드론용 보안모듈 개발에 관한 연구

김웅, 김종오*
㈜에프아이시스

wkim1006@fisys.co.kr, jokim@fisys.co.kr

A Study on Security Module for Dron

Woong Kim, Jong-Oh Kim*
FISYS Inc.

요 약

드론은 산업분야와 국방분야에서 다양한 서비스를 위해 이용 및 활용되고 있다. 드론을 이용하여 카메라 영상과 같은 개인정보가 전송되고 있고, 드론의 형태 또한 대형화되고 있어 제어와 서비스 데이터에 대한 보안적용이 요구되고 있어서, 제어와 서비스 데이터에 대한 암호 통신를 위해 보안모듈을 적용하고 있다. 본 연구에서는 드론에 탑재되는 보안모듈의 보안성을 확보하기 위한 방안에 대해 기술하고자 한다.

1. 서론

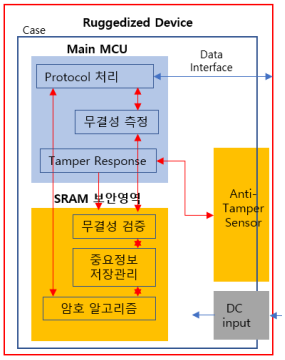
현재 상용화된 드론은 지상의 RC 송신기, 지상 제어국과의 통신에 업체별로 다양한 통신방식과 보안을 위한 방식을 적용하고 있으며[1], 보안 등급이 높은 드론 이용 분야에서는 드론과 RC 송신기에 보안모듈을 장착하여 드론과 RC 송신기, 지상 제어국 간에 암호 통신을 요구하고 있다. 보안모듈에 적용되는 암호 통신기능을 수행하는 제품은 보안적합인증 시험을 통해서 인증을 획득한 제품의 적용을 요구하고 있다 [2]. 본 연구에서는 드론과, RC 송신기 및 지상 제어국에 장착되는 보안모듈의 보안성을 확보하기 위한 방법으로 보안모듈에 적용될 SRAM 보안영역 기능과 Tamper-Proof 기능을 소개하고자 한다.

2. 본론

보안모듈에는 암호 통신을 위한 키 정보와 보안 알고리즘 S/W 등 보안정보가 탑재된다. 보안정보는 보안모듈의 저장매체에 기록되기 때문에 보안모듈에 대한 해킹의 위험에서 보호하기 위해서, 운용 중에 보안정보의 저장시간 및 유효 시간을 제어하고 필요 시에 저장매체의 기록을 소거하는 방식을 구현하여 보안정보의 보안성을 구현한다. 또한 최근에 출시되는 다양한 MCU 에는 내부에 접근이 쉽지 않은 보안영역을 구현하여 해킹으로부터 보안정보를 보호하는 방안을 제시한다 [3]. 하지만 사용되는 저장정보의 사이즈가 커질수록 저장매체에 접근하여 업데이트 하기위해서 필요한 시간이 증가하여 보안정보가 유사 시에 유출될 가능성이 존재하고, MCU 가 제공하는 보안영역 또한 업체의 고유기술이기에 보안정보의 보안성 또한 업체의 기술에 의존성을 갖게 될 것으로 예상된다.

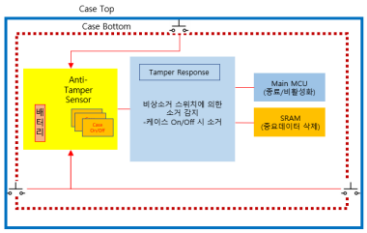
본 연구가 소개하는 SRAM 보안영역 기능은 SRAM 에 전원이 인가되지 않을 때 SRAM 정보가 초기화되는 특성을 이용하여 보안정보를 SRAM 에 저장하는 것이다. 보안모듈 내부의 MCU 가 외부메모리로 사용하는 SRAM 에 보안정보를 저장하고, 유사 시에 SRAM 동작 전원을 차단하여 보안정보가 삭제되도록

하는 방식이다. 평상 시에는 SRAM 에 저장된 보안정보가 삭제되지 않도록 SRAM 에 전원을 제어하여 비휘발성 메모리와 동일하게 동작하는 기능이 제공되며, 유사 시에만 SRAM 의 전원을 차단하는 기능을 제공한다.



