 이때 $TS2$ 는 최신 타임스탬프이이며, GWN 는 $M_2 = \{TS_2, DID_i, DID_{GWN}, C_{GWN}, A_i\}$ 생성하고 M_2를 선택한 센서노드 S_j 에게 전달한다.

(A3) 센서 노드 S_j 는 $M_2 = \{TS_2, DID_i, DID_{GWN}, C_{GWN}, A_i\}$를 전송 받은 후, 먼저 TS_2 의 최신성을 검증하게 된다. TS_2 값이 기준치를 벗어나게 되면, 인증과정을 중단하게 되고, 허용범위 이내라면 S_j 는 $F_i = DID_{GWN} \oplus H(DID_i || TC_j || TS_2)$를 계산해내고, 이를 활용하여 $H(F_i || TC_j || A_i || TS_2)$ 값을 계산한다. S_j 는 계산한 과 C_{GWN} 이 동일한지 확인하여 게이트웨이를 검증하게 된다. 값이 같으며 S_j 는 랜덤값 $b \in Z^*_{p-1}$ 를 생성하고, $B_j = bP$를 계산한다. 이를 활용하여 사용자와 센서 노드 간에 사용할 세션키 $SK_{ij} = H(bA_i) = H(abP)$를 계산해둔다. 그후 $C_j = H(TC_j || F_i || SID_j || B_j || TS_3)$을 계산하며, 이때 TS_3 는 최신 타임스탬프이다. 그리고 Sj의 동적 ID인 $DSID_j = SID_j \oplus F_i$ 를 계산한다. S_j 는 $M_3 = \{DSID_j, TS_3, C_j, B_j\}$를 생성하고 GWN 에게 전달한다.

(A4) M_3를 전달받은 GWN 은 우선 TS_3 의 최신성을 검증한 후, $DSID_j = SID_j \oplus F_i$를 계산한다. 이를 활용하여 $H(TC_j || ID_i || SID_j || B_j || TS_3)$를 계산하여, M_3 에 포함된 C_j 값과 동일한 값인지를 확인한다. 값이 다르면 인증이 실패하여 인증과정이 중단되며, 값이 같으면 GWN 는 S_j 를 인증하게 된다. 그리고 GWN 는 $E_{GWN} = H(ID_i || TC_i || D_i || B_j || TS_4 || DSID_j)$를 계산하며 이때 TS_4 는 GWN의 최신 타임스탬프이다. GWN 은 $M_4 = \{DSID_j, TS_4, B_j, E_{GWN}\}$을 생성하고 사용자 U_i에게 전달한다.

User U_i | GWN

$\langle ID_i, PW_i \rangle$ | $\langle K_{GWN-U}, K_{GWN-S} \rangle$

Chooses ID_i and PW_i ;
Generate r_i ;
$HPW_i = H(PW_i \| ID_i \| r_i)$;

$\xrightarrow{\langle ID_i, HPW_i \rangle}$

$TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$;
$PTC_i = TC_i \oplus HPW_i$;
Store $\langle ID_i, TE_i \rangle$;
Stores $\langle H(\cdot), y, TE_i, PTC_i \rangle$ into smart card ;

$\xleftarrow{\text{Smart card } \langle H(\cdot), y, TE_i, PTC_i \rangle}$

$HPW_i' = H(h(ID_i \| PW_i \| r_i) \bmod m)$;
Smart card $\langle H(\cdot), y, TE_i, PTC_i, r_i, HPW_i' \rangle$ into smart card ;

<그림 5> 제안하는 프로토콜의 등록과정

User U_i | GWN | Sensor node S_j

$\langle ID_i, PW_i \rangle$ | $\langle K_{GWN-U}, K_{GWN-S} \rangle$ | $\langle TC_j \rangle$

Inputs ID_i and PW_i ;
$TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$;
Generates $a \in Z_{p-1}^*$;
$A_i = aP$;
$D_i = ay = axP$;
$DID_i = ID_i \oplus H(A_i \| D_i)$;
$C_i = H(ID_i \| TS_1 \| D_i \| A_i \| TC_i)$;

