IoT 환경에서 Ring-LPN을 이용한 경량 인증 프로토콜[1)]

최락용* 김광조*

*카이스트 전산학과

New Lightweight Authentication Protocol based on Ring-LPN problem in the IoT environment

Rakyong Choi* Kwangjo Kim*

*Department of Computer Science, KAIST

요 약

최근 주목받고 있는 IoT 환경에서 암호화 기능을 적용하기 위해서는 사전에 디바이스를 인증하는 과정이 반드시 필요하다. 하지만 기존의 인증 프로토콜들은 앞으로 나올 양자 컴퓨터를 이용한 공격에 대해서는 안전성이 증명되어있지 않다.

이에 본 연구는 기존에 쓰던 IoT 환경에서의 인증 프로토콜의 유형과 그 취약점에 대해서 논의하고 IoT 환경에서의 새로운 인증 프로토콜로 후 양자 암호 문제 중 하나인 Ring-LPN 문제를 이용한 Lapin* 인증 프로토콜 기법을 제안한다.

I. 서론

사물인터넷(Internet of Things, 이하 IoT) 환경이란 인간과 사물, 사물과 사물간의 서비스가 인간의 개입 없이도 서로 연결되어지는 환경을 의미하며 앞으로의 미래사회는 이런 IoT 환경 아래 있을 것이다.

IoT 환경의 보안 요구사항으로는 데이터 기밀성, 데이터 무결성, 디바이스 무결성, 시스템 가용성, 사물과 사물 간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 네트워크 오용 방지, 프라이버시 보호, 추적성 방지, 부인 방지 등이 있으며[1] 이 중 사물과 사물 간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 부인 방지 등을 위해 반드시 각 디바이스의 인증을 위한 인증 프로토콜이 필요하다.

1) 본 연구는 미래부가 지원한 2014년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음 [1391104001, 생체모방 알고리즘(Bio-inspired Algorithm)을 활용한 통신기술 연구]

이러한 인증 프로토콜들은 자원이 제한되는 IoT 환경의 특성상 경량 인증이어야 하고 그밖에도 앞으로의 양자 컴퓨터를 이용한 공격들을 대처하기 위해서는 기존의 후 양자 암호를 이용해야 한다. 이에 본 논문은 IoT 환경에서 양자 컴퓨터 공격에 대해서도 안전하게 사용하는 경량 인증 프로토콜에 대해서 논의한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. 우선 II장에서는 IoT 환경에서의 기존 인증 프로토콜의 유형에 대해 간단히 소개하고 각 인증 프로토콜의 취약점에 대해서 분석한다. 이후 III장은 기존의 인증 프로토콜 중 후 양자 암호 방식을 이용하는 인증 프로토콜들이 어떤 것들이 있는지에 대해 소개한 뒤 IV장에서 제안하는 경량 인증 프로토콜을 설명한다. 마지막으로 V장에서는 기존 인증 프로토콜들과 비교하여 개발중인 인증 프로토콜이 가지는 장점에 대해서 설명하고 차후 진행방향에 대해 설명한다.

II. IoT 환경에서 기존 인증 프로토콜의 유형과 취약점

2.1 기존 인증 프로토콜의 유형

IoT 환경에서 공격자는 IoT 환경 내부로의 접근 권한을 얻으려고 하며 이를 위해 위장 공격, 재사용 공격, DoS 공격, Man-in-the-middle(이하 MITM) 공격 등의 공격을 한다.

기존의 IoT 환경에서 이를 방지하기 위해 쓰던 인증 프로토콜로는 다음의 다섯 가지가 있다[2].

