Phòng chống phương tiện bay không người lái dựa trên chiếm quyền điều khiển giao thức: Một số vấn đề kỹ thuật và giải pháp minh họa

Bùi Công Thành*, Phùng Đức Dũng, Đồng Xuân Chinh

Viện Nghiên cứu 486, Bộ Tư lệnh 86, phường Xuân Đỉnh, Hà Nội, Việt Nam

Ngày nhận bài 8/11/2024; ngày gửi phản biện 10/11/2024; ngày nhận phản biện 5/12/2024; ngày chấp nhận đăng 12/12/2024

Tóm tắt:

Phương tiện bay không người lái (UAV) ngày càng đóng vai trò quan trọng trong cả lĩnh vực dân sự và quân sự nhờ tính linh hoạt, chi phí vận hành thấp và khả năng thực hiện nhiệm vụ kéo dài. Tuy nhiên, sự phổ biến rộng rãi này cũng đặt ra nhiều thách thức về an ninh, đặc biệt trong việc quản lý và ngăn chặn các hoạt động UAV trái phép. Trong số các kỹ thuật phòng chống UAV hiện nay, phương pháp chiếm quyền điều khiển bằng cách khai thác lỗ hổng trong giao thức điều khiển đang được đánh giá là hướng tiếp cận tiềm năng và tiết kiệm chi phí, đặc biệt phù hợp với mục tiêu nghiên cứu và ứng dụng trong quốc phòng. Bài báo trình bày một số kết quả nghiên cứu liên quan đến phương án phòng chống UAV thông qua chiếm quyền điều khiển giao thức MAVLink - một giao thức truyền thông nhẹ được sử dụng rộng rãi cho việc điều khiển và truyền thông tin UAV. Kết quả cho thấy, do MAVLink 1.0 thiếu mã hóa và xác thực, kẻ tấn công có thể dễ dàng giành quyền điều khiển UAV. Mô phỏng này góp phần hỗ trợ đào tạo, nghiên cứu trong điều kiện thiếu trang thiết bị thực tế, đồng thời mở ra các hướng nghiên cứu chiến lược phòng chống UAV chủ động và hiệu quả hơn trong tương lai.

Từ khóa: **MAVLink, phòng chống phương tiện bay không người lái, phương tiện bay không người lái.**

Research on control takeover techniques for counter-UAV (Unmanned Aircraft Vehicle)

Cong Thanh Bui*, Duc Dung Phung, Xuan Chinh Dong

Institute 486, Command 86, Xuan Dinh Ward, Hanoi, Vietnam

Received 8 November 2024; revised 5 December 2024; accepted 12 December 2024

Abstract:

Unmanned aerial vehicles (UAVs) have become increasingly integral in both civilian and military domains due to their flexibility, cost-effectiveness, and mission endurance. However, this widespread adoption introduces complex security challenges, especially in terms of managing and preventing unauthorized UAV activities. Among the emerging counter-UAV techniques, hijacking UAVs by exploiting control protocol vulnerabilities is considered a promising and cost-efficient approach, particularly for research and defense applications. This paper presents technical findings related to hijacking-based countermeasures against UAVs by targeting the MAVLink protocol - a widely adopted lightweight communication protocol for UAV command and telemetry. The research outlines

*Tác giả liên hệ: Email: phungducdung@gmail.com

the architecture of UAV control systems, identifies protocol vulnerabilities and demonstrates how spoofed control packets can lead to full UAV takeover. The results show that, due to the lack of encryption and authentication in MAVLink 1.0, an attacker can successfully disrupt and override mission commands, effectively hijacking UAVs. This virtual simulation provides a valuable resource for education, training, and further research on UAV cybersecurity, particularly in environments where access to real UAV systems and field conditions is limited. The study emphasizes the importance of protocol security in UAV systems and opens new directions for proactive defense strategies.

Keywords: **Counter-UAV, MAVLink, Unmanned aerial vehicle.**

1. Đặt vấn đề

Phương tiện bay không người lái là loại phương tiện hoạt động không cần người lái, được chế tạo dựa trên nhiều công nghệ trong một hệ thống chỉnh thể, tinh vi cả về phần cứng, cơ khí, phần mềm và chiến thuật. Nhờ những ưu điểm như khả năng cơ động độc lập, hoạt động trong điều kiện khắc nghiệt, thời gian dài, chi phí thấp và khả năng che giấu tốt, UAV ngày càng trở nên phổ biến trong mọi lĩnh vực đời sống, xã hội, bao gồm cả nhà máy, nông nghiệp… và quốc phòng, an ninh. Từ đó cũng tạo ra nhiều vấn đề mới về quản lý, phòng chống UAV để đảm bảo quốc phòng, an ninh [1].

Trong quân đội của các nước phát triển, UAV là lực lượng được biên chế chính thức và phổ biến như hầu hết các hệ thống vũ khí thông thường [2, 3].

