http://dx.doi.org/10.14400/JDC.2016.14.10.287

무선센서네트워크에서 익명의 사용자 인증과 키동의 기법에 대한 가장 공격

최해원*, 김현성**,***
경운대학교 컴퓨터공학과*, 경일대학교 사이버보안학과**, 말라위대학교 수학과***

Impersonation Attacks on Anonymous User Authentication and Key Agreement Scheme in Wireless Sensor Networks

Hae-Won Choi*, Hyunsung Kim,*****
Dept. of Computer Engineering, Kyungwoon University*
Dept. of Cyber Security, Kyungil University**
Dept. of Mathematical Sciences, University of Malawi***

요 약 무선센서네트워크는 다양한 응용을 가지고 있고 아주 넓은 지역에 배치된다. 특히, 이들 네트워크는 잠재적인 위험을 포함한 환경에 배치됨으로 이에 대한 보안 이슈를 해결하기 위한 많은 노력이 있다. 최근에 무선센서네트워크에서 대칭키암호시스템에 기반한 익명의 사용자 인증과 키동의 기법 (AUAKAS)이 제안되었다. AUAKAS는 가장공격을 포함한 다양한 공격에 안전하다고 주장하였다. 하지만 본 논문은 AUAKAS가 게이트웨이에 등록된 정당한 사용자에 의하여 사용자 가장 공격과 게이트웨이 가장 공격에 취약함을 보인다. 본 논문의 보안 분석은 다양한 새로운 보안 기법의 설계에 있어서 미리 고려할 중요한 특성 분석에 있어서 도움을 줄 수 있을 것이다.

주제어 : 무선센서네트워크, 상호인증, 키동의, 스마트카드, 가장공격

Abstract Wireless sensor networks (WSNs) have many applications and are deployed in a wide variety of areas. They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these WSNs. Recently, an anonymous user authentication and key agreement scheme (AUAKAS) was proposed based on symmetric cryptosystem in WSNs. It is claimed in AUAKAS that it assures security against different types of attacks including impersonation attacks. However, this paper shows that AUAKAS does not cope from user impersonation attack and gateway impersonation attack from the legally registered user on the gateway. The security analysis could guide the required features of the security scheme to be satisfied.

Key Words : Wireless sensor network, Mutual authentication, Key agreement, Smart card, Impersonation attack

1. 서론

무선선세네트워크(Wireless sensor network)는 과학적, 의학적, 군사적, 상업적 용도 및 다양한 응용에 활용되고 있다[1-6]. 특히, 기존 네트워크로 구성이 어려웠던 유독물질 감염 지역이나 지진 피해지역 및 전쟁터와 같

Received 25 August 2016, Revised 26 September 2016
Accepted 20 October 2016, Published 28 October 2016
Corresponding Author: Hyunsung Kim(Kyungil University)
Email: kim@kiu.ac.kr

ISSN: 1738-1916

이 사람이 직접 모니터링하기 위험하고 접근이 어려운 지역의 정보수집에 활용될 수 있는 장점이 있다. 하지만, 이러한 광범위한 무선센서네트워크의 활용은 해킹으로 인한 정보유출 발생 시 다양한 형태로 국가/사회적인 혼란을 야기할 수 있다[7,8].

Lamport가 1981년 원격 패스워드 인증 기법을 제안한 이래 다양한 보안 기법 및 프로토콜이 연구되었다[9,10,11,12,13,14,15]. 특히, 무선센서네트워크에서 사용자 중심의 데이터 수집을 위한 인증 기법이 Das에 의해 개발되었다. 하지만 Kim과 Lee는 Das 기법이 보안에 취약함을 보이고 강화된 기법을 제안하였다[13]. Kim과 Lee의 기법은 해쉬 체인의 재설정을 지원한다. 최근에는 Chen등이 안전한 사용자 인증 기법을 제안하고 제안한 기법이 다양한 공격에 안전함을 보였다[14]. 하지만, Jung등은 Chen등의 기법이 스마트카드 분실 공격과 서비스 거부 공격에 취약함을 보이고 이를 해결하기 위한 대칭키 기반의 익명의 사용자 인증 및 키동의 기법(AUAKAS)을 제안하였다[15].

