논문 18-43-12-27 The Journal of Korean Institute of Communications and Information Sciences '18-12 Vol.43 No.12
https://doi.org/10.7840/kics.2018.43.12.2215

무선 센서 네트워크 환경에서 경량화된 사용자 인증 및 키 합의 방식

유 성 진◆, 박 기 성*, 박 요 한**, 박 영 호°

Lightweight User Authentication and Key Agreement Scheme in Wireless Sensor Network Environments

SungJin Yu◆, KiSung Park*, YoHan Park**, YoungHo Park°

요 약

최근 정보통신기술 및 임베디드 기술의 발달로 사용자는 초소형 센서와 같은 저사양 및 저전력 디바이스를 통해 IoT, 헬스 케어, 의료, 스마트홈 등 다양한 서비스를 언제 어디서나 제공 받을 수 있다. 그러나 이러한 서비스들은 공개된 네트워크를 통하여 제공되므로 사용자의 민감한 데이터가 공격자의 삽입, 도청 및 수정 등을 다양한 공격에 노출될 수 있다. 따라서 사용자가 프라이버시를 보장받기 위하여 합법적인 사용자에게만 서비스를 제공하는 인증 및 키 합의 방식에 대한 연구가 필요하다. 2017년 Tai 등은 무선 센서 네트워크 환경에서 사용자 익명성을 보장하기 위한 인증 및 키 합의 방식을 제안하였다. 본 논문에서는 Tai 등의 방식이 스마트카드 도난 공격, 세션 키 노출 공격 등 다양한 공격에 안전하지 않음을 보이고 이를 개선한 안전한 사용자 인증 및 키 합의 방식을 제안한다. 또한 제안한 방식이 스마트카드 도난 공격, 세션 키 노출 공격 및 사용자 위장 공격 등 다양한 공격에 안전함을 informal 분석을 통하여 입증하였으며 BAN logic 분석을 사용하여 제안하는 방식이 상호인증을 제공함을 증명하였다. 따라서 제안하는 방식은 다양한 공격에 안전하며 저사양 기기를 고려하여 제안되었으며 무선 센서 네트워크 환경에 보다 효율적으로 적용 가능한 인증 및 키 합의 방식이다.

Key Words : Wireless sensor network, IoT, User authentication, Key agreement, BAN logic, Lightweight

ABSTRACT

With the development of information communication technology and embedded technology, users can use various services using low-power devices such as IoT, health-care, smart home at anytime and anywhere. However, these services can be vulnerable to various attacks because transmitted information is provided through a public channel, and an adversary can try to modify, eavesdrop, delete the transmitted messages in order to obtain user's sensitive information. Therefore, secure authentication and key agreement scheme have been needed to provide secure services to legitimate user. In 2017, Tai et al. proposed an authentication and key agreement scheme for wireless sensor networks. In this paper, we show that Tai et al. scheme cannot resist various attacks such as smart card stolen, session key attacks and their scheme cannot provide secure mutual authentication. We

※ 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2017R1A2B1002147)
◆ First Author : (ORCID:0000-0002-3245-781X)Kyungpook National University, darkskiln@naver.com, 학생회원
° Corresponding Author : Kyungpook National University,, parkyh@knu.ac.kr, 종신회원
* (ORCID:0000-0002-6172-9175)Kyungpook National University, kisung2@ee.knu.ac.kr, 학생회원
** (ORCID:0000-0002-9011-8410)Korea Nazarene University, hanny12@gmail.com, 정회원
논문번호 : 201810-305-C-RE, Received October 2, 2018; Revised November 5, 2018; Accepted November 13, 2018

also propose lightweight user authentication and key agreement protocol in WSN environment to resolve the these security weaknesses. We demonstrate that our proposed scheme is secure against various attacks such as smart card stolen, session key and user impersonation attacks using informal analysis. Furthermore, we prove that our scheme provide secure mutual authentication sing the BAN logic. Therefore, our proposed scheme is efficient and suitable to practical WSN environment.

Ⅰ. 서 론

최근 모바일 기기 및 무선통신 기술의 발전으로 WSN(Wireless sensor network) 환경에서 사용자는 초소형 센서와 같은 저사양 및 저전력 기기를 통하여 IoT(Internet of Things), Health-care, Smart home 등 다양한 서비스를 언제 어디서나 제공 받을 수 있다. 그러나 이러한 서비스들은 공개된 채널을 통하여 제공되므로 공격자의 데이터 삽입, 도청, 수정, 재전송 및 중간자 공격 등 다양한 공격에 취약하며 이는 개인적 피해뿐만 아니라 국가적인 피해까지 일으킬 수 있다. 따라서 WSN 환경에서 사용자의 프라이버시를 보장하며 합법적인 사용자에게 안전한 서비스를 제공하기 위하여 효율적인 인증 및 키 합의 방식에 대한 연구가 필요하며 이에 대한 관련 연구 또한 활발히 이루어지고 있다[1-7].

2011년 Yeh 등은[8] WSN 환경에서 사용자의 프라이버시를 보장하기 위하여 타원 곡선 암호를 사용한 사용자 인증 프로토콜을 제안하였으나 Yeh 등의 방식은 공개키 기반 암호를 사용하므로 초소형 센서와 같은 저사양 기기들을 사용하는 WSN 환경에 비효율적인 문제점이 있다. 2014년 Turkanovic 등은[9] 이종 애드혹 무선 센서 네트워크를 위한 IoT 기반 사용자 인증 및 키 합의 방식을 제안하였다. 그러나 2015년 Chang 등은[10] Turkanovic 등의 방식이 센서 노드와 게이트웨이 노드 간의 무결성을 제공하지 않으며 검증 단계의 문제점을 밝혔다. 또한 2017년 Tai 등은[11] Turkanovic 등의 방식이 사용자 주척 공격과 세션 키 노출 공격에 안전하지 않음을 보이며 이를 개선한 IoT 기반 인증 및 키 합의 방식을 제안하였다.

본 논문에서는 Tai 등의 방식이 스마트카드 도난 공격 및 세션 키 노출 공격에 취약하며 상호 인증을 보장하지 않음을 보이고 이를 개선한 WSN 환경에서 경량화된 사용자 인증 및 키 합의 프로토콜을 제안한다. 또한 제안하는 인증 방식이 중간자 공격, 재전송 공격, 위장 공격 및 스마트 카드 도난 공격 등 다양한 공격에 안전함을 informal 분석을 통하여 입증하였으며 BAN(Burrows-Abadi-Needham) logic 분석을 통하여 상호 인증이 가능함을 증명하고 기존의 인증 방식 및 제안하는 인증 방식의 연산량 및 성능을 분석하였다. 따라서 제안하는 인증 및 키 합의 방식은 저사양 기기를 고려하여 설계되었으므로 실제 WSN 환경에서 보다 효율적으로 활용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구의 배경 지식과 Tai 등이 제안한 인증 방식 및 Tai 등이 제안한 방식의 보안 취약점에 대해 설명한다. 그리고 4장에서 본 논문에서 제안한 사용자 인증 방식을 설명하고 5장에서는 제안한 방식의 안전성과 성능을 분석한다. 마지막으로 6장에서는 본 논문에 대한 결론을 제시한다.

Ⅱ. 관련 연구

2.1 WSN

WSN은 센서 노드, 사용자 및 게이트웨이로 구성된 무선 통신 네트워크로 의료 서비스, 스마트 홈, 스마트 그리드 등 다양한 환경에서 사용자에게 서비스를 제공하기 위하여 활용되고 있다. 센서 노드는 데이터를 수집 및 추출하여 다른 사물 또는 게이트웨이로 전송하며 게이트웨이는 전송받은 데이터를 처리하여 사용자에게 제공한다. WSN 환경에서 안전한 서

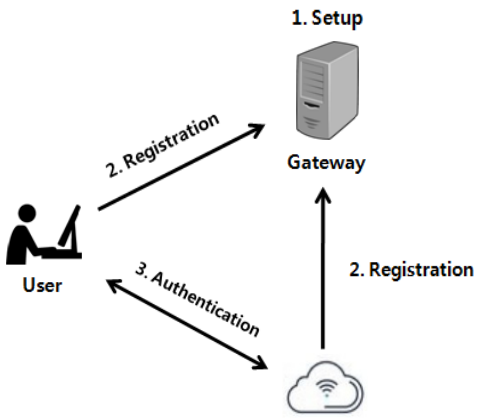

그림 1. WSN 시스템 인증 방식 수행 과정
Fig. 1. WSN system authentication scheme process

비스를 제공하기 위한 사용자 인증 과정은 그림 1과 같으며 각 단계는 다음과 같다.

