Journal of Korea Multimedia Society Vol. 18, No. 12, December 2015(pp. 1483-1491)
http://dx.doi.org/10.9717/kmms.2015.18.12.1483

사물인터넷에서 ID기반 원격 사용자 인증 방식

박기성†, 이성엽††, 박요한†††, 박영호††††

An ID-Based Remote User Authentication Scheme in IoT

KiSung Park†, SungYup Lee††, YoHan Park†††, YoungHo Park††††

ABSTRACT

Applications of Internet of Things (IoT) supply various conveniences, however unsolved security problems such as personal privacy, data manipulation cause harm to persons, even nations and an limit the applicable areas of Internet of IoT technology. Therefore, study about secure and efficient security system on IoT are required. This paper proposes ID-based remote user authentication scheme in IoT environments. Proposed scheme provides untraceability of users by using different pseudonym identities in every session and reduces the number of variables. Our proposal is secure against inside attack, smart card loss attack, user impersonation attack, server masquerading attack, online/offline password guessing attack, and so on. Therefore, this can be applied to the lightweight IoT environments.

Key words: Internet of Things, Authentication, ID-based, Untraceability

1. 서 론

사물인터넷은 기존의 유선통신을 기반으로 한 인터넷이나 모바일 인터넷보다 진화된 단계로 인터넷에 연결된 사물이 사람의 개입 없이 상호간에 자율적으로 정보를 주고받아 처리하는 기술이다. 사물인터넷은 스마트 그리드, 지능형 교통 시스템, 스마트 홈, 원격 진료 등과 같이 실생활에 적용되고 있다. 이러한 사물인터넷 응용 기술들은 인간의 편의를 제공하는 반면 보안문제 해결 없이는 프라이버시문제, 데이터 조각으로 인한 물리적 피해 등과 같은 개인 수준의 위험 뿐 아니라 국가 수준의 보안 위험이 발생할 수 있으므로 그 응용 범위가 제한받을 수 있다. 따라서 사물인터넷의 효율성과 안전성을 고려한 보안체계에 대한 연구가 필요 하다. 특히, 사물인터넷의 데이터 수집을 위한 사물 디바이스들은 대부분 저용량 환경이므로 기존 서버와 통신망 환경에서 적용 중인 보안 체계와는 달리 사물인터넷의 디바이스 용량을 고려하여 연산량을 최소화하며 안전한 보안체계가 필요하다.[1-3]

사물인터넷은 구조적으로 정보를 취득하는 대량의 사물 디바이스들, 이를 취합하는 게이트웨이, 어플리케이션 기반 데이터베이스 그리고 사용자로 구분될 수 있다. 이와 같은 환경에서 사용자가 필요한 정보를 안전하게 공유하기 위해서는 인증이 필요하다.

최근까지 연구된 사물인터넷 환경에서 사용자 인증의 대표적 방식들은 다음과 같다. 2009년 Wang

※ Corresponding Author : YoungHo Park, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, FAX : +82-53-950-5505, E-mail : parkyh@knu.ac.kr
Receipt date : Aug. 28, 2015, Revision date : Oct. 23, 2015
Approval date : Oct. 30, 2015
† School of Electronics Engineering, Graduate School, Kyungpook National University
(E-mail : kisung2@ee.knu.ac.kr)
†† School of Electronics Engineering, Graduate School, Kyungpook National University
(E-mail : lsy0307@ee.knu.ac.kr
††† Department of Electronics Engineering, Kyungpook National University
(E-mail : hanny12@gmail.com)
†††† School of Electronics Engineering, Kyungpook National University

등은[4] 기존의 Das 등이[5] 제안한 논문에서 공격자가 카드를 습득한 뒤 임의의 패스워드를 이용해 가장 공격이 가능함을 보였다. Wang 등은 Das 등의 방식의 장점을 그대로 보존하면서 가장공격에 안전한 새로운 인증 방식을 제안 하였다. 2013년 Chang 등은[6] Wang 등의 방식에서 인증에 사용되는 값들 중 고정적으로 사용되는 값을 이용하여 가장공격이 가능함을 보이고 이를 개선한 새로운 방식을 제안하였다. Chang 등은 제안한 방식에서 ID가 드러나지 않기 때문에 불추적성(untraceability)이 보장된다고 주장 하였으나 2015년 Li 등은[7] Chang 등이 주장한 불추적성이 달성되지 못하였고, 오프라인 패스워드 추측 공격, 가장 공격, 카드 도난 공격 등에 취약하다는 점을 밝혔다. 또한 Li 등은 Chang 등이 제안한 인증 방식이 인증과정 중 도청에 의해 사용자의 ID가 드러남을 보였다. 2014년 Kumari 등은[8] Chang 등의 인증 방식이 스마트카드를 분실하거나 도난당할 경우에 오프라인 패스워드 추측 공격, 사용자 위장 공격, 서버 가장 공격이 가능하다는 점과 적절한 상호인증이 되지 않음을 보이고 문제점을 개선한 새로운 인증 방식을 제안하였다. 그러나 Kumari 등의 인증 방식은 인증에 사용되는 난수 및 변수의 수가 많아 난수 관리 문제가 있다. 따라서 보다 적은 난수 및 변수를 사용하는 간단한 인증 방식이 요구된다.

