경량 암호를 이용한 IoT Secure SNAIL 플랫폼 구성(Ⅰ)

정제성,[1] 김경민,[2] 김학주,[2] 박준정,[1]
안수현,[1] 이동수,[2] 최락용,[2] 김광조,[2] 김대영[2]
KAIST [1]정보보호 대학원 / [2]전산학과

Configuration of IoT Secure SNAIL Platform Using Lightweight Crypto primitives(Ⅰ)

Je-Seong Jeong,[1] Kyung-min Kim[2], HakJu Kim,[2]
Joon-jeong Park,[1] Soo-Hyun, Ahn,[1] Dongsoo Lee,[2]
Rakyong Choi,[2] Kwangjo Kim,[2] Daeyoung Kim,[2]
[1]Graduate School of Information Security, KAIST
[2]Department of Computer Science, KAIST

요 약

사물인터넷(Internet of Things, IoT)은 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망이다. 이러한 IoT는 현재 미래 기술로 각광을 받고 있으나 여러 가지 기술이 통합되어 특정 서비스를 구성하기 때문에 각 요소 자체의 보안 취약성으로 인한 문제가 발생 할 수 있다.

따라서, 본 논문에서는 IoT 보안 문제를 해결하기 위하여 Oliot(Open Language for Internet of Things)와 SNAIL(Sensor Networks for All IP world) 상에 경량 암호 및 인증 프로토콜을 구현할 플랫폼 구성을 제안한다.

I. 서론

사람, 사물, 공간, 데이터 등 모든 것이 연결되는 초연결사회가 도래함에 따라, 사물인터넷(IoT)은 새로운 미래의 경제성장 동력으로 부상하고 있으며 다양한 산업분야 뿐만 아니라 우리생활과 밀접한 홈·가전·의료 ·교통분야에서도 적용 될 것이다. 그리고 이미 우리나라를 비롯해 세계 주요국 및 기업들이 IoT 분야에 적극적으로 투자 ·육성하고 있다. 그러나 IoT 분야는 실생활의 모든 사물에 '직접 접목'(e.g. 스마트홈, 스마트 의료 등) 되기 때문에, 기존 사이버공간의 위험이 현실세계로 전이·확대 될 수 있다. 그리고 이러한 IoT 보안 위협은 오동작·정지 등 사람의 생명을 위협할 만큼 치명적이며, 도입 후에는 사후 보안 조치가 불가능 하거나 고비용이 수반된다. 또한, 보안이 적용 되지 않은 IoT 제품·서비스는 글로벌 시장에서 경쟁력을 상실 할 것이다. 따라서 정보보호가 담보된 안전한 IoT 이용환경을 조성 하여야 한다.[6]

하지만, IoT 환경에서는 보호해야 할 기기의 수가 우리 일상생활의 모든 사물로 확대되고, 그 특성도 다양화(경량·저전력, 초연결성 등) 되면서 기존 보안기술 적용에 한계가 있다.

IoT 적용에 따른 보안 위협과 요구사항은

다음과 같다.

첫째 센서 디바이스 분야이다. 디바이스들이 다양화되고, 종류가 늘어나면서 저사양 기기 사용이 늘어나고, 현재 보안 기술로는 저사양(메모리, CPU 전력 등) 기기에 백신, 암호화, 인증 등 보안을 적용하기 곤란한 경우가 많을 것이다. 그리고 디바이스 수가 많아지고, 보안패치 적용 곤란, 통신 내용 모니터링 곤란에 따른 보안 취약성이 증가 할 것이다. 이를 해결 위해서는 저사양 기기를 포함해 다양한 기기 특성을 반영한 경량 보안 기술(백신, 암호화, 인증 등) 개발 및 적용이 필요 할 것이다. 또한 기기 운영 신뢰성 보장, 무결성 검증 등을 위해 센서/디바이스 보안패치 적용 기술 개발, 센서/디바이스 모니터링 체계를 마련해야 할 것이다.[6