$\xrightarrow{M_1 = \langle DID_i, A_i, TS_1, C_i \rangle}$

Checks TS_1 ;
$D_i = xA = xaP$;
$ID_i = DID_i \oplus H(A_i \| D_i)$;
Check ID_i and Retrieve TE_i ;
$TC_i = H(K_{GWN-U} \| ID_i) \| TE_i)$;
Check $H(ID_i \| TS_1 \| D_i \| A_i \| TS_2)$;
$TC_j = H(K_{GWN-S} \| SID_j)$;
$F_i = H(ID_i \| TS_2)$;
$DID_{GWN} = F_i \oplus H(DID_i \| TC_j \| TS_2)$;
$C_{GWN} = H(F_i \| TC_j \| A_i \| TS_2)$;

$\xrightarrow{M_2 = \langle TS_2, DID_i, DID_{GWN}, C_{GWN}, A_i \rangle}$

Checks TS_2 ;
$F_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_2)$;
Check $C_{GWN} \stackrel{?}{=} H(F_i \| TC_j \| A_i \| TS_2)$;
Generate $b \in Z_{p-1}^*$;
$B_j = bP$;
$SK_{ij} = H(bA_i) = H(abP)$;
$C_j = H(TC_j \| F_i \| SID_j \| B_j \| TS_3)$;
$DSID_j = SID_i \oplus F_i$;

;

$\xleftarrow{M_3 = \langle DSID_j, TS_3, C_j, B_j \rangle}$

Checks TS_3;
$SID_j = DSID_j \oplus F_i$;
Check $C_j \stackrel{?}{=} H(TC_j \| F_i \| SID_j \| B_j \| TS_3)$;
$E_{GWN} = H(ID_i \| TC_i \| D_i \| B_j \| TS_4 \| DSID_j)$;

$\xleftarrow{M_4 = \langle DSID_j, TS_4, B_j, E_{GWN} \rangle}$

Check TS_4 ;
Check $E_{GWN} \stackrel{?}{=} H(ID_i \| TC_i \| D_i \| B_j \| TS_4 \| DSID_j)$;
$SK_{ij} = H(aB_j) = H(abP)$;

<그림 6> 제안하는 프로토콜의 로그인 및 인증 과정

(A5) 우선은 U_i 는 TS_4 의 최신성을 검토하여 기준값을 초과하면 인증과정을 중단한다. 기준값 이내이면, 사용자는 $H(ID_i || TC_i || D_i || B_j || TS_4 || DSID_j)$를 계산하여, M4를 통해 전송된 E_{GWN} 와 동일한 값인지 확인한다. 같으면 U_i는 S_j와 GWN를 인증하게 된다. 마지막으로 U_i 는 센서 노드와의 통신에서 사용할 공유 세션키 $SK_{ij} = H(aB_j) = H(abP)$ 를 계산한다. 본 과정을 통해 공유된 세션키 SK_{ij}를 통하여 사용자와 센서노드는 안전한 통신을 하게 된다

4.4 패스워드 변경 과정

(PC1) 그림 4과 같이 U_i 가 PW_i 를 변경하고자 할 때 스마트 카드를 터미널에 넣고 ID_i 와 PW_i 를 입력한다.

User U_i

$\langle ID_i, PW_i, PW_i' \rangle$

Insert smart card ;
Input previous ID and PW ID_i, PW_i ;
Compute $HPW_i^* = H(h(ID_i \| PW_i \| r_i) \bmod m)$;
Check $HPW_i^* \stackrel{?}{=} HPW_i'$;
Input new PW PW_i' ;
Compute $PTC_i' = TC_i \oplus RPW_i \oplus H(r \| PW_i')$;
Replace PTC_i with PTC_i' ;

<그림 7> 제안하는 프로토콜의 패스워드 변경 과정

(PC2) Ui의 스마트 카드는 $HPW_i^* = H(H(ID_i || PW_i || r_i) \bmod m)$을 계산하고, 기존에 스마트 카드에 저장되어 있는 HPW_i 와 동일한지 검증한다. 값이 다르면, 패스워드 변경과정이 중단되고, 값이 같으면 U_i 에게 새로운 패스워드 PW_i' 를 입력하고 $PTC_i' = TC_i \oplus RPW_i \oplus H(r || PW_i)$ 계산하고 기존의 PTC_i 를 PTC_i' 로 대체함으로써 패스워드를 변경과정이 완료된다.