본 논문은 사물인터넷에서 ID기반 원격사용자 인증 방식을 제안한다. 제안하는 방식은 인증 과정 중 임의의 ID를 사용한다. 또한 등록과정에서 패스워드는 연산을 거쳐 서버로 전송되므로 서버는 사용자의 패스워드를 알 수 없다. 따라서 공격자는 사용자의 실제 ID를 알 수 없고 공격자가 인증 메세지 및 스마트카드를 얻더라도 사용자에 대한 어떠한 정보도 얻을 수 없다. 제안한 인증 방식은 Kumari등의 인증 방식에서 변수 생성을 위한 난수의 수를 줄이고 인증 과정 중 서버로 전송되는 변수의 수를 개선하였다. 따라서 Kumari 등의 인증 방식 보다 적은 난수를 사용하므로 난수 및 변수 관리가 용이하고 보다 작은 용량과 저메모리를 가진 사물인터넷에서도 효율적으로 사용할 수 있다. 제안한 방식은 불추적성이 보장되고 서비스 거부(DoS) 공격, 사용자1 위장 공격, 서버 가장 공격, 패스워드 추측 공격, 스마트카드 분실 공격, 리플레이 공격 등에 안전하다.

2. 기존의 사용자 인증 방식

공개된 채널에서 원격 사용자 인증 시스템은 Lamport에[9] 의해서 제안되었다. 정보를 보호하고 안전한 로그인 요청을 생성하기 위해서 스마트카드 기반 패스워드 인증 방식들이 활발히 연구되고 있고[10,11] 이를 통해 사용자는 자신이 원할 때 안전하게 서버와 인증할 수 있다. 본 장에서는 기존에 연구된 대표적인 인증 방식들을 기술한다.

2.1 Wang 등의 방식

Wang 등은[4] Das 등이[5] 제안한 방식에서 인증 과정 중 패스워드가 인증에 독립적으로 사용된다는 점을 파악하고, 공격자가 카드를 습득하면 이 점을 이용해 임의의 패스워드 값으로 정상적인 사용자인 것처럼 위장 공격이 가능함을 보였다. 또한 기존의 Das 등이 제안한 구조의 이점을 그대로 가져 오면서 기존의 방식보다 향상된 패스워드 인증 구조를 가지고 상호인증이 가능함을 보였다.

Wang 등의 방식은 위 그림 1, 2 및 3과 같이 등록, 로그인 그리고 인증 단계로 이루어진다. Wang 등은 기존의 Das 등의 인증 방식에서 패스워드가 독립적으로 사용되어 임의의 패스워드로 인증이 가능하다는 점을 개선하기 위해 서버에서 사용자의 ID를 검증하는 방식을 제안하였다. 서버에서 검증을 위해 생성하는 $ID_i^{'}$에는 패스워드에 관한 요소가 포함되어 더 이상 패스워드가 인증에서 독립적으로 사용되지 않

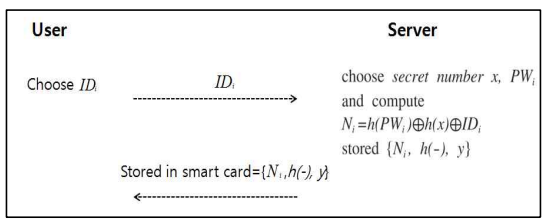

Fig. 1. Registration phase of the scheme of Wang et al..

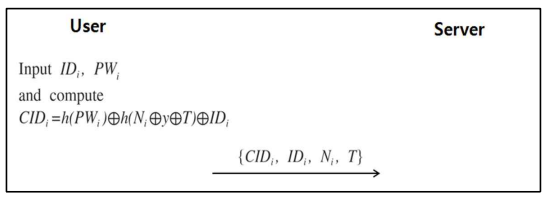

Fig. 2. Login phase of the scheme of Wang et al..

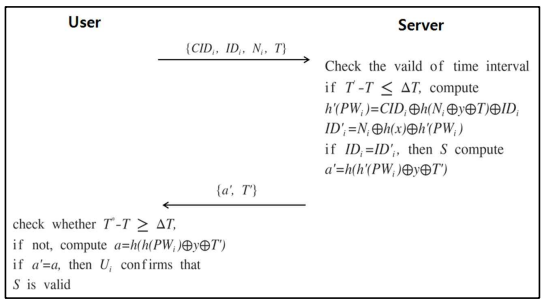

Fig. 3. Authentication phase of the scheme of Wang et al..

는다. 따라서 Wang 등은 Das 등의 인증 방식의 문제점을 개선하였다고 주장하였다.