1) 초기화 단계 : 게이트웨이는 시스템 매개변수 및 인증에 필요한 공유 비밀 키를 생성한다.
2) 등록 단계 : 사용자와 센서는 게이트웨이에게 자신의 신원을 등록요청 하고 게이트웨이는 합법적인 사용자 및 센서를 등록한다.
3) 인증 단계 : 사용자는 서비스를 제공받기 위하여 게이트웨이를 통해 센서 노드의 인증을 요청하고 사용자와 게이트웨이, 게이트웨이와 센서는 서로 상호 인증을 수행한다.

2.2 Tai 등의 사용자 익명 인증 방식

2017년 Tai 등이 제안한 WSN 환경에서 사용자의 익명성을 보장하기 위하여 인증 및 키 합의 방식을 제안하였다. Tai 등이 제안한 방식은 사용자 등록, 센서 등록, 인증 단계 및 패스워드 변경 단계로 구성되며 각 단계의 수행절차는 다음과 같다.

2.2.1 사용자 등록 단계

Tai 등의 방식의 사용자 등록 단계는 그림 2와 같으며 각 단계는 다음과 같다.

- 1단계 : 사용자(U)는 신원 ID_i와 패스워드 PW_i을 선택하고 안전한 통신 채널을 통해 게이트웨이(GWN)에게 전송한다.
- 2단계 : 메시지를 수신 받은 GWN은 랜덤 비밀 패스워드 키 X_{GWN-i}와 비밀 키 X_U를 선택한 후 $f_i = h(ID_i \| X_{GWN})$, $x_i = h(ID_i \| PW_i \| X_{GWN-i})$, $e_i = h(PW_i) \oplus X_U$을 계산한다. 그런 다음 GWN은 $\{ID_i, X_{GWN-i}\}$을 데이터베이스 내에 저장하고 $\{f_i, x_i, e_i, X_{GWN-i}\}$ 값을 스마트 카드(SC) 내에 저장한 후 $\{SC\}$을 U에게 전송한다.

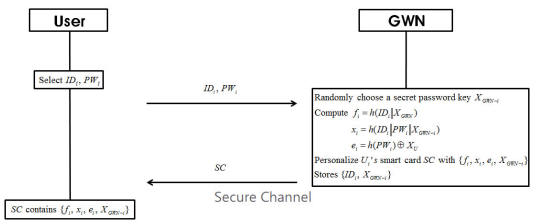

그림 2. Tai et al. 사용자 등록 단계
Fig. 2. User registration phase of Tai et al. scheme

- 3단계 : U은 GWN로부터 스마트카드를 전송 받은 후 등록 단계를 마친다.

2.2.2 센서 등록 단계

Tai 등의 방식의 센서 등록 단계는 그림 3과 같으며 각 단계는 다음과 같다.

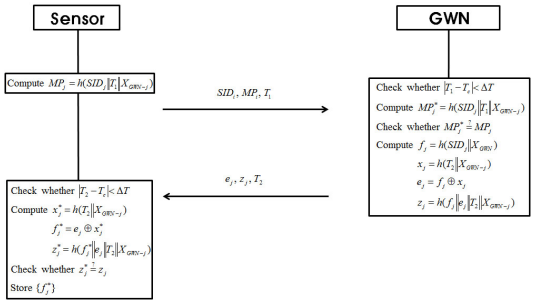

그림 3. Tai et al. 센서 등록 단계
Fig. 3. Sensor registration phase of Tai et al. scheme

- 1단계 : 센서(SN)는 $MP_j = h(SID_j \| T_1 \| X_{GWN-j})$을 계산한 후 GWN에게 $\{SID_j, MP_j, T_1\}$을 전송한다.
- 2단계 : 메시지를 수신 받은 GWN은 타임스탬프 $|T_1 - T_c| < \Delta T$가 유효한지 여부를 확인한다. 만약 유효하지 않다면 세션을 종료하고 그렇지 않다면 GWN은 $MP_j^* = h(SID_j \| T_1 \| X_{GWN-j})$을 계산하고 $MP_j^* = ? MP_j$이 올바른 값인지 체크한다. 만약 올바른 값이라면 GWN은 $f_j = h(SID_j \| X_{GWN})$, $x_j = h(T_2 \| X_{GWN-j})$, $e_j = f_j \oplus x_j$, $z_j = h(f_j \| e_j \| T_2 \| X_{GWN-j})$을 계산하고 SN에게 $\{e_j, z_j, T_2\}$을 전송한다.
- 3단계 : 메시지를 수신 받은 SN은 $|T_2 - T_c| < \Delta T$가 유효한지 여부를 확인한다. 만약 유효하다면 SN은 $x_j^* = h(T_2 \| X_{GWN-j})$, $f_j^* = e_j \oplus x_j^*$, $z_j^* = h(f_j^* \| e_j \| T_2 \| X_{GWN-j})$을 계산한 후 $z_j^* = ? z_j$이 올바른 값인지 체크한다. 만약 올바른 값이라면 SN은 $\{f_j^*\}$을 자신의 디바이스에 저장하고 등록 단계를 마친다.

2.2.3 인증 단계

Tai 등의 방식의 인증 단계는 그림 4와 같으며 각 단계는 다음과 같다.

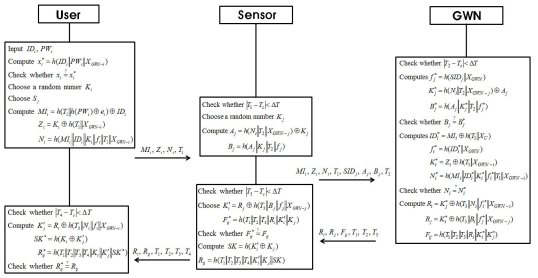

그림 4. Tai et al. 인증 등록 단계
Fig. 4. Authentication phase of Tai et al. scheme

- 1단계 : 사용자는 카드 리더기에 스마트카드 삽입한 후 ID_i와 PW_i을 선택한 후 $x_i^* = h(ID_i \| PW_i \| X_{GWN-i})$을 계산한다. 그런 다음 U은 $x_i^* = ?x_i$이 올바른 값인지 체크한다. 만약 올바르지 않다면 세션을 종료하고 그렇지 않으면 U은 랜덤 값 K_i을 선택한 후 $MI_i = h(T_1 \| h(PW_i) \oplus e_i) \oplus ID_i$, $Z_i = K_i \oplus h(T_1 \| X_{GWN-i})$, $N_i = h(MI_i \| ID_i \| K_i \| f_i \| T_1 \| X_{GWN-i})$을 계산하고 공개 채널을 통하여 SN에게 $\{MI_i, Z_i, N_i, T_1\}$을 전송한다.
- 2단계 : 메시지를 수신 받은 SN은 타임스탬프 $|T_1 - T_e| < \Delta T$의 유효성을 체크한다. 만약 타임스탬프가 유효한 시간 내에 전송된 값이라면 SN은 랜덤 값 K_j을 선택한 후 $A_j = h(N_i \| T_2 \| X_{GWN-j}) \oplus K_j$, $B_j = h(A_j \| K_j \| T_2 \| f_j)$을 계산한다. 그런 다음 GWN에게 $\{MI_i, Z_i, N_i, T_1, SID_j, A_j, B_j, T_2\}$을 전송한다.
- 3단계 : 메시지를 수신 받은 GWN은 타임스탬프 $|T_2 - T_e| < \Delta T$가 유효한지 체크한다. 만약 유효한 시간 내에 전송된 값이라면 GWN은 $K_j^* = h(N_i \| T_2 \| X_{GWN-j}) \oplus A_j$, $f_j^* = h(SID_j \| X_{GWN})$, $B_j^* = h(A_j \| K_j^* \| T_2 \| f_j^*)$을 계산하고 인증 요청 메시지 $B_j^* = ?B_j$가 유효한 값인지 확인한다. 만약 유효한 값이라면 GWN은 $ID_i^* = MI_i \oplus h(T_1 \| X_U)$, $f_i^* = h(ID_i^* \| X_{GWN})$, $K_i^* = Z_i \oplus h(T_1 \| X_{GWN-i})$, $N_i^* = h(MI_i \| ID_i^* \| K_i^* \| f_i^* \| T_1 \| X_{GWN-i})$을 계산한다. 그런 다음 GWN은 인증 요청 메시지 $N_j^* = ?N_j$가 올바른 값인지 체크한다. 만약 올바른 값이라면 GWN은 $R_i = K_j^* \oplus h(T_3 \| N_i \| f_j^* \| X_{GWN-i})$, $R_j = K_i^* \oplus h(T_3 \| B_j \| f_j^* \| X_{GWN-j})$, $F_{ij} = h(T_1 \| T_2 \| T_3 \| R_i \| K_i^* \| K_j^*)$을 계산한다. 마지막으로 GWN은 SC에게 공개 채널을 통해 $\{R_i, R_j, F_{ij}, T_1, T_2, T_3\}$을 전송한다.
- 4단계 : 메시지를 수신 받은 SN은 타임스탬프 $|T_3 - T_e| < \Delta T$을 체크 한 후 올바른 값이라면 $K_i' = R_j \oplus h(T_3 \| B_j \| f_j \| X_{GWN-j})$, $F_{ij}^* = h(T_1 \| T_2 \| T_3 \| R_i \| K_i' \| K_j)$을 계산한다. 그런 다음 SN은 인증 메시지 $F_{ij}^* = ?F_{ij}$가 유효한 값인지 체크한 후 유효한 값이라면 세션 키 $SK = h(K_i' \oplus K_j)$와 인증 메시지 $R_{ij} = h(T_1 \| T_2 \| T_3 \| T_4 \| K_i' \| K_j \| SK)$을 계산한다. 마지막으로 SN은 U에게 공개 채널을 통해 $\{R_i, R_{ij}, T_1, T_2, T_3, T_4\}$을 전송한다.
- 5단계 : 메시지를 수신 받은 U은 타임스탬프 $|T_4 - T_e| < \Delta T$가 유효한지 체크한다. 만약 올바른 값이라면 U은 $K_j' = R_i \oplus h(T_3 \| N_i \| f_i \| X_{GWN-i})$, $SK^* = h(K_i \oplus K_j')$, $R_{ij}' = h(T_1 \| T_2 \| T_3 \| T_4 \| K_i \| K'_j \| SK^*)$을 계산한다. 마지막으로 U은 인증 메시지 $R_{ij}^* = ?R_{ij}$가 올바른 값이라면 인증 단계를 마친다.

