사물인터넷을 위한 저전력 보안 아키텍쳐

윤선우 · 박나은 · 이일구*

성신여자대학교

Low Power Security Architecture for the Internet of Things

Sun-woo Yun · Na-eun Park · Il-gu Lee*

Sungshin Women's University

E-mail : nus0205@naver.com / 20180912@sungshin.ac.kr / iglee@sungshin.ac.kr

요 약

사물인터넷은 통신 네트워크 기술과 센서를 활용하여 시공간의 제약 없이 사람과 사물을 유기적으로 연결하고, 실시간으로 데이터를 송수신할 수 있는 기술이다. 전 산업 분야에서 활용되고 있는 사물인터넷은 디바이스의 크기, 메모리 용량, 데이터 전송 성능 등 스토리지 할당 측면의 제약사항을 가지고 있어 제한적인 배터리 용량을 효과적으로 활용할 수 있도록 전력 소모량을 관리하는 것이 중요하다. 종래 연구에서는 주로 암호 모듈의 보안 알고리즘을 경량화하여 전력 효율을 개선한 대신 보안성이 열화되는 문제가 있다. 본 연구에서는 사물인터넷 환경에서 고성능의 보안 알고리즘을 활용할 수 있는 저전력 보안 아키텍처를 제안한다. 이는 무결성 검사를 수행하는 작은 로직을 추가하여 검사 결과에 따라 위협 탐지가 필요한 경우에만 보안 모듈을 실행시켜 저전력 환경에서 상대적으로 복잡도가 높은 보안 모듈을 활용해 높은 보안성과 전력 효율성을 제공할 수 있다.

ABSTRACT

The Internet of Things (IoT) is a technology that can organically connect people and things without time and space constraints by using communication network technology and sensors, and transmit and receive data in real time. The IoT used in all industrial fields has limitations in terms of storage allocation, such as device size, memory capacity, and data transmission performance, so it is important to manage power consumption to effectively utilize the limited battery capacity. In the prior research, there is a problem in that security is deteriorated instead of improving power efficiency by lightening the security algorithm of the encryption module. In this study, we proposes a low-power security architecture that can utilize high-performance security algorithms in the IoT environment. This can provide high security and power efficiency by using relatively complex security modules in low-power environments by executing security modules only when threat detection is required based on inspection results.

키워드

Internet of Things, Security, Low Power Architecture, Energy Efficiency, Integrity

Ⅰ. 서 론

사물인터넷과 통신 네트워크 기술의 발전으로 시공간 제약 없이 사람과 사물 간의 유기적인 연결이 이뤄지면서 사이버 공격으로 인한 피해 규모와 범위가 급격히 증가하고 있다. 특히, 전 산업분야에서 활용되고 있는 사물인터넷은 사이버 위협의 주요 타겟이 되었으며, 그 위험성 및 파급력이 매우 크다. 종래 연구에서는 한정된 배터리 용량을 가진 사물인터넷 환경에서 효율적으로 전력 소모량을 관리하고 통신 네트워크의 보안성을 개선하기 위해 경량 보안 모듈을 개발하여 기기의 물리적인 크기 및 메모리 용량, 데이터 전송 성능 등 스토리지 할당 측면의 제약을 개선하였다. 그러나 대규모 정보 시스템 및 네트워크를 대상으로 한 지능적 공격에 효과적 대응이 불가능한 기술적 한계가 존재한다. 이에 따라 사물인터넷 플랫폼에서

* corresponding author

저전력으로 고성능 보안 모듈을 적용하는 방안에 관한 연구가 필요하다. 본 논문에서는 사물인터넷 플랫폼에 무결성 검사기를 서브 로직으로 추가하여 이상 탐지 시에만 메인 로직의 고성능 보안 모듈을 사용하는 저전력 보안 아키텍처를 제안한다. 이는 종래의 경량 보안 모듈과 고성능 보안 모듈을 사용하는 모델 대비 높은 보안성과 전력 효율성을 가질 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 종래의 사물인터넷을 위한 경량 보안 기법에 관한 연구를 소개하고, 3장에서는 저전력 환경에서 고성능 보안 모듈을 사용할 수 있는 보안 아키텍처를 제안한다. 4장에서는 수식 증명을 기반으로 종래 보안 모듈 대비 제안 모듈의 전력 효율성 개선 효과를 입증하였으며, 5장에서는 논문을 요약하며 결론을 내린다.