2.2 Chang 등의 방식

Chang 등은[6] Wang 등이 제안한 인증 방식이 가장공격에 취약하다는 치명적인 약점을 발견하였다. Chang 등은 인증과정에서 사용되는 파라미터의 일부 값들이 고정되어 사용되고 있는 점을 발견하고, 임의의 ID를 선택해 정상적인 사용자인 것처럼 가장 공격이 가능함을 보였다. 이 과정에서 공격자는 사용자의 ID값을 추측할 수 있다. Wang 등의 인증 방식에서 ID 값은 항상 고정되어 있으므로 공격자는 ID를 통해 사용자의 습관이나 행동을 알 수 있다. 이러한 이유로 Chang 등은 공격자가 ID를 추적할 수 없도록 하는 새로운 방식을 아래 그림 4, 5 및 6과 같이 등록, 로그인 그리고 인증 단계로 제안하였다.

Chang 등은 Wang 등과는 다르게 인증 과정에서

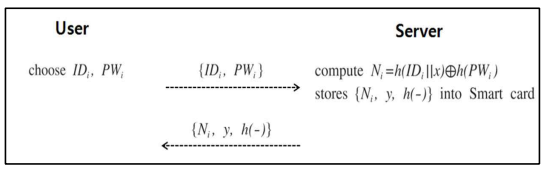

Fig. 4. Registration phase of the scheme of Chang et al..

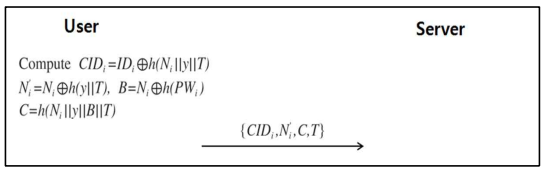

Fig. 5. Login phase of the scheme of Chang et al..

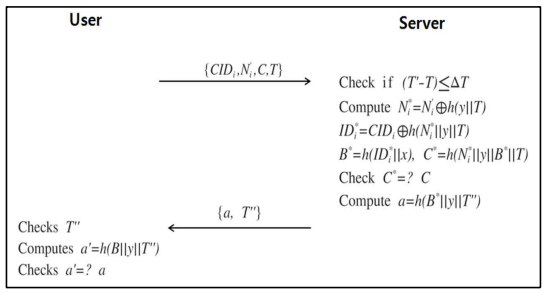

Fig. 6. Authentication phase of the scheme of Chang et al..

인증에 사용되는 변수 값들을 XOR연산과 hash연산을 통해 계속 변경한다. Wang 등의 인증 방식에서는 스마트카드의 N_i를 계속 반복하여 사용하였으나, Chang 등의 인증 방식에서는 N_i를 연산을 거쳐 $N_i^{'}$으로 만들고 새로운 값 C를 인증에 사용하여 인증에 사용되는 변수 값들을 계속 변경한다. 이와 같은 방법으로 Chang 등은 Wang 등의 인증 방식의 문제점을 개선한 새로운 인증 방식을 제안하였다. 2015년 Li 등은[7] Chang 등의 방식의 안전성을 분석하여 인증 과정 중 도청에 의해 ID가 추적가능 함을 보이고 오프라인 패스워드 추측 공격, 가장 공격, 카드 도난 공격에 취약한 점을 밝혔다. 또한 Chang 등의 인증 방식에서 패스워드 검증과정과 패스워드 갱신 과정이 비효율적이라 주장하고 다음과 같이 ID를 밝히는 과정을 분석하였다. 공격자는 다음과 같은 과정으로 ID를 찾아낸다. 먼저 인증과정 중 로그인 요정 메세지 $CID_i, N_i^{'}, y, T$ 를 도청하여 습득한다. 그리고 카드에 저장되어 y와 T를 이용하여 N_i를 찾아내고 $h(N_i\|y\|T)$를 생성한다. CID_i는 $ID_i \oplus h(N_i\|y\|T)$ 이므로 $CID_i \oplus h(N_i\|y\|T)$를 통해 ID_i를 찾을 수 있다. 이와 같이 Li 등은 Chang 등이 주장한 불추적성이 불가능함을 보였다.

2.3 Kumari 등의 방식

Kumari 등은[8] Chang 등의 구조가 스마트카드를 분실하거나 도난당할 경우, 스마트카드 안에 저장되어 있는 secret number y에 의해 오프라인 패스워드 추측 공격, 유저 위장 공격, 서버 가장 공격이 가능함을 보였다. 그리고 사용자의 ID가 추적이 불가능하다는 Chang 등의 주장과 달리 y를 이용하여 사용자의 ID가 추적이 가능함을 증명했다. 또한 사용자의

패스워드를 공격자가 임의의 패스워드로 변경하거나 사용자의 패스워드 변경 요청이 거절될 수 있음을 보이고, 적절한 상호인증이 되지 않음을 주장하였다.