둘째, 네트워크 분야이다. Zigbee, Wi-fi, Bluetooth 등 이동 무선 네트워크 간 상호연동이 되면서, 일정한 보안수준을 유지하기 어렵고, 디바이스 간 통신이 지원되면서, 디바이스 인증이 제한적으로 지원이 될 것이다. 그리고 클라우드 가상화 서비스를 통한 좀비 PC 대량 생산, 냉장고, 청소 로봇, 의료기기 등 대규모 디바이스에 악성코드를 감염시켜 트래픽 폭증 공격이 가능 해 질 것이다. 이를 해결하기 위해 이중망 연동을 위한 프로토콜 상호운용성 기준 마련, 이기종 저사양 연결 통신 네트워크 환경에 적합한 보안기술이 필요 할 것이며 또한 대규모 기기·네트워크에 대한 보안 상태 모니터링 및 감시가 필요 할 것이다.

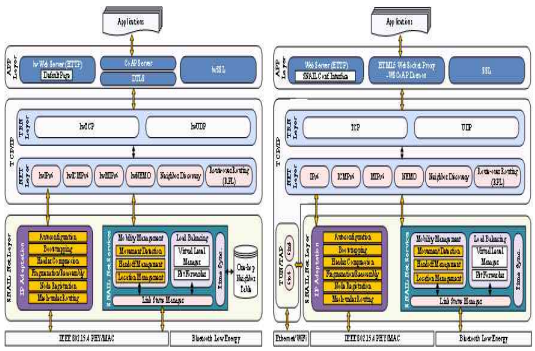
셋째, 플랫폼/서비스 분야이다. 공개 플랫폼을 통한 기기-서비스 간 허위 데이터 전송/오작동 등 공격이 예상되며 IoT 디바이스가 수집한 단편 정보의 중앙 집중 및 조합으로 사용자 신원정보 유출이 될 것이다. 이를 해결하기 위해 안전한 개방형 플랫폼 이용지침 마련, 디바이스/사용자 서비스 간 상호 인증 및 키관리, 신뢰관리 필요, 기기의 개인 정보수집/추적 방지 및 개인 식별 정보 필터링 기술이 필요 할 것이다.

따라서, 본 논문에서는 이러한 IoT 보안취약 분야를 해결하기 위해 Ⅱ장에서는 IoT 보안 플랫폼 구성방안, Ⅲ장에서는 경량 암호와 인증 프로토콜의 구성 방안을 제안하며, Ⅳ장에서는 결론을 맺는다

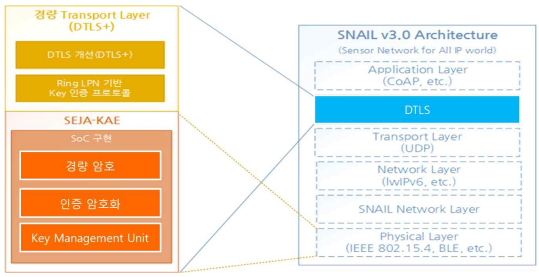
II. IoT Secure 플랫폼

현재 개방형 IoT 서비스 환경에서 기기인증, 부인방지 및 프라이버시(위치, ID 등) 보호를 위한 국내 서비스보안 플랫폼의 기술수준은 미흡한 상황이다.

본 논문에서는 GS1 국제 표준 기반 IoT 인프라 오픈 소스 플랫폼이며, 다양한 사물 인터랙션, Stream 처리 미들웨어, 분산 데이터 스토리지가 적용된 Oliot(Open Language for Internet of Things)[8]과 IETF 6LoWPAN 기반의 초경량 IPv6 프로토콜 스택으로 사물의 IPv6 Seamless 연결을 위한 IoT Connectivity 지원 프로토콜인 SNAIL[Sensor Networks for All IP world)[7]에(그림 1) DTLS+[9] 계층을 추가하여 초경량 암호화 및 인증 암호화 기술이 적용(그림 2) 된 SoC로 구현하여 사물에 모듈 형태로 탑재되고, SNAIL IPv6 프로토콜의 암호 및 인증 스택에 통합을 하여 사물들을 Oliot 플랫폼과 보안 방식으로 통신할 것을 제안한다. 이는 (그림 3) 과 비교하여 보안성이 한층 강화 되었다.