Trong thập kỷ qua, chúng ta đã chứng kiến sự đầu tư quyết liệt của các nước cho UAV. Năm 2012, Hoa Kỳ chi gần 5 tỷ USD dành cho nghiên cứu, phát triển và mua sắm UAV chiến lược. Tổng thống Nga Putin công bố khoản ngân sách 12,2 tỷ USD đầu tư cho phát triển UAV trong khoảng thời gian 2013-2020; tính đến năm 2010, đã có 42 chính phủ nước ngoài mua UAV của Israel [3]. Theo Bộ Quốc phòng Hoa Kỳ, tính từ năm 2001 đến năm 2023, hơn 23 triệu giờ bay đã được ghi nhận cho các UAV của quân đội Hoa Kỳ, riêng trong năm 2023 đã có hơn 2 triệu giờ bay [4].

Sự đầu tư cho nghiên cứu, phát triển việc quản lý, kiểm soát mà gọi chung là phòng chống UAV cũng được đặc chú trọng, đặc biệt là trong Quân đội. Tính đến 3/2024 trong cuộc xung đột Nga - Ukraine, Nga đã kiểm soát, tiêu diệt hơn 16 ngàn chiếc UAV; số liệu này từ phía Ukraine là hơn 8 ngàn [5]. Trong nước, một số các sản phẩm phòng chống UAV được biết đến như CA-18 do Học viện Kỹ thuật Quân sự sản xuất, DroneGun do Hãng Drone Shield sản xuất được sử dụng tại một số đơn vị an ninh, dân quân.

Các công nghệ chống UAV thường được áp dụng cho từng trường hợp, từng mục đích và từng loại UAV tương ứng để đạt hiệu quả cao. Với các cuộc xung đột gần đây, ta có thể thấy rằng, những phương thức như gây nhiễu, giả mạo hay tác động mặt vật lý đều đã quá phổ dụng ở các nước lớn, chi phí lớn và thường hiệu quả chưa đạt mong muốn. Với việc đa số các UAV đang sử dụng nền tảng TCP/IP cho các kênh điều khiển, việc nghiên cứu phòng chống UAV dựa trên tấn công mạng điều khiển UAV đang được đánh giá là tiềm năng, giúp giảm thiểu kinh phí và tổn thất lực lượng.

Bên cạnh đó, trong điều kiện hạ tầng cho học tập, nghiên cứu UAV còn hết sức khó khăn, đặc biệt là lĩnh vực tác chiến không gian mạng vào UAV. Do các thách thức như: thiếu trang thiết bị, phương tiện cho nghiên cứu, điều kiện không gian cho thử nghiệm UAV, môi trường mạng liên quan đến UAV, quá trình thử nghiệm cần phải tổ chức cả đội hình nên tốn nhiều công sức... [1]. Do vậy, việc nghiên cứu mô phỏng kịch bản phòng chống UAV luôn được quan tâm nghiên cứu [1, 6], kết quả nghiên cứu giúp hỗ trợ cho công tác huấn luyện, nghiên cứu về phòng chống UAV.

Trong nội dung tiếp theo, phần 2 sẽ trình bày một số kiến thức có tính lý thuyết nền tảng liên quan đến nghiên cứu; phần 3 phân tích khả năng tấn công

chiếm quyền điều khiển đối với giao thức MAVLink; phương án mô phỏng kịch bản tấn công mạng vào UAV bằng các công cụ, phần mềm sẵn có được trình bày trong phần 4.