본 논문에서는 AUAKAS를 살펴보고 이 기법의 보안 취약점을 보이는데 그 목적이 있다. AUAKAS에 존재하는 가장 공격의 취약점을 제시하기 위해서 게이트웨이 노드에 적법적으로 등록한 사용자를 공격자로 가정한다. 즉, AUAKAS는 사용자 가장 공격과 게이트웨이 가장 공격에 취약함을 본 논문에서 보인다.

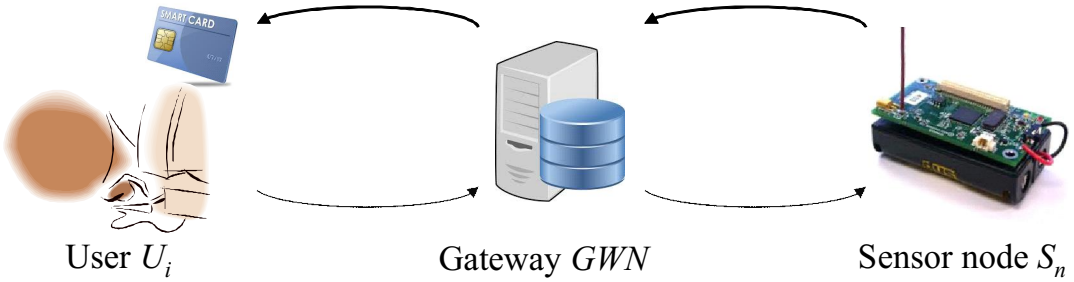
본 논문의 구성은 다음과 같다. 2장에서 본 논문의 네트워크 환경을 살펴본다. 3장에서 AUAKAS의 작동원리를 살펴본다. 4장에서 AUAKAS가 두 가지 가장 공격에 취약함을 보인다. 끝으로 5장에서 결론 및 향후 연구 방향을 도출한다.

2. 무선센서네트워크 환경

본 장에서는 Jung등이 제안한 AUAKAS의 네트워크 환경에 대한 자세한 이해를 위해 다양한 사용자 중심의 데이터 수집을 위한 무선센서네트워크 환경에 대해 살펴본다[16]. 이러한 네트워크 환경은 일반적으로 [Fig. 1]에서 보여주는 바와 같이 사용자 U_i가 게이트노드 *GWN*을 통하여 센서노드 S_n의 데이터를 수집하는 시나리오를 가정한다.

*GWN*은 네트워크의 신뢰성을 제공하는데 있어서 아주 중요한 역할을 수행한다. 일반적으로 센서노드들이 거친환경(Harsh environment)에 배치되기 때문에 *GWN*을 통한 사용자와 센서노드 사이의 인증은 필수적이다. 네트워크를 구성하는 세 참여자들은 다음과 같은 기능을 수행한다.

- 사용자 U_i : 무선센서네트워크에서 센서노드의 데이터를 수집하기 위한 역할을 수행한다. 이를 위해 사용자는 *GWN*에 등록될 필요가 있고, 데이터 수집 전에 *GWN*으로부터 센서노드 접근에 대한 적법한 인증을 거쳐야 한다.
- 게이트웨이 *GWN* : 네트워크의 인증서버 역할을 수행한다. 이를 위해 사용자와 센서노드 사이에서 신뢰의 근원을 제공한다.
- 센서노드 S_n : 주변 환경으로부터 센싱된 데이터를 수집하고 이를 *GWN*이나 사용자에게 제공한다. 이러한 과정에서 *GWN*에게 인증된 요청에 대해서만 요구사항을 수행한다.



[Fig. 1] Target Wireless Sensor Network Configuration

3. 익명의 사용자 인증과 키동의 기법

본 장에서는 Jung등이 제안한 AUAKAS의 동작 원리를 살펴본다[15]. AUAKAS는 2장에서 기술한 네트워크 환경에서 세 개의 통신 참여자인 사용자 U_i와 게이트웨이 GWN 그리고 센서노드 S_n으로 구성된다. 이 기법은 등록, 로그인, 검증 그리고 패스워드 변경의 네 가지 단계(Phase)로 구성된다. 본 논문에서 사용하는 기호에 대한 정의는 <Table 1>과 같다.

