The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 4, pp.63-70, Aug. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.4.63
JIIBC 2015-4-8

계층적 무선 센서 네트워크를 위한 패스워드 기반 사용자 인증 스킴의 보안 취약점 분석

Analysis on Security Vulnerabilities of a Password-based User Authentication Scheme for Hierarchical Wireless Sensor Networks

주영도*

Young-Do Joo*

요 약 유비쿼터스 시대의 도래와 함께 센서를 기반으로 하는 무선 센서 네트워크의 응용 분야는 광범위하게 확산되고 있다. 따라서 무선 센서 네트워크에서 센서들로부터 수집되는 기밀 데이터를 허가 받지 않은 사용자로부터 보호하기 위해, 널리 사용되어지는 스마트카드와 패스워드 기반의 사용자 인증도 견고한 보안을 요구한다. 최근 무선 센서 네트워크는 클러스터 헤드와 센서 노드 이원화를 통해 운용상 보다 효과적인 계층적 무선 센서 네트워크로 전개 발전되고 있다. 2012년 Das 등은 계층적 무선 센서 네트워크에 실제 적용 가능한 동적 패스워드 기반 사용자 인증 스킴을 제안하였다. 본 논문은 안정성 분석을 통해 Das 등의 스킴이 그들의 주장과 달리 여전히 중간자 공격, 패스워드 추측 공격, 패스워드 변경 공격을 막을 수 없을 뿐 아니라, 필수적인 보안 요구사항인 사용자와 클러스터 헤드 간의 상호인증을 투명하게 제공하지 못함을 입증한다.

Abstract The numerous improved schemes of user authentication based on password have been proposed in order to prevent the data access from the unauthorized person. The importance of user authentication has been remarkably growing in the expanding application areas of wireless sensor networks. Recently, emerging wireless sensor networks possesses a hierarchy among the nodes which are divided into cluster heads and sensor nodes. Such hierarchical wireless sensor networks have more operational advantages by reducing the energy consumption and traffic load. In 2012, Das et al. proposed a user authentication scheme to be applicable for the hierarchical wireless sensor networks. Das et al. claimed that their scheme is effectively secure against the various security flaws. In this paper, author will prove that Das et al.'s scheme is still vulnerable to man-in-the-middle attack, password guessing/change attack and does not support mutual authentication between the user and the cluster heads.

Key Words : Hierarchical Wireless Sensor Network, Man-in-the-middle Attack, Mutual Authentication

Ⅰ. 서 론

무선 센서 네트워크(WSN: Wireless Sensor Network)는 수 많은 센서들이 무선으로 연결된 네트워크로서, 유비쿼터스 통신 시대의 도래와 함께 광범위한 응용분야에서 적용되어 다양한 통신 목적을 효과적으로 수행하고

*정회원, 강남대학교 컴퓨터미디어정보공학부
접수일자 2015년 7월 15일, 수정완료 2015년 8월 3일
게재확정일자 2015년 8월 7일

Received: 15 July, 2015 / Revised: 3 August, 2015 /
Accepted: 7 August, 2015
*Corresponding Author: ydjoo@kangnam.ac.kr
Dept. of Computer & Media Information, Kangnam University, Korea

있다. 최근에 무선 센서 네트워크는 센서의 에너지 소모를 줄이면서 제한된 데이터 전송/처리 능력을 향상시킴으로 운용상의 이점을 발휘할 수 있는 계층적 무선 센서 네트워크(HWSN: Hierarchical Wireless Sensor Network)로 진화되고 있다. WSN은 게이트웨이 노드(Gateway Node)에 해당하는 베이스 스테이션(BS: Base Station)과 센서 노드로 구성되어 있는 반면, HWSN은 센서 노드들이 H-센서(high-end sensor)와 L-센서(low-end sensor)의 두 가지 형태의 계층구조로 나누어 구성된다[1]. H-센서는 보다 큰 메모리 용량, 베터리 용량 및 데이터 처리 능력을 갖추고 있어 L-센서로부터 센싱 데이터를 수집한다. HWSN에서 H-센서는 클러스터 헤드(CH: Cluster Head)에 해당하며, 보다 많은 수의 L-센서는 하나의 클러스터를 구성하는 멤버로서 기존의 통상적인 센서 노드(SN: Sensor Node)에 해당한다. CH는 다른 CH들과 통신할 뿐 아니라, 자신의 클러스터 멤버들과 BS와의 통신 연결을 가능하게 한다. 궁극적으로 사용자가 HWSN으로부터 실시간 데이터를 획득하고자 하는 경우, 사용자는 접점인 BS를 통해 특정 CH로부터 사용자 인증을 받아야 한다. 그림 1은 계층적 무선 센서 네트워크 개념적인 구조를 보여주고 있다.