Kumari 등의 인증 방식은 그림 7, 8과 같이 등록 그리고 로그인 및 인증 단계로 구성된다. Kumari 등의 인증 방식은 Chang 등의 인증 방식과 달리 등록 과정에서 난수 b와 y_i가 추가되어 변수 값을 생성하는데 사용되었다. 그리고 인증에 사용되는 모든 값은 XOR 또는 hash 연산을 거쳐 저장되며 공격자가 스마트카드에 저장되어 있는 난수 및 변수를 이용해도 사용자의 ID를 찾아낼 수 없다. 따라서 공격자가 스마트카드의 정보를 습득하더라도 악의적인 목적으로 사용할 수 없다. 또한 Kumri 등의 인증 방식에서는 이전의 인증 방식들과 달리 새로운 값 A_i와 M_i를 생성하여 로그인 단계에서 올바른 ID와 패스워드가 입력되었는지 확인하는 과정이 추가되었다.

3. 제안한 ID기반 원격 사용자 인증 방식

본 논문에서 제안한 방식은 Kumari 등의 방식이 가진 장점을 그대로 보존하면서 인증과정 중 변수

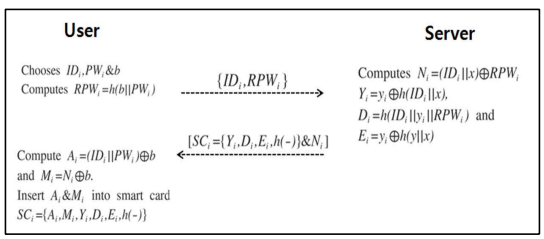

Fig. 7. Registration phase of the scheme of Kumari et al..

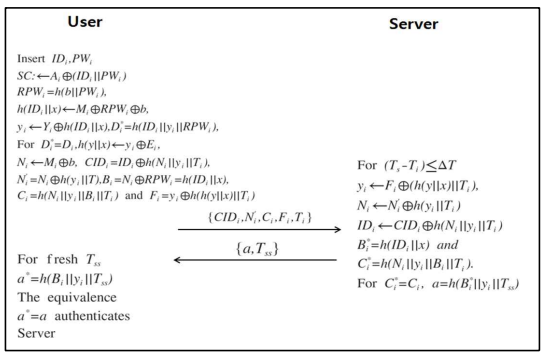

Fig. 8. Login & Authentication phase of the scheme of Kumari et al..

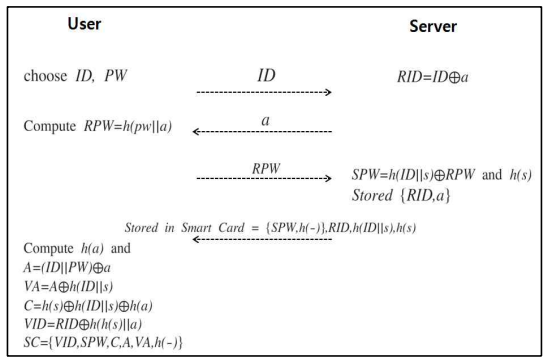

Fig. 9. Registration phase of the proposed scheme.

및 난수의 수를 개선하였다. 제안한 방식에서는 Kumari 등의 방식과 다르게 인증에 난수 y_i, x, b, y를 사용하지 않고 난수 a와 서버의 비밀키를 사용한다. 또한 로그인 요청 메시지에 포함된 변수가 하나 줄어 난수 및 변수의 수를 개선하였다. 따라서 제안된 방식은 난수 관리에 용이하고 기존의 방식들에 비해 아래와 같은 많은 장점을 가진다.

1) 사용자는 패스워드를 등록단계에서 평문으로 보내지 않고 RPW로 연산하여 전송한다. 따라서 서버는 사용자의 패스워드를 알 수 없다.

2) 서버는 각 각의 사용자들 마다 다른 난수 a를 분배 하므로 모든 사용자는 같은 난수를 이용하지 않는다. 결과적으로 인증에 사용되는 난수의 수가 줄어들어 난수 관리 문제를 해결할 수 있다.

3) 서버가 분배하는 난수 a와 서버의 비밀키는 평문으로 카드에 저장되어있지 않고 연산을 거쳐 저장되어 안전하다.

4) 스마트카드는 timestamp를 이용하여 카드가 언제 기기에 주입되는지 그리고 올바른 패스워드가 입력되었는지 알 수 있다.

5) 기존의 방식들보다 적은 난수 및 변수를 사용하는 인증과정을 가지므로 작은 메모리와 용량을 가진 기기에서 효율적으로 사용 가능하다.

본 논문에서 제안한 방식의 등록과정에서 서버는 안전하며 내부공격자는 데이터를 조작하는 active 공격은 불가능하다고 가정한다.

위 그림 9는 제안한 방식 중 등록 단계를 나타내고 등록 단계는 아래와 같은 과정으로 이루어진다.