II. 경량 보안 기법

사물인터넷은 센서와 통신 기술을 통해 객체 간 유기적인 연결을 지원하고 정보를 수집, 생성, 공유, 활용하는 기술로서 다양한 크기와 형태를 가진다. 종래 디지털 통신 환경에서는 송수신되는 데이터의 오남용을 방지하기 위해 데이터 암호화 기법을 주로 사용하고 있다. 그 중 사물인터넷과 같이 제한된 배터리 용량과 메모리를 가지는 경우, 전통적 암호화 알고리즘이 적합하지 않아 저전력 환경에서 활용할 수 있는 경량 암호화 알고리즘에 관한 연구가 활발히 진행되고 있다[1].

AES(Advanced Encryption Standard)는 현재 표준으로 가장 많이 활용되는 블록 암호 기술이다. 128-bit의 블록 사이즈 및 128, 192, 256-bit의 키를 통해 암호화할 수 있다[2]. 스토리지 측면의 한계점을 갖는 사물인터넷의 마이크로프로세서에 적합하며, 모든 프로세서에서 높은 성능을 보이는 장점을 가진다[3]. PRESENT는 저전력의 높은 하드웨어 효율성을 목표로 제안된 암호화 알고리즘으로 ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) 표준으로 정의되었다. 64-bit의 블록사이즈와 80-bit, 128-bit의 키 크기를 가지며, AES보다 2.5배 작은 하드웨어 설계가 가능해 경량 알고리즘 구현이 유리하다[4]. KATAN은 ARX(Addition, Rotation, eXclusive-or) 기반의 암호화 알고리즘으로, 사칙 연산을 가지고 블록 알고리즘을 구성하는 것이 특징이다[5]. 32, 48, 64-bit 블록 사이즈를 가지며, 80-bit의 키 사이즈를 사용한다. non-linear, boolean, shift, xor 연산으로 구성되며, 254번의 round 함수를 수행한다.

III. 저전력 보안 아키텍처 제안

본 절에서는 저전력 환경에서의 높은 보안성 및 전력 효율성 제공을 위한 '고성능 보안 알고리즘을 활용할 수 있는 저전력 보안 아키텍처'을 제안한다. 아키텍처의 전체 구조는 그림 1과 같다.

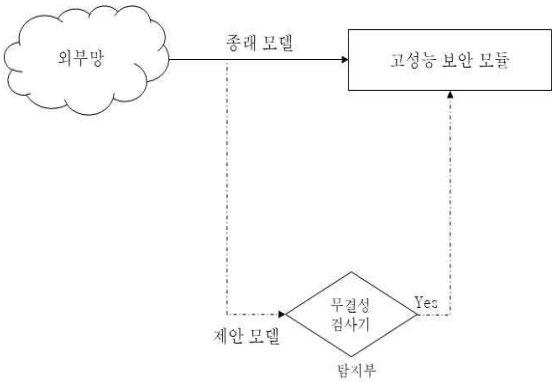

그림 1. 사물인터넷 보안 메커니즘 구조도

그림 1은 사물인터넷 기기가 수신한 외부 신호에 대해 별도의 사전 탐지 없이 고성능 보안 모듈로 이상 행위 탐지 등 보안 조치를 수행하는 종래 방식과 별도의 로직으로 사전에 이상 행위 탐지를 수행하고 이상 감지가 된 경우에만 고성능 보안 모듈을 호출하여 보안 조치를 수행하는 제안 방식인 저전력 보안 아키텍처에 대한 구조도이다.

종래에는 매 수신 신호마다 고성능 보안 모듈 혹은 경량 모듈을 실행해 저전력 환경에 비효율적이거나 보안성이 열화되는 한계점을 가진다. 반면, 제안 방식은 서브 로직의 탐지부에서 이상 행위가 감지된 경우에만 메인 로직의 고성능 보안 모듈을 호출하여 수행함으로써, 저전력 환경에서도 복잡도가 높은 고성능 보안 모듈을 활용할 수 있다.

IV. 평 가

본 절에서는 Ⅲ절에서 제안한 저전력 보안 아키텍처의 성능 평가를 위해 서브 로직이 있는 제안 모델과 서브 로직 없이 메인 로직에서 고성능 보안 모듈 및 경량 모듈을 사용하는 종래 모델의 전력효율성을 수식으로 증명한다. 전체 에너지 소모량(E)은 메인 로직(m)과 서브 로직(s)의 각 전력 소모량(P)에 각 실행 시간(T)을 곱한 값으로, 아래의 수식으로 정의된다. 이때, P_m과 T_m은 메인 로직이, P_s와 T_s는 서브 로직이 각각 소모하는 전력 소모량과 실행 시간을 나타낸다.

