군용 IoT 장비의 통신 보안 이슈 및 경량 암호 기술 동향

배영채

LIG 넥스원

youngchae.bae@lignex1.com

Communication Security Issues in Military IoT Equipment and Lightweight Cryptographic Technology Trends

Bae Young Chae

LIG Nex1

요 약

군용 IoT 장비는 실시간 전장 정보 수집, 무인 자산 제어 등 현대 전장에서 군사 작전 수행에 필수적이나, 제한된 연산 자원과 무선 통신 특성으로 인해 다양한 보안 위협에 노출된다. 제한된 환경에서 여러 위협으로부터 무기체계를 보호하기 위해서는 일반 암호기술보다 경량화 된 암호기술을 적용하는 것이 효율적일 수 있으며, 이와 관련된 기술에 대한 지속적인 관심이 필요하다. 경량 암호는 IoT, 모바일 등 저사양 환경에 적합하도록 단순한 연산과 구조로 설계되었으며, 국내 상용 제품에 적용된 사례가 있다. 본 논문에서는 군용 IoT 환경의 특성 및 위협 요인을 분석한다. 또한, 경량 암호 기술의 국내외 기술 동향과 실제 다양한 분야에서 경량 암호 기술을 적용한 사례를 조사하여 정리하였다. 이를 바탕으로 군용 IoT 환경에서 경량 암호를 적용할 때 이점을 가질 수 있으며 향후 무기체계를 보호하는 수단으로 경량 암호에 대한 지속적인 관심과 연구에 대한 지원이 필요함을 보인다.

Ⅰ. 서 론

군용 IoT(Internet of Things) 기술은 실시간 전장 감시를 통한 병력 위치 파악, 무인 자산 제어 등 다양한 분야에 활용되며 현대 전장에서 핵심 인프라 중 하나로 떠오르고 있다. 그러나 이러한 장비들은 대부분 부품 소형화로 인한 연산 능력 제한, 배터리 사용에 따른 소모 전력 제한 등 여러 제약사항이 존재한다. 또한 무선으로 통신하기 때문에 재밍, 도청, 위조 명령, 재전송 공격 등 많은 보안 위협에 노출되기 쉽고, 이러한 위협들은 전장 상황에서 매우 결정적인 실패로 이어질 수 있다.

본 논문에서는 군용 IoT 환경의 특성 및 위협에 대해 고찰하고, 군용 장비에 적합한 경량 암호(Lightweight Cryptography) 기술에 대한 정의, 기술 동향, 적용 사례를 살펴본다.

Ⅱ. 본론

1. 군용 IoT 장비의 보안 이슈

1.1 군용 IoT 장비의 특성

군용 IoT 장비는 전장 상황 감시, 병력 위치 추적, 무인 자산 제어 등 다양한 임무 수행에 활용되고 있으며 센서, 드론 등 각 임무에 맞는 임베디드 기기를 활용하고 있다. 무기체계는 운용자 명령 수신, 수집 데이터 송신 등 군 네트워크를 통해 중요 정보를 실시간으로 교환한다. 따라서 데이터가 노출되지 않도록 통신 구간의 보안을 강화하는 것이 중요하다.

또한 군용 임베디드 장비는 다양한 크기의 무기체계에 적용할 수 있도록 소형화, 경량화, 저전력 등 플랫폼 최적화를 고려하여 설계된다. 전력 소모량이나 연산 능력에 제약이 있기 때문에, 작전 수행 성능 고도화의 한계점이 될 수 있다.

1.2 군용 IoT의 통신 보안 취약성

러시아-우크라이나 전쟁에서 감시, 정찰, 공격 수단으로 대규모의 드론을 사용한 것처럼, 현대 전쟁에서는 군용 IoT 장비의 활용이 군사 작전 수행의 핵심으로 대두되고 있다. 이러한 무인 장치들은 운용자와 실시간으로 안전하게 통신하는 것이 중요하다. 그러나 무선 기반 장비들은 도청 및 스니핑, 재밍, 스푸핑 등의 공격에 노출되기 쉽다. 따라서 통신 구간을 암호화하여 데이터를 보호하는 것이 중요하다.