1) 사용자는 ID와 PW를 선택하고 ID를 서버로 전

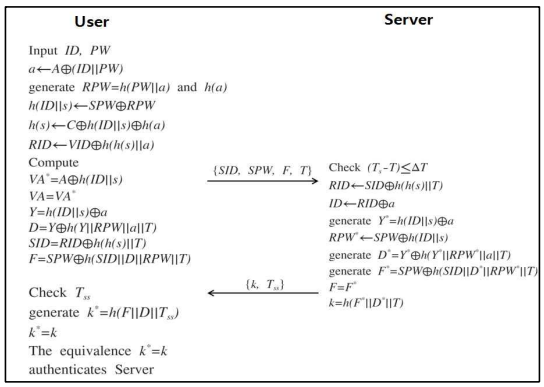

Fig. 10. Login & Authentication phase of the proposed scheme.

송한다. 서버는 다른 사용자와 중복되지 않는 난수 a를 선택하고 RID를 계산한다.

2) 서버는 a를 사용자에게 전송하고 사용자는 RPW를 계산하여 서버로 전송한다.

3) 서버는 RPW를 전송받고 SPW를 계산하여 스마트카드에 SPW, h(-)를 저장하고 RID, h(ID||s), h(s)를 스마트카드와 함께 사용자에게 전송한다. 또한 RID와 a를 서버에 저장하여 사용자 식별에 사용한다. 이 때 s는 서버의 비밀키이다.

4) 사용자는 h(a), A, VA, C, VID를 계산하고 스마트카드에 VID, SPW ,C, A ,VA ,h(-)를 저장하여 발행하고, 전송받은 RID, h(ID||s)와 h(s)는 삭제한다.

위 그림 10은 제안한 방식에서 등록 및 로그인 단계를 기술한 것이다.

1) 사용자는 인증을 위해 스마트카드를 기기에 넣고 ID와 PW를 입력한다.

2) 입력 받은 ID, PW를 이용하여 스마트카드는 $A \oplus (ID \| PW)$ 연산을 통해 a를 찾아내고, RPW와 h(a)를 생성한다. 생성한 RPW는 SPW와 XOR연산되어 h(ID||s)를 찾는데 이용된다.

3) 스마트카드는 C와 h(ID||s) 그리고 h(a)를 XOR연산하여 h(s)를 찾아낸다. 그리고 h(h(s)||a)를 생성해 VID와 XOR연산 후 RID를 찾아낸다.

4) 스마트카드는 $VA^* = A \oplus h(ID \| s)$를 계산하여 카드에 저장된 VA와 동일한지 검증한다. 만약 $VA = VA^*$라면 올바른 ID와 PW가 입력되었다고 판단하고 인증을 위한 값을 생성하고, 그렇지 않다면 인증에 사용되는 값을 생성하지 않는다.

5) $VA = VA^*$의 경우, 스마트카드는 인증에 사용될 값 $Y = h(ID \| s) \oplus a$를 생성하고 Y를 이용해 $D = Y \oplus h(Y \| RPW \| a \| T)$를 생성한다. 그리고 RID 값에 h(h(s)||T)를 XOR연산하여 SID를 생성한다.

6) 스마트카드는 Y를 포함된 D를 이용해 $F = SPW \oplus h(SID \| D \| RPW \| T)$값을 만들고 로그인 요청 메시지 {SID, SPW, F, T}를 공개된 채널을 통해 서버로 전송한다.

7) 서버는 로그인 요청 메시지를 받고 timestamp freshness test를 실시한다. 사용자의 로그인 요청 메시지가 허가된 시간 $T_s - T \leq \Delta T$ 안에 도착했다면, $SID \oplus h(h(s) \| T)$연산을 통하여 RID를 찾아내고 서버에 저장되어 있는 RID와 a를 이용하여 ID를 찾는다.

8) 서버는 $Y^* = h(ID \| s) \oplus a$를 생성하고, $SPW \oplus h(ID \| s)$를 통해 RPW^*를 찾아낸다. 그리고 찾아낸 RPW^*와 Y^*를 이용하여 $D^* = Y \oplus h(Y^* \| RPW^* \| a \| T)$를 생성하고 인증에 필요한 값 F^*를 생성한다.

9) 서버는 사용자로부터 전송받은 F와 생성해 낸 F^*이 일치하는지 확인하고 일치한다면 서버는 $k = h(F^* \| D^* \| T)$ 값과 timestamp freshness test를 위한 timestamp값을 사용자에게 전송한다.

10) 사용자는 서버로부터 받은 timestamp가 적합한 시간 안에 왔는지 판단하고 k^*를 생성해 서버가 전송한 k와 일치하는지 판단한다. 두 값이 일치하면 서버와 사용자간의 인증은 완료된다.