<Table 1> Notations

Symbol	Description
U_i	Remote user i
S_n	Sensor node n
GWN	Gateway node
ID_i, PW_i	Identity and password of U_i
SID_n	Identity of S_n
DID_i	Dynamic identity of U_i
k	The symmetric key
E_k, D_k	Encryption/Decryption with k
x_a	The secret parameter generated by GWN
x_s	The secret key between GWN and S_n
$h(x_s\|\|SID_n)$	The secret key instead of x_s stored in S_n
b	A random number chosen by U_i
R_i	Cryptographic random numbers
$h()$	One way hash function
$\|\|$	Concatenation operation
$\oplus$	XOR operation
T_1, T_2, T_3, T_4	Current timestamp
SK	Session key
$\triangle T$	The maximum of transmission delay time

3.1 등록 단계

사용자 등록 단계는 사용자 U_i가 자신의 식별자(Identification)와 해쉬된 패스워드를 GWN에게 보낼 때 실행된다. GWN은 중요한 정보가 저장된 스마트카드를 발급해서 등록요청에 대한 응답으로 U_i에게 보낸다. 등록단계의 구체적인 처리과정은 다음과 같다.

(1) U_i가 ID_i와 PW_i를 선택하고 난수 b를 생성한 후, 마스크된 패스워드 (masked password) $PW_i^*=h(PW_i||b)$를 계산하고 안전한 채널을 통해 $<ID_i, PW_i^*>$를 GWN에게 보낸다.

(2) GWN은 $v=h(x_a)$, $N_i=h(ID_i||PW_i^*)\oplus v$, $M_i=h(PW_i^*||v)$를 계산하고 v를 데이터베이스에 저장한다. GWN은 새로운 스마트카드를 선택하여 $\{N_i, M_i, h()\}$를 메모리에 쓴다.

(3) 스마트카드를 받은 후 U_i는 난수 b를 메모리에 쓴다. 최종적으로 스마트카드는 $\{N_i, M_i, h(), b\}$를 저장한다.

3.2 로그인 단계

로그인 단계는 U_i가 네트워크에 접근을 획득하고자 할 때 마다 수행된다. 이 단계에서 U_i는 GWN에게 로그인 요청을 보낸다. 상세한 처리과정은 다음과 같다.

(1) U_i는 자신의 스마트카드를 터미널에 넣고 ID_i와 PW_i를 입력한다. 스마트카드는 마스크된 패스워드 $PW_i'= h(PW_i||b)$와 $v'=N_i\oplus h(ID_i||PW_i')$를 계산한다. 스마트카드는 $M_i'=h(PW_i'||v')$를 계산하고 이것을 저장된 M_i와 비교한다. 만약 두 값이 일치하면 스마트카드는 U_i의 적법성을 알리고 다음 단계를 수행하고 그렇지 않으면 이 단계를 종료한다.

(2) 스마트카드는 난수 $R_1\in\{0, 1\}^l$을 선택하고 $DID_i= h(ID_i||R_1)$를 계산한다. 그런 후 스마트카드는 $k= h(DID_i||v'||T_1)$와 $A_i=E_k(DID_i||R_1||T_1)$를 계산한다.

(3) 마지막으로 U_i는 공개 채널(Public channel)을 통하여 $<DID_i, A_i, T_1>$를 GWN에게 보낸다.

3.3 검증 단계

이 단계는 U_i와 GWN 그리고 센서노드 S_n의 적법성을 판단하기 위해서 모든 전송된 메시지를 테스트함으로서 상호인증을 수행한다. 또한, 네트워크에 포함된 모든 참여자들 간 세션키 동의를 수행한다. GWN이 U_i로부터 로그인 요청을 받으면 다음과 같이 검증과정을 수행한다.