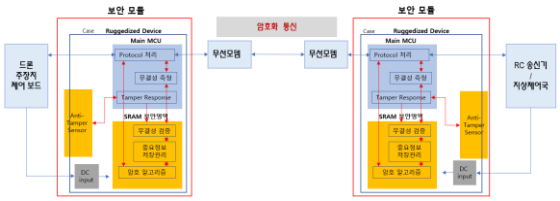
(그림 1) 보안모듈의 SRAM 보안영역 구성도.

Tamper-Proof 기능은 해킹의 징후가 센서를 통해서 감지되면 SRAM 의 전원을 차단해서 SRAM 에 저장된 보안정보를 소거하는 것이다. Tamper-Proof 를 통해서 보안모듈에 저장된 보안정보는 외부로 노출되지 않고 삭제되며 보안모듈의 보안성을 확보하는 역할을 수행한다. 보안모듈은 외부로의 노출을 방지하고 은폐할 수 있도록 기구물을 이용하여 차폐시킨다. Tamper-Proof 기능은 보안모듈을 차폐한 기구물의 안쪽에 센서를 적용하여 차폐 기능이 해지되는 것을 감지하고, 센서의 감지를 통해서 해킹의 징후가 감지되면 SRAM 의 전원을 차단하는 기능을 구현하여 Tamper-Proof 역할을 수행한다.



(그림 2) Tamper-Proof 구성도.

SRAM 보안영역 기능과 Tamper-Proof 기능이 적용되는 보안 모듈은 (그림 3) 드론과 지상간 보안모듈의 적용 예와 같이 드론과 RC 송신기 혹은 지상제어국에 각각 적용되어 드론의 제어를 위한 데이터와 드론에서 취득되는 사용자 데이터에 대한 암호화/복호화를 수행하여 암호 통신을 구현한다. 암호 통신을 구현하기 위해서 필요한 키정보와 암호알고리즘의 보안정보를 SRAM 에 저장하여 암호 통신에 사용하고, Tamper-Proof 기능을 이용하여 해킹의 징후가 감지될 경우 보안정보를 삭제하여 보안정보에 대한 외부로의 노출을 차단하여 결과적으로 보안모듈에 탑재되는 보안정보에 대한 보안성을 확보할 수 있다.



(그림 3) 드론과 지상간 보안모듈의 적용 예.

3. 결론

본 연구는 드론과 드론제어에 사용되는 RC 송수신기 혹은 지상제어국에 적용되어 암호화통신 구현에 사용되는 보안모듈의 사용 예를 제시하였다. 그리고, 보안모듈이 암호화통신을 위해 사용하는 보안정보에 대한 보안성을 확보하기에 적합한 SRAM 보안영역 기능과 Tamper-Proof 기능을 소개하였다. SRAM 보안영역 기능과 Tamper-Proof 기능은 보안모듈에 대한 해킹 위험을 감지하고 보안모듈에 기록되어 있는 보안정보가 외부로 노출이 되지 않도록 즉시 소거함으로써 보안정보에 대한 보안성을 확보할 것으로 기대된다. 보안모듈에 적용되는 CPU 의 성능에 따라서 드론 이외의 암호화 통신이 필요한 다양한 분야에서 해킹의 위험으로부터 보안성을 확보하기 위한 방안으로 활용할 수 있을 것으로 기대된다.

감사의 글

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

참고문헌

[1] DJI Enterprise 사용자 데이터 보호

https://enterprise.dji.com/kr/data-security

[2] TTAK.KO-12.0317, 드론 기반 서비스를 위한 보안요구사항, TTA 표준,2017.12

[3] ST, STM32 Security Trust Zone, https://www.st.com/resource/en/application_note/an5347-arm-trustzone-features-for-stm32l5-and-stm32u5-series-stmicroelectronics.pdf