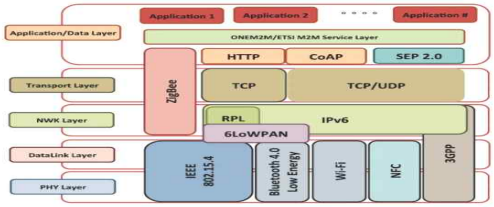


(그림 1) IETF 6LoWPAN 국제표준 기반 초경량 IPv6 플랫폼 (SNAIL)



(그림 2) Secure SNAIL 구조

(그림 3)은 IoT Research EU에서 제시한 구조이다.



(그림 3) Heterogeneous standards environment in IoT(Source : IoT Research EU)

III. 경량 암호와 인증 프로토콜

IoT 환경에서의 보안을 위한 필요사항으로는 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 있다[3]. 이 중에서 사물과 사물 간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 부인 방지 등을 위해서는 반드시 인증 암호와 인증 프로토콜이 필요하므로, IoT에서 인증 암호와 인증 프로토콜의 역할은 매우 중요하다.

현재 IoT 환경에서 디바이스 사이의 프로토콜로 고려되고 있는 것은 DTLS(Datagram Transport Layer Security)와 HIP(Host Identity Protocol)가 있다. 그런데 이 둘은 보안적인 측면이나 성능적인 면에서 부족하여 더 보완되어야 한다. 또한, 현재 IoT 환경에서 쓰이고 있는 인증 프로토콜들의 대부분은 앞으로 나올 양자 컴퓨터를 이용한 공격에 대해서는 안전성이 보장되지 않았다. 따라서, 자원이 제한되는 IoT 환경의 특성에 맞게 인증 암호부분을 경량으로 개선하고, 양자 컴퓨터 공격에 내성을 가지는 프로토콜로 사용하여야 한다. 이러한 사항을 모두 고려한 IoT 환경에서의 프로토콜인 DTLS+을 사용한다.

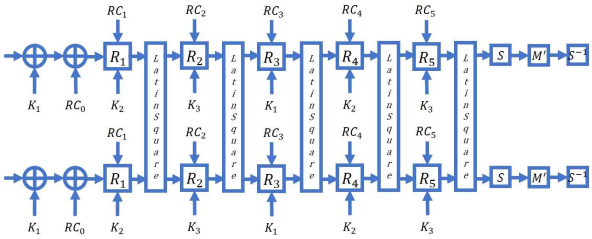
3.1 경량 암호

연산 능력과 전원 등과 같은 자원이 제한되어 있는 IoT 환경에서 현재 다른 분야에서 쓰이고 있는 AES, SHA-3 등의 보안 솔루션을 그대로 적용하기에는 각 디바이스에 부담이 된다. 이러한 환경적 특성으로 인해 최근 IoT에 적합한 경량 암호화 관련 연구가 많이 진행되고 있다. 이에 우리는 알려진 경량 암호 중 하나인 PRINCE[1]를 기반으로 하여 경량이며, 안정성 또한 높은 인증 암호의 사용을 제안한다[2].

작은 하드웨어 칩과 빠른 알고리즘 속도는 경량 암호의 필요조건 중 하나이다. 이를 달성하기 위해 우리는 inverse-free한 구조를 제안한다. inverse-free란 복호화를 할 때 암호화의 역을 취하지 않아도 되는 것이다. 따라서 inverse-free한 구조를 가진다면 복호화를 대비한 하드웨어를 고려하지 않아도 되므로 칩의 크기가 줄어든다. PRINCE는 inverse-free한 구조를 갖기 위해 α-reflection 속성을 가지고 있다. PRINCE가 가지는 α-reflection 속성이란 $PRINCE_{(k)}$의 역과 $PRINCE_{(k\ XOR\ \alpha)}$이 같은 값을 의미한다. 이 구조로 인해 PRINCE의 하드웨어 칩은 AES-128에 비해 14~15배, 여타 다른 경량 암호들에 비해 4~7배 작은 칩 크기를 가진다. 그리고 한 사이클 이내에 암호화가 가능하다.