(1) GWN은 먼저 타임스탬프의 적법성 $|T_1'-T_1|<\triangle T$을 검사한다. GWN은 $k'=h(DID_i||h(x_a)||T_1)$를 계산하고 $D_{k'}(A_i)=\{DID_i||R_1||T_1\}$ 수행한다. 그런 후 수신한 값과 메시지 안의 DID_i와 T_1을 비교한다. 만약 조건이 만족하면 GWN은 U_i의 적법성을 인지하고 다음 단계를 진행한다. 그렇지 않다면 이 단계를 종료한다.

(2) GWN은 난수 $R_2\in\{0, 1\}^l$를 선택하고 $M_i=R_2\oplus h(x_s||\ SID_n)$를 계산한다. 그리고 GWN는

$SK=h(DID_i||h(x_s||SID_n)||R_2||T_2)$와 $B_i=h(DID_i||SK||h(x_s||SID_n)||SID_n||T_2)$를 계산하고 공개 채널을 통해 $<M_i, DID_i, B_i, T_2>$를 S_n에게 전송한다.

(3) S_n은 먼저 $|T_2^{'}-T_2|<\Delta T$를 검사한다. 조건이 만족하지 않으면 이 단계를 종료한다. 그렇지 않으면 $R_2^{'}=M_i \oplus h(x_s||SID_n)$와 $SK^{'}=h(DID_i||h(x_s||SID_n)||R_2^{'}||T_2)$를 계산한다. 그리고 S_n은 $B_i^{'}=h(DID_i||SK^{'}||h(x_s||SID_n)||SID_n||T_2)$를 계산하고 수신한 값과 비교한다. 조건이 만족하면 S_n은 GWN의 적법성을 믿는다. 그렇지 않으면 이 단계를 종료한다.

(4) S_n은 $C_i=h(h(x_s||SID_n)||SK||DID_i||SID_n||T_3)$를 계산하고 GWN에게 공개 채널을 통해 $<C_i, T_3>$을 전송한다.

(5) GWN은 먼저 $|T_3^{'}-T_3|<\Delta T$를 검사한다. 조건이 만족하지 않으면 이 단계를 종료한다. 그렇지 않으면 $C_i^{'}=h(h(x_s||SID_n)||SK||DID_i||SID_n||T_3)$를 계산하고 수신한 값과 비교한다. 조건이 만족하면 GWN은 S_n의 적법성을 믿는다. 그렇지 않으면 이 단계를 종료한다.

(6) GWN은 $D_i=E_{k'}(DID_i||SID_n||SK||R_1||T_4)$를 계산하고 U_i에게 공개 채널을 통해 $<D_i, T_4>$을 전송한다.

(7) U_i는 먼저 $|T_4^{'}-T_4|<\Delta T$를 검사한다. 조건이 만족하지 않으면 이 단계를 종료한다. 그렇지 않으면 $D_k(D_i)=\{DID_i||SID_n||SK||R_1||T_4\}$를 계산하고 이전 값 DID_i와 R_1 그리고 T_4와 비교한다. 조건이 만족하면 U_i는 GWN의 적법성을 믿고 성공적으로 이 단계를 끝낸다.

3.4 패스워드 변경 단계

이 단계는 사용자 U_i가 오래된 패스워드를 새로운 패스워드로 변경하고자 할 때 실행된다. 이 단계에서 U_i는 GWN으로부터 어떤 도움도 필요하지 않다. 구체적인 처리과정은 다음과 같다.

(1) U_i는 자신의 스마트카드를 터미널에 넣고 ID_i와 현재 패스워드 PW_i^{old} 그리고 변경할 패스워드 PW_i^{new}를 입력한다. 스마트카드는 현재 패스워드의 마스크된 패스워드 $PW_i^{old'}=h(PW_i^{old}||b)$와 $v^{'}=N_i \oplus h(ID_i||PW_i^{old'})$를 계산한다. 스마트카드는 $M_i^{'}=h(PW_i^{old'}||v^{'})$를 계산하고 이것을 저장된 M_i와 비교한다. 만약 두 값이 일치하지 않으면 스마트카드는 이 단계를 종료한다. 그렇지 않다면 다음 처리를 수행한다.

(2) 스마트카드는 $PW_i^{new'}=h(PW_i^{new}||b)$와 $N_i^{'}=v^{'} \oplus h(ID_i||PW_i^{new})$ 그리고 $M_i^{'}=h(PW_i^{new'}||v^{'})$를 계산한다.