DJI 드론의 전송 프로토콜이 암호화되지 않아 무선 신호를 통해 드론과 조종사의 위치 정보가 실시간으로 노출되고, 공격자가 시스템 권한을 획득해 데이터를 조작하는 등 심각한 보안 위협이 발생함을 분석한 연구 결과가 있다[1]. 또한 과거 미국 드론의 영상 전송 신호가 암호화되지 않아 기밀 작전이 노출된 사례처럼, 군사 작전 중 암호화의 부재는 작전 수행에 큰 영향을 미치고 실패까지 이어질 수 있다.

2. 경량 암호 기술 동향

2.1 경량 암호

경량 암호는 하드웨어 및 소프트웨어 경량화를 목적으로, 연산량, 회로 면적, 전력 소모 등을 고려하여 설계된 암호 알고리즘이다. IT 기술의 발달은 장비의 지능화 및 소형화로 이어지고 있으며[2], IoT 디바이스, 임베디드 시스템, 모바일 등 소형 기기에서 통신할 수 있도록 발전했다. 이러한 소형 장치는 제한된 자원 내에서 효율적으로 동작 및 안전한 통신을 할 수 있어야 하므로, 경량 환경에 최적화된 암호 기술의 필요성이 제기되었다. 미국 NIST는 2013년부터 LWC 프로젝트를 통해 경량 암호 국제 표준화를 진행했고, 2023년 ASCON 알고리즘을 표준으로 채택하였다. 이외에도 경량 암호 알고리즘 설계, 검증, 적용 방향성 등에 대한 연구가 국내외로 활발하게 진행되고 있다.

2.2 국내외 경량 암호 기술 현황

다음은 대표적인 국내외 경량 암호 알고리즘이다.

- LEA: 국가보안기술연구소(NSRI)에서 개발한 경량 블록 암호로, 128비트 블록 크기와 128/192/256비트 키 길이를 지원한다. 라운드 함수를 ARX(Add-Rotate-XOR) 연산만으로 구성하였고, S-box 사용을 배제하여 경량화하였다[3].
- HIGHT: KISA, 고려대학교, ETRI에서 개발한 경량 블록 암호로, 64비트 블록 크기와 128비트 키 길이를 지원한다. 일반화된 Feistel 변형 구조이며 XOR, 순환, 덧셈과 같은 단순한 연산으로만 구성되는 등 경량, 저전력으로 설계되어 있다[4].
- SPECK: 미국 국가안보국(NSA)에서 개발한 경량 블록 암호로, 다양한 블록 크기(32~128비트) 및 키 길이(64~256비트)를 지원한다. 일반적인 ARX 구조를 가진다. 특히 구조가 단순하고, 메모리 사용량이 적어서 소프트웨어 구현에 최적화 되어있다[5][6].
- SIMON: 미국 NSA에서 개발한 경량 블록 암호로, SPECK과 함께 경량 암호 표준화 후보로 제시되었다. Feistel 구조를 기반으로 하며, modular Addition 연산자 대신 And 연산자를 사용하는 ARX 구조를 가진다. 특히 AND, XOR 등의 단순한 비트 연산으로 구성되어, 병렬 처리가 가능하고 하드웨어 구현에 최적화 되어있다[7].
- ASCON: NIST 경량 암호화 표준으로 최종 채택된 경량 암호화 알고리즘이다. 스펀지 구조를 기반으로 하며, addition of constant, S-box, linear diffusion layer로 구성되는 순열 연산을 통해 암호화 보안을 강화한다[8].

2.3 경량 암호 적용 사례

LEA는 국내에서 여러 상용 제품 및 서비스에 적용되고 있다. 이스트소프트 社의 압축 소프트웨어인 '알집(버전 10.5 이상)'에서는 파일 압축 시 암호화 알고리즘으로 LEA를 선택할 수 있다. 스마트그리드 지능형 전력계량(AMI) 사업에서는 가정용 전력량계와 AMI 서버 간 데이터 통신을 담당하는 DCU(Data Collection Unit)에 LEA가 적용되었다. 또한 이니텍 社의 'INISAFE Net' 등 금융·공공기관용 보안 솔루션에도 LEA가 적용되어 있으며, 이외에도 클라우드, 빅데이터 등 다양한 분야에 적용할 수 있도록 확대되고 있다.

