MTD-IDS Approach for Communication Interruption in Secure Targeted Drone Navigation

Subhajit Ghosh[1], Avik Kumar Das[1], Neepa Biswas[2]

Department of Computer Science, University of Engineering & Management, New Town Action Area – III, Kolkata, West Bengal, India[1]

Department of IT, Narula Institute of Technology, Agarpara, Kolkata, West Bengal, India[2]

Corresponding author: Subhajit Ghosh, Email: mastersubhajit.ghosh2021@uem.edu.in

Ensuring that communication remains secure and uninterrupted during targeted drone navigation is a significant challenge, especially in areas vulnerable to cyber threats and signal disruptions. This paper presents an innovative approach that combines Moving Target Defense (MTD) and an Intrusion Detection System (IDS) to tackle communication interruptions in autonomous drone operations. By utilizing dynamic frequency hopping, encryption techniques, and anomaly detection algorithms, our method boosts resilience against adversarial attacks like jamming, spoofing, and unauthorized access. The system continuously monitors network traffic and adjusts its communication channels to effectively respond to evolving threats in real time. Performance evaluations show that our approach greatly lowers the success rate of attacks while keeping drone navigation stable and efficient. A comparative analysis with existing security frameworks underscores the benefits of our method in terms of adaptability, detection accuracy, and operational reliability. This research plays a vital role in enhancing secure drone communications by incorporating proactive defense strategies, ultimately strengthening the robustness of autonomous aerial systems in mission-critical applications.

Keywords: UAV, moving target defense, drone communication, drone attacks, Intrusion Detection System.

2025. In Puneet Kumar Gupta (ed.), *Computational Models for Intelligence and Automation*, 96–103. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-1-8-9

1 Introduction

The rapid progress in computing technology has brought about Cyber-Physical Systems (CPS), exemplified by Unmanned Aerial Vehicles (UAVs) [13]. These UAVs combine cyber aspects with physical attributes, such as sensors and communication channels, finding applications in various fields, including military [11], commercial ventures [6, 8], and disaster response [4, 10]. Despite their benefits, UAVs are vulnerable to cyber threats due to static wireless networks connecting drones and controllers. This paper investigates these vulnerabilities through experiments, revealing potential weaknesses that attackers can exploit. To counter this, the study proposes a strategic defense approach. By integrating wireless encryption, intrusion detection systems, and the Moving Target Defense (MTD) technique [12], the paper enhances system resilience. These defenses complicate attacks, and MTD introduces dynamic changes to thwart them. The findings lay the groundwork for improved UAV network security, advocating a proactive stance with continuous adaptation to evolving threats. The study's comprehensive approach ensures the protection of UAVs across industries and applications, fostering a secure UAV ecosystem.

2 Related Work