$$E = P \times T = (P_s \times T_s) + (P_m \times T_m) \quad \cdots \ (1)$$

수식 (1)에 따르면, 제안 모델은 메인 로직과 서브 로직에서 소모되는 각 전력 소모량과 수행 시

간의 곱을 합한 값과 같다. 반면, 종래 모델은 서브 로직의 동작 없이 메인 로직만 실행되므로 P_s와 T_s가 0이다. 이때 보안성은 보안 모듈의 키 길이에 비례하므로 로직의 회로 크기(C)에 비례하며, 이는 수식 (2)의 이론적 가정에 의해 전력 소모량(P)과 비례한다[6].

$$P = C \times f \times V^2 \quad \cdots\cdots\cdots\cdots \quad (2)$$

수식(1)에 따라 각 모듈 별 에너지 소모량을 비교하면 표 1과 같다. 전체 실행 시간을 10으로 가정하였으며 메인 로직이 전체 시간을 사용하는 종래 모델과 서브 로직과 메인 로직이 동작하는 제안 모델의 경우, 각 로직의 실행 시간 비율에 따라 전력 소모량이 달라지므로 각각 1:9, 5:5, 9:1일 때를 각각 비교한다. 전력 소모량은 서브 로직은 1, 메인 로직은 100으로 가정하였다.

표 1. 보안 모델별 전력 효율성

	서브 로직 ($P_s \times T_s$)	메인 로직 ($P_m \times T_m$)	에너지 소모량(E)
종래 모델	0	100×10	1000
제안 모델	1×1	100×9	901
	1×5	100×5	505
	1×9	100×1	109

표 1과 같이, 제안 모델은 서브 로직과 메인 로직의 비율에 따라 전체 에너지 소모량의 차이가 있으나, 전체 실행 시간 동안 메인 로직만 수행하는 종래 모델 대비 효율적임을 확인할 수 있다.

Ⅴ. 결 론

사물인터넷은 스토리지 할당 측면의 제약사항으로 제한적인 배터리 용량을 효과적으로 활용하기 위한 전력 소모량 관리가 중요하다. 종래에는 저전력 환경을 위해 경량 보안 모듈을 탑재하였으나 사물인터넷 기기의 보안성이 열화되는 한계점이 존재했다. 본 논문은 저전력 환경에서 고성능 보안 모듈을 활용하기 위한 보안 아키텍처를 제안하여 전력 효율성과 보안성을 개선하였다. 서브 로직의 탐지부에서 수신한 신호 중 이상 행위가 탐지된 경우에만 메인 로직을 실행시킴으로써 저전력 환경에서 상대적으로 복잡도가 높은 고성능 보안 모듈을 활용할 수 있다. 종래 모델과 제안 모델에 대한 수식적 정의·분석 결과, 제안 모델의 경우 서브 로직과 메인 로직의 비율에 따라 전체 에너지 소모량의 차이는 보이나 종래 모델 대비 최저 효율로 가정한 1:9의 비율에서 약 9.9%, 최대 효율인 9:1의 비율에서 약 89.1%의 에너지가 감소하는 것을 확인할 수 있었다. 향후에는 제안 모델을 통해 높은 보안성을 요구하는 개인 정보 관련 산업 분야에서도 막강한 보안 모듈을 탑재한 사물인터넷 기반 서비스를 제공할 수 있을 것으로 기대한다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아 수행된 연구임.

References

[1] Gunathilake, N. A., Al-Dubai, A., & Buchana, W. J., “Recent Advances and Trends in Lightweight Cryptography for IoT Security,” in 2020 16th International Conference on Network and Service Management (CNSM), IEEE, pp. 1-5, Nov. 2020.

[2] Daemen, Joan, and Vincent Rijmen, “AES proposal: Rijndael.” Proc. 1st Adv. Encryption Standard Candidate Conf. NIST, pp1-45, Mar. 1999.

[3] Seo, H., & Kim, H., “사물인터넷을 위한 경량 암호 알고리즘 구현,” Review of KIISC, 25(2), 12-19, Apr. 2015.

[4] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y. & Vikkelsoe, C, “PRESENT: An ultra-lightweight block cipher,” In International workshop on cryptographic hardware and embedded systems, Springer, Berlin, Heidelberg, pp. 450-466, Sep. 2007.

[5] Eisenbarth, T. et al., “Compact implementation and performance evaluation of block ciphers in ATtiny devices,” In International Conference on Cryptology in Africa, Springer, Berlin, Heidelberg, pp. 172-187, July. 2012.

[6] Neri, D. A., Medina, R. P., & Sison, A. M., “An XBOX-based key generation technique for vigenere algorithm,” In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Malaysia, Kuala Lumpur, pp. 66-70, January, 2019.