(3) 스마트카드는 N_i와 M_i를 새로운 값인 $N_i^{'}$와 $M_i^{'}$으로 변경한다.

3.5 AUAKAS에 대한 속성 및 안전성

Jung등은 AUAKAS를 제안하고 다음과 같은 보안의 14가지 속성 및 안전성을 제공함을 주장하였다[15].

(P1) 사용자 익명성을 보증한다.
(P2) 상호 인증을 제공한다.
(P3) 세션키 동의를 제공하다.
(P4) 스마트카드 분실 공격에 안전하다.
(P5) 오프라인 패스워드 추측 공격에 안전하다.
(P6) 사용자 가장 공격에 안전하다.
(P7) 잘못된 패스워드를 쉽게 탐지한다.
(P8) 재전송 공격에 안전하다.
(P9) 내부자 공격에 안전하다.
(P10) 서비스 거부 공격에 안전하다.
(P11) 훔친 검증자 공격에 안전하다.
(P12) 오프라인 식별자 추측 공격에 안전하다.
(P13) 패스워드 변경에 편의성 및 효율성을 제공한다.
(P14) 게이트웨이 가장 공격에 안전하다.

4. 가장 공격

본 장에서는 AUAKAS[15]가 사용자 가장 공격과 게이트웨이 가장 공격에 취약함을 보인다. 즉, AUAKAS에서 주장한 14가지 속성 및 안전성 중 (P6)과 (P14)를 제공하지 못함을 보인다.

이들 두 가지 공격을 제시하기 위해 본 논문에서는 적법한 사용자로 등록된 공격자 U_a를 가정한다. 즉 U_a는

*GWN*으로부터 {N_a, M_a, $h()$} 정보가 저장된 스마트카드를 발급 받을 수 있음을 의미한다. 적법한 스마트카드를 발급받은 적법한 사용자는 AUAKAS에서 임의의 사용자에 대한 가장 공격과 게이트웨이 가장 공격을 수행할 수 있다.

4.1 사용자 가장 공격

사용자 가장 공격이 가능함을 보이기 위해 U_a가 임의의 적법한 사용자 U_b로 *GWN*에게 의해 인증될 수 있음을 보인다. 공격을 위해 U_a는 인증 단계를 이용하여 공격을 수행할 수 있다. 구체적인 공격 과정은 다음과 같다.

(UA1) U_a는 자신의 스마트카드를 터미널에 넣고 ID_a와 PW_a를 입력한다. 스마트카드는 마스크된 패스워드 $PW_a'=h(PW_a||b)$와 $v'=N_a \oplus h(ID_a||PW_a')$를 계산한다. 스마트카드는 $M_a'=h(PW_a'||v')$를 계산하고 이것을 저장된 M_i와 비교한다. 두 값이 일치하기 때문에 스마트카드는 U_a의 적법성을 알리고 다음 단계를 수행하고자 한다. 이 과정에서 U_a는 v'을 시스템에 저장한다.

(UA2) U_a는 난수 $R_1 \in \{0, 1\}^l$을 선택하고 $DID_b=h(ID_b||R_1)$를 계산한다. 그런 후 $k=h(DID_b||v'||\ T_1)$와 $A_b=E_k(DID_b||R_1||T_1)$를 계산한다.

(UA3) U_a는 공개 채널을 통하여 $<DID_b, A_b, T_1>$를 *GWN*에게 보낸다.

$<DID_b, A_b, T_1>$를 받은 *GWN*은 검증 단계의 (1) 처리과정을 통해 사용자 인증을 수행한다.

(UV1) *GWN*은 먼저 타임스탬프의 적법성 $|T_1'-T_1|<\Delta T$을 검사한다. *GWN*은 $k'=h(DID_b||v||T_1)$를 계산하고 $D_{k'}(A_b)=\{DID_b||R_1||T_1\}$ 수행한다. 그런 후 수신한 값과 메시지 안의 DID_b와 T_1을 비교한다. 조건이 만족할 것이기 때문에 *GWN*은 U_b의 적법성을 인지하고 다음 단계를 진행한다.