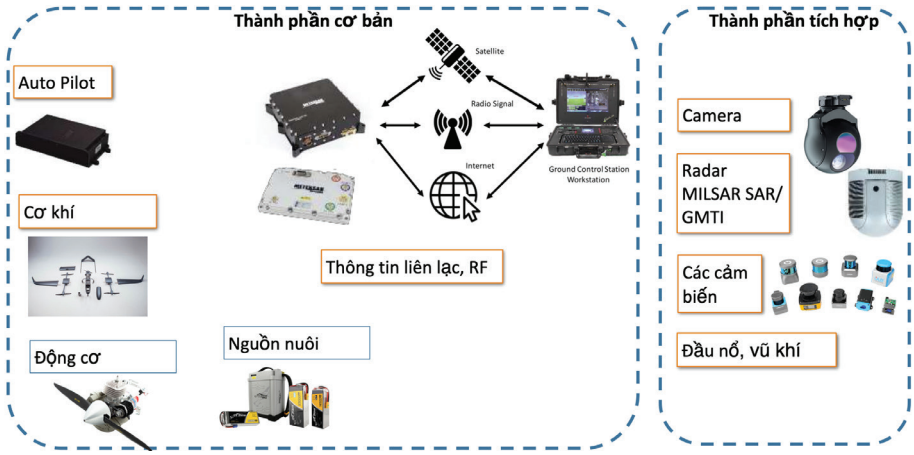
2. Cơ sở lý thuyết liên quan

2.1. Kiến trúc của phương tiện bay không người lái

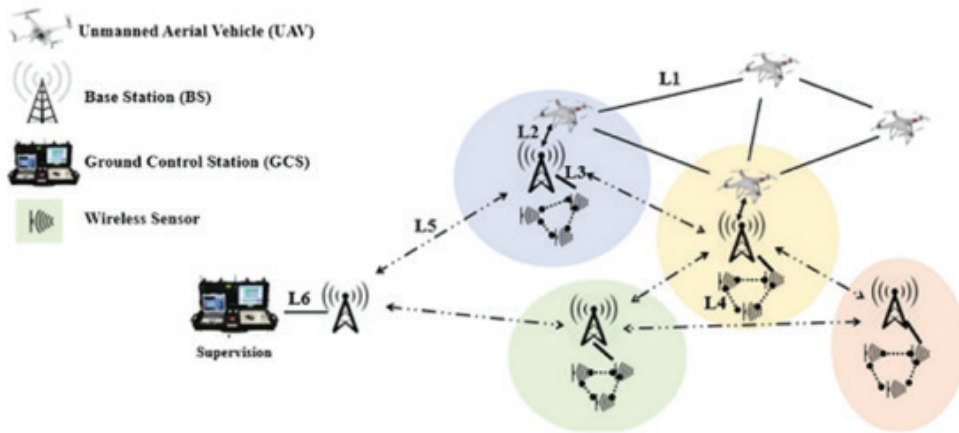
Một hệ thống UAV là tổ hợp nhiều thành phần công nghệ, các khối chính có thể chia làm hai nhóm: Khối thành phần cơ bản, là các thành phần cần thiết cho một UAV ở cả phía thiết bị bay và trạm điều khiển; Khối thành phần tích hợp, là thành phần có tính nâng cao theo từng mục tiêu cụ thể, bao gồm các loại chính như camera, cảm biến, hệ thống rađa tích hợp, vũ khí. Mô tả từng thành phần cơ bản như trên hình 1.

Để đảm bảo hoạt động tự hành thông minh, các UAV thường bao gồm rất nhiều kênh thông tin như tại hình 2 [7], trong đó: L1 là liên kết liên lạc giữa các UAV dựa theo chuẩn thông dụng IEEE 802.11; L2 tương ứng là các giao tiếp giữa UAV và trạm phát sóng (BS); L3 là liên kết truyền thông giữa cảm biến không dây (WS) và BS; L4 liên lạc giữa các nút cảm biến không dây WS; L5 liên lạc giữa các BS; L6 liên lạc tương ứng giữa điều khiển qua trạm mặt đất (Ground control station - GCS) và BS.

Liên lạc từ xa với UAV qua sóng vô tuyến là xương sống trong việc điều khiển thành công thiết bị bay. Để liên lạc với UAV, thông tin phải được truyền liên tục từ UAV đến GCS, do đó liên kết hai chiều được thiết lập giữa chúng để đảm bảo gửi lệnh và thực hiện lệnh từ xa theo thời gian thực. Thông tin trả về chứa dữ liệu về vị trí địa lý, tốc độ bay,



Hình 1. Các thành phần liên quan đến phương tiện bay không người lái.



Hình 2. Các kênh liên lạc thông tin liên quan đến phương tiện bay không người lái [7].

các thông số đo được từ cảm biến về môi trường xung quanh... ghi lại trong suốt quá trình bay. Kênh thông tin điều khiển UAV được gửi lên từ GCS chứa các lệnh để điều khiển như hướng bay tiếp, tốc độ bay mới, lên cao hay xuống thấp... Đây cũng là đối tượng chính được bài báo tập trung trình bày, cụ thể hơn là ở lớp giao thức điều khiển UAV.

2.2. Tấn công mạng vào phương tiện bay không người lái

Dưới góc độ tấn công mạng, UAV có các thành phần chính có thể bị khai thác bởi tác chiến mạng như sau:

- Kênh định vị, dẫn đường: UAV có nhiều cơ chế để xác định phương hướng di chuyển như sử dụng hệ thống định vị GNSS, trạm điều khiển mặt đất bay theo bầy đàn, hay tự hành thông qua nhận dạng quang học. Do vậy, có thể tác chiến mạng đến vận hành, di chuyển của UAV [7].

- Kênh điều khiển hoạt động: thường bao gồm kênh điều khiển lệnh và kênh nhận trạng thái UAV. Kênh điều khiển đường lên để truyền lệnh điều khiển bay từ khối điều khiển từ xa đến UAV. Kênh trạng thái đường xuống để truyền thông tin trạng thái bay (vị trí, độ cao, lượng điện, tốc độ…) từ UAV về người điều khiển [7].

- Kênh truyền thông dữ liệu: Với mục tiêu trinh sát thông tin, UAV thu thập đa dạng thông tin, ở các kiểu dữ liệu khác nhau (hình ảnh, âm thanh, nhiệt độ, mức độ bức xạ RF...). Các dữ liệu này sẽ được truyền đến các trạm cố định, di động hay các UAV khác qua kênh thông tin dữ liệu; các UAV thương mại thường phải tuân thủ các chuẩn giao thức điều khiển, kết nối theo quy định. Do vậy, phòng chống UAV thông qua tác chiến mạng đến dữ liệu và các kênh thông tin liên lạc này là hoàn toàn có cơ sở [7].