2.2.4 패스워드 변경 단계

Tai 등의 방식에서 사용자는 자신의 패스워드를 자유롭게 변경할 수 있으며 패스워드 변경 단계는 다음 그림 5와 같고 세부 단계는 다음과 같다.

- 1단계 : U_i은 자신의 스마트카드 SC을 카드 단말기 삽입하고 자신의 신원 ID_i와 패스워드 PW_i^{old}를 기입한다.
- 2단계 : 스마트카드 SC은 $x_i^* = h(ID_i \| PW_i^{old} \| X_{GWN-i})$을 계산하고 $x_i^* = ?x_i$이 유효한지 체크한다.
- 3단계 : 만약 값이 일치하지 않는다면 패스워드 변경 요청을 거절한다. 그렇지 않으면 SC은 유저에게 새로운 패스워드 PW_i^{new}를 요청한다.
- 4단계 : 새로운 패스워드를 전송 받은 SC은 $x_i^{new} = h(ID_i \| PW_i^{new} \| X_{GWN-i})$, $e_i^{new} = e_i \oplus h(PW_i^{old}) \oplus h(PW_i^{new})$을 계산한다. 그런 다음 SC은 메모리 내에 저장되어있던 e_i, x_i값을

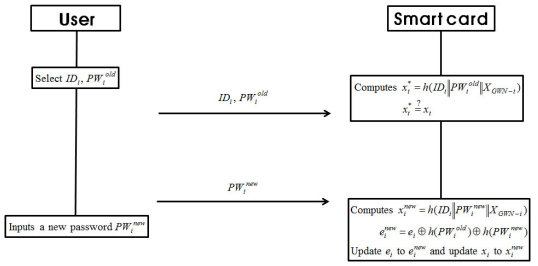

그림 5. Tai et al. 패스워드 변경 단계
Fig. 5. Password change phase of Tai et al. scheme

e_i^{new}, x_i^{new}로 업데이트한다.

Ⅲ. Tai 등이 제안한 방식의 보안 취약점 분석

본 장에서는 Tai 등이 방식이 세션 키 노출 공격 및 스마트카드 도난 공격에 취약하며 상호인증을 제공하지 않음을 보였으며 각 공격은 다음과 같다.

3.1 스마트카드 도난 공격

공격자가 사용자의 스마트카드를 훔친 후 전력분석 공격을[12] 통하여 스마트카드 내부의 정보를 얻고 공개 채널로 전송되는 메시지를 획득한 경우 공격자는 다음과 같은 단계로 합법적인 사용자로 위장할 수 있다.

- 1단계 : 공격자는 사용자의 스마트카드를 획득하고 안에 저장된 비밀 매개 변수 $\{f_i, x_i, e_i, X_{GWN-i}\}$을 얻는다.
- 2단계 : 공격자는 공개 채널을 통해 전송되는 메시지 $\{MI_i, Z_i, N_i, T_1\}$ 및 $R_i, R_{ij}, T_1, T_2, T_3, T_4$을 얻은 후 사용자가 생성한 랜덤 값 $K_i = Z_i \oplus h(T_1 \| X_{GWN-i})$과 센서가 생성한 랜덤 값 $K_j = R_i \oplus h(T_3 \| N_i \| f_i \| X_{GWN-i})$을 계산한다.
- 3단계 : 공격자는 획득한 사용자의 랜덤 값과 센서의 랜덤 값을 사용하여 세션 키 $SK^* = h(K_i \oplus K_j^*)$을 계산할 수 있다.
- 4단계 : 마지막으로 공격자는 인증 메시지 $R_{ij}^* = h(T_1 \| T_2 \| T_3 \| T_4 \| K_i \| K_j^* \| SK^*)$을 계산하여 인증을 완료한다.

3.2 세션 키 노출 공격

Tai 등은 제안한 방식에서 인증 과정의 메시지 $\{MI_i, Z_i, N_i, T_1, SID_j, A_j, B_j, T_2\}$를 통하여 게이트웨이가 랜덤 값 K_i, K_j의 유효성을 검증하고 센서는 $\{R_i, R_{ij}\}$를 계산하여 전송하므로 랜덤 값 K_i, K_j를 공격자가 얻을 수 없다고 주장하였다. 그러나 Tai 등의 방식에서 공격자는 스마트카드 도난 공격을 통하여 사용자의 랜덤 값 K_i,와 센서의 랜덤 값 K_j를 성공적으로 얻을 수 있으므로 올바른 세션 키를 생성할 수 있다. 따라서 Tai 등의 방식은 세션 키 노출 공격에 취약하다.

3.3 상호 인증

3.1의 스마트카드 도난 공격 및 3.2의 세션 키 노출 공격에 따라 공격자는 세션 키 $SK^* = h(K_i \oplus K_j^*)$와 인증 메시지 $R_{ij}^* = h(T_1 \| T_2 \| T_3 \| T_4 \| K_i \| K_j^* \| SK^*)$를 성공적으로 계산할 수 있으므로 센서와 상호인증을 수행할 수 있다. 따라서 Tai 등의 방식은 상호인증을 보장하지 않는다.

Ⅳ. 제안한 방식

본 장에서는 Tai 등이 제안한 방식의 보안 취약점을 개선하기 위하여 무선 센서 네트워크 환경에서 안전한 서비스를 제공하기 위한 사용자 인증 및 키 합의 방식을 제안한다. 제안한 방식은 사용자 및 센서 등록, 인증 단계, 패스워드 변경 단계 등 4단계로 구성되며 시스템 초기화 단계와 센서 등록 단계는 Tai 등이 제안한 방식과 동일하다. 제안한 방식의 각 단계 및 시스템 매개 변수는 다음과 같다.

4.1 시스템 매개 변수

표 1. 매개 변수 표기법
Table 1. Parameter Notations

표기법	의미
U_i	User
ID_i	$U's$ identity
PW_i	$U's$ password
SN	Sensor
GWN	Gateway
X_{GWN}	GWN's secret key
X_{GWN-j}	Pre-distributed secret key between SN and GWN
SC	Smart card
$h()$	Hash function
T	Timestamp
$\|$	Concatenation operation
$\oplus$	XOR operation

4.2 사용자 등록 단계

제안한 방식의 사용자 등록 단계는 그림 6과 같으며 각 단계는 다음과 같다.

