무선 센서 네트워크 환경에서 효율적인 인증 및 키 합의 방식 개발

권덕규, 이준영, 유성진*, 박영호

경북대학교, *한국전자통신연구원

kdk145@knu.ac.kr, harry250@knu.ac.kr, *sj.yu@etri.re.kr, parkyh@knu.ac.kr

Design of Efficient Authentication and Key Agreement Scheme for Wireless Sensor Networks

Kwon Deok Kyu, Lee Joon Young, Yu Sung Jin*, Park Young Ho

Kyungpook National Univ, *Electronic and Telecommunications Research Institute.

요 약

2020년, Moghadam 등은 무선 센서 네트워크(Wireless Sensor Network) 환경에서 효율적인 인증 및 키 합의 방식을 제안하였다. 본 논문에서는 비정형 보안 분석을 통하여 Moghadam 등이 제안한 인증 및 키 합의 방식이 내부자 공격 및 세션 특정 난수 유출 공격에 취약함을 증명하고 완전 순방향 비밀성을 보장할 수 없음을 입증한다. 또한 증명한 보안 취약점을 바탕으로 Moghadam 등의 방식을 효율적으로 개선할 수 있는 경량화 인증 및 키 합의 방식을 제안한다.

Ⅰ. 서 론

최근 무선 통신 기술의 발전으로 무선 센서 네트워크(Wireless Sensor Network)는 헬스 케어[1], 사물 인터넷(Internet of Things)[2] 및 스마트 홈[3] 등 다양한 환경에 적용되고 있다. 그러나 무선 센서 네트워크 환경에서 사용자는 공개 채널을 통해 게이트웨이 및 센서와 데이터를 교환하기 때문에 사용자의 민감한 정보가 공격자에게 유출되어 다양한 보안 공격에 취약해질 수 있다. 따라서 무선 센서 네트워크 환경에서 사용자의 개인 정보를 보호할 수 있는 안전하고 효율적인 인증 및 키 합의 방식에 대한 연구가 필요하다[4,5].

2020년, Moghadam 등은[6] Elliptic Curve Diffie-Hellman(ECDH)을 이용한 인증 및 키 합의 방식을 제안하였다. 본 논문에서는 Moghadam 등의 방식이 내부자 공격 및 세션 특정 난수 유출 공격에 취약하며 완전 순방향 비밀성을 보장하지 못함을 입증한다. 또한 Moghadam 등의 방식이 가진 문제점을 개선한 효율적인 인증 및 키 합의 방식을 제안한다.

Ⅱ. 시스템 모델

본 논문에서 사용하는 시스템 모델은 그림 1과 같다.

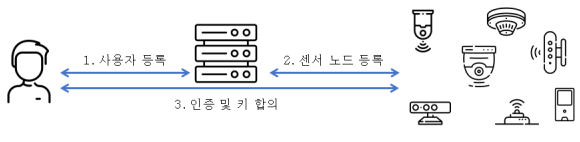

그림 1. 시스템 모델

사용자와 센서 노드는 게이트웨이에 자신을 등록한다. 이후 인증 및 키 합의 단계에서 사용자는 센서 노드와 통신을 수행하기 위해 로그인 절차를 수행하고 게이트웨이에 인증 요청 메시지를 전송한다. 게이트웨이는 사용자의 합법성을 판단한 후 센서 노드에게 메시지를 전송해 키 합의를 시도한다. 센서 노드는 게이트웨이 및 사용자의 합법성을 확인한 뒤 세션 키를 계산하고 게이트웨이에게 메시지를 송신한다. 게이트웨이는 수신한 메시지로 세션 키를 계산한 후 사용자에게 메시지를 전송한다. 최종적으로 사용자는 해당 메시지를 이용하여 세션 키를 합의하게 된다.

Ⅲ. Moghadam 등이 제안한 인증 및 키 합의 방식

Moghadam 등이 제안한 방식은 사용자 등록, 센서 노드 등록 및 인증 및 키 합의 단계로 구성되며 본 논문에서는 인증 및 키 합의 단계를 소개한다. Moghadam 등의 방식에서 사용하는 매개 변수는 표 1과 같다.

표 1. 매개 변수

기호	의미
U_i, GW, S_j	사용자, 게이트웨이, 센서 노드
ID_i, PW_i, PID_i	사용자의 ID, 패스워드, Pseudo-ID
SID_j	센서 노드의 ID
k_{GWN}	게이트웨이의 마스터 키
KG	센서 노드와 게이트웨이 간의 공유 키
G, P	타원 곡선 군, 생성자
T_k	타임스탬프
sk	세션 키
E_k, D_k	키 k를 이용한 암호화/복호화 함수
$\|$	결합 연산자
$\oplus$	Exclusive-OR 연산자
$h(\cdot)$	단 방향 해시 함수

3.1 Moghadam 등의 인증 및 키 합의 단계

Moghadam 등이 제안한 인증 및 키 합의 단계는 그림 2와 같다.