- Khối điện tử và phần mềm UAV: Bản chất UAV có chứa các thành phần cho phép điều khiển bay, thông tin điều khiển, thông tin liên lạc. Các khối này bản chất là các bo mạch, firmware, phần mềm và hệ điều hành. Do vậy, tiềm ẩn các lỗ hổng bảo mật và có thể là mục tiêu khai thác tác chiến mạng. Ngoài ra, việc UAV thường có tài nguyên hạn chế để giảm tải trọng, năng lượng cũng dẫn đến dễ bị tấn công dạng từ chối dịch vụ.

- Trạm điều khiển mặt đất, trung tâm chỉ huy: Trạm mặt đất và trung tâm chỉ huy thường chứa cơ sở dữ liệu quản lý, điều hành và dữ liệu trinh sát của UAV. Các trạm mặt đất thường kết nối online/offline với các hệ thống mạng công nghệ thông tin chuyên dụng để trao đổi dữ liệu. Do vậy, việc tác chiến vào các trung tâm mặt đất này có thể giúp thu thập được các thông tin cơ mật, qua đó giúp phòng chống UAV hiệu quả.

2.3. Kênh điều khiển hoạt động UAV

Có hai kiểu cơ bản cho điều khiển UAV, điều khiển từ xa trực tiếp và GCS. Trong hệ thống điều khiển từ xa trực tiếp, người dùng quan sát UAV hoặc quan sát camera gắn trên UAV và điều khiển camera bằng bộ điều khiển. UAV được điều khiển trong thời gian thực bằng cách truyền mệnh lệnh qua kênh điều khiển hoạt động.

Cả bộ điều khiển và UAV được kết nối thông qua một mô-đun thực hiện giao tiếp giữa chúng với sự trợ giúp của các giao thức truyền thông. Thông thường là wifi, ZigBee và nhiều thiết bị mạng khác được sử dụng để liên lạc.

Đối với hệ thống trạm điều khiển mặt đất, sử dụng một máy tính để kết nối phần mềm với UAV, sau đó thực hiện lệnh nhiệm vụ do người dùng tải lên. Bằng cách thu thập thông tin từ nhiều cảm biến được cài đặt trên UAV, GCS có thể theo dõi trạng thái UAV, chẳng hạn như độ cao hiện tại, khoảng cách, vị trí bản đồ và trạng thái nhiệm vụ thực tế.

Các UAV được điều khiển hoạt động bay qua các kết nối vô tuyến với công nghệ như trải phổ nhảy tần (FHSS/DSSS) hệ thống dịch vụ dẫn đường toàn cầu vệ tinh (GNSS), wifi, bluetooth, 5G/LTE.

Thu thập và nhận dạng giao thức điều khiển của UAV là quá trình thu thập thông tin về các tín hiệu và giao thức được sử dụng để điều khiển máy bay không người lái, sau đó phân tích dữ liệu điều khiển, nhận dạng giao thức điều khiển để thực hiện các tấn công leo thang tiếp theo.

Bằng cách phân tích dữ liệu đã giải điều chế, ta có thể xác định các trường thông tin quan trọng trong gói tin, bao gồm địa chỉ nguồn, đích và các lệnh điều khiển gửi đến UAV. Sau khi đã hiểu rõ cấu trúc của gói tin và các thông tin quan trọng trong

đó, chúng ta có thể tiến hành giả mạo các gói tin điều khiển. Điều này có thể thực hiện bằng cách tạo ra các gói tin giả mạo có cấu trúc tương tự như gói tin gốc và truyền chúng đến UAV. Khi UAV nhận được các gói tin này, nó có thể bị đánh lừa và thực hiện các hành động không mong muốn, như thay đổi hướng di chuyển hoặc thậm chí là bị kẻ tấn công chiếm toàn quyền điều khiển.

Nghiên cứu này chỉ tập trung vào một số vấn đề kỹ thuật ở lớp giao thức điều khiển UAV, phân tích lỗ hổng giao thức, giả mạo gói tin, chiếm quyền điều khiển UAV và tập trung đề xuất, xây dựng môi trường ảo minh họa kịch bản tấn công mạng chiếm quyền điều khiển UAV.

3. Phân tích khả năng tấn công phương tiện bay không người lái thông qua giả mạo giao thức điều khiển MAVLink

MAVLink (Micro air vehicle Link) là một giao thức truyền thông rất nhẹ, được sử dụng để tương tác với các hệ thống không người lái hoặc các thiết bị khác trên bo mạch [6, 8]. Chẳng hạn, MAVLink cho phép người dùng tải lên các nhiệm vụ bay, lấy dữ liệu chuyến bay hoặc thay đổi các tham số của hệ thống không người lái. Giao thức này được thiết kế dựa trên mô hình kết hợp giữa việc xuất bản - theo dõi hoặc giao tiếp điểm - điểm. Các luồng dữ liệu được gửi hoặc xuất bản dưới dạng các chủ đề, trong khi các tiểu giao thức cấu hình như giao thức nhiệm vụ, hoặc giao thức tham số sử dụng giao tiếp điểm - điểm với việc truyền lại. Tính nhẹ của MAVLink xuất phát từ việc nó sử dụng ít dữ liệu thừa trên mỗi gói tin. MAVLink v1 chỉ có tiêu đề 8 byte cho mỗi thông điệp, trong khi MAVLink v2 có tiêu đề 14 byte nhưng cung cấp bảo mật và khả năng mở rộng tốt hơn.