하지만 PRINCE는 64-bit 크기의 블록과 128-bit 크기의 키만 지원을 하여 유동적이지 않다. 이러한 특성은 128-bit 블록과 유동적인 키 크기를 지원하는 다른 현대 암호들에 비해 전수 조사 공격에 약하다. 이에 우리는 블록 크기를 128-bit으로 늘리고, 유동적인 키 크기를 가지는 형태로 확장하는 방법을 제안한다. 이를 위한 방법은 Swapping 방식과 Orthogonal Latin Square 등이 있다. Swapping 방식은 단순히 각 라운드의 결과를 교차적으로 연결하고, 라운드 수를 늘리는 것인데, 이 방법은 암호 알고리즘의 안정성 향상에 기여하지 못한다. Orthgonal Latin Square는 안전한 혼합 함수로, PRINCE의 inverse-free한 특성에 영향을 끼치지 않고, 라운드 수도 증가시키지 않으면서 128-bit 블록 크기와 128/192/256-bit의 키 크기를 지원할 수 있다. 또한 암호 알고리즘의 안정성에 악영향을 끼치지 않는다. 따라서 PRINCE의 블록 크기와 키 크기를 확장시키기 위해

Orthogonal Latin Square를 제안한다. Orthogonal Latin Square로 확장한 PRINCE는 [그림 4]와 같다.



[그림 4] Orthogonal Latin Suqare로 확장한 PRINCE

3.2 IoT에서의 후 양자 암호 기반 경량 인증 프로토콜

후 양자 암호란 양자 컴퓨터를 이용한 알고리즘에 의한 공격에 내성이 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[4]. 이 중 본 논문에서는 Code 기반 암호 중 Ring-LPN(Ring-Learning Parity with Noise)문제를 응용한 새로운 후 양자 암호 기반 경량 인증 프로토콜 Lapin*[5]를 이용한다. Lapin*는 양자 컴퓨터 공격에 대해 내성을 가짐과 동시에 중간자 공격에도 저항할 수 있다.

IV. 결론

위에서 제안한 방법을 이용한다면 IoT에 최적화된 솔루션을 얻을 수 있고 최근 전 세계적으로 일어나고 있는 IoT 플랫폼 보안과 IoT 인증 암호관련 연구에서의 요구조건을 충분히 만족하는 연구 결과를 도출할 수 있을 것을 예상한다. 이는 미래창조과학부가 제안한 IoT 로드맵에서 언급한 3대 추진 전략인 '보안이 내재화된 IoT 기반 조성', '글로벌 IoT 보안 선도기술 개발', 'IoT 보안 산업 경쟁력 강화' 등의 목표를 이루는데 이루는 데에 필수적인 역할을 할 것으로 사료되며, 본 연구의 후속 과제로서 제안한 보안 IoT 플랫폼을 실제 구현하여 각종 성능 평가와 안전성 검증 등[10]이 있다.

[참고문헌]

[1] Julia Borghoff, *et al.,* "PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications", Advances in Cryptology - ASIACRYPT2012, Springer, pp.208-225, 2012.

[2] HakJu Kim, Kwangjo Kim, "Toward an Inverse-free Lightweight Encryption Scheme for IoT", 2014 Conference on Information Security & Cryptography, Dec. 6 2014, Hanyang University, Republic of Korea

[4] 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

[5] 최락용, 김광조, "IoT 환경에서의 Ring-LPN을 이용한 경량 인증 프로토콜", 2014년 한국정보보호학회 동계학술대회, 2014.12.06, 한양대학교

[6] 미래창조과학부: 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵 (2014년 10월 31일)

[7] Sungmin Hong, *et al.,* "SNAIL: an IP-based wireless sensor network approach to the internet of things" Wireless Communications, IEEE Vol. 17.6, pp.34-42, 2010.

[8] Oliot(Open Language for Internet of Things)<http://gs1oliot.github.io/oliot/>

[9] 안수현, 김광조, "IoT 환경에 적합한 경량 DTLS 프로토콜 구성 방법", 2014년 한국 정보보호학회 동계학술대회, 2014.12.06., 한양대학교

[10] 정제성 외 8명, "경량 암호를 이용한 IoT Secure SNAIL 플랫폼 구성(II)", (작성 중)