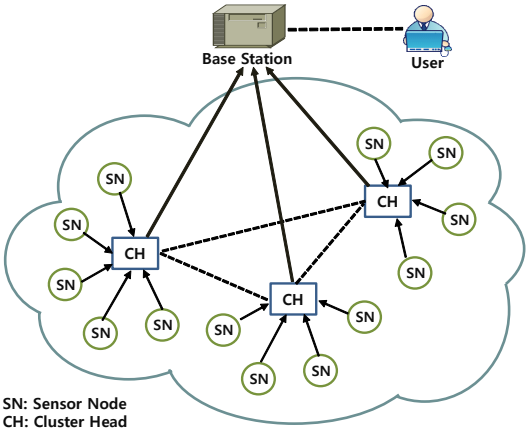

그림 1. 계층적 무선 센서 네트워크 구조
Fig. 1. Architecture of Hierarchical Wireless Sensor Network

따라서 HWSN에서 수집되는 중요한 기밀 데이터를 허가받지 않은 사용자가 불법으로 획득하는 것을 막기 위해 스마트카드 기반 사용자 인증은 주요한 보안 대책으로 사용된다. 특히 HWSN에서 SN과 CH가 공격자의 해킹에 노출되어 있어 보다 강력한 인증 프로토콜을 갖춘 사용자 인증 스킴이 요구된다. HWSN 환경의 점진적인 확산과 함께 데이터 무결성, 접근 통제 및 통신 보안을 위한 패스워드 기반의 다양한 사용자 인증 스킴들이 지속적으로 연구되고 제안되어 왔다. 허나, 여전히 부주의한 패스워드 관리와 지능적인 해킹 공격에 의한 무단 서비스 접근을 완벽하게 차단하지 못하고 있다. HWSN 상의 인증 스킴은 사용자와 네트워크 구성요소인 BS와 CH들 사이에서 투명한 상호인증 방안을 제공해야 한다.

2012년 Das[2] 등은 HWSN에 적용 가능한 스마트카드를 사용한 동적 패스워드 기반 사용자 인증 스킴을 소개하였다. Das 등은 별도의 인증 테이블을 유지함이 없이 HWSN 환경에서 사용자와 CH사이의 상호인증과 세션키 확립을 통해서 안전한 통신을 제공하며, 따라서 패스워드 추측 공격, 패스워드 변경 공격, 사용자 가장 공격 및 재전송 공격 등을 막을 수 있다고 주장하였다. 본 논문은 Das 등의 스킴을 분석하여 제안된 스킴이 중간자 공격 및 알려진 다양한 공격에 취약함을 갖고 있으며, 상호인증을 제공하지 못함을 밝혀낸다.

본 논문의 구성은 다음과 같다. 2장에서는 HWSN과 관련된 기존의 사용자 인증에 대한 연구들을 살펴본다. 3장에서는 Das 등이 제안한 스킴을 고찰하고, 4장에서는 Das 등의 스킴이 갖고 있는 보안상 취약점을 분석하고 5장에서 결론을 맺는다.

II. 관련 연구

스마트카드를 이용하여 원격지에 있는 사용자를 인증하는 연구는 Lamport[3]의 제안 이후 보안성과 효율성을 향상시키며 지속적으로 개선되어 왔다. 2000년대 초부터 WSN의 보안과 관련된 다양한 연구가 시작되었다. Watro[4] 등은 RSA와 Diffie-Hellman 알고리즘을 기반으로 한 공개키(public key) 기술을 이용하여 WSN을 위한 사용자 인증 프로토콜을 제안하였다. Watro 등의 스킴에서 공격자는 사용자의 공개키를 획득하여 세션 키를 암호화하여 사용자에게 보내고, 사용자는 암호된 메시지가 센서 노드로부터 온 것으로 믿고 자신의 사설키(private key)로 메시지를 해독하게 된다. 따라서 Watro 등의 스킴에서 공격자가 세션 키를 이용하여 수행하는 임의의 공격을 막는 것이 불가능하다. Wong[5] 등은 WSN에 적

용하기 위해 해쉬함수를 활용한 패스워드 기반의 사용자 인증 프로토콜을 제안하였다. 그러나 Wong 등의 스킴은 사용자의 패스워드와 아이디를 위한 테이블을 유지해야 하므로, 인증 테이블이 도난(stolen-verifier attack)되었을 경우에 다양한 해킹 공격에 노출되는 치명적인 단점을 갖고 있다.