○ ID/password 기반 인증 프로토콜:
각 사용자의 ID와 password를 서버에 저장하고 저장된 지식을 바탕으로 인증하는 방식.
○ MAC 주소 기반 인증 프로토콜:
디바이스의 MAC 주소로 인증하는 방식.
○ 암호 프로토콜 기반 인증 프로토콜:
기존에 알려진 암호 프로토콜 혹은 문제를 이용하여 인증하는 방식으로 보안수준이 암호 프로토콜의 보안수준과 일치.
○ 인증서 기반 인증 프로토콜:
인증서 같은 전자서명으로 인증하는 방식
○ Identity 기반 인증 프로토콜:
Identity 기반 암호를 기반으로 한 인증 프로토콜을 설계하여 인증하는 방식

2.2 IoT 환경에서의 보안 요구사항 및 기존 인증 방법의 문제점

IoT 환경에서 인증 프로토콜은 기본적으로 경량 인증 프로토콜이어야 하며(경량 인증) 또한 정상적인 디바이스만이 인증을 통과하고 데이터를 주고받아야하고(인증의 건전성), 디바이스가 메시지의 송수신 여부에 대해 부인하는 것을 방지하기 위해서 디바이스간의 송수신 사실을 증명할 수 있는 부인방지 시스템 역시 필요하다(부인방지 가능). 여기에서 기존 인증 프로토콜의 유형별 취약점은 다음과 같다.

○ ID/password 기반 인증 프로토콜 및 MAC 주소 기반 인증 프로토콜:
정보가 노출되었을 경우 공격자와 사용자(기기) 사이의 차이를 확인할 수 없어 건전성을 만족할 수 없다.
○ 암호 프로토콜 기반 인증 프로토콜:
암호 프로토콜에서 취약점이 발견될 경우 인증 프로토콜 또한 취약점이 발생한다.
하지만 적절한 암호 프로토콜을 사용한다면 경량 인증, 인증의 건전성, 부인방지 가능을 모두 만족할 수 있다.
○ 인증서 기반 인증 프로토콜:
인증서의 특성상 경량 인증이 되기 어렵다.
○ Identity 기반 인증 프로토콜:
공개된 정보를 사용하기 때문에 Identity를 위장한 공격에는 건전성을 보장할 수 없다.

이 중 여기에서 제안하는 인증 프로토콜은 보안 요구사항을 만족하는 암호 프로토콜 기반 인증 프로토콜이다.

III. 기존의 후 양자 암호 기반 경량 인증 프로토콜

후 양자 암호란 양자 컴퓨터, 혹은 양자 컴퓨터를 이용한 알고리즘에 의한 공격에 대해 견딜 수 있는 암호를 말하며 기존에 알려진 후 양자 암호로는 Hash 기반 암호, Code 기반 암호, Lattice 기반 암호, MQE(다변수 2차 다항식) 기반 암호 등이 제안되었다[3].

이 중 본 논문에서는 이중 상대적으로 높은 안전성을 가지는 Code 기반 암호와 Lattice 기반 암호에 집중하여 이를 이용하는 기존의 경량 인증 프로토콜을 정리한다.

3.1 Code 기반 암호

Code 기반 암호를 이용한 인증 프로토콜들은 어떤 $\leftarrow Z^k$에 대해 $v \xleftarrow{U} Z_2^k$, $\epsilon \leftarrow Ber$, $b = v, s\rangle \oplus \epsilon$라고 할 때, (v, b)에서 s를 찾아내는 문제인 LPN(Learning Parity with Noise)

문제를 주로 이용하며 이러한 LPN 문제는 양자 컴퓨터 공격에 견딜 수 있는 어려운 문제로 잘 알려져 있다.

LPN 문제 기반 프로토콜로는 HB (Hopper-Blum) 프로토콜[4]을 시작으로 HB 프로토콜을 변형해서 만든 Juels와 Weis가 제안한 HB+ 프로토콜[5], Duc과 Kim이 제안한 HB* 프로토콜[6] 등이 있다.