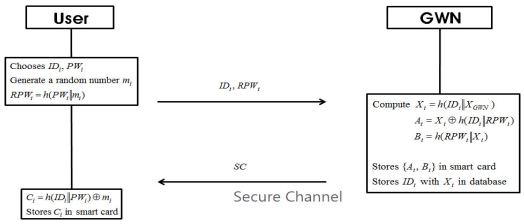

그림 6. 제안한 방식의 사용자 등록 단계
Fig. 6. User registration phase of propose scheme

- 1단계 : 사용자(U)는 ID_i, PW_i 및 임의의 랜덤 값 m_i을 선택한 후 $RPW_i = h(PW_i \| m_i)$ 값을 계산하고 안전한 통신 채널을 통해 게이트웨이(GWN)에게 $\{ID_i, RPW_i\}$를 전송한다.
- 2단계 : 게이트웨이는 $\{ID_i, RPW_i\}$를 수신한 후 $X_i = h(ID_i \| X_{GWN})$, $A_i = X_i \oplus h(ID_i \| RPW_i)$, $B_i = h(RPW_i \| X_i)$을 계산한다. 또한 GWN은 ID_i와 X_i를 데이터베이스에 저장하고 $\{A_i, B_i\}$ 값을 스마트카드에 저장한 후 스마트카드를 사용자에게 전송한다.
- 3단계 : 스마트카드를 수신한 사용자는 $C_i = h(ID_i \| PW_i) \oplus m_i$을 계산하여 스마트카드에 저장한 후 등록 단계를 마친다.

4.3 센서 등록 단계

제안한 방식의 센서 등록 단계는 그림 7과 같으며 각 단계는 다음과 같다.

- 1단계 : 센서(SN)는 $MP_j = h(SID_i \|$ $T_1 \| X_{GWN-j})$를 계산한 후 GWN에게 $\{SID_j, MP_j, T_1\}$을 전송한다.
- 2단계 : GWN는 메시지 $\{SID_j, MP_j, T_1\}$를 수신한 후 타임스탬프 $|T_1 - T_e| < \Delta T$의 유효성을 확인한다. 만약 유효하지 않다면 GWN는 세션을 종료하고 그렇지 않다면 $MP_j^* = h(SID_j \| T_1 \| X_{GWN-j})$을 계산하여 $MP_j^* = ? MP_j$이 올바른 값인지 확인한다. 또한 GWN는 $f_j = h(SID_j \| X_{GWN})$, $x_j = h(T_2 \| X_{GWN-j})$, $e_j = f_j \oplus x_j$, $z_j = h(f_j \| e_j \| T_2 \| X_{GWN-j})$을 계산하고 SN에게 $\{e_j, z_j, T_2\}$을 전송한다.
- 3단계 : 메시지를 수신 받은 SN은 $|T_2 - T_e| < \Delta T$가 유효한지 여부를 확인한다. 만약 유효하다면 SN은 $x_j^* = h(T_2 \| X_{GWN-j})$, $f_j^* = e_j \oplus x_j^*$, $z_j^* = h(f_j^* \| e_j \| T_2 \| X_{GWN-j})$을 계산한 후 $z_j^* = ? z_j$이 올바른 값인지 확인하고 올바른 값이라면 SN은 $\{f_j^*\}$을 자신의 메모리에 저장하고 등록 단계를 마친다.

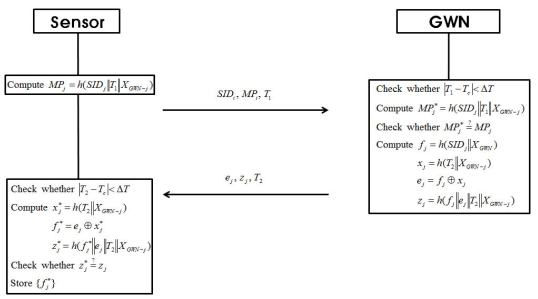

그림 7. 제안한 방식의 센서 등록 단계
Fig. 7. Sensor registration phase of propose scheme

4.4 인증 단계

제안한 방식의 인증 단계는 그림 8과 같으며 각 단계는 다음과 같다.

- 1단계 : 사용자 U는 카드 리더기에 스마트카드를 삽입한 후 자신의 ID_i와 PW_i를 입력하고 $m_i = h(ID_i \| PW_i) \oplus C_i$, $RPW_i = h(PW_i \| m_i)$, $X_i = A_i \oplus h(ID_i \| RPW_i)$, $B_i^* = h(RPW_i \| X_i)$를 계산한다. 그 후 U은 $B_i^* = ? B_i$이 유효한 값인지 확인하고 만약 유효한 값이라면 랜덤 값 K_1을 생성한 뒤 $M_1 = X_i \oplus K_1$, $MID_i = h(X_i \| K_1) \oplus ID_i$, $M_2 = h(X_i \| ID_i \| K_1 \| T_1)$을 계산하고 공개 채널을 통해 SN에게 $\{M_1, M_2, MID_i, T_1\}$을 전송한다.
- 2단계 : 메시지를 수신 받은 SN은 $|T_1 - T_e| < \Delta T$가 유효한지 체크한 후 만약 타임스탬프가 유효한 시간 내에 전송된 값이라면 랜덤 값 K_2을 선택하고 $M_3 = h(M_2 \| T_2 \| X_{GWN-j} \| f_j) \oplus K_j$, $M_4 = h(M_3 \| f_j \| K_2 \| T_2)$을 계산한다. 그 후 SN은 GWN에게 $\{M_1, M_2, MID_i, T_1, M_3, M_4, T_2\}$을 전송한다.
- 3단계 : 메시지를 수신한 후 GWN은

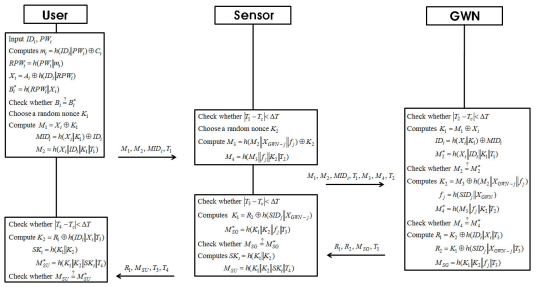

그림 8. 제안한 방식의 인증 단계
Fig. 8. Authentication phase of propose scheme

$|T_2 - T_e| < \Delta T$이 유효한지 확인하고 만약 유효한 값이라면 GWN은 사용자의 랜덤 값 $K_1 = M_1 \oplus X_i$, 신원 $ID_i = h(X_i \| K_1) \oplus MID_i$, $M_2^* = h(X_i \| ID_i \| K_1 \| T_1)$을 계산한다. 그 후 GWN은 $M_2^* = ?M_2$의 유효성을 확인하고 만약 값이 유효하다면 $K_2 = M_3 \oplus h(M_2 \| X_{GWN-j} \| T_2 \| f_j)$, $f_j = h(SID_j \| X_{GWN})$, $M_4^* = h(M_3 \| f_j \| K_2 \| T_2)$를 계산한 후 $M_4^* = ?M_4$이 올바른 값인지 확인한다. 만약 올바른 값이라면 GWN은 $R_1 = K_2 \oplus h(ID_i \| X_i \| T_3)$, $R_2 = K_1 \oplus h(SID_j \| X_{GWN-j} \| T_3)$, 인증 메시지 $M_{SG} = h(K_1 \| K_2 \| f_j \| T_3)$을 계산하고 SN에게 $\{R_1, R_2, M_{SG}, T_3\}$을 전송한다.

- 4단계 : 메시지를 수신 받은 SN은 타임스탬프 $|T_3 - T_e| < \Delta T$이 올바른지 확인하고 만약 타임스탬프가 유효한 시간 내에 전송된 값이라면 SN은 $K_1 = R_2 \oplus h(SID_j \| X_{GWN-j} \| T_3)$, $M_{SG}^* = h(K_1 \| K_2 \| f_j \| T_3)$을 계산 한다. 그 후 SN은 $M_{SG}^* = ?M_{SG}$이 유효한 값인지 확인한 후 유효한 값이라면 SN은 세션 키 $SK = h(K_1 \| K_2)$, 인증 메시지 $M_{SU} = h(K_1 \| K_2 \| SK_i \| T_4)$을 계산하여 U에게 $\{R_1, M_{SU}, T_3, T_4\}$을 전송한다.
- 5단계 : 메시지를 수신한 후 U는 타임스탬프 $|T_4 - T_e| < \Delta T$이 유효한지 확인하고 유효한 값이라면 U는 $K_2 = R_1 \oplus h(ID_i \| X_i \| T_3)$, $SK_i = h(K_1 \| K_2)$, $M_{SU}^* = h(K_1 \| K_2 \| SK_i \| T_4)$을 계산한 후 $M_{SU}^* = ?M_{SU}$이 유효한 값인지 확인한다. 만약 유효한 값이라면 인증 단계를 정상적으로 마친다.

4.5 패스워드 변경 단계

제안하는 방식에서 사용자는 자신의 패스워드 변경을 원할 경우 게이트웨이의 도움 없이 자유롭게 패스워드를 변경할 수 있으며 패스워드 변경 단계는 그림 9과 같고 각 세부 단계는 다음과 같다.