2010년을 전후하여 HWSN을 위한 수많은 사용자 인증 스킴이 제안되었다. 2009년 Das[6]는 검증을 위해 타임스템프를 사용하는 효과적인 사용자 인증 스킴을 소개하였다. 그러나 2010년 Khan과 Alghathbar[7]는 Das의 스킴이 BS 우회공격과 내부자 공격에 안전하지 않음을 보여주었다. 그럼에도 불구하고 Das의 스킴은 이후에 HWSN에 적용 가능한 여러 유용한 사용자 인증 스킴 연구를 이끌어 내었다[8-10]. 한편 2010년 Yuan[11] 등은 Das의 스킴과 유사한 개념을 사용하여 Wong 등의 스킴이 갖고 있는 보안 취약점인 인증 테이블 도난 공격을 견디어 낼 수 있는 사용자 인증 방법을 제시하였다. Yuan 등은 패스워드와 함께 개인의 지문, 얼굴, 홍채, 망막, 정맥 등의 생체정보(biometrics) 키와 해쉬 함수를 사용하여 다른 스킴에 비해 상대적으로 높은 인증 신뢰성을 추구하였다. Yuan 등의 스킴은 BS와 SN과의 상호인증을 제공하지 못하고 이로 인해 서비스 거부 공격(denial-of-service attack) 등의 보안 취약점을 갖고 있지만, HWSN에서 생체정보를 기반으로 향후 보다 개선된 사용자 인증 연구에 기여할 것으로 예상된다[12-13].

2012년 Das[2] 등은 HWSN에 적용하기 위해 보다 개선된 사용자 인증시킴을 제시하였다. 그들은 대규모 급 HWSN에서 동적으로 노드 추가를 지원하고, 하나의 노드 해킹이 다른 노드에 영향을 주지 못하도록 하여 네트워크 차원의 서비스 거부 공격을 막을 수 있는 실용적인 사용자 인증 스킴을 소개하였다.

Ⅲ. Das 등의 인증 스킴 고찰

이 장에서는 2012년에 Das 등이 HWSN에 적용하기 위해 제안한 동적 패스워드 기반 사용자 인증 스킴을 살펴본다. Das 등의 스킴은 사전설치 단계(pre-deployment phase), 등록 단계(registration phase), 로그인 단계(login phase), 인증 단계(authentication phase), 그리고 패스워드 변경 단계(password change phase)에 걸친 5개의 단계로 구성된다. 표 1은 본 논문에서 사용된 약어 표기 및 정의를 요약한 것이다.

표 1. 약어 표기 및 정의
Table 1. Abbreviation Notation and Definition

표기	정의
U_i	사용자(User i)
BS	베이스 스테이션(Base Station)
S_j	센서 노드(Sensor Node j)
CH_j	j 번째 Cluster의 Cluster Head
PW_i	사용자 i의 패스워드
ID_i	사용자 i의 아이디
ID_{CHj}	Cluster Head, CH_j 의 아이디
ID_{Sj}	Sensor Node, S_j의 아이디
MK_{CHj}	각각의 CH_j를 위한 마스터 키
MK_{Sj}	각각의 S_j를 위한 마스터 키
T	현재의 Timestamp
X_s	BS의 비밀키 값
X_A	사용자와 BS가 공유하는 비밀키 값
h()	단방향 해쉬(hash) 함수
$x \oplus y$	x 와 y에 대한 XOR 연산
$x \| y$	x 와 y에 대한 Concatenation 연산

■ 사전설치 단계

이 단계는 서버에 해당하는 베이스 스테이션(BS)이 센서 노드(SN)와 클러스터 헤드(CH)를 실제 응용 필드에 설치하기 전,오프 라인 상에서 실행하는 단계로서, 다음의 과정을 수행한다.

(1) BS는 클러스터 헤드 CH_j와 센서 노드 S_j에 유일무이한 아이디 ID_{CHj}와 ID_{Sj}를 각각 배정한다.

(2) BS는 각각의 CH_j에게 BS 자신과 공유하는 마스터 키 MK_{CHj}를 랜덤하게 지정한다. 마찬가지로 각각의 S_j에게도 자신과 공유하는 마스터 키 MK_{Sj}를 지정한다.

(3) BS는 각각의 CH_j와 S_j에게 해당정보 (ID_{CHj}, MK_{CHj})와 (ID_{Sj}, MK_{Sj})를 최종적으로 저장하고 사전 설치를 마친다.

■ 등록 단계

이 단계는 사용자 U_i가 HWSN으로부터 데이터를 액세스하기 전에 BS에 등록을 하기 위하여 다음과 같이 실행된다.

(1) 사용자 U_i는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 식 (1)에 의해 RPW_i를 계산하여, 안전한 채널을 이용하여 ID_i와 마스크된 패스워드 RPW_i를 BS에 보낸다.

$$RPW_i = h(y \| PW_i) \quad (1)$$

여기서 y는 사용자 U_i에게만 알려져 있는 랜덤 수이다.

(2) 사용자의 등록요청을 수신한 BS는 아래의 수식들로부터 f_i, x, r_i, e_i를 계산한다.

$$f_i = h(ID_i \| X_s) \quad (2)$$

$$x = h(RPW_i \| X_A) \quad (3)$$

$$r_i = h(y \| x) \quad (4)$$

$$e_i = f_i \oplus x = h(ID_i \| X_s) \oplus h(RPW_i \| X_A) \quad (5)$$

여기서 X_s는 BS에게만 알려져 있는 비밀 키이고, X_A는 사용자와 BS가 공유하는 비밀 키이다.