그밖에 Heyse 등이 제안한 Lapin 프로토콜[7]의 경우 LPN 문제의 각종 매개변수를 환(ring)으로 변경한 Ring-LPN 문제를 이용한 프로토콜로 LPN을 이용한 프로토콜들에 비해 훨씬 효율적이며 Ring-LPN 기반 프로토콜은 가장 강력한 차세대 후 양자 암호 기반 경량 인증 프로토콜 후보이다.

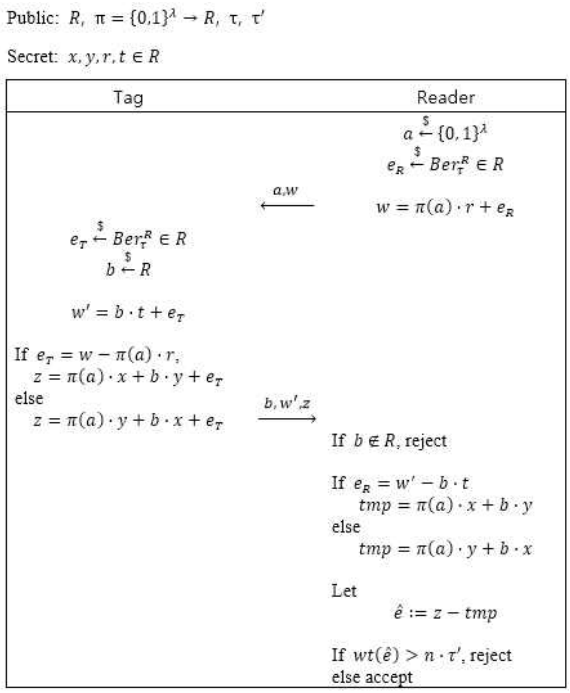
3.2 Lattice 기반 암호

Lattice를 기반으로 한 어려운 문제에는 LPN 문제를 Lattice로 확장해 오늘날엔 완전동형암호 등에 많이 쓰이는 LWE (Learning with Errors) 문제, 어떤 식을 만족하는 가장 작은 정수를 찾는 SIS(Small Integer Solution) 문제 등이 있다. 또한 경량 인증 프로토콜에 한해서는 간단한 키 생성을 통해 효율적으로 쓸 수 있는 NTRU 문제가 주로 쓰인다[8].

NTRU 문제를 실제로 효율적으로 적용한 예로 El Moustaine과 Laurent는 NTRU 문제에 기반한 challenge/response RFID 인증 프로토콜을 만들었으며[9], Ducas 등은 SIS 문제를 NTRU 기존의 Lattice 기반 서명 방식보다 짧은 길이의 공개키와 서명 길이를 가진 서명 기법을 만들었다[10]. 하지만 두 논문 모두 Ring-LPN 기반 Lapin 프로토콜에 비해 뛰어난 결과를 얻지는 못하였다.

IV. 제안하는 경량 인증 프로토콜

기존의 Code 기반 암호와 Lattice 기반 암호를 이용한 인증 프로토콜들 중 가장 효율적이었던 프로토콜인 Lapin 프로토콜[7]과 Ring-LPN 문제를 이용해 Duc과 Kim의 HB* 프로토콜[6]에 적용하면서 각 매개변수를 환에서 가져오도록 바꾸고 안전성 증명은 Lapin과 비슷한 형태로 이루어지도록 Ring-LPN 기반 프로토콜을 [그림 1]과 같이 구성하였다.



[그림 1] 제안하는 프로토콜 Lapin*

위 프로토콜 Lapin*에서 보안 매개변수 에 대해 $n(\lambda)$이 있어 차수가 n인 방정식 f에 대해 환 $= F[x]/(f)$을 찾을 수 있다. 또한 π는 환 R로 보내지는 사상이며 τ는 Bernoulli 분포의 매개변수, τ'은 수락하기 위한 임계값을 의미한다. 키 생성 알고리즘을 통해 비밀키 x, y, r, t를 만들고 [그림 1]의 프로토콜에 따라 태그를 생성하여 인증한다. 이 때 Lapin*의 안전성 증명은 Lapin 프로토콜의 증명을 이용한다.