- 1단계 : 사용자는 자신의 스마트카드를 카드 리더기에 삽입하고 신원 ID_i^*와 패스워드 PW_i^*를 기입한다.
- 2단계 : 스마트카드는 $m_i^* = h(ID_i^* \| PW_i^*) \oplus C_i$, $RPW_i^* = h(PW_i^* \| m_i^*)$, $X_i^* = h(ID_i^* \| RPW_i^*) \oplus A_i$, $B_i^* = h(RPW_i^* \| X_i^*)$를 계산한 후 계산한 B_i^*와 카드의 B_i 값과 비교한다. 만약 값이 일치한다면 스마트카드는 사용자에게 새로운 패스워드를 요청한다..
- 3단계 : 사용자는 새로운 패스워드 PW_i^{new}를 스마트카드에게 입력한다.
- 4단계 : 스마트카드는 새로운 패스워드를 수신한 후 $C_i^{new} = h(ID_i^* \| PW_i^{new}) \oplus a_i^*$, $RPW_i^{new} = h(PW_i^{new} \| m_i^*)$, $A_i^{new} = X_i^* \oplus h(ID_i^* \| HPW_i^{new})$, $B_i^{new} = h(RPW_i^{new} \| X_i^*)$을 계산하고 최종적으로 스마트카드에 저장된 값들을 $\{A_i^{new}, B_i^{new}, C_i^{new}, RPW_i^{new}\}$로 업데이트한다.

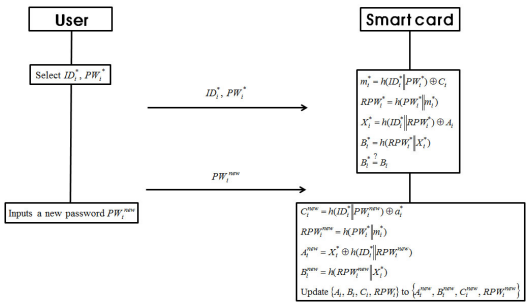

그림 9. 제안한 방식의 패스워드 변경 단계
Fig. 9. Password change phase of propose scheme

V. 성능 분석

본 장에서는 제안한 인증 방식과 기존의 Tai 등의 방식의 연산량을 비교 분석하고 제안한 인증 방식의 안전성을 informal 안전성 분석으로 분석하였다. 또한 제안한 방식이 상호 인증을 보장함을 BAN logic[13] 분석을 통하여 입증하였다.

5.1 연산량 분석

본 논문에서는 제안한 인증 방식과 Tai 등의 인증 방식의 연산량을 사용자, 센서 노드, 게이트웨이 별로 비교 분석하였으며 비교 분석 결과는 표 2와 같다. 따라서 제안한 방식은 Tai 등의 방식과 비교하여 2번의 적은 해시 연산을 가지므로 더욱 효율적인 인증 방식이다.

표 2. 연산량 비교 분석
Table 2. Comparison of computation overhead

Authentication Scheme	User	Sensor node	GWN	ToTal
Xue et al.[14]	$7T_h$	$6T_h$	$13T_h$	$26T_h$
Turkanovic et al.[9]	$7T_h$	$5T_h$	$7T_h$	$19T_h$
Tai et al.[11]	$8T_h$	$6T_h$	$10T_h$	$24T_h$
Proposed scheme	$9T_h$	$6T_h$	$7T_h$	$22T_h$

T_h : Hash operation

5.2 안전성 분석

본 논문에서는 informal 안전성 분석을 통하여 제안한 인증 방식이 중간자 공격, 재전송 공격, 스마트카드 도난 공격, 위장공격, 중간자 공격에 안전함을 보이고 BAN logic을 사용하여 상호인증이 가능함을 입증하였다. Informal 안전성 분석 및 BAN logic 안전성 분석의 결과는 다음과 같다.

5.2.1 중간자 공격

중간자 공격은 공격자가 사용자와 센서, 센서와 게이트웨이 중간에서 데이터 도청, 변조 및 위조를 시도하는 공격 방식이다. 제안한 인증 방식에서 공격자는 비밀 변수 X_i, 사용자의 랜덤 값 K_1을 알 수 없으므로 인증 메시지 $M_1 = h(X_i \| ID_i \| K_1 \| T_1)$, $MID_i = h(X_i \| K_1) \oplus ID_i$를 성공적으로 생성할 수 없다. 따라서 제안하는 인증 방식은 중간자 공격에 안전하다.

5.2.2 재전송 공격

재전송 공격은 공격자가 이전 세션에서 전송한 사용자의 메시지를 탈취하여 해당 세션에서 다시 재전송하여 중요한 정보를 얻거나 인증을 수행하는 공격이다. 제안한 방식에서 전송되는 메시지 $\{M_2, M_4, M_{SG}, M_{SU}\}$는 매 세션마다 생성되는 임의의 값 K_1, K_2을 사용하여 생성된다. 따라서 공격자는 이전에 전송되었던 메시지를 재사용할 수 없으므로 제안한 방식은 재전송 공격에 안전하다.

5.2.3 내부자 공격

내부자 공격은 시스템의 다른 합법적인 사용자가 공격자가 되어 다른 사용자의 아이디 및 패스워드와 같은 민감한 정보를 얻거나 인증을 시도하는 공격이다. 제안한 방식에서 사용자는 랜덤 값 K_1 및 비밀 변수 X_i를 사용하여 $M_1 = X_i \oplus K_1$, $MID_i = h(X_i \| K_1) \oplus ID_i$, $M_2 = h(X_i \| ID_i \| K_1 \| T_1)$를 계산하므로 내부공격자는 실제 사용자의 ID_i 없이 사용자의 정보를 얻을 수 없다. 따라서 제안하는 방식은 내부자 공격에 안전하다.

5.2.4 스마트카드 도난 공격

스마트카드 도난 공격은 공격자가 사용자의 스마트카드를 도난 및 획득한 후 스마트카드에 저장된 데이터를 이용하여 사용자의 정보를 얻으려고 시도하는 공격이다. 제안한 방식에서 공격자는 사용자의 스마트카드를 도난 및 획득하여 카드내의 정보 $\{A_i, B_i, C_i\}$를 얻더라도 실제 사용자의 ID_i 및 PW_i는 알 수 없으며 $\{M_1, MID_i, M_2\}$와 같은 중요한 인증 값들을 계산할 수 없다. 따라서 제안하는 방식은 스마트카드 도난 공격에 안전하다.

5.2.5 위장 공격

위장 공격은 공격자가 합법적인 사용자 또는 게이트웨이로 위장하여 인증을 수행하는 공격이다. 제안한 방식에서 공격자는 $\{ID_i, X_i, K_1, K_2\}$ 값을 얻을 수 없으므로 로그인 요청 메시지 및 인증 메시지들을 성공적으로 생성할 수 없다. 따라서 제안하는 방식은 위장 공격에 안전하다.

5.3 BAN logic 분석

BAN(Burrows – Abadi – Needham) logic[13] 증명 방식은 보안 프로토콜의 상호 인증을 증명하기 위하여 제안되었으며 보안 프로토콜의 안전성을 분석하기 위하여 널리 사용되고 있다. 제안하는 방식은 BAN logic 분석을 통하여 상호 인증이 가능함을 입증하였으며 BAN logic에 사용되는 표기법은 다음 표 3과 같다. 또한 BAN logic 분석에 사용되는 규칙, 보안 목표, 가정 및 이상화 형태는 다음과 같다.

5.3.1 BAN logic 표기법

표 3. BAN logic 표기법
Table 3. BAN logic notation

Notation	Description
$P\|\equiv X$	P believes a statement X
$\#X$	X is fresh
$P\triangleleft X$	P sees X
$P\|\sim X$	P once said X
$P\|\Rightarrow X$	P control X
$\langle X\rangle_Y$	X is combined with the formula Y
$\{X\}_K$	X is encrypted by the key K
$P\overset{K}{\longleftrightarrow}Q$	P and Q communicate using shared key K
SK	The session key used in the current session

5.3.2 규칙

BAN logic 분석을 위한 필수 규칙들의 표기법 및 의미는 다음과 같다.