(3) BS는 m개의 클러스터 헤드를 선택하여 키와 아이디 값을 $\{(K_j, ID_{CHj}) | 1 \le j \le m\}$와 같이 부여한다. 여기서 $K_j = E_{MKCHj}(ID_i \| ID_{CHj} \| X_s)$이다. BS는 향후 보안에 문제가 되는 클러스터 헤드 교체를 위해 m′개의 클러스터 헤드를 준비하여 키와 아이디 값을 $\{(K_{m+j}, ID_{CHm+j}) | 1 \le j \le m'\}$와 같이 제공한다.

(4) BS는 ID_i, y, X_A, r_i, e_i, h()와 m+m′개의 (K_j, ID_{CHj}) 정보를 저장한 스마트카드를 안전한 채널을 통해 U_i에게 발급한다.

■ 로그인 단계

사용자 U_i가 HWSN으로부터 데이터를 액세스하기 원할 때 로그인 단계가 실행되며, 다음의 과정을 수행한다.

(1) U_i는 발급받은 스마트카드를 카드 리더기에 넣고 자신의 패스워드 PW_i를 입력한다.

(2) 스마트카드는 U_i의 $RPW_i^* = h(y \| PW_i)$를 계산하고 나서, $x^* = h(RPW_i^* \| X_A)$와 $r_i^* = h(y \| x^*)$를 구한다. 그리고 r_i와 r_i^* 값이 동일한지를 검증한다. 만약 두 값이 다를 경우 로그인 요청은 실패하고, 동일한 경우에 사용자는 다음 과정을 계속한다.

(3) 스마트카드는 식 (6)에 의해 N_i를 계산한다.

$$N_i = h(x^* \| T_1) \quad (6)$$

여기서 T_1는 현재의 시간을 나타내는 타임스탬프이다.

(4) U_i는 클러스터 헤드 CH_j를 선택하고 스마트카드로부터 CH_j의 K_j를 읽어 와서 암호 메시지 $E_{Kj}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)$를 계산한다. 사용자 U_i는 공중 채널로 로그인 요청 메시지 $\{ID_i \| ID_{CHj} \| E_{Kj}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)\}$를 BS에 전송한다.

■ 인증 단계

로그인 요청 메시지를 수신한 BS는 사용자 U_i를 인증하기 위해 다음 과정을 수행한다.

(1) BS는 클러스터 헤드 CH_j의 마스터 키 MK_{CHj}를 이용하여 $K = E_{MKCHj}(ID_i \| ID_{CHj} \| X_s)$를 계산한다. 구하여진 값 K를 사용하여 BS는 $D_k[E_{Kj}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)]$을 해독하여 계산함으로 $(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)$를 밝혀낸다.

(2) BS는 해독한 ID_i와 ID_{CHj}를 받아들인 ID_i와 ID_{CHj}이 같은지를 비교한다. 만약 같다면, BS는 T_1와 T_1^* 간의 시간 차이의 유효성을 검증한다. 여기서 T_1^*는 BS가 로그인 요청 메시지를 받은 시점의 타임스탬프이다. 즉 ΔT_1값이 HWSN의 전송지연의 예상시간 간격일 때, $|T_1^* - T_1| > \Delta T_1$인 경우 사용자 인증은 실패한다. 한편 $|T_1^* - T_1| \le \Delta T_1$이면 BS는 인증을 계속하여 $X = h(ID_i \| X_s)$, $Y = e_i \oplus X$, $Z = h(Y \| T_1)$를 계산한다. 만약 Z와 N_i가 같다면 BS는 U_i의 로그인 요청을 받아들인다. 값이 다른 경우에는 요청은 거절된다.

(3) BS는 현재 타임스탬프인 T_2에 의해 $u = h(Y \| T_2)$를 계산하고 MK_{CHj}를 통해 $E_{MKCHj}(ID_i \| ID_{CHj} \| u \| T_1 \| T_2 \| X \| e_i)$를 구한다. 이어서 BS는 해당하는 클러스터 헤드 CH_j에게 메시지 $\{ID_i \| D_{CHj} \| E_{MKCHj}(ID_i \| ID_{CHj} \| u \| T_1 \| T_2 \| X \| e_i)\}$를 보낸다.