Về bản chất, UAV sử dụng MAVLink để được giám sát và điều khiển. MAVLink hỗ trợ các loại lớp vận chuyển khác nhau nhờ cấu trúc gọn nhẹ. Nó có thể truyền qua wifi, Ethernet (mạng TCP/IP) hoặc các kênh băng thông thấp hoạt động ở tần số 433, 868 và 915 MHz [8]. Kết nối MAVLink được thiết lập như sau:

Khi UAV khởi động, nó truyền một thông điệp có tên là HEARTBEAT theo diện tin quảng bá hoặc có thể mang địa chỉ chỉ định của GCS. Đồng thời, GCS lắng nghe bản tin HEARTBEAT trên mặt đất. Khi GCS phát hiện được bản tin của HEARTBEAT từ UAV gửi tới, nếu bản tin chứa địa chỉ của GCS mà nó cần truyền, GCS sẽ gửi lại bản tin HEARTBEAT cho UAV, sau đó cả 2 gửi liên tục bản tin này cho nhau mỗi giây để giữ cho liên lạc này tồn tại. Sau một khoảng thời gian kết nối được thiết lập hoàn toàn, UAV liên tục báo về trạng thái kết nối hiện tại để GCS có thể theo dõi tình trạng của UAV. Tần suất báo về thường khác nhau, phụ thuộc vào loại UAV, băng thông cho phép… GCS gửi bản tin MAVLink đến UAV được kết nối khi người điều khiển thực hiện gửi lệnh mới, cập nhật nhiệm vụ. Trình phân tích bản tin MAVLink được thực hiện sẽ không đề cập tới giá trị nào trong tiêu đề giao thức, ví dụ như địa chỉ IP đích nguồn… Do vậy, MAVLink dễ bị tấn công bằng cách tiêm bản tin sai nếu payload hợp lệ. Ngoài ra, GCS trao đổi dữ liệu với UAV thông qua một kênh không được xác thực và không có mã hóa. Những kết nối này có thể dễ dàng bị tấn công, bị khai thác bởi đối tượng có thiết bị phát phù hợp, có thể giao tiếp với máy bay không người lái, đưa lệnh vào phiên hiện có và dễ dàng khởi chạy tấn công vào UAV.

Sau khi đạt được thông tin về giao thức điều khiển của MAVLink, ta có thể tạo ra các tín hiệu giả (Spoofing Signal) để truyền đến UAV mục tiêu, nhằm khiến UAV hiểu nhầm rằng tín hiệu nhận được từ người tấn công chính là từ GCS gốc. Thuật toán thu thập và giải mã gói tin MAVLink như sau [9]:

Thuật toán: Thu thập và giải mã gói tin dạng bản rõ

Đầu vào: *Gói tin thu thập được*
Đầu ra: *Bản rõ*

```
    Thủ tục (Khai thác Mavlink)
1   Tạo Đối Tượng Drone
2   Định Nghĩa Trình Xử Lý Tin Nhắn Mavlink
3   D0 ← đọc (Gói_DữLiệu)
4   Trong khi (KếtNối! = 0):
5       Gói Tin ← Lấy(độ_dài, địa_chỉ, cổng)
6       Phản Hồi (ThưViện_Mavlink) ← đọc (TinNhắn_Mavlink)
7       Với (i ← Đọc (GóiTin)):
8           D0 ← PhânTích(GóiTin) + 0x00ff (khung bắt đầu STX bản v1.0)
9           D1 ← PhânTích(KýTự_Hex)
10              ĐốiTượngDrone ← SẵnSàng(D0, D1)
11              nếu (GóiTin! = Null)
12                  GiảiNén (GóiTin)
13                  DữLiệu_ĐãNhận (DạngNhịPhân, Hex)
14                  BảnRõ ← ChuyểnĐổi(DạngNhịPhân, Hex)
15                  ThôngTin_BảoMật ← Lấy (GPS, tải_trọng, độ_cao, kinh_độ, vĩ_độ, v.v.)
16  Kết thúc thủ tục
```

Khi UAV thực hiện nhiệm vụ và bắt đầu trình bay, người tấn công gửi một bản tin MISSION_COUNT vừa gửi từ GCS tới UAV và khởi tạo gói tin nhiệm vụ cho UAV. UAV sẽ gửi MISSION_REQUEST tới GCS yêu cầu thông tin nhiệm vụ mà GCS đã gửi trước đó nên nó sẽ không truyền nữa. Vì thế, UAV chuyển sang trạng thái chờ thông tin nhiệm vụ tiếp theo. Khi đó, ta có thể dễ dàng chiếm quyền điều khiển UAV.

4. Mô phỏng tấn công phương tiện bay không người lái thông qua giả mạo giao thức điều khiển

4.1. Cài đặt môi trường thử nghiệm

- Thành phần UAV ảo: sử dụng nền tảng mở jmavsim kết hợp PX4 (phần mềm điều khiển bay nguồn mở).