4. 분 석

Kumari 등의 인증 방식은 인증 값 생성을 위해 난수 y_i, x, b, y를 사용하고 5개의 변수를 로그인 요청 메세지로 사용한다. 제안된 인증 방식은 Kumari 등의 인증 방식과 달리 서버가 분배한 난수 a와 서버의 비밀키를 사용하여 인증 값을 생성하고 4개의 변수를 로그인 요청 메시지로 사용한다. 따라서 제안된 인증 방식은 난수 및 변수의 수를 줄여 사물인터넷 환경에서 보다 적은 메모리와 용량을 가진 사물에서도 효과적으로 동작할 수 있다. 본 논문에서 제안한 방식은 다음과 같은 informal analysis를 이용하여 안전성을 분석한다.

4.1 Insider Passive Attack

제안한 방식에서 사용자의 패스워드는 서버로 전

송될 때 평문이 아닌 각 유저에게 할당되어 있는 난수 a로 hash 연산되어 전송된다. 서버는 hash 연산된 값인 RPW만 알 수 있으며 사용자의 실제 비밀번호는 알 수 없다. 만약 내부공격자가 사용자의 패스워드를 얻기 위해서는 RPW값에서 패스워드를 유도해 내야 한다. 또한 내부공격자가 h(s)를 얻더라도 h(a) 값을 알 수 없기 때문에 사용자의 ID를 알 수 없다. 제안한 인증 방식은 내부공격자가 사용자의 패스워드와 난수 a값을 알 수 없으므로 insider passive attack에 대해 안전하다.

4.2 Smart Card Loss Attack

공격자는 스마트카드를 습득하여 스마트카드에 저장되어 있는 값 $\{VID, SPW, C, A, VA, h(-)\}$를 추출해 낼 수 있다. 그러나 공격자는 $\{a, s, PW, ID\}$에 관한 어떠한 값도 알 수 없으므로 스마트카드 분실 공격에 대해 안전하다. 예를 들어 공격자가 SID를 이용하여 ID를 알아내려 한다면 RID값을 얻어야 한다. 그러나 RID값은 $h(h(s)||a)$와 XOR연산되어 카드 내에 VID로 저장되어 있으며 공격자는 사용자의 고유 난수 a를 알 수 없다. 따라서 공격자는 RID를 얻을 수 없다. 또한 공격자가 SPW, C, A, VA를 이용하여 정보를 얻으려고 시도해도 $\{a, s, PW, ID\}$ 없이는 $h(s), h(ID||s), h(a), h(h(s)||T)$ 값을 생성할 수 없고 따라서 공격자는 사용자의 정보를 추측 할 수 없다.

4.3 User Impersonation and Server Masquerading Attack

공격자가 허가된 사용자인 것처럼 위장하기 위해서는 유효한 로그인 요청 메시지를 생성할 수 있어야 한다. 유효한 로그인 요청 메시지 $F = SPW \oplus h(SID \| D \| RPW \| T)$를 만들기 위해서 $Y = h(ID \| s) \oplus a$, $RPW = h(PW \| a)$, $D = Y \oplus h(Y \| RPW \| a \| T)$가 반드시 필요하고 이 값들은 $\{ID, PW, a\}$와 $h(ID||s)$값을 알고 있어야 생성 가능하다. 그러나 스마트카드 안에는 어떠한 유저의 정보도 직접적으로 저장되어 있지 않고 스마트카드가 직접 변수 값을 계산하여 전송한다. 따라서 공격자는 로그인 요청 단계에서 메시지들을 가로채거나 스마트카드 안에 저장된 값들을 이용하여도 $\{ID, PW, a\}$와 $h(ID||s)$값 없이는 인증을 위한 올바른 값들을 생성 할 수 없다. 또한 공격자가 서버로 위장하기 위해서는 서버에서 사용자에게 전송되지는 메시지 $\{k, T_{ss}\}$를 직접 생성해 낼 수 있어야 한다. 그러나 k는 $h(F^* \| D^* \| T)$이므로 공격자는 D^*의 값을 알 수 없고 hash 연산의 one-way 특성으로 인해 k의 값을 생성 할 수 없다. 따라서 공격자는 사용자 위장공격이나 서버 가장 공격을 할 수 없다.

4.4 Denial of Service (DoS) Attack

제안한 방식의 인증 단계에서는 로그인 요청 메시지를 보내기 전에 카드에 저장된 VA와 새로 생성해 낸 VA^*를 검증하는 단계를 거친다. $VA = A \oplus h(ID \| s) = (ID \| PW) \oplus a \oplus h(ID \| s)$이므로 올바른 ID와 패스워드가 입력이 되었을 때만 로그인 요청 메시지를 전송한다. 따라서 사용자의 실수 및 공격자에 의해 임의의 값이 입력되었을 때 로그인 요청 메세지를 서버로 보내지 않으므로 불필요한 시간, 에너지, 계산자원 등을 아낄 수 있다.