- Message meaning rule : 만약 P가 비밀 암호 키 K를 Q와 공유하고 있는 사실을 신뢰하며 K로 암호화된 메시지 X를 목격하면 P는 Q가 X를 언급한 사실을 신뢰한다. Message meaning rule은 식 (1)과 같다.

$$\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,\ P\triangleleft\{X\}_K}{P|\equiv Q|\sim X} \tag{1}$$

- Nonce verification rule : 만약 P가 X를 이번 세션에만 사용된 변수임을 신뢰하고 Q가 X를 언급한 사실을 신뢰하면 P는 Q가 X를 언급한 사실을 신뢰한다. Nonce verification rule은 식 (2)과 같다.

$$\frac{P|\equiv\#(X),\ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X} \tag{2}$$

- Jurisdiction rule : 만약 P는 Q가 X를 제어하는 사실을 신뢰하고 Q가 X를 언급한 사실을 신뢰하면 P는 X를 신뢰한다. Freshness rule은 식 (3)과 같다.

$$\frac{P|\equiv Q|\Rightarrow X,\ P|\equiv Q|\equiv X}{P|\equiv X} \tag{3}$$

- Freshness rule : 만약 P가 X를 이번 세션에만 사용된 변수임을 신뢰하면 P는 $(X,\ Y)$에 대한 현재성을 신뢰한다. Freshness rule은 식 (4)과 같다.

$$\frac{P|\equiv(X,Y)}{P|\equiv X} \tag{4}$$

- Belief rule : 만약 P가 $(X,\ Y)$를 신뢰하면 P는 X를 신뢰한다. Belief rule은 식 (5)과 같다.

$$\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)} \tag{5}$$

5.3.3 보안 목표

제안한 방식에서 인증 과정 후 키 합의를 수행하고 있으므로 BAN logic 분석 결과 안전성을 보장하기 위하여 만족해야하는 보안 목표는 다음과 같다.

Goal 1.
$U_i|\equiv(U_i\overset{SK}{\longleftrightarrow}S_j)$
Goal 2.
$U_i|\equiv S_j|\equiv(U_i\overset{SK}{\longleftrightarrow}S_j)$
Goal 3.
$S_j|\equiv(U_i\overset{SK}{\longleftrightarrow}S_j)$
Goal 4.
$S_j|\equiv U_i|\equiv(U_i\overset{SK}{\longleftrightarrow}S_j)$

5.3.4 가정

제안한 방식에서 BAN logic 분석을 위한 초기 상태 가정은 다음과 같다.

A1. $GWN|\equiv\#(T_1)$
A2. $GWN|\equiv\#(T_2)$
A3. $S_j|\equiv\#(T_3)$
A4. $U_i|\equiv\#(T_4)$
A5. $GWN|\equiv\#(K_1)$
A6. $GWN|\equiv\#(K_2)$
A7. $S_j|\equiv\#(K_1'=K_1)$

A8. $U_i \mid \equiv \#(K_2' = K_2)$

A9. $U_i \mid \equiv (U_i \xleftarrow{X_i = h(ID_i \| X_{GWN})} GWM)$

A10. $GWN \mid \equiv (U_i \xleftarrow{X_i = h(ID_i \| X_{GWN})} GWM)$

A11. $S_j \mid \equiv (S_j \xleftarrow{f_j = h(SID_i \| X_{GWN})} GWM)$

A12. $GWN \mid \equiv (S_j \xleftarrow{f_j = h(SID_i \| X_{GWN})} GWM)$

A13. $GWN \mid \equiv (U_i \xleftarrow{X_i} GWN)$

A14. $GWN \mid \equiv (S_j \xleftarrow{X_i} GWN)$

A15. $GWN \mid \equiv U_i \mid \equiv (S \xleftarrow{K_1} GWN)$

A16. $GWN \mid \equiv U_i \mid \equiv (U_i \xleftarrow{ID_i} GWN)$

A17. $GWN \mid \equiv S_j \mid \equiv (S_j \xleftarrow{SID_j} GWN)$

A18. $GWN \mid \equiv S_j \mid \equiv (S \xleftarrow{K_2} GWN)$

A19. $S_j \mid \equiv GWN \mid \equiv (S_j \xleftarrow{K_1' = K_1} GWN)$

A20. $U_i \mid \equiv GWN \mid \equiv (U_i \xleftarrow{K_2' = K_2} GWN)$

A21. $S_j \mid \equiv U_i \mid \equiv (U_i \xleftarrow{K_1' = K_1} S_j)$

A22. $U_i \mid \equiv S_j \mid \equiv (U_i \xleftarrow{K_2' = K_2} S_j)$

5.3.5 이상화 형태

제안한 방식에서 전송되는 각 파라미터를 BAN logic 분석을 위하여 주요 파라미터를 포함한 이상화 형태로 변환하여야하며 변환된 이상화 형태는 다음과 같다.

Message 1.

$$U_i \xleftarrow{\text{Via } S_j} GWN : \langle ID_i, T_1, (U_i \xleftarrow{ID_i} GWN) \rangle_{\hat{x}}$$

Message 2.

$$U_i \xleftarrow{\text{Via } S_j} GWN : \langle K_1, M_1, M_2, T_1, (U_i \xleftarrow{ID_i} GWN), (U_i \xleftarrow{K_1} GWN) \rangle_{X_i}$$

Message 3.

$$S_j \longrightarrow GWN : \langle SID_j, T_2, S_j \xrightarrow{SID_j} GWN \rangle_{X_{GWN-j}}$$

Message 4.

$$S_j \longrightarrow GWN : \langle SID_j, K_2, M_4, T_1, T_2, f_j, (S_j \xrightarrow{SID_j} GWN), S_j \xrightarrow{K_2} GWN \rangle_{X_{GWN-j}}$$

Message 5.

$$GWN \longrightarrow S_j : \langle R_2, T_3, (S_j \xleftarrow{SID_j} GWN), (S_j \xleftarrow{K_1' = K_1} GWN) \rangle_{f_j' = f_i}$$

Message 6.

$$U_i \xleftarrow{\text{Via } GWN} S_j : \langle K_1' = K_1, T_3, (S_j \xleftarrow{SID_j} GWN), (S_j \xleftarrow{K_1' = K_1} GWN), (U_i \xleftarrow{SK} S_j) \rangle_{f_j' = f_j}$$

Message 7.

$$GWN \xleftarrow{\text{Via } S_j} U_i : \langle K_2' = K_2, R_1, T_3, (U_i \xleftarrow{\text{Via } ID_i} GWN), (U_i \xleftarrow{K_2' = K_2} GWN) \rangle_{X_i}$$

Message 8.

$$S_j \longrightarrow U_i : \langle R_1, T_3, T_4, (U_i \xleftarrow{ID_i} GWN), (U_i \xleftarrow{K_2' = K_2} GWN), (U_i \xleftarrow{SK} S_j) \rangle_{SK}$$

5.3.6 증명

Step 1. 이상화 형태 Message 1과 표기법에 따라 다음 식 (6)을 얻는다.

$$(S_1) : GWN \triangleleft \langle ID_i, T_1, (U_i \xleftarrow{ID_i} GWN) \rangle_{X_i} \quad (6)$$

Step 2. S_1과 A_{13}에 따라 message meaning rule을 적용하여 다음 식 (7)을 얻는다.

$$(S_2) : GWN \mid \equiv U_i \mid \sim \langle ID_i, T_1, (U_i \xleftarrow{ID_i} GWN) \rangle \quad (7)$$

Step 3. A_1에 따라 freshness rule을 적용하여 식 (8)을 얻는다.

$$(S_3) : GWN \mid \equiv \# \langle ID_i, T_1, (U_i \xleftarrow{ID_i} GWN) \rangle \quad (8)$$

Step 4. S_2과 S_3에 따라 nonce verification rule을 적용하여 식 (9)을 얻는다.

$$(S_4) : GWN \mid \equiv U \mid \equiv \langle ID_i, T_1, (U_i \xleftarrow{ID_i} GWN) \rangle \quad (9)$$

Step 5. S_4로부터 belief rule을 적용하여 식 (10)을 얻는다.

$$(S_5): GWN \mid \equiv U \mid \equiv \left\langle (U_i \xleftrightarrow{ID_i} GWN) \right\rangle \quad (10)$$

Step 6. S_6와 A_5에 따라 jurisdiction rule을 적용하여 식 (11)을 얻는다.

$$(S_6): GWN \mid \equiv (U_i \xleftrightarrow{ID_i} GWN) \quad (11)$$

Step 7. 이상화 형태 Message 2와 표기법에 따라 다음 식 (12)을 얻는다.

$$(S_7): GWN \triangleleft \left\langle K_1, M_1, M_2, T_1, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{K_1} GWN) \right\rangle_{X_i} \quad (12)$$

Step 8. S_7과 A_{10}에 따라 message meaning rule을 적용하여 다음 식 (13)을 얻는다.

$$(S_8): GWN \mid \equiv U_i \mid \sim (K_1, M_1, M_2, T_1, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{K_1} GWN)) \quad (13)$$

Step 9. A_5와 A_1에 따라 freshness rule을 적용하여 식 (14)을 얻는다.

$$(S_9): GWN \mid \equiv \#(K_1, M_1, M_2, T_1, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{K_1} GWN)) \quad (14)$$

Step 10. S_8과 S_9에 따라 nonce verification rule을 적용하여 식 (15)을 얻는다.

