MAVLink 프로토콜의 보안 취약점 분석

최준표*, (교신저자) 김현성*,**
*경일대학교 컴퓨터사이언스학부, **말라위대학교 수학과
vy4515@naver.com, *kim@kiu.ac.kr

Security Scheme Proposal for MAVLink Protocol

Junpyo Choi*, (Corresponding Author) Hyunsung Kim*,**
*School of Computer Science, Kyungil Univ., **Math. Science Dept., Univ. of Malawi

요 약

4 차 산업혁명의 핵심 기술이 적용 가능한 드론 통신을 위하여 MAVLink 프로토콜이 경량화에 초점을 두고 개발되었다. MAVLink 는 소형 무인기를 위한 통신 프로토콜이다. MAVLink 는 통신을 위한 기본 기능은 제공하지만 보안을 위한 어떤 기법도 제공하지 않고 있어서 다양한 보안 취약점이 있다. 본 논문에서는 MAVLink 분석을 통한 보안 취약점 및 보안 공격들을 분석한다.

Ⅰ. 서 론

4 차 산업혁명의 핵심 기술인 인공지능, 빅데이터, 사물인터넷 등의 핵심 기술들을 적용할 수 있는 드론(Drone)은 그림 1 과 같이 지상통제센터 (Ground Control Station)와의 무선 통신을 수행한다[1]. 전송 프로토콜에서 여러 보안의 위험성으로부터 안전한 통신환경을 설립하기 위하여 인증과정은 중요한 단계 중 하나이다. 인증의 취약성으로 인하여 보안 문제점이 발생한다면 최악의 경우 공격자는 이 취약성을 이용하여 메시지 탈취, 드론의 통제권 무효 등의 심각한 보안 문제점이 발생할 수 있다. 보안 취약성으로 인한 이용 장애는 드론의 통신과정에서 심각하게 고려되어야 할 문제이다.

본 논문에서는 MAVLink 프로토콜의 기본적인 기능을 살펴보고, 통신 과정에서 발생할 수 있는 여러가지 보안상 문제점들을 분석하며 이를 통한 공격을 살펴본다.

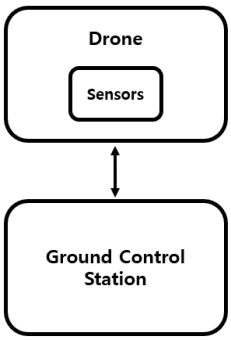

그림 1. 드론과 지상통제센터 간 통신 환경.

Ⅱ. 드론 통신 MAVLink 프로토콜

2.1 MAVLink 개요

MAVLink 는 Meier 에 의해 오픈소스로 개발되었다[2]. 이는 군용 드론 프로토콜인 STANAG 4586 과는 다르게 민간용으로 사용되는 소형 무인기를 제어하기 위해 개발된 프로토콜이다. 프로토콜의 목적은 제한된 통신 구역에서 사용 가능한 단순한 통신 기능 제공에 있다. 이로 인해서 보안 기능을 제공하기 위한 기법이 고려되지 못한 문제가 있다.

2.2 MAVLink 의 통신 과정

기본 통신 과정은 그림 2 와 같다. 드론과 지상통제센터 간의 통신으로 등록 단계와 인증 단계로 구성된다. 등록 단계는 통신 전 사전 작업으로 1 회만 진행한다.

[등록 단계] 드론과 지상통제센터 가 키(Key)를 모아둔 리스트(List)를 공유한다.

[인증 단계]

단계 1: 제어 권한 요청을 위해 지상통제센터에서 드론에게 제어권한 메시지와 키를 전송한다.

단계 2: 드론으로부터 전송받은 키를 이용하여 저장되어 있는 키리스트의 멤버와 대조해보고 이 테이블에 포함이 된 경우 인증한다.

즉, 사전 공유한 키를 가지고 개체 인증을 진행하는 인증 과정으로 제어권을 승인한다. 이로 인해서 공격자가 키를 도청할 경우 드론의 제어권을 탈취할 수 있는 가능성이 있다.

그림 2. MAVLink 인증 과정.

경량화에 초점을 맞춘 MAVLink 는 파워 부족, 무게 제약 등의 문제로 한정적인 자원에 대한 요구사항 지원이 가장 중요한 문제이다. 이로 인해 연산을

최소화해야 하고 이로 인해 단순한 패킷 구조를 가진다. 어떠한 보안 기법도 제공하지 못하고 단순한 인증 과정을 통해 드론과 지상통제센터 간의 통신을 수행하는 MAVLink 는 기밀성과 무결성의 부재로 인하여 다양한 보안 취약점에 노출되어 있다.

Ⅲ. 취약점 분석

MAVLink 프로토콜은 드론과 지상통제센터 간의 통신 과정에서 제어 명령어와 드론의 위치, 시스템 정보와 같은 데이터를 암호화하지 않는다. 이로 인해 중요한 정보가 그대로 노출된 형태의 메시지를 전송한다. 이는 메시지 기밀성을 제공하지 못하는 문제와 연계된다. 또한 메시지에 어떠한 보안 기법도 제시되지 못하므로 위변조에 취약하고 이로 인해 무결성을 제시하지 못한다. 이러한 문제들을 토대로 MAVLink 는 기밀성과 무결성을 제공하지 못하고 이를 바탕으로 다음과 같은 공격이 가능하다.