V. 제안하는 프로토콜 안전성 분석

제안하는 프로토콜의 안전성을 분석하기 위해 기존의 Jiang 등이 제안한 프로토콜에서 분석된 취약점을 포함하여 안전성을 분석하였다.

5.1 상호인증 충족

U_i 는 $E_{GWN} = H(ID_i || TC_i || D_i || B_j || TS_4 || DSID_j)$에 포함되어 있는 IDi를 통하여 GWN를 인증하게 된다. GWN는 H $(ID_i || TS_1 || D_i || A_i || TC_i)$와 Ci 값의 동일성를 검증하는 과정을 통하여 U_i 를 인증하게 되므로, U_i 와 GWN는 상호 인증을 충족한다.

GWN은 $H(TC_j || ID_i || SID_j || B_j || TS_3)$ 값과 M_3 에 포함된 C_j 값과 동일한 값인지를 확인하면서 SIDj를 통하여 S_j를 인증하게 된다. S_j 는 $C_{GWN} = H(F_i || TC_j || A_i || TS_2)$에 TC_j 이 포함되어 있는 것으로 GWN을 인증하게 되므로, GWN와 S_j는 상호 인증을 충족한다.

U_i 는 $E_{GWN} = H(ID_i || TC_i || D_i || B_j || TS_4 || DSID_j)$에 $DSID_j$ 가 포함되어 있는 것을 통해 S_j를 인증하게 된다. S_j는 $C_{GWN} = H(F_i || TC_j || A_i || TS_2)$에 F_i 가 포함되어 있는 것을 통하여 U_i를 인증하게 된다. $F_i = H(ID_i || TS_2)$와 같이 Fi에는 ID_i 값을 포함하고 있기 때문이다. 이를 통해 U_i 와 S_j는 상호 인증을 하게 된다. 그러므로 본 논문에서 제안하는 프로토콜에서는 U_i, S_j, GNW 의 3 가지 구성요소 간에 상호인증을 제공하고 있다. 이를 통해 3 가지 노드 간의 신뢰성있는 통신이 가능해진다.

5.2 SID 변조 공격에 대한 방어

제안하는 프로토콜에서는 메시지 $M_4 = \{DSID_j, TS_4, B_j, E_{GWN}\}$와 $E_{GWN} = H(ID_i || TC_i ||$

$D_i||B_j||TS_4$ || $DSID_j$) 에 모두 $DSID_j$ 값을 전송하게 함으로써, SID 변조 공격을 막고 있다. 센서 노드의 ID 가 $DSID_j$ 이 아닌 공격자는 $E_{GWN} = H(ID_i$ $||TC_i$ || $D_i||B_j||TS_4$ || $DSID_j)$를 생성할 수 없으므로, SID 값만을 변조하여 사용자가 공격자를 정당한 센서 노드로 속이는 공격이 불가능해지게 된다. 즉 SID 값만 변조하여 인증을 회피를 하려고 하는 공격자를 예방할 수 있다.

5.3 센서 익명성 충족

제안하는 프로토콜에서는 센서 노드에게도 익명성을 제공하기 위해서 DSIDj 를 사용하고 있다. DSIDj = SIDi ⊕ Fi을 이용하므로, Fi을 계산할 수 있는 정당한 GWN 이외에는 SIDi을 알아낼 수가 없다. 이를 통하여 제안하는 프로토콜의 3가지 구성 요소인 Ui 와 GWN, Sj 가 각각 DIDi, DIDGWN, DSIDj 를 사용하여 익명성을 충족시키고 있다. 즉, 3가지 구성요소가 사용하는 ID가 매 통신 마다 변경되어 프라이버시가 강화되었다.