즉, AUAKAS는 *GWN*에 등록된 사용자가 임의의 다른 적법한 사용자인척 할 수 있으므로 안전하지 않다. 이는 이들이 주장하는 (P6)에 위배된다.

4.2 게이트웨이 가장 공격

게이트웨이 가장 공격이 가능함을 보이기 위해서 U_a가 적법한 사용자 U_i에게 적법한 응답 메시지를 보낼 수 있고, 이 메시지가 U_i에 의해 적법한 *GWN*으로 인증될 수 있음을 보인다. 공격을 위해 U_a는 검증 단계를 이용하여 공격을 수행할 수 있다. 또한 공격을 위해 U_a는 (UA1) 과정을 이용하여 v'를 저장하고 있다고 가정한다. U_i로부터 로그인 요청 메시지$<DID_i, A_i, T_1>$를 받은 U_a는 다음과 같은 공격 과정을 수행한다.

(GA1) U_a는 먼저 타임스탬프의 적법성 $|T_1'-T_1|<\Delta T$을 검사한다. U_a는 $k'=h(DID_i||v'||T_1)$를 계산하고 $D_{k'}(A_i)=\{DID_i||R_1||T_1\}$ 수행한다. 그런 후 수신한 값과 메시지 안의 DID_i와 T_1을 비교한다. 만약 조건이 만족하면 U_a은 U_i의 적법성을 인지하고 다음 단계를 진행한다. 그렇지 않다면 이 단계를 종료한다.

(GA2) U_a는 검증단계의 (2)-(5)를 건너뛰고 적법한 센서노드의 SID_n와 난수 SK를 선택하여 $D_i=E_{k'}(DID_i||\ SID_n||SK||R_1||T_4)$를 계산하고 U_i에게 공개 채널을 통해 $<D_i, T_4>$를 전송한다.

$<D_i, T_4>$를 받은 U_i는 검증 단계의 (7) 처리과정을 통해 *GWN* 인증을 수행한다.

(GV1) U_i는 먼저 $|T_4'-T_4|<\Delta T$를 검사한다. 적법한 사용자인 U_a는 *GWN*와 타임스탬프가 동기화 되어 있으므로 이 조건을 성공적으로 통과한다. U_i는 $D_k(D_i)=\{DID_i||SID_n||SK||R_1||T_4\}$를 계산하고 이전 값 DID_i와 R_1 그리고 T_4와 비교한다. 조건이 만족함으로 U_i는 U_a를 적법한 *GWN*으로 인식한다.

즉, AUAKAS는 *GWN*에 등록된 사용자가 임의의 다른 적법한 사용자에게 *GWN* 가장 공격을 수행 수 있으므로 안전하지 않다. 이는 이들이 주장하는 (P14)에 위배된다.

5. 결론 및 향후연구

본 논문에서는 최근에 제안된 무선센서네트워크에서 대칭키 암호시스템에 기반한 익명의 사용자 인증과 키동의 기법 (AUAKAS)을 살펴보고 AUAKAS에 존재하는 두 가지 가장 공격의 취약성을 보였다. 특히, 이러한 인증 및 키동의 기법은 다양한 사물인터넷을 위한 기본 정보보호 기법으로 활용되고 있는 상황에서 보안에 취약한 기법이 실제 응용에 적용되면 치명적인 문제로 야기될 수 있음으로 더욱더 주의를 기울여야 한다.

향후 연구로는 본 논문에서 제시된 취약성을 해결할 수 있는 프라이버시를 제공하면서 안전성을 제시할 수 있는 경량의 보안 기법의 설계가 제시될 필요가 있다. 특기, 이러한 기법의 설계에 있어서 사용자 등록 과정에서 GWN의 비밀키 관련된 정보가 정당한 사용자에게도 노출되지 않도록 안전한 분배가 고려된 기법 설계를 통해 본 논문에서 제시된 가장공격의 문제점에 대한 해결책을 제시할 수 있을 것이다.