3.1 중간자 공격

대부분의 드론 상의 통신은 승인 및 상태 업데이트 등과 같은 동일한 환경 설정 정보를 모든 사용자들이 공유할 수 있도록 전송한다. 하지만 이를 이용해 네트워크 참여자로 위장한 공격자는 동일한 설정 정보를 이용하여 드론과 지상통제센터 사이에서 정보를 탈취하는 중간자 공격이 가능하다. 이는 기밀성과 무결성 제시를 통해 공격에 대한 보안을 제공할 수 있지만, MAVLink 는 변경없는 데이터 전송으로 인한 기밀성의 부재와 전송된 데이터의 임의 조작 가능성으로 인한 무결성을 제시 못하는 취약성으로 인하여 이 공격에 취약한 구조이다.

3.2 하이재킹

MAVLink 통신 과정에서 공격의 가능성이 존재하다는 점을 3.1 절에서 살펴본 바와 같이 기밀성과 무결성에 초점을 맞춘 보안 취약성을 통하여 중간자 공격이 가능했다. 이를 통하여 공격자는 전송 프로토콜의 취약성을 이용하여 드론에게 허가되지 않은 명령을 전송하고 다양한 제어권을 지상통제센터로부터 획득할 수 있다. 즉, MAVLink 는 세션 하이재킹 공격으로부터 보안성을 제시하지 못한다.

3.3 서비스 거부 공격

서비스 거부 공격은 드론이 지상통제센터에 응답하지 않거나 반대로 지상통제센터가 드론에 응답하지 못하도록 하는 공격이다. 이를 통해 명령 전송과 같은 실시간 통신이 이루어져야 할 드론 환경에서 원할한 통신 과정이 이루어 지지 못하도록 막는 공격이다. 이는 전송 프로토콜에서 다양한 보안 서비스 기능 도입을 통해 공격에 대한 저항성을 제시할 수 있다. 하지만 MAVLink 의 경우에는 아무런 보안 기능도 제공하지 못하고 있다. 따라서 MAVLink 는 서비스 거부 공격으로부터 취약한 구조를 가지고 있다는 것을 알 수 있다.

Ⅳ. 결론 및 고찰

본 논문에서는 기존에 드론과 지상통제센터에서 사용된 통신 프로토콜인 MAVLink 의 동작 원리를 살펴보고 이에 대한 취약점을 분석하였다. MAVLink 프로토콜은 보안을 제공하기 위한 어떠한 기능도 제공하지 못하기 때문에 다양한 공격에 취약할 수 있음을 확인하였다. 특히, 중간자 공격, 서비스 거부공격과 하이재킹과 같은 심각한 보안 취약점으로 이어질 수 있음을 확인하였다. 즉, MAVLink 의 통신 과정은 프라이버시 및 보안 기능을 제공하지 못하는 문제가 있다. 최근들어 드론을 활용한 다양한 프라버시 이슈가 제기되고 있다. 다양한 응용에 드론이 활용되고 도입되는 추세에 있어서 더 이상 보안 및 프라이버시가 제공되지 못한 드론의 사용은 불가능하다. 지속적인 드론 보안 및 프라이버시 연구는 필수적인 것이다.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

참 고 문 헌

[1] A. Sharma, P. Vanjini, N. Paliwal, C. M. W. Basnayaka, D. N. K. Jayakody, H. Wang, P. Muthuchidambaranathan, “Communication and networking technologies for UAVs: A survey,” *Journal of Network and Computer Applications*, vol. 168, 102739, 2020.

[2] J. Li, Y. Zhou, L. Lamont, “Communication arch2tectures and protocols for networking unmanned aerial vehicles,” *Proc. of 2013 IEEE Globecom*, pp. 1415-1420, 2013.

[3] J. A. Marty, *Vulnerability Analysis of the MAVLink Protocol for Command and Control of Unmanned Aircraft*, Thesis and Dissertation, Air Force Institute of Technology, 2014.

[4] A. Allouch, O. Cheikhrouhou, A. Koubaa, M. Khalgui, T. Abbes, “ MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems,” *arXiv*: 1905.00265vl [cs.CR] 1 May 2019.

[5] L. Meier, “sMAVLink-Secure MAVLink, Request for Comments, ” Available: https://diydrones.com/profiles/blogs/smavlink-secure-mavlink-request-for-comments, 2013.

[6] T. Kim, S. Lee, S. Jung, H. Wi, O. Yi, “A Research on the on he Security of Drone Control Data Using Quantum Entropy-Based Random Number Generator, ” *Journal of The Korea Institute of Information Security & Cryptology*, vol. 31, no. 2, pp. 133-144, 2021.