(4) BS로부터 메시지를 받은 CH_j는 자신의 마스터 키, MK_{CHj}를 사용하여 $E_{MKCHj}(ID_i \| ID_{CHj} \| u \| T_1 \| T_2 \| X \| e_i)$를 해독한다. CH_j는 찾아낸 ID_i와 ID_{CHj}를 수신한 ID_i와 ID_{CHj}이 같은지를 비교한다. 만약 같은 경우에 CH_j는 $|T_2^* - T_2| \le \Delta T_2$를 확인한다. 여기서 T_2^*는 CH_j가 메시지를 받은 타임스탬프이다. 만약 T_2와 T_2^* 간의 시간 차이가 유효하다면 CH_j는 식 (7)과 (8)에 의해 v와 w를 계산한다.

$$v = e_i \oplus X = h(RPW_i \| X_A) \quad (7)$$

$$w = h(v \| T_2) = h(h(RPW_i \| X_A) \| T_2) \quad (8)$$

다음에 CH_j는 w와 u가 동일한지를 검사한다. 다르면 인증은 실패하고, 만약 값이 서로 같다면 U_i

는 CH_j에게 적법한 사용자로 인증을 받게 되고, CH_j는 U_i와 공유하는 비밀 세션 키 SK를 식 (9)와 같이 구한다.

$$SK = h(ID_i \| ID_{CHj} \| e_i \| T_1) \quad (9)$$

궁극적으로 CH_j는 다른 클러스터 헤드와 BS를 통해 U_i에게 응답 메시지를 보내고 사용자 쿼리(query)에 응답한다.

(5) CH_j로부터 응답 메시지를 받은 U_i는 T_1, ID_i, ID_{CHj}, e_i를 이용하여 CH_j와 동일한 세션 키 SK를 계산한다. 이후 U_i와 CH_j는 바로 이 값 SK를 사용하여 상호간 통신을 지속 수행한다.

■ 패스워드 변경 단계

이 단계는 사용자 U_i가 자신의 패스워드를 변경하고자 할 때 실행되며 BS의 도움 없이 다음의 과정을 수행한다.

(1) U_i는 스마트카드를 카드 리더기에 넣고, 자신의 아이디 ID_i, 이전 패스워드 PW_i와 새로운 패스워드 PW_i^{new}를 입력한다. 스마트카드는 $RPW_i^* = h(y \| PW_i)$를 계산하고, 식 (10)과 (11)에 의해 M_1과 M_2를 구한다.

$$M_1 = h(RPW_i^* \| X_A) \quad (10)$$

$$M_2 = h(y \| M_1) \quad (11)$$

(2) 스마트카드는 M_2와 r_i가 같은지를 비교하여 틀린 경우는 U_i가 이전 패스워드를 부정확하게 입력한 결과로 패스워드 변경이 실패한다. 같은 경우 스마트카드는 식 (12), (13), (14)에 의해 M_3, M_4, M_5를 계산한다.

$$M_3 = e_i \oplus M_1 = h(ID_i \| X_s) \quad (12)$$

$$M_4 = h(y \| PW_i^{new}) \quad (13)$$

$$M_5 = h(M_4 \| X_A) \quad (14)$$

(3) 스마트카드는 r_i^*와 $e_i^* = M_3 \oplus M_5$를 식 (15)과 (16)에 의해 계산한 뒤, 최종적으로 r_i와 e_i를 r_i^*와 e_i^*로 각각 변경한다.

$$r_i^* = h(y \| M_4) = h(y \| h(y \| PW_i^{new})) \quad (15)$$

$$e_i^* = h(ID_i \| X_s) \oplus h(h(y \| PW_i^{new}) \| X_A) \quad (16)$$

Ⅳ. Das 등의 스킴의 보안 취약점 분석

Das 등의 인증 스킴에 대한 안전성을 분석하기 위해, Kocher[14] 등과 Messerges[15] 등의 연구를 통해 입증된 바와 같이 공격자는 합법적인 사용자로 가장하여 스마트카드에 저장된 정보들을 전력소비를 모니터링함으로 불법적으로 추출할 수 있다고 가정한다. 공격자(attacker)는 사용자와 베이스 스테이션 그리고 클러스터 헤드 간에 전송되는 메시지를 가로채고 추출한 정보를 바탕으로 메시지를 위조할 수 있다. 이 장에서는 Das 등의 인증 스킴이 그들의 주장과 달리 중간자 공격, 패스워드 추측 공격, 패스워드 변경 공격 등에 보안 취약성을 갖고 있으며, 사용자와 클러스터 헤드 간 상호인증을 제공할 수 없음을 증명한다.

■ 중간자 공격

공격자가 적법한 사용자 U_i의 스마트카드로부터 등록 단계에서 저장된 비밀정보 ID_i, y, X_A, r_i, e_i, h()을 비롯하여 (K_j, ID_{CHj})를 불법으로 추출하고, 클러스터 헤드 CH_j를 해킹하여 마스터 키 MK_{CHj}를 획득하게 되면, 공격자는 사용자와 BS, CH_j 사이에 주고받는 메시지를 가로채기(interception)하여 중간자 공격(man-in-the-middle attack)을 감행할 수 있다.