$$(S_{10}): GWN \mid \equiv U_i \mid \equiv (K_1, M_1, M_2, T_1, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{K_1} GWN)) \quad (15)$$

Step 11. S_{10}, S_5 및 S_6에 따라 belief rule을 적용하여 식 (16)을 얻는다.

$$(S_{11}): GWN \mid \equiv U_i \mid \equiv (U_i \xleftrightarrow{K_1} GWN) \quad (16)$$

Step 12. A_{15}와 S_{11}에 따라 jurisdiction rule을 적용하여 게이트웨이는 식 (17)을 얻는다.

$$(S_{12}): GWN \mid \equiv (U_i \xleftrightarrow{K_1} GWN) \quad (17)$$

Step 13. 이상화 형태 Message 3과 표기법에 따라 다음 식 (18)을 얻는다.

$$(S_{13}): GWN \triangleleft \left\langle SID_j, T_2, (S_j \xleftrightarrow{SID_j} GWN) \right\rangle_{X_{GWN-j}} \quad (18)$$

Step 14. S_{13}과 A_{14}에 따라 message meaning rule을 적용하여 다음 식 (19)을 얻는다.

$$(S_{14}): GWN \mid \equiv S_j \mid \sim \left\langle SID_j, T_2, (S_j \xleftrightarrow{SID_j} GWN) \right\rangle \quad (19)$$

Step 15. A_2에 따라 freshness rule을 적용하여 다음 식 (20)을 얻는다.

$$(S_{15}): GWN \mid \equiv \# \left\langle SID_j, T_2, (S_j \xleftrightarrow{SID_j} GWN) \right\rangle \quad (20)$$

Step 16. S_{14}와 S_{15}에 따라 nonce verification rule을 적용하여 다음 식 (21)을 얻는다.

$$(S_{16}): GWN \mid \equiv S_j \mid \equiv \left\langle SID_i, T_2, (S_j \xleftrightarrow{SID_j} GWN) \right\rangle \quad (21)$$

Step 17. S_{16}에 따라 belief rule을 적용하여 다음 식 (22)을 얻는다.

$$(S_{17}): GWN \mid \equiv S_j \mid \equiv \left\langle (S_j \xleftrightarrow{SID_j} GWN) \right\rangle \quad (22)$$

Step 18. A_{17}과 S_{17}에 따라 jurisdiction rule을 적용하여 다음 식 (23)을 얻는다.

$$(S_{18}): GWN \mid \equiv (S_j \xleftrightarrow{SID_j} GWN) \quad (23)$$

Step 19. 이상화 형태 Message 4과 표기법에 따라 다음 식 (24)을 얻는다.

$$(S_{19}): GWN \triangleleft \left\langle SID_j, K_2, M_4, T_1, T_2, f_j, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_2} GWN) \right\rangle_{X_{GWN-j}} \quad (24)$$

Step 20. S_{19}와 A_{12}에 따라 message meaning rule을 적용하여 다음 식 (25)을 얻는다.

$$(S_{20}): GWN \mid \equiv S_j \mid \sim \left\langle SID_j, K_2, M_4, T_1, T_2, f_j, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_2} GWN) \right\rangle \quad (25)$$

Step 21. A_2와 A_6에 따라 freshness rule을 적용하여 다음 식 (26)을 얻는다.

$$(S_{21}): GWN \equiv \#\langle SID_j, K_2, M_4, T_1, T_2, f_j, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_2} GWN)\rangle \quad (26)$$

Step 22. S_{20}과 S_{21}에 따라 nonce verification rule을 적용하여 다음 식 (27)을 얻는다.

$$(S_{22}): GWN \equiv S_j \equiv \langle SID_j, K_2, M_4, T_1, T_2, f_j, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_2} GWN)\rangle \quad (27)$$

Step 23. S_{22}, S_{17} 및 S_{18}에 따라 belief rule을 적용하여 다음 식 (28)을 얻는다.

$$(S_{23}): GWN \equiv S_j \equiv \langle (S_j \xleftrightarrow{K_2} GWN)\rangle \quad (28)$$

Step 24. A_{18}과 S_{23}에 따라 jurisdiction rule을 적용하여 다음 식 (29)을 얻는다.

$$(S_{24}): GWN \equiv (S_j \xleftrightarrow{K_2} GWN) \quad (29)$$

Step 25. 이상화 형태 Message 5과 표기법에 따라 다음 식 (30)을 얻는다.

$$(S_{25}): S_j \lhd \langle R_2, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN)\rangle_{f_j'=f_j} \quad (30)$$

Step 26. S_{25}와 A_{11}에 따라 message meaning rule을 적용하여 다음 식 (31)을 얻는다.

$$(S_{26}): S_j \equiv GWN \sim \langle R_2, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN)\rangle \quad (31)$$

Step 27 A_3과 A_7에 따라 freshness rule을 적용하여 다음 식 (32)을 얻는다.

$$(S_{27}): S_j \equiv \#\langle R_2, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN)\rangle \quad (32)$$

Step 28. S_{26}과 S_{27}에 따라 nonce verification rule을 적용하여 다음 식 (33)을 얻는다.

$$(S_{28}): S_j \equiv GWN \equiv \langle R_2, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN)\rangle \quad (33)$$

Step 29. S_{28}, S_{17} 및 S_{18}에 따라 belief rule을 적용하여 다음 식 (34)을 얻는다.

$$(S_{29}): S_j \equiv GWN \equiv \langle (S_j \xleftrightarrow{K_1'=K_1} GWN)\rangle \quad (34)$$

Step 30. A_{19}와 S_{29}에 따라 jurisdiction rule을 적용하여 다음 식 (35)을 얻는다.

$$(S_{30}): S_j \equiv (S_j \xleftrightarrow{K_1'=K_1} GWN) \quad (35)$$

Step 31. 이상화 형태 Message 6과 표기법에 따라 다음 식 (36)을 얻는다.

$$(S_{31}): S_j \lhd \langle K_1' = K_1, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN), (S_j \xleftrightarrow{SK} GWN)\rangle_{f_j'=f_j} \quad (36)$$

Step 32. S_{31}과 A_{11}에 따라 message meaning rule을 적용하여 다음 식 (37)을 얻는다.

$$(S_{32}): S_j \equiv U_i \sim \langle K_1' = K_1, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN), (S_j \xleftrightarrow{SK} GWN)\rangle \quad (37)$$

Step 33. A_3과 A_7에 따라 freshness rule을 적용하여 다음 식 (38)을 얻는다.

$$(S_{33}): S_j \equiv \#\langle K_1' = K_1, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN), (S_j \xleftrightarrow{SK} GWN)\rangle \quad (38)$$

Step 34. S_{26}과 S_{27}에 따라 nonce verification rule을 적용하여 다음 식 (39)을 얻는다.

$$(S_{34}): S_j \mid \equiv U_i \mid \equiv \left\langle K_1' = K_1, T_3, (S_j \xleftrightarrow{SID_j} GWN), (S_j \xleftrightarrow{K_1'=K_1} GWN), (S_j \xleftrightarrow{SK} GWN) \right\rangle \quad (39)$$

Step 35. S_{29}, S_{34}, S_{17} 및 S_{18}에 따라 belief rule을 적용하여 다음 식 (40)을 얻는다.

$$(S_{35}): S_j \mid \equiv U_i \mid \equiv \left\langle (U_i \xleftrightarrow{SK} S_j) \right\rangle \quad \textbf{(Goal 4)} \quad (40)$$

Step 36. A_{19}와 S_{29}에 따라 jurisdiction rule을 적용하여 다음 식 (41)을 얻는다.

$$(S_{36}): S_j \mid \equiv (U_i \xleftrightarrow{SK} S_j) \quad \textbf{(Goal 3)} \quad (41)$$

Step 37. 이상화 형태 Message 7과 표기법에 따라 다음 식 (42)을 얻는다.

$$(S_{37}): U_i \triangleleft \left\langle K_2' = K_2, R_1, T_3, (U_i \xleftrightarrow{\text{Via } ID_i} GWN), (S_j \xleftrightarrow{K_2'=K_2} GWN) \right\rangle_{X_i} \quad (42)$$

Step 38. S_{37}과 A_9에 따라 message meaning rule을 적용하여 다음 식 (43)을 얻는다.

$$(S_{38}): U_i \mid \equiv GWN \mid \sim \left\langle K_2' = K_2, R_1, T_3, (U_i \xleftrightarrow{\text{Via } ID_i} GWN), (S_j \xleftrightarrow{K_2'=K_2} GWN) \right\rangle \quad (43)$$

Step 39. A_8에 따라 freshness rule을 적용하여 다음 식 (44)를 얻는다.