5.4 센서노드 상의 사용자 ID 노출 방지

제안하는 프로토콜에서는 센서에서 노출될 수 있는 ID_i 를 대신하여 $F_i = H(ID_i || TS_2)$을 사용하고 있다. 이를 통해 공격자가 센서 노드에 접근하여 사용자 ID_i 를 알아내는 노출 공격을 방지할 수 있게 되었다. 공격자가 센서 노드에 접근하여 센서 노드의 비밀값인 TC_j 값을 알아내더라도, $F_i = H(ID_i || TS_2)$에서 사용자의 ID_i 값을 알아낼 수가 없으므로 노출이 방지되는 것이다. 그러므로 제안하는 프로토콜은 센서 노드에서도 사용자의 ID_i 가 노출되지 않으므로 익명성이 충분히 제공하여 사용자의 프라이버시를 잘 보호하고 있다. 즉, 센서노드의 관리자, 혹은 센서 노드에 접근한 공격자라고 할지라도 센서노드를 이용하는 사용자 ID를 알아낼 수 없게 된 것이다.

5.5 추적 불가성

제안하는 프로토콜에서 전송되는 $M_1 = \{ DID_i, A_i, TS_1, C_i \}$, $M_2 = \{ TS_2, DID_i, DID_{GWN}, C_{GWN}, A_j\}$, $M_3 = \{ DSID_j, TS_3, C_j, B_j \}$, $M_4 =\{ DSID_j, TS_4, B_j, E_{GWN} \}$ 에서는 모두 $DID_i = ID_i \oplus H(A_i || D_i)$, $DID_{GWN} = F_i \oplus H(DID_i || TC_j||TS_5)$, $DSID_j = SID_i \oplus F_i$ 를 사용하여 매 인증과정마다 다른 값이 사용되므로 사용자, 게이트웨이 노드, 센서 노드의 익명성을 보장하면서 추적도 불가능하게 하였다. 즉, 3가지 각 노드들은 자신과 통신을 하고 있는 노드들이 정당한 노드인지를 확인하지만, 어떠한 노드인지를 특정하지는 못하게 하여 익명성을 강화하게 된 것이다.

5.6 세션키 공유

제안하는 프로토콜에서는 센서 노드에서는 $SK_{ij} = H(bA_i) = H(abP)$를 이용하고 사용자는 $SK_{ij}= H(aB_j) = H(abP)$를 이용하여 같은 세션키 SK_{ij}를 계산한다. 이 방식은 타원 곡선 암호의 특성을 이용하는 것으로 센서 노드와 사용자 말고는 세션키 SK_{ij} 를 계산해낼 수 없다[13].즉, 사용자와 센서 노드 간의 세션키를 취득하려는 의도가 있는 공격자뿐만 아니라, 사용자와 센서노드 간의 통신을 중계하는 게이트웨이 노드도 공유 세션키 SK_{ij} 를 계산해낼 수 없기 때문에 안전성을 보장할 수 있다.

5.7 재전송 공격에 대한 안전성

제안하는 프로토콜에서는 모든 메시지 $M_1 = \{ DID_i, A_i, TS_1, C_i \}$, $M_2 = \{ TS_2, DID_i, DID_{GWN}, C_{GWN}, A_j\}$, $M_3 = \{ DSID_j, TS_3, C_j, B_j \}$, $M_4 =\{ DSID_j, TS_4, B_j, E_{GWN} \}$에 타임 스탬프 TS_1, TS_2 ,TS_3, TS_4를 사용하고

매번 최신성을 확인하고 메시지를 검증하기 때문에 재전송 공격에 안전하다. 이를 통해 공격자가 기존에 전송되었던 메시지를 전송하더라도 각 노드들은 인증과정에서 재전송 공격을 알아낼 수 있다.