미국 공군사관학교(USAFA)에서 경량 암호 알고리즘 ASCON을 실제 IoT 환경에 적용하여 영향성을 평가한 연구가 있다. 해당 연구에서는 MQTT 프로토콜을 통한 메시지 암호화에 ASCON을 적용하였으며, 정보 공유 성능을 낮추지 않으면서도 충분한 보안과 무결성을 제공할 수 있다는 분석 결과를 도출했다. 또한 ASCON은 AES와 유사한 성능을 보이면서도 더 적은 메모리 사용이 가능해, 군용 IoT 기기와 같은 자원이 제한적인 환경에서의 활용 가능성을 높게 평가하였다[9].

이처럼 경량 암호는 기존 암호 기술에 비해 단순한 연산과 구조로 설계되어 있으나 충분한 보안성을 제공하여, 다양한 상용 제품에 활용되고 있다. 군용 IoT 장비 또한 제한된 자원으로 효율적인 기능을 수행하는 것을 목표로 하며, 통신 구간에 대한 보안을 고려해야 한다. 따라서 경량 암호 기술은 이러한 소형 무기체계 환경에 적용하기 가장 적합하며, 장비의 성능 저하를 최소화하면서 보안을 강화할 수 있는 효과적인 방안이 될 것으로 전망한다.

Ⅲ. 결론

본 논문에서는 군용 IoT 환경의 특성 및 보안 취약성과 함께 이를 보완할 수 있는 경량 암호 기술에 대해 살펴보았다. 군용 IoT 장비는 실시간 정보 수집 등 여러 군사 작전에 투입되어 핵심 기능을 수행하고 있지만, 물리적 제약과 무선 통신의 특성으로 인해 다양한 보안 위협에 노출될 수 있다. 기존의 고성능 암호 기술을 적용하여 보안을 강화할 경우, 장비의 성능에 영향을 미쳐 실제 운용에 부담을 줄 수 있다. 따라서 본 논문에서는 경량 암호의 개념 및 동향을 설명하고, 실제 민수의 상용 장비들에서 경량 암호 기술을 적용하고 있는 사례들을 소개했다. 이러한 사례들을 통해서 군용 IoT 환경에서도 경량 암호 기술을 적용한다면 제한된 환경에서의 보안 위협들에 대응하여 안전한 작전 수행 및 작전 성공률을 높이는 데 도움이 될 것으로 생각한다. 따라서, 군용 IoT 장비의 성능에 크게 영향을 주지 않으면서도 보안을 강화할 수 있도록 무기체계에 경량 암호를 적용하는 연구 및 영향성 검증 연구가 지속되어야 한다.

참 고 문 헌

[1] Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars, Thorsten Eisenhofer, Tobias Scharnowski, Felix Domke, Lea Schonherr, Thorsten Holz, "Drone Security and the Mysterious Case of DJI's DroneID", NDSS Symposium, 2023

[2] 홍득조, "경량 블록암호 알고리즘 설계 연구 동향", 정보보호학회지, 30(3), 25-29, 2020

[3] 손승일, "경량 블록암호 LEA용 암·복호화 IP 설계", 인터넷정보학회논문지, 18(5), 1-8, 2017

[4] 손승일, "블록 암호 HIGHT를 위한 암·복호화기 코어 설계", 한국정보통신학회논문지, 16(4), 778-784, 2012

[5] 양현준, 신경욱, "8가지 블록/키 크기를 지원하는 SPECK 암호 코어", 전기전자학회논문지, 24(2), 97-103, 2020

[6] 장경배, 김현준, 임세진, 서화정, "NVIDIA CUDA PTX를 활용한 SPECK, SIMON, SIMECK 병렬 구현", 정보보호학회논문지, 31(3), 423-431, 2021

[7] 권혁동, 장경배, 김현지, 서화정, "블록암호 SIMON의 카운터 모드 사전 연산 고속 구현", 한국정보통신학회논문지, 25(4), 588-594, 2021

[8] 오진섭, 최찬호, 최두호, "Width 효율적 ASCON 양자 회로를 이용한 Grover 기반 양자 보안비도 분석", 정보보호학회논문지, 34(6), 1189-1199, 2024

[9] J. Avery, B. Fraelich, W. Duran, A. Lee, A. Sullivan, Z. Mechalke, B. Birrer, S. Dick, and J. Cochran, "Analysis of Practical Application of Lightweight Cryptographic Algorithm ASCON," NIST Lightweight Cryptography Workshop, 2022