$$(S_{39}): U_i \mid \equiv \#\left\langle K_2' = K_2, R_1, T_3, (U_i \xleftrightarrow{\text{Via } ID_i} GWN), (S_j \xleftrightarrow{K_2'=K_2} GWN) \right\rangle \quad (44)$$

Step 40. S_{38}과 S_{39}에 따라 nonce verification rule을 적용하여 다음 식 (45)을 얻는다.

$$(S_{40}): U_i \mid \equiv GWN \mid \equiv \left\langle K_2' = K_2, R_1, T_3, (U_i \xleftrightarrow{\text{Via } ID_i} GWN), (S_j \xleftrightarrow{K_2'=K_2} GWN) \right\rangle \quad (45)$$

Step 41. S_{40}, S_5 및 S_6에 따라 belief rule을 적용하여 식 (46)을 얻는다.

$$(S_{41}): U_i \mid \equiv GWN \mid \equiv \left\langle (U_i \xleftrightarrow{K_2'=K_2} GWN) \right\rangle \quad (46)$$

Step 42. S_{41}과 A_{20}에 따라 jurisdiction rule을 적용하여 서버는 식 (47)을 얻는다.

$$(S_{42}): U_i \mid \equiv (U_i \xleftrightarrow{K_2'=K_2} GWN) \quad (47)$$

Step 43. 이상화 형태 Message 8과 표기법에 따라 다음 식 (48)을 얻는다.

$$(S_{43}): U_i \triangleleft \left\langle R_1, T_3, T_4, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{X_i} GWN), (U_i \xleftrightarrow{K_2'=K_2} GWN), (U_i \xleftrightarrow{SK} S_j) \right\rangle_{SK} \quad (48)$$

Step 44. S_{43}과 A_9에 따라 message meaning rule을 적용하여 다음 식 (49)을 얻는다.

$$(S_{44}): U_i \mid \equiv S_j \mid \sim \left\langle R_1, T_3, T_4, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{X_i} GWN), (U_i \xleftrightarrow{K_2'=K_2} GWN), (U_i \xleftrightarrow{SK} S_j) \right\rangle \quad (49)$$

Step 45. A_4와 A_8에 따라 freshness rule을 적용하여 다음 식 (50)를 얻는다.

$$(S_{45}): U_i \mid \equiv \#\left\langle R_1, T_3, T_4, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{X_i} GWN), (U_i \xleftrightarrow{K_2'=K_2} GWN), (U_i \xleftrightarrow{SK} S_j) \right\rangle \quad (50)$$

Step 46. S_{44}와 S_{45}에 따라 nonce verification rule을 적용하여 다음 식 (51)을 얻는다.

$$(S_{46}): U_i \mid \equiv S_j \mid \equiv \left\langle R_1, T_3, T_4, (U_i \xleftrightarrow{ID_i} GWN), (U_i \xleftrightarrow{X_i} GWN), (U_i \xleftrightarrow{K_2'=K_2} GWN), (U_i \xleftrightarrow{SK} S_j) \right\rangle \quad (51)$$

Step 47. S_{41}, S_5, S_6 및 S_{46}에 따라 belief rule을

적용하여 다음 식 (52)을 얻는다.

$$(S_{47}): U_i | \equiv S_j | \equiv \langle (U_i \xleftrightarrow{SK} S_j) \rangle \quad \textbf{(Goal 2)} \quad (52)$$

Step 48. S_{42}, A_{22}및 식 (47)에 따라 jurisdiction rule을 적용하여 다음 식 (53)을 얻는다.

$$(S_{48}): U_i | \equiv (U_i \xleftrightarrow{SK} S_j) \quad \textbf{(Goal 1)} \quad (53)$$

Ⅵ. 결 론

WSN 환경에서 사용자는 언제 어디서나 편리하게 IoT, health-care, smart home, smart grid 등 다양한 서비스를 제공받을 수 있다. 그러나 이러한 서비스들은 인터넷을 통하여 제공되므로 공개 채널로 전송되는 민감한 정보가 공격자에게 노출될 경우 사용자에게 프라이버시가 침해될 수 있다. 따라서 합법적인 사용자만 서비스를 사용하고 데이터에 접근할 수 있도록 하는 인증 방식이 반드시 필요하다. 또한 WSN 환경에서 센서는 제한된 배터리 용량과 연산 능력을 가지므로 이를 고려한 효율적인 인증 방식이 요구된다.

본 논문에서는 Tai 등이 제안한 WSN 환경에서 안전한 인증 방식이 스마트카드 도난 공격 및 세션 키 노출 공격에 취약함을 보이고 상호 인증을 제공하지 않음을 보였다. 또한 이를 개선한 경량화 된 인증 및 키 합의 방식을 제안하였으며 informal 보안 분석을 통하여 제안한 인증 방식이 스마트카드 도난 공격, 세션 키 노출 공격 등 다양한 공격에 안전함을 보이고 BAN logic 분석을 통하여 제안한 방식이 상호 인증을 제공함을 증명하였다. 그리고 제안한 방식과 기존의 인증 방식들의 성능을 비교를 분석하여 제안한 방식이 기존의 Tai 등의 방식보다 효율적임을 보였다. 따라서 제안한 인증 방식은 저사양 및 저전력 성능을 가지는 센서를 고려하여 제안되었으며 실제 WSN 환경에서 보다 효율적으로 적용 가능한 인증 방식이다.

References

[1] Q. Jiang, J. F. Ma, X. Lu, and Y. L. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Networking and Appl.*, vol. 8, no. 6, pp. 1070-1081, 2015.

[2] D. Wang and P. Wang, "An efficient identity based conditional privacy preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics and Secur.*, vol. 10, no. 12, pp. 2681-2691, 2015.

[3] Y. S. Choi, D. H. Lee, J. Y. Kim, J. W. Jung, J. H. Nam, and D. H. Won "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081-10106, 2014.

[4] K. Chatterjee, A. De, and D. Gupta, "A secure and efficient authentication protocol in wireless sensor network," *Wireless Pers. Commun.*, vol. 81, no. 1, pp. 17-37, 2015.

[5] Y. H. Park and Y. H. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, pp. 1-17, 2016.

[6] R. Amin and G. P. Biswas, "A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, no. 2, pp. 58-80, 2016.

[7] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network based smart vehicular system," *Vehicular Commun.*, vol. 9, pp. 64-71, 2017.

[8] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767-4779, 2011.

[9] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96-112, 2014.

[10] Y. F. Chang, J. H. Yang, W. H. Li, and W. L. Tai, "Comments on an IoT notion based authentication and key agreement scheme for heterogeneous ad hoc wireless sensor

networks," in *Proc. the 3rd Annu. Conf. on Eng. and Inf. Technol.*, pp. 264-270, 2015.

[11] W. L. Tai, Y. F. Chang, and W. H. Li, "An IoT notion based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," *J. Inf. Secur. and Appl.*, vol. 34, no. 2, pp. 133-141, 2011.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *CRYPTO'99*, pp. 388-397, 1999.

[13] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Computer Syst.*, vol. 8, no. 1, pp. 18-36, 1990.

[14] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal credential based mutual authentication and key agreement scheme for wireless sensor networks," *J. Network and Comput. Appl.*, vol. 36, no. 1, pp. 316-323, 2013.

유 성 진 (SungJin Yu)

2017년 2월 : 대구대학교 전자공학과 학사

2017년 3월~현재 : 경북대학교 대학원 전자공학부 석사과정

<관심분야> 정보보호, 무선통신보안, 네트워크보안

박 기 성 (KiSung Park)

2015년 2월 : 경북대학교 산업전자전기공학부 학사

2017년 2월 : 경북대학교 대학원 전자공학부 석사

2017년 3월~현재 : 경북대학교 대학원 전자공학부 박사과정

<관심분야> 정보보호, 네트워크보안, PQ암호

박 요 한 (YoHan Park)

2006년 2월 : 경북대학교 전자전기컴퓨터학부 졸업

2008년 2월 : 경북대학교 전자공학과 석사

2013년 2월 : 경북대학교 전자전기컴퓨터학부 박사

2017년 2월~현재 : 나사렛대학교 조교수

<관심분야> 암호학이론, 무선통신보안, IoT 보안

박 영 호 (YoungHo Park)

1989년 2월 : 경북대학교 전자공학과 학사

1991년 2월 : 경북대학교 전자공학과 석사

1995년 2월 : 경북대학교 전자공학과 박사

1996년~2008년 : 상주대학교 전자전기공학부 교수

2003년~2004년 : Oregon State Univ. 방문 교수

2008년~현재 : 경북대학교 전자공학부 교수

<관심분야> 정보보호, 네트워크보안, 모바일 컴퓨팅