공격자는 아래의 과정을 통해 적법한 사용자를 가장(user impersonation)하여, BS로부터 인증을 획득한다.

(1) 공격자는 적법한 사용자 U_i가 BS에 보내는 로그인 요청 메시지 $\{ID_i \| ID_{CHj} \| E_{Kj}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)\}$를 가로챈다.

(2) 공격자는 MK_{CHj}를 사용하여 $K_j = E_{MKCHj}(ID_i \| ID_{CHj} \| X_s)$를 해독하여 쉽게 $(ID_i \| ID_{CHj} \| X_s)$를 구할 수 있다. 따라서 BS의 비밀 키 값 X_s를 ID_{CHj}로부터 성공적으로 도출한다.

(3) 공격자는 등록되지 않은 불법 아이디, ID_i^*를 선택하여 아래의 수식들로부터 f_i^*, e_i^*, K_j^*,를 계산한다.

$$f_i^* = h(ID_i^* \| X_s) \quad (17)$$

$$e_i^* = f_i^* \oplus x = h(ID_i^* \| X_s) \oplus h(RPW_i \| X_A) \quad (18)$$

$$K_j^* = E_{MKCHj}(ID_i^* \| ID_{CHj} \| X_s) \quad (19)$$

공격자는 ID_i^*, X_A, e_i^*, h(), (K_j^*, ID_{CHj}) 정보를 스마트카드에 저장한다.

(4) 공격자는 식 (20)에 의해 N_i^*를 계산하고, N_i^*에 의해 $E_{Kj*}(ID_i^* \| ID_{CHj} \| N_i^* \| e_i^* \| T_1^*)$를 위조한다.

$$N_i^* = h(x^* \| T_1^*) = h(h(RPW_i \| X_A) \| T_1^*) \quad (20)$$

(5) 최종적으로 공격자는 미등록 불법 아이디에 의해

위조된 로그인 메시지 $\{ID_i^* \| ID_{CHj} \| E_{Kj*}(ID_i^* \| ID_{CHj} \| N_i^* \| e_i^* \| T_1^*)$를 BS에 전송하여 사용자 가장 공격을 통한 인증을 받게 된다.

또한 공격자는 아래의 과정을 통해 적법한 CH_j를 위장(server masquerading)하여, 사용자로부터 인증을 획득한다.

(1) 공격자는 적법한 사용자 U_i의 로그인 요청 메시지를 유효한 시간 차이 검증을 통해 인증한 BS가 CH_j에게 보내는 메시지 $\{ID_i \| D_{CHj} \| E_{MKCHj}(ID_i \| ID_{CHj} \| u \| T_1 \| T_2 \| X \| e_i)\}$를 가로챈다.

(2) 공격자는 이미 알고 있는 CH_j의 마스터 키 MK_{CHj}를 이용하여 $E_{MKCHj}(ID_i \| ID_{CHj} \| u \| T_1 \| T_2 \| X \| e_i)$를 해독하여 시간 차이 검증을 통과한다.

(3) 이어서 공격자는 스마트카드로부터 추출한 정보들과 위의 사용자 가장 단계에서 도출한 BS의 비밀키, X_s를 이용하여 식 (21)과 (22)와 같이 v^*와 w^*를 계산한다.

$$v^* = e_i \oplus X = e_i \oplus h(ID_i \| X_s) \quad (21)$$

$$w^* = h(v^* \| T_2) = h(e_i \oplus h(ID_i \| X_s) \| T_2) \quad (22)$$

검증된 $v^* = w^*$에 의해 공격자는 적법한 CH_j를 위장하여 사용자를 인증하고 사용자와 공유하는 비밀 세션 키 $SK = h(ID_i \| ID_{CHj} \| e_i \| T_1)$를 만들고 사용자에게 응답 메시지를 보낸다.

(4) 공격자에 의해 위장된 CH_j로부터 응답메시지를 받은 사용자는 공격자를 적법한 CH_j로 인증한다. 그리고 공격자와 통신을 위한 동일한 세션 키 SK를 생성한다.

■ 패스워드 추측 공격

일반적으로 대부분의 사용자들은 편리성 때문에 쉽게 기억되는 패스워드를 선택하는 경향이 있다. 그러나 이러한 패스워드는 잠재적으로 패스워드 추측 공격(password guessing attack)에 취약하다. 본 연구에서 가정한 바와 같이 공격자(attacker)는 적법한 사용자의 스마트카드에 접근하여 저장된 비밀정보를 추출할 수 있다. 공격자는 등록단계에서 BS가 발급한 사용자의 스마트카드로부터 ID_i, y, X_A, r_i, e_i, h(), (K_j, ID_{CHj}) 정보를 획득할 수 있다. 추출한 정보를 이용하여 오프라인 패스워드 추측 공격 시도가 가능하게 된다. 즉 사용자의 올바른 패스워드 PW_i를 찾아내기 위하여 공격자는 r_i와 r_i^* 가 같을 때 까지 식 (23)에 의해 PW_i^*를 계속 바꾸면서 r_i^*의 검증을 반복 수행한다.

$$r_i^* = h(y \| x^*) = h(y \| h(RPW_i^* \| X_A)) = h(y \| h(h(y \| PW_i^*) \| X_A)) \quad (23)$$

궁극적으로 공격자는 사용자의 정확한 패스워드 PW_i를 찾아내어 로그인 요청을 성공할 수 있다.