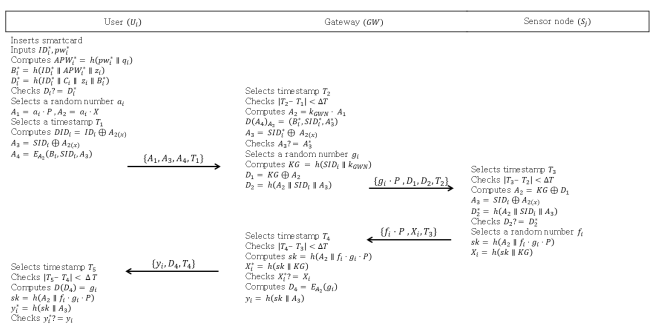

그림 2. Moghadam 등이 제안한 인증 및 키 합의 단계.

Ⅳ. Moghadam 등이 제안한 방식의 보안 취약점 및 대응 방안

본 논문에서는 비정형 보안 분석을 통해 Moghadam 등의 방식이 가진 취약점을 입증하고 이에 대한 대응 방안을 제시한다. Moghadam 등이 제안한 방식의 보안 취약점 및 대응 방안은 다음과 같다.

4.1 보안 취약점

4.1.1 내부자 공격

공격자는 네트워크의 합법적인 사용자 U_i로 등록하고 게이트웨이 GW 및 센서 노드 S_j와 인증 및 키 합의를 시도하는 과정에서 공개 채널 상의 메시지 $\{g_i \cdot P, D_1, D_2, T_2\}$를 얻는다. D_1과 자신이 생성한 A_2를 이용하여 공격자는 GW와 S_j간의 공유 키 $KG = D_1 \oplus A_2$를 계산할 수 있다. 공격자는 다른 합법적인 사용자 U_i^l의 인증 및 키 합의에서 전송하는 메시지 $\{g_i^l \cdot P, D_1^l, D_2^l, T_2^l\}$를 얻는다. 공격자는 KG를 사용하여 U_i^l의 비밀 값 $A_2^l = D_i^l \oplus KG$를 계산하고 메시지 $\{g_i^l, D_4^l, T_4^l\}$의 값 $D_4^l = E_{A_2^l}(g_i^l)$을 복호화한다. 마지막으로 공격자는 메시지 $\{f_i^l \cdot P, X_i^l, T_3^l\}$를 이용하여 U_i^l의 세션 키 $sk^l = h(A_2^l \| f_i^l \cdot g_i^l \cdot P)$를 계산할 수 있으므로 Moghadam 등의 방식이 내부자 공격에 안전하지 않음을 입증할 수 있다.

4.1.2 세션 특정 난수 유출 공격

세션 상의 특정 난수 a_i가 유출되었을 때 공격자는 합법적인 사용자 U_i의 비밀 값 $A_2 = a_i \cdot X$를 계산할 수 있다. 공격자는 공개 채널 상의 메시지 $\{y_i, D_4, T_4\}$와 A_2를 이용하여 $D_4 = E_{A_2}(g_i)$를 복호화한다. 결론적으로 메시지 $\{f_i \cdot P, X_i, T_3\}$와 g_i 및 A_2를 통해 공격자는 세션 키 $sk = h(A_2 \| f_i \cdot g_i \cdot P)$를 계산할 수 있다. 따라서 Moghadam 등의 방식은 세션 특정 난수 유출 공격에 취약하다.

4.1.3 완전 순방향 비밀성

GW의 마스터 키 k_{GWN}이 노출되었을 때 공격자는 사용자 U_i의 인증 요청 메시지 $\{A_1, A_3, A_4, T_1\}$를 이용하여 U_i의 비밀 값 $A_2 = A_1 \cdot k_{GWN}$을 계산할 수 있다. A_2를 통해 공격자는 메시지 $\{y_i, D_4, T_4\}$에서 $g_i = D_{A_2}(D_4)$를 계산하고 $\{f_i \cdot P, X_i, T_3\}$를 사용하여 세션 키 $sk = h(A_2 \| f_i \cdot g_i \cdot P)$를 계산한다. 따라서 Moghadam 등이 제안한 방식은 완전 순방향 비밀성을 보장하지 않는다.

4.2 대응 방안

Moghadam 등이 제안한 방식은 내부자 공격 및 세션 특정 난수 유출 공격에 취약하며 완전 순방향 비밀성을 보장하지 않는 문제점을 가지고 있다. 이러한 문제점을 개선하기 위해 본 논문에서는 GW가 생성한 난수 및 사용자의 Pseudo-ID를 이용하여 공유 키 KG를 암호화하는 방안을 제시한다. 또한 타원곡선 암호 체계가 가진 계산 부하를 줄이고 효율성을 높이기 위해 경량화 암호 체계를 활용한 인증 및 키 합의 방식을 제안한다.