4.5 Online Password Guessing Attack

공격자가 스마트카드를 이용해 여러 번의 로그인 시도를 하는 것은 카드 안에 내재되어 있는 검증 메카니즘과 온라인 환경 때문에 불가능하다. 카드 안의 검증 메카니즘은 로그인 요청 메시지를 보내기 이전에 먼저 올바른 ID와 패스워드가 입력되었는지 판단하므로 공격자가 로그인요청을 보내기 위해서는 올바른 ID와 패스워드를 알고 있어야 한다. 또한 일반적으로 온라인 환경에서는 잘못된 ID, 패스워드를 여러 번 입력 했을 경우 로그인 시도가 봉쇄되고, 해제 코드 PUK(private unbloking key)가 있어야 다시 재활성화 된다. 이러한 검증 메카니즘과 온라인 검증 환경 때문에 제안한 인증 방식은 온라인 패스워드 추측 공격에 대해서 안전하다.

4.6 Offline Password Guessing Attack

공격자는 습득한 카드 안에서 $\{VID, SPW, C, VA, A, h(-)\}$를 추출할 수 있고 안전성분석 4.1.2와 같은 이유로 공격자가 스마트카드로부터 $\{ID, a, h(ID||s)\}$에 대한 값들을 얻을 수 없으므로 패스워드를 polynomial 시간 안에 추측할 수 없다. 패스워드를 추측하기 위해서는 패스워드가 포함되어 있는 값 A, VA, SPW, F의 구성요소 중 최소 2개 이상의

값을 정확하게 polynomial 시간 안에 찾아내야 하는데 이것은 불가능하다. 예를 들어 공격자가 $A=(ID\|PW)\oplus a$를 통해서 패스워드를 추측하려 한다면 ID와 a에 대한 값을 정확히 알고 있어야 하고, $SPW=h(ID\|s)\oplus RPW$를 통해 패스워드를 추측하려 한다면 $h(ID//s)$와 a를 정확히 추측 해내야 한다. 이러한 이유로 공격자가 로그인 요청 메시지 $\{SID, SPW, F, T\}$와 카드 안의 저장된 값$\{VID, SPW, C, VA, A, h(-)\}$를 가지고 있더라도 $\{ID, a, h(ID//s)\}$ 없이는 polynomial 시간 안에 패스워드를 추측할 수 없다.

4.7 Replay Attack

제안한 인증 방식은 Kumari 등과 Chang 등의 인증 방식 중 각 메시지와 모든 요소들에 timestamp를 붙여 전송하는 장점을 그대로 보존한다. 각 메시지의 요소들은 timestamp를 독자적으로 포함하고 있으며 timestamp freshness test를 통해 replay attack을 예방할 수 있다. 예를 들어, 서버가 로그인 요청 메시지 $\{SID, SPW, F, T\}$를 받고난 뒤 서버는 timestamp를 이용해 로그인 요청 메시지가 유효한 시간 안에 도착했는지를 판단할 수 있다. 메시지가 유효한 시간 안에 로그인 요청 메시지가 도착했다면 서버는 더 이상의 로그인 요청 메시지를 받지 않고 인증을 진행한다. 또한 서버가 일정 세션동안 사용자와 통신을 이어가고 싶다면 $\{k, T_{ss}\}$를 사용자에게 전송한다. 사용자가 timestamp freshness test를 진행한 후 유효한 시간 내에 메세지가 도착했다면 일정 세션동안 통신이 이루어진다. 이와 같이 매번 통신마다 서버와 사용자는 timestamp freshness test를 진행하므로 replay attack에 대해 안전하다.

4.8 Anonymity and Untraceability

공격자가 스마트카드를 습득해 카드 안의 모든 값 $\{VID, SPW, C, A, VA, h(-)\}$을 추출해 내더라도 ID를 얻기 위해서는 $\{RID, a, s\}$, $\{s,PW,a\}$, $\{a,s\}$, $\{PW,a\}$, $\{PW,a,s\}$를 각각 알고 있어야 한다. 또한 공격자가 로그인 요청 메시지 $\{SID, SPW, F, T\}$를 가로채더라도 ID를 알기 위해서는 $\{a, s, h(ID//s), h(h(s)//T\}$를 알고 있어야하므로 공격자는 유저의 ID를 알 수 없다. 또한 SID는 $RID\oplus h(h(s)\|T)$로 timestamp값에 의해 매번 SID값이 변한다. 따라서 사용자의 익명성과 불추적성은 보장된다.

4.9 Smart Card Possess Inbuilt Verification Mechanism

스마트카드는 로그인 요청 메시지를 서버로 보내기 전에 먼저 입력한 사용자의 ID와 패스워드가 올바른지 판단한다. 만약 올바르지 않은 값들이 입력된다면 로그인 요청 메시지를 서버로 전송하지 않는다. 만약 3회 이상 올바르지 않은 값들이 입력된 경우 로그인 시도는 봉쇄되고, 해제코드 PUK가 있어야 다시 재활성화 된다. 올바른 값들이 입력되었다면 서버는 VA^*를 생성해 카드에 저장된 VA와 VA^*가 일치하는지 검증한다. VA와 VA^*가 일치한다면 로그인 요청 메시지를 서버로 전송한다. 이러한 검증 메카니즘과 온라인 환경에서는 공격자가 로그인 시도할 수 있는 수가 제한적이므로 공격자가 무차별적으로 로그인 시도를 하는 것은 불가능하다.