■ 패스워드 변경 공격

공격자는 패스워드 추측공격에서 성공적으로 획득한 패스워드 PW_i를 사용하여 올바른 이전 패스워드와 새로운 패스워드 PW_i^{new}를 입력함으로 패스워드 변경 공격(password change attack)을 쉽사리 수행할 수 있다. 공격자는 스마트카드에서 추출한 정보들과 중간자 공격에서 획득한 X_s를 이용하여 식 (24)와 (25)에 의해 r_i^*와 e_i^*를 계산해 낼 수 있다.

$$r_i^* = h(y \| h(y \| PW_i^{new})) \quad (24)$$

$$e_i^* = h(ID_i \| X_s) \oplus h(h(y \| PW_i^{new}) \| X_A) \quad (25)$$

궁극적으로, 공격자는 스마트카드에 저장된 r_i와 e_i를 r_i^*와 e_i^*로 바꿈으로써 성공적으로 패스워드 변경 공격을 수행한다.

■ 재전송 공격

공격자에 의해 가로채기를 당할 수 있는 로그인 요청 메시지 $\{ID_i \| ID_{CHj} \| E_{Kj}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)\}$의 재전송 공격(replay attack)을 방지하기 위하여 통상적으로 인증 스킴들은 재전송된 메시지의 시스템 시간을 이용하여 시간 차이의 유효성을 검증하여 재전송 공격을 차단하려는 시도를 널리 사용한다. Das 등의 스킴은 사용자와 BS간 그리고 BS와 CH_j간 메시지 재전송 공격을 막기 위해, BS가 로그인 요청 메시지를 받은 시점의 타임스탬프 T_1^*와 CH_j가 메시지를 받은 타임스탬프 T_2^*를 이용하여 $(T_1^* - T_1) \le \Delta T_1$ 와 $(T_2^* - T_2) \le \Delta T_2$를 검증하는 방법을 사용한다. 하지만 공격자가 스마트카드의 비밀정보를 추출한다면, 로그인 요청 메시지 검증을 위한 $X = h(ID_i \| X_s)$, $Y = e_i \oplus X$, $Z = h(Y \| T_1)$, $u = h(Y \| T_2)$를 계산하여 적법한 사용자로 BS에게 인증을 받을 수 있다. 그리고 BS로부터 메시지를 받은 CH_j는 $v = e_i \oplus X = h(RPW_i \| X_A)$와 $w = h(v \| T_2) = h(h(RPW_i \| X_A) \| T_2)$를 계산하여 공격자는 CH_j로부터 인증을 받고 데이터에 접근 가능하다. 따라서 Das 등의 스킴이 사용하는 재전송 공격 방지책은 본 연구의 보안 취약성 분석 관점에서는 실효성을 갖고 있지 않다.

■ 상호인증

중간자 공격에서 살펴본 바와 같이 공격자는 스마트 카드로부터 비밀 정보를 추출할 수 있을 뿐 아니라, 클러스터 헤드 CH_j를 해킹하여 찾아낸 마스터 키 MK_{CHj}를 이용하여 BS의 비밀 키 값 X_s를 도출하는 것이 가능하다. 이러한 정보를 바탕으로 공격자는 로그인 요청 메시지를 위조하여 BS로부터 적법한 사용자로 가장하여 인증을 획득한다. 한편 로그인 요청을 받아들인 BS가 CH_j에게 보내는 메시지를 가로채어 공격자는 적법한 CH_j로 위장하여 사용자를 인증하고 위조된 응답메시지를 사용자에게 보낸다. 사용자는 응답메시지를 받고 공격자를 적법한 CH_j로 인증한다. 결국 사용자 가장 공격과 서버 위장 공격에 의해 공격자는 무단으로 HWSN의 기밀 데이터에 접근하는 것이 가능하다. 따라서 Das 등의 스킴은 그들의 주장과 달리 사용자와 클러스터 헤드들 간에 상호인증(mutual authentication)을 투명하게 제공하지 못함이 입증된다.