Ⅴ. 제안한 인증 및 키 합의 방식

제시한 대응 방안을 바탕으로 본 논문에서 제안한 인증 및 키 합의 방식은 사용자 등록, 센서 노드 등록 및 인증 및 키 합의 단계로 구성된다.

5.1 사용자 등록 단계

본 논문에서 제안한 사용자 등록 단계는 그림 3과 같다.

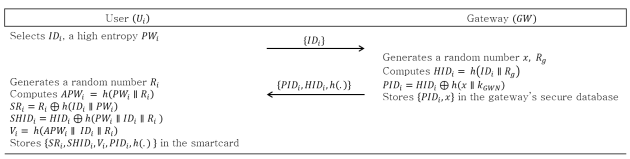

그림 3. 제안한 사용자 등록 단계.

5.2 센서 노드 등록 단계

본 논문에서 제안한 센서 노드 등록 단계는 그림 4와 같다.

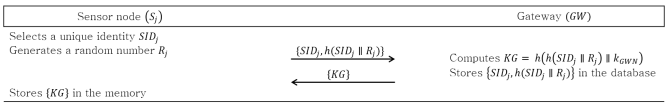

그림 4. 제안한 센서 노드 등록 단계.

5.3 인증 및 키 합의 단계

본 논문에서 제안한 인증 및 키 합의 단계는 그림 5와 같다.

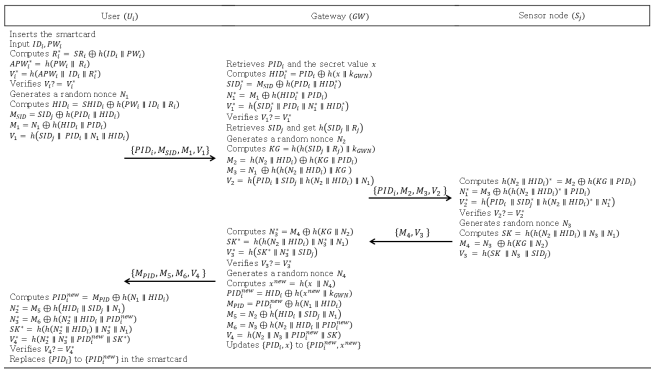

그림 5. 제안한 인증 및 키 합의 단계.

Ⅵ. 결론

본 논문에서는 Moghadam 등이 제안한 인증 및 키 합의 방식의 보안 취약점을 분석하였다. 비정형 보안 분석을 통해 Moghadam 등의 방식은 내부자 공격 및 세션 특정 난수 유출 공격에 취약하며 완전 순방향 비밀성을 보장하지 않음을 입증하였다. Moghadam 등이 제안한 방식의 문제점을 개선하기 위해 본 논문에서는 게이트웨이가 생성한 난수와 사용자의 Pseudo-ID를 이용하여 공유 키를 암호화하는 방법과 경량화 암호 체계를 사용하여 효율성을 높이는 인증 및 키 합의 방식을 제안하였다. 따라서 공격자는 합법적인 사용자로 네트워크에 등록하거나 마스터 키를 획득하여도 세션의 중요한 정보를 계산할 수 없다. 그러므로 제안한 방식은 무선 센서 네트워크 환경에 적합한 인증 방식이며 추후 제안한 방식을 실제 구현하여 안전하고 효율적인 보안 체계를 설계할 예정이다.

참 고 문 헌

[1] Park, K., Noh, S., Lee, H., Das A. K., Kim, M., Park, Y., and Wazid, M. “LAKS-NVT: Provably Secure And Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things,” IEEE Access, vol 8, pp. 119387-119404, 2020.

[2] Yu, S., Park, K., and Park, Y. “A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment,” Sensors, vol. 19, no. 16, pp. 1-20, 2019.

[3] Oh, J., Yu, S., Lee, J., Son, S., Kim, M., and Park, Y. “A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes,” Sensors, vol 21, no. 4, pp. 1-24, 2021.

[4] Yu, S., and Park, Y. “SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks,” Sensors, vol. 20, no. 15, pp. 1-26, 2020.

[5] Lee, J., Yu, S., Kim, M., Park, Y., and Das A. K. “On The Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks,” IEEE Access, vol 8, pp. 107046-107062, 2020.

[6] Moghadam M. F., Nikooghadam, M., Al Jabban M. A. B., Alishahi, M., Mortazavi, L., and Mohajerzadeh, A. “An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network,” IEEE Access, vol 8, pp. 73182 - 73192, 2020.