5.8 오프라인 패스워드 공격에 대한 안전성

제안하는 프로토콜에서는 오프라인으로 패스워드를 알아내기 어렵게 하기 위해서 $HPW_i = H(PW_i || ID_i || r_i)$에서처럼 r_i를 이용하고 있다. 스마트카드 안에 저장된 값들은 전력 모니터링 분석 방식으로 알아낼 수 있지만, r_i은 저장되어 있지 않으므로 계산해낼 수 없다. 그러므로 HPW_i를 알더라도 r_i을 알 수 없으므로 사용자의 패스워드 PW_i을 알아낼 수가 없다[14]. 그래서 공격자가 사용자의 스마트카드만을 가진 상황에서는 사용자의 패스워드를 알아낼 수 없다.

5.9 내부자 공격에 대한 안전성

제안하는 프로토콜에서는 사용자 U_i가 PW_i와 $H(PW_i)$를 대신하여 $HPW_i = H(PW_i || ID_i || r_i)$를 사용하고 있다. 그 결과, GWN은 r_i 값을 알수가 없으므로, 사용자의 패스워드인 PW_i를 계산해낼 수 없다. 그러므로 게이트웨이 노드의 내부자라도 하더라도 사용자의 패스워드를 알아낼 수 없으므로, 제안하는 프로토콜은 내부자 공격에 안전하다[15]. 즉, 사용자 패스워드 등록과정을 운영하는 관리자도 사용자의 패스워드를 알아낼 수가 없기 때문에 안정성을 보장할 수 있게 된다.

5.10 메시지 변조 공격에 대한 안전성

제안하는 프로토콜에서는 모든 메시지 $M_1 = \{DID_i, A_i, TS_1, C_i\}$에서는 $C_i = (ID_i || TS_1 || D_i || A_i || TC_i)$를 통해서, $M_2 = \{TS_2, DID_i, DID_{GWN}, C_{GWN}, A_j\}$에서는 $C_{GWN} = H(F_i || TC_j || A_i || TS_2)$를 통하여, $M_3 = \{DSID_j, TS_3, C_j, B_j\}$에서는 $C_j = H(TC_j || ID_i || SID_j || B_j || TS_3)$를 통해서, $M_4 = \{DSID_j, TS_4, B_j, E_{GWN}\}$에서는 $E_{GWN} = H(ID_i || TC_i || D_i || B_j || TS_4 || DSID_j)$를 통하여 메시지의 변조를 확인하고 검증하고 있다. 그러므로 제안하는 프로토콜은 메시지 변조 공격에 안전하다. 이를 통해, 공격자가 각 노드에서 전달되는 메시지를 변조하게 되면, 수신한 노드에서 변조된 사실을 알아낼 수 있게 되어 정상적이지 못한 인증이 진행되는 것을 막을 수 있게 된다[16-17].

VI. 결론

본 논문에서는 Jiang 등이 제안한 프로토콜의 동작과정을 분석하여, 상호인증 및 센서 익명성을 제공하지 못하고 센서 노드 상에서 ID가 노출되며 SID 변조 공격에 취약하다는 것을 밝혀냈다. Jiang 등이 제안한 프로토콜에서 발견된 취약점을 해결하기 위해 본 논문에서는 무선 센서 네트워크 환경을 위한 보안성이 향상된 프라이버시 보호형 two-factor 인증 프로토콜을 제안하였다. 그리고 안전성 분석을 통하여 제안한 프로토콜이 상호인증 및 익명성을 제공하고 있으며, 사용자를 추적할 수 없다는 것과 안전하게 세션키를 공유할 수 있다는 것을 증명하였다. 또한 추가적인 안전성 분석을 통해 본 논문에서 제안하는 인증 프로토콜이 다양한 공격방식에도 안전하다는 것을 증명함으로써 안전성과 프라이버시가 향상되었다는 것을 밝혔다.