한편 적법한 CH_j로 위장한 공격자는 사용자를 인증하고 향후 사용자와 안전한 통신을 위해 $SK = h(ID_i \| ID_{CHj} \| e_i \| T_1)$를 구하여 사용자와 공유하는 비밀 세션 키(secret session-key)를 확립한다. 응답메시지를 받은 사용자는 공격자를 적법한 CH_j로 인증하고 동일한 세션 키를 생성한다. 결과적으로 Das 등의 스킴에서는 사용자와 클러스터 헤드 간 세션 키 일치 및 확립(session-key agreement and establishment)은 구현되었지만, 비밀 세션 키가 노출되는 취약점이 존재하며, 중간자 공격에서 밝힌 바와 같이 상호인증의 제공은 불가능하다.

V. 결 론

본 논문은 Das 등이 제시한 계층적 무선 센서 네트워크를 위한 사용자 인증 스킴을 살펴보고, 그들의 스킴에서 노출될 수 있는 보안 취약점을 분석하였다. Das 등의 스킴은 중간자 공격, 패스워드 추측 공격, 패스워드 변경 공격 등을 막을 수 없음을 본 연구는 밝혀내었다. 또한 HWSN상에서 공격자의 허가되지 않은 데이터 획득을 막기 위해 절실히 요구되는 사용자와 클러스터 헤드 간의 상호인증이 지원되지 않음도 보여주었다. Das 등의 스킴은 대규모급의 HWSN에 실질적으로 적용이 가능한 개선된 인증 기능을 구현했다는 점에서 향후 연구에 기여를 했다고 볼 수 있다. 향후 연구 과제는 본 논문에서 입증된 보안 취약점을 극복하기 위해, 사용자와 클러스터 헤드 사이 뿐 아니라, 베이스 스테이션과 클러스터 헤드와의 상호인증도 함께 가능한 인증 스킴을 설계하는 것이다.

References

[1] A. K. Das, “An Unconditionally Secure Key Management Scheme for Large-scale Wireless Sensor Networks”, IEEE International Conference on Communication systems and Networks, pp. 1-10, 2009.

[2] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, “A Dynamic Password-based User Authentication Scheme for Hierarchical Wireless Sensor Networks”, Journal of Network and Computer Applications, Vol. 35, No, 5, pp. 1646-1656, 2012.

[3] L. Lamport, “Password Authentication with Insecure Communication”, Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[4] R. Watro, and D. Kong, et al., “Securing Sensor Network with Public Key Technology”, ACM Workshop Security of Ad Hoc Sensor Network, pp. 59-64, 2004.

[5] K. Wong, Y. Zheng, and J. Cao, et al., “A Dynamic User Authentication Scheme for Wireless Sensor Networks”, IEEE International Conference Sensor Networks, Ubiquitous and Trustworthy Computing, IEEE Computing Society, pp. 244-251, 2006.

[6] M. L. Das, “Two-factor User Authentication Scheme in Wireless Sensor Network”, IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1086-1090, 2009.

[7] M. K. Khan, and K. Alghathbar, “Cryptanalysis and Security Improvements of Two-factor User Authentication in Wireless Sensor Networks”, Sensors, Vol. 10, No. 3, pp. 2450-2459, 2010.

[8] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, “An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks”, Ad Hoc & Sensor Wireless Networks, Vol. 10, No. 4, pp. 361-371, 2010.

[9] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, “A Secure Authentication Protocol for Wireless Sensor Network Using Elliptic Curve Cryptography”, Sensors, Vol. 11, No. 5, pp. 4767-4779, 2011.

[10] C. T. Li, C. Y. Weng, and C. C. Lee, et al., “Security Flaws of a Password Authentication Scheme for Hierarchical WSNs”, Journal of Advances in Computer Networks, Vol. 1, No. 2, pp. 121-124, 2013.

[11] J. Yuan, C. Jiang, and Z. Jiang, “A Biometric-Based User Authentication for Wireless Sensor Networks”, Wuhan University Journal of Natural Science, Vol. 15, No. 3, pp. 272-276, 2010.

[12] H. Lee, and Y. Park, “A Design and Implementation of User Authentication System using Biometric Information”, Journal of the Korea Academia-Industrial Cooperation Society(JKAIS), Vol. 11, No. 9, pp. 3548-3557, 2010.

[13] Y. Joo, “Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks”, Journal of the Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 14, No. 2, pp. 147-153, 2014.

[14] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, Proceedings of Advances in Cryptology, pp. 388-397, 1999.

[15] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks”, IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, 2002

저자 소개

주 영 도(정회원)

- 1983년 : 한양대학교 전자통신공학과 학사
- 1988년 : 미국 University of South Florida 컴퓨터공학과 석사
- 1995년 : 미국 Florida State University 전산학과 박사
- 1996년 ~ 2000년 : KT 통신망 연구소 선임 연구원
- 2000년 ~ 2005년 : 시스코 시스템즈 코리아 상무
- 2005년 ~ 2006년 : 화웨이 기술 코리아 부사장
- 2007년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수

<관심분야 : 정보보안, 네트워크 보안, 정보검색, 데이터베이스>

※ 이 논문은 강남대학교 교내 연구비 지원을 받아 연구된 것임.