5. 결 론

사물인터넷 환경에서 사용자가 필요한 정보를 안전하게 공유하기 위해서는 인증이 필요하다. 사물인터넷의 데이터 수집을 위한 사물 디바이스들은 대부분 저용량 환경이므로 기존 통신망 환경에서 적용중인 인증 방식과는 달리 변수 및 난수의 수를 최소화하며 안전한 인증 방식이 요구된다.

본 논문에서는 사물인터넷에서 ID기반 원격사용자 인증 방식을 제안한다. 제안한 인증 방식은 Kumari 등의 인증 방식에서 인증 과정 중 사용되는 4개의 난수를 2개로 줄이고 인증 과정에서 로그인 요청 메세지로 사용되는 변수 값을 5개에서 4개로 개선하였다. 따라서 제안된 인증 방식에서는 난수 및 변수 관리에 용이하고 서비스 거부 공격, 내부자 공격, 스마트카드 분실 공격, 사용자 위장 공격, 서버 가장 공격, 온라인 및 오프라인 패스워드 추측 공격, 리플레이 공격 등에 안전하며 저사양 사물인터넷 환경에 효과적으로 적용될 수 있다.

REFERENCE

[1] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, and D.

Qui, “Security of the Internet of Things: Perspectives and Challenges,” *Wireless Networks,* Vol. 20, No. 8, pp. 2481-2501, 2014.

[2] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” *Computer Networks,* Vol. 76, No. 15, pp. 146-164, 2015.

[3] YoHan Park, and YoungHo Park, “Secure Private Key Revocation Scheme in Anonymous Cluster-Based MANETs ,” *Journal of Korea Multimedia Society,* Vol. 18, No. 4, pp. 499-505, 2015.

[4] Y. Wang, J. Liu, F. Xiao, and J. Dan, “A more Efficient and Secure Dynamic ID-based Remote User Authentication Scheme,” *Computer Communications,* Vol. 32, No. 4, pp. 583-585, 2009.

[5] M.L. Das, A. Saxena, and V.P. Gulati, “A Dynamic ID-based Remote User Authentication Scheme,” *IEEE Transactions on Consumer Electronics,* Vol. 50, No. 2, pp. 629-631, 2004.

[6] Y. Chang, W. Tai, and H. Chang, “Untraceable Dynamic-identity-based Remote User Authentication Scheme with Verifiable Password Update,” *International Journal of Communication Systems,* Vol. 27, No. 11, pp. 3430-3440, 2014.

[7] X. Li, J. Niu, J. Liao, and W. Liang, “Cryptanalysis of a Dynamic Identity-based Remote User Authentication Scheme with Verifiable Password Update,” *International Journal of Communication Systems,* Vol. 28, No. 2, pp. 374-382, 2015.

[8] S. Kumari, M.K. Khan, and X. Li, “An Improved Remote User Authentication Scheme with Key Agreement,” *Computers & Electrical Engineering,* Vol. 40, No. 6, pp. 1997-2012, 2014.

[9] L. Lamport, “Password Authentication with Insecure Communication,” *Communications of the ACM,* Vol. 24, No. 11, pp. 770-772, 1987.

[10] M.S. Hwang and L.H. Li, “A New Remote User Authentication Scheme using Smart Cards,” *IEEE Transactions on Consumer Electronics,* Vol. 46, No. 1, pp. 28-30, 2002.

[11] B.L. Chen, W.C. Kuo, and L.C. Wuu, “Robust Smart-card-based Remote User Password Authentication Scheme,” *International Journal of Communications,* Vol. 27, No. 2, pp. 377-389, 2014.

박 기 성

2015년 2월 경북대학교 산업전자전기공학부 학사
2015년 3월~현재: 경북대학교 대학원 전자공학부 석사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안

이 성 엽

2015년 2월 대구한의대학교 IT콘텐츠학과 학사
2015년 3월~현재 경북대학교 대학원 전자공학부 석사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안

박 요 한

2006년 2월 경북대학교 전자전기컴퓨터 학부 학사
2008년 2월 경북대학교 전자공학과 석사
2008년 3월~2013년 2월: 경북대학교 전자전기컴퓨터학부 박사
2013년~2014년: National University of Singapore 박사후연구원
2014년~현재 경북대학교 산업전자공학과 시간강사
관심분야 : 정보보호, 무선통신보안, 네트워크보안

박 영 호

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. 방문교수
2008년~2014년 경북대학교 산업전자공학과 교수
2014년~현재 경북대학교 전자공학부 교수
관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