추론1. 어떤 사상 π와 환 R이 있고 여기서 Ring-LPN 문제가 (t, q, ϵ)에서 어려운 문제라고 하면 어떤 t', ϵ'이 있어 Lapin 프로토콜은 적극적 공격자에 대해 (t', q, ϵ')에서 안전하다.*

*정리2. 인증 프로토콜 Lapin*는 MITM 공격에 안전하다.*

(증명)
Lapin*는 HB*의 매개변수를 환으로 변경한 프로토콜이므로 MITM 공격에 저항할 수 있는 프로토콜이다. ■

V. 결론

IoT 환경에서 암호화 기능을 적용하기 위해서는 사전에 디바이스에 대한 경량 인증이 반드시 필요하다. 이 때 암호 프로토콜 기반 인증 프로토콜을 제외한 나머지 경량 인증 프로토콜들은 인증의 건전성이 깨지거나 부인방지가 불가능해지며 혹은 경량 암호를 만드는 것이 어렵다.

하지만 암호 프로토콜 기반 인증 프로토콜은 이용하는 암호 프로토콜에 따라 강력한 인증 프로토콜이 되므로 [표 1]에서 보는 것과 같이 제안하는 Ring-LPN 기반의 인증 프로토콜 Lapin*은 MITM 공격에 안전하며 따라서 미래 IoT 환경에서 디바이스를 인증할 때 강력한 인증 프로토콜이 될 것이다.

[표 1] LPN 기반 경량 인증 프로토콜의 비교

	HB	HB*	Lapin	Lapin*
격자	LPN	LPN	Ring-LPN	Ring-LPN
MITM 공격에 대한 안전성	안전하지 않음	안전	안전하지 않음	안전

차후 진행방향으로는 우선 Lapin*에 대한 안전성 증명을 더욱 정밀하게 하고 MITM 공격만이 아니라 IoT 환경에서 가능한 모든 공격을 방어할 수 있는 인증 프로토콜을 개발하고 이를 IoT 기반 플랫폼에 적용할 예정이다.

[참고문헌]

[1] 은선기 외, “안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜,” 정보보호학회논문지 제20권 제1호, p.73-83, 2010

[2] 한국정보보호학회, “사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구,” 방송통신위원회, 2010, www.kcc.go.kr/download.do?fileSeq=31995

[3] Daniel J. Bernstein, “A brief survey of post-quantum cryptography,” Invited talk of PQCrypto 2008, 2008, http://cr.yp.to/talks/2008.10.18/slides.pdf

[4] Nicholas J. Hopper and Manuel Blum, “Secure human identification protocols,” ASIACRYPT 2001, Volume 2248 of LNCS, p.52-66, 2001.

[5] Arie Juels and Stephen A. Weis, “Authenticating pervasive devices with human protocols,” Advances in Cryptology - CRYPTO 2005, Volume 3621 of LNCS, p.293-308, 2005

[6] Dang Nguyen Duc and Kwangjo Kim, “Securing HB+ against GRS man-in-the-middle attack”, Proc. Of SCIS 2007, p.23-26, 2007

[7] Stefan Heyse *et al.*, “Lapin: An efficient authentication protocol based on ring-lpn,” Fast Software Encryption 2012, Volume 7549 of LNCS, p.346-365, 2012

[8] Charalampos Manifavas *et al.*, “Lightweight cryptography for embedded systems - a comparative analysis.” Data Privacy Management and Autonomous Spontaneous Security, p.333-349, 2014

[9] Ethmane El Moustaine and Maryline Laurent, “A lattice based authentication for low-cost RFID,” RFID-Technologies and Applications(RFID-TA), 2012 IEEE International Conference on. IEEE, p.68-73, 2012.

[10] Léo Ducas *et al.*, “Lattice signatures and bimodal Gaussians,” Advances in Cryptology - CRYPTO 2013, p.40-56, 2013