Acknowledge

본 논문은 2019년 호원대학교 교비학술연구비 지

원과 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5017492)

참고문헌

[1] Kumari, Saru, Muhammad Khurram Khan, and Mohammed Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," Ad Hoc Networks, 2015, pp.159-194.

[2] Jiang, Qi, et al, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," International Journal of Network Management, Vol.27, No.3, 2017.

[3] Choi, Younsung, et al, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, Vol.14, No.6, 2014, pp.10081-10106.

[4] Khan, Muhammad Khurram, and Khaled Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," Sensors, Vol.10, No.3, 2010, pp.2450-2459.

[5] Das, Manik Lal, "Two-factor user authentication in wireless sensor networks," IEEE transactions on wireless communications Vol.8, No.3, 2009, pp.1086-1090.

[6] Chaudhry, Shehzad Ashraf, et al, "An improved and provably secure privacy preserving authentication protocol for SIP," Peer-to-Peer Networking and Applications, Vol.10, No.1, 2017, pp.1-15.

[7] He, Daojing, et al, "An enhanced two-factor user authentication scheme in wireless sensor networks," Ad hoc & sensor wireless networks, Vol.10, No.4, 2010, pp.361-371.

[8] Yeh, Hsiu-Lien, et al, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, Vol.11, No.5, 2011, pp.4767-4779.

[9] Shi, Wenbo, and Peng Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," International Journal of Distributed Sensor Networks, Vol.9, No.4, 2013.

[10] Chen, Tien-Ho, and Wei-Kuan Shih, "A robust mutual authentication protocol for wireless sensor networks," ETRI journal, Vol.32, No.5, 2010, pp.704-712.

[11] Wang, Ding, et al, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," IEEE Transactions on Dependable and Secure Computing, Vol.12, No.4, 2014, pp.428-442.

[12] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone, "Guide to elliptic curve cryptography," Computing Reviews, Vol.46, No.1, 2005.

[13] Choi, Younsung, et al, "Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics," The Scientific World Journal, 2014.

[14] Choi, Younsung, Youngsook Lee, and Dongho Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," International Journal of Distributed Sensor Networks, Vol.12, No.1, 2016.

[15] Jung, Jaewook, et al, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," Sensors, Vol.16, No.8, 2016.

[16] 박중오, "무선 네트워크 환경에서 기기 관리 및 사용자 인증을 위한 안전한 통신 프레임워크 설계", 디지털산업정보학회 논문지, 제15권, 제2호, 2019, pp.43-52.

[17] 이재영, "스마트카드 기반의 사용자 인증 기법에 관한 연구", 디지털산업정보학회 논문지, 제14권, 제2호, 2018, pp.27-33.

논문접수일 : 2019년 10월 24일
수 정 일 : 2019년 11월 28일
게재확정일 : 2019년 12월 3일

■ 저자소개 ■

최 윤 성
Choi, Younsung

2016년 3월~현재
호원대학교 컴퓨터공학부 조교수
(사이버보안전공)
2015년 8월 성균관대학교
전자전기컴퓨터공학부 (공학박사)
2007년 8월 성균관대학교
전자전기컴퓨터공학부 (공학석사)
2006년 2월 성균관대 정보통신공학부
(공학학사)

관심분야 : 정보보호, 디지털포렌식,
산업정보보호
E-mail : yschoi@howon.ac.kr

장 범 환
Chang, Beom-Hwan

2012년 3월 ~ 현재
호원대학교 컴퓨터학부 교수
(사이버보안전공)
2003년 3월 ~ 2012년 2월
한국전자통신연구원 선임연구원
2003년 2월 성균관대학교
전자전기컴퓨터공학부 (공학박사)
1999년 2월 성균관대학교
전기전자컴퓨터공학과(공학석사)
1997년 2월 성균관대학교 전자공학과(공학사)

관심분야 : 네트워크 보안, 빅데이터 시각화,
인공지능
E-Mail : bchang@howon.ac.kr