- Thành phần GCS: Sử dụng nền tảng mở QgroundControl, là một GCS cho phép kiểm soát và cấu hình chuyến bay đầy đủ cho các phương tiện PX4.

- Kẻ tấn công (Attacker): Sử dụng nền tảng mở GCS dạng dòng lệnh Python script của thư viện Pymavlink, dùng MAVProxy (phần mềm mã nguồn mở đóng vai trò router) kết hợp các công cụ tấn công mạng có trong bộ Kali Linux.

Các thành phần khác nhau được giả lập trên các máy tính, kết nối nhau thông qua Wifi và sử dụng giao thức MAVLink trong điều khiển giữa GCS và UAV.

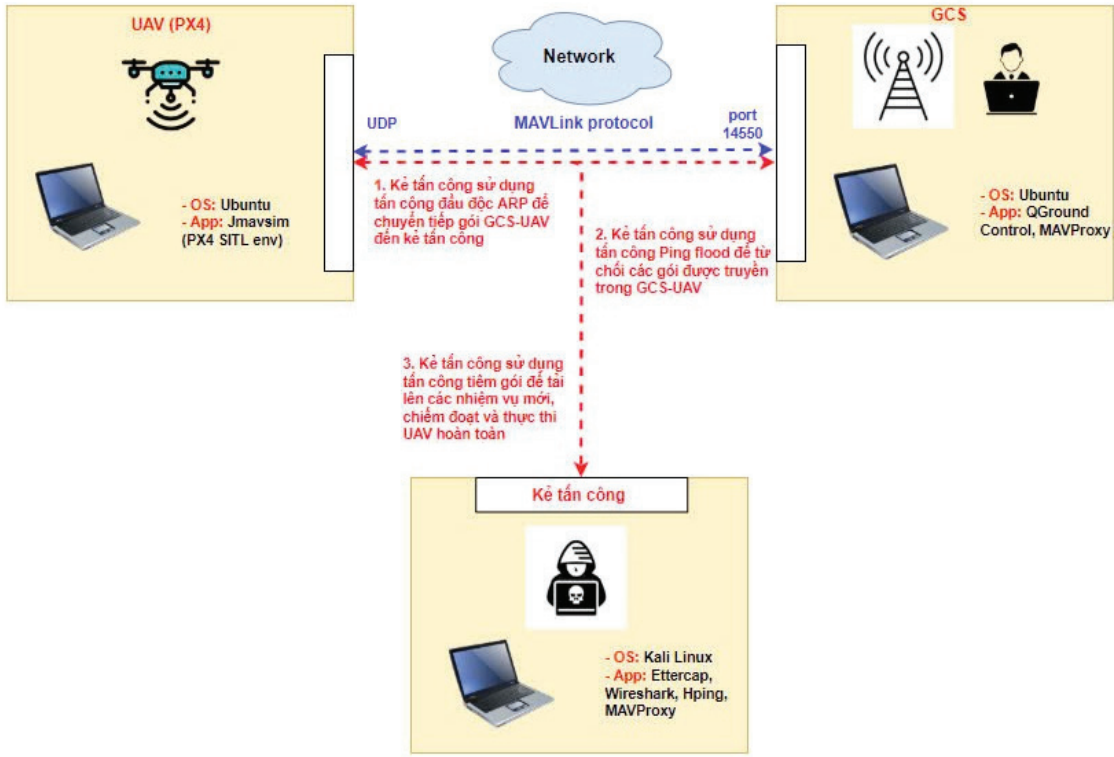
Kịch bản tấn công như mô tả trên hình 3.