REFERENCES

[1] H.-J. Mun, H.-Y. Jeong, K.-H. Han, "Improved Trialateration Method on USN for reducing the Error of a Moving Node Position Measurement", Journal of Digital Convergence, (2016), Vol. 14, No. 5, pp. 301-307.

[2] K.-H. Lee, "A Study of Security Policy for U-Healthcare Service", The Journal of Digital Convergence, (2013), Vol. 11, No. 11, pp. 747-751.

[3] K.-K. Lim. Y.-H. Lim, "A Study on User Satisfaction in u-IT New Technology Verification Projects Focused on Domestic RFID/USN Pilot Projects", Journal of Digital Convergence, (2010), Vol. 8, No. 1, pp. 1-10.

[4] B.-S. Kim, "U-Healthcare & Medical Information System of Status and Operative Challenges for Integrated Medical Information System", Journal of Digital Convergence, (2011), Vol. 9, No. 5, pp. 65-75.

[5] S.-J. Choi, B.-G. Kang, "The Windows Push Server System with Smart Device Identifying Fingerprints over IEEE 802.15.4 Protocol", The Journal of Digital Convergence, (2012), Vol. 10, No. 11, pp. 419-425.

[6] B.-H. Shin, H.-K. Jeon, K.-Y. Chung, "An Energy Efficient Clustering Method Based on ANTCLUST in Sensor Network", Digital Convergence, (2012), Vol. 10, No. 1, pp. 371-378.

[7] H.-W. Choi, M.-C. Ryoo, C.-S. Lee, H. Kim, "Secure Data Gathering Protocol over Wireless Sensor Network", The Journal of Digital Convergence, (2013), Vol. 11, No. 12, pp. 367-380.

[8] H. Kim, "Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS", Sensors, (2014), Vol. 14, doi:10.3390/s141223742.

[9] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, (1981), Vol. 24, pp. 770-772.

[10] S.-W. Lee, H. Kim, K.-Y. Yoo, "Improved efficient remote user authentication scheme using smartcards", IEEE Trans. on Consumer Electronics, (2004), Vol. 50, No. 2, pp. 565-567

[11] S.-W. Lee, H. Kim, K.-Y. Yoo, "Efficient verifier-based key agreement protocol for three parties without server's public key", Applied Mathematics and Computation, (2005), Vol. 167, No. 2, pp. 996-1003.

[12] M. L. Das, "Two-factor user authentication scheme in wireless sensor networks", IEEE Trans. on Wirel. Commun., (2009), Vol. 8, pp. 1086-1090.

[13] H. Kim, S.-W. Lee, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks", IEEE Trans. on Consumer Electronics, (2009), Vol. 55, No. 2, pp. 492-498.

[14] L. Chen, F. Wei, C. Ma, "A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques", Int. J. Distrib. Sens. Netw., (2015), doi:10.1155/2015/704502.

[15] J. Jung, J. Kim. Y. Choi, D. Won, "An Anonymous User Authentication Scheme based on a Symmetric Cryptosystem in Wireless Sensor Networks", Sensors, (2016), Vol. 16, doi:10.3390/s16081299.

[16] H. Kim, S. W. Lee, "Authenticated Key Agreement Scheme with Forward Secrecy for Wireless Sensor

Networks", International Journal of Control and Automation, (2015), Vol. 8, No. 11, pp. 279-288.

최 해 원(Choi, Hae Won)

・2009년 2월 : 경북대학교 컴퓨터공학과(공학박사)
・2006년 9월 ~ 현재 : 경운대학교 컴퓨터공학과 교수
・2015년 10월 ~ 현재 : ㈜T.A.Think 대표이사
・관심분야 : 유비쿼터스 컴퓨팅, 알고리즘, 생명정보학, 정보보호
・E-Mail : chw@ikw.ac.kr

김 현 성(Kim, Hyun sung)

・2002년 2월 : 경북대학교 컴퓨터공학과(공학박사)
・2012년 3월 ~ 현재 : 경일대학교 사이버보안학과 교수
・2010년 2월 ~ 현재 : 정보융합보안연구소 소장
・2015년 12월 ~ 현재 : 말라위대학교 수학과 방문교수
・관심분야 : 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호
・E-Mail : kim@kiu.ac.kr