4.2. Kịch bản thực hành và kết quả

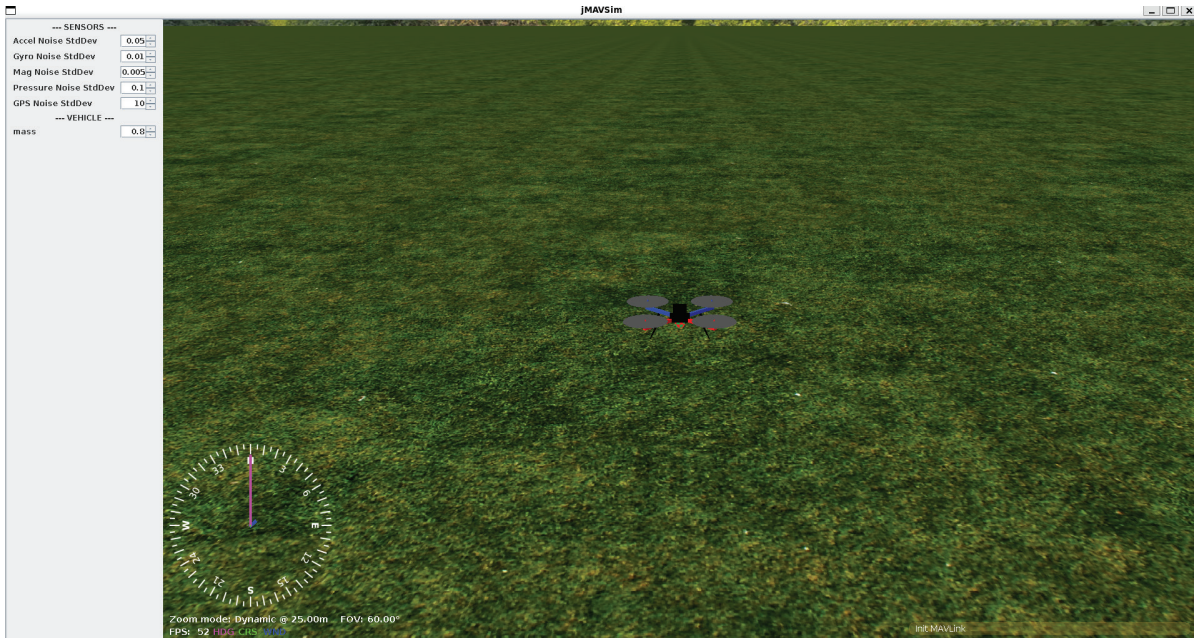
Sau khi cài đặt xong chương trình, ta tiến hành dựng kịch bản khai thác giao thức MAVLink 1.0 và tấn công chiếm quyền điều khiển UAV. Kịch bản sẽ mô phỏng sau khi đã hoàn tất cài đặt các thành phần và mạng như sau:

Bước 1: Khởi động UAV, sau khi khởi chạy, giao diện cho thấy như trên hình 4.

Bước 2: Điều khiển UAV bằng GCS. Thực hiện đẩy một nhiệm vụ lên UAV bằng QGroundControl, UAV sẽ hoạt động tuân theo nhiệm vụ từ GCS di chuyển theo tuyến được giao (các waypoint).



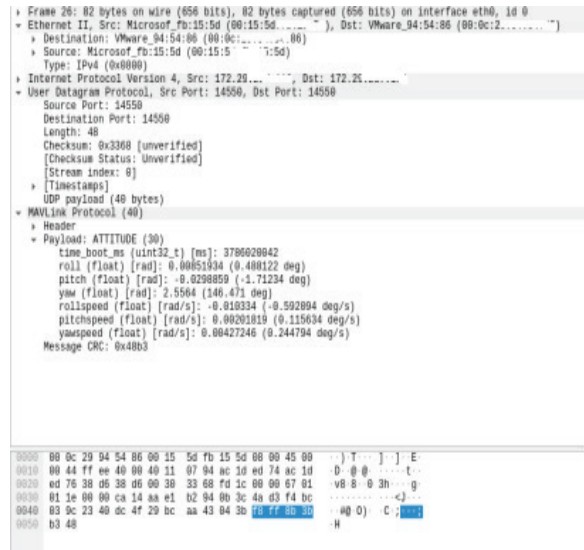
Hình 3. Mô hình kịch bản thực hành tấn công chiếm quyền điều khiển phương tiện bay không người lái.



Hình 4. Hình ảnh giả lập.

Bước 3: Trinh sát, thu thập và phân tích thông tin. Kẻ tấn công thực sử dụng Ettercap, thu thập, trinh sát các thông tin về UAV và GCS (port, protocol…), thông qua Wireshark để phân tích gói tin thu thập được. Kẻ tấn công thu thập, phân tích dựa trên các thông tin như: cổng giao tiếp (thường là các cổng MAVLink phổ biến như 14550 trong phiên UDP); giao thức được sử dụng (MAVLink); cấu trúc của các payload (chẳng hạn như các lệnh nhiệm vụ, heartbeat, dữ liệu viễn thông). Một số kết quả thực hành như trên các hình 5 và 6.

Hình 5. Trinh sát các thành phần tham gia mạng kết nối phương tiện bay không người lái - điều khiển qua trạm mặt đất.

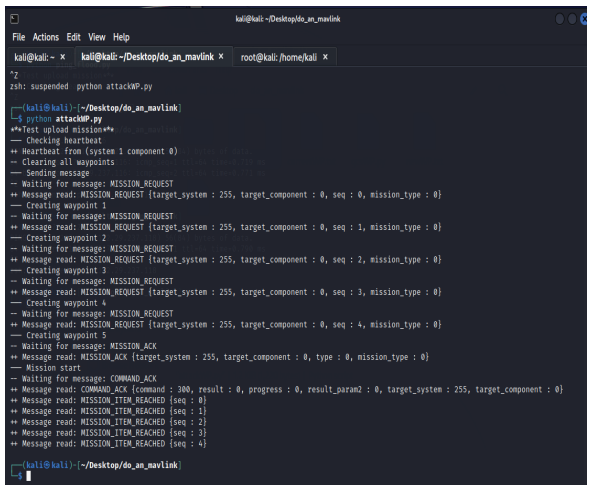


Hình 6. Minh họa phân tích giao thức MAVLink.

Bước 4: Khởi tạo tấn công từ chối dịch vụ đến UAV. Trên cơ sở thông tin đã trinh sát, thu thập tại bước 3, thực hiện tấn công từ chối dịch vụ làm UAV dừng lại giữa không trung, không thể tiếp tục thực hiện nhiệm vụ đã định hoặc phản hồi các lệnh mới từ GCS, trạng thái bay chuyển sang chờ và treo, tiếp tục đợi nhiệm vụ bay để thực thi.

Bước 5: Kẻ tấn công thực hiện chiếm quyền điều khiển UAV. Sau khi làm gián đoạn giao tiếp giữa GCS gốc và UAV, kẻ tấn công ngừng can thiệp

nhưng lợi dụng việc giao thức MAVLink thiếu xác thực người dùng, không xác thực lệnh đến, điều này cho phép kẻ tấn công tiêm các lệnh mới. Kẻ tấn công sử dụng MAVProxy để: Xóa nhiệm vụ hiện tại đã tải lên bởi phi công hợp pháp trước đó; đẩy lên nhiệm vụ mới là tập hợp waypoint mới theo quỹ đạo của kẻ tấn công. Do vậy, UAV giờ đây tuân theo các lệnh của kẻ tấn công và không còn phản hồi với sự điều khiển của phi công ban đầu. Nhiệm vụ đã bị chiếm quyền hoàn toàn. Kết quả thể hiện trên giao diện dòng lệnh cho thấy như hình 7.



Hình 7. Giao diện dòng lệnh thể hiện kết quả chiếm quyền, chuyển lệnh điều khiển đến phương tiện bay không người lái thành công.

5. Kết luận

Nội dung bài báo đã trình bày một số kết quả nghiên cứu về phòng chống UAV sử dụng phương án chiếm quyền điều khiển giao thức lớp mạng, đã thực hành mô phỏng phương án chiếm quyền điều khiển UAV.

Phương pháp tấn công dựa trên phân tích giao thức điều khiển đối với UAV đang ngày càng được quan tâm nghiên cứu. Tuy vậy, phương pháp này gặp nhiều thách thức lớn như: khó khăn trong việc phân tích đối với dữ liệu hay tín hiệu điều khiển đã được mã hóa; thời gian phân tích thường lớn, do vậy, không phù hợp đối với các bài toán yêu cầu thời gian thực, cần tấn công tức thì. Khi các UAV hoạt động bầy đàn, việc phân tích giao thức để chế áp cho từng thiết bị một là không hiệu quả. Ngoài ra, đối với các UAV thế hệ mới có khả năng tự hành, phương pháp này cũng khó khả thi.

Hướng nghiên cứu này có thể phù hợp với mục tiêu nghiên cứu, phân tích các giao thức điều khiển UAV, từ đó leo thang các chiến lược bắt giữ UAV trinh sát để thực hiện các nghiên cứu sâu hơn. Ngoài ra, thực hiện chiếm quyền đối với các UAV dân dụng vi phạm các vùng cấm bay, việc sử dụng phương pháp tấn công thông qua chiếm giao thức điều khiển cho thấy tiềm năng, tính hiệu quả cao.

TÀI LIỆU THAM KHẢO

[1] Y. Jiang (2021), "Development of a laboratory platform for UAV cybersecurity education", *2021 ASEE Virtual Annual Conference*, 8pp.

[2] I. Guvenc, F. Koohifar, S. Singh, et al. (2018), "Detection, tracking, and interdiction for amateur drones", *IEEE Communications Magazine*, **56**, pp.75-81.

[3] R.A. Zitar, M.A. Betar, M. Ryalat, et al. (2022), "A review of UAV visual detection and tracking methods", *Computational Science & Computational Intelligence*, pp.2-10.

[4] J.H. Kim, N. Kim, C.S. Won (2023), "High-speed drone detection based on yolo-V8", *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing*, DOI: 10.1109/ICASSP49357.2023.10095516.

[5] Y. Wang, Y. Chen, J. Choi, et al. (2019), "Towards visible and thermal drone monitoring with convolutional neural networks", *APSIPA Transactions on Signal and Information Processing 8*, DOI: 10.48550/arXiv.1812.08333.

[6] Y.M. Kwon, J. Yu, B.M. Cho, et al. (2018), "Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles", *IEEE Access*, **6**, pp.43203-43212, DOI: 10.1109/ACCESS.2018.2863237.

[7] L. Krichen, F. Mohamed, L.C. Fourati (2018), "Communication architecture for unmanned aerial vehicle system", *International Conference on Ad-hoc Networks and Wireless*, pp.213-225, DOI: 10.1007/978-3-030-00247-3_20.

[8] A. Koubâa, A. Allouch, M. Alajlan, et al. (2019), "Micro air vehicle link (mavlink) in a nutshell: A survey", *IEEE Access*, **7**, pp.87658-87680, DOI: 10.1109/ACCESS.2019.2924410.

[9] N.A. Khan, N.Z. Jhanjhi, S.N. Brohi, et al. (2022), "A secure communication protocol for unmanned aerial vehicles", *Comput. Mater. Contin.*, **70(1)**, pp.601-618, DOI: 10.32604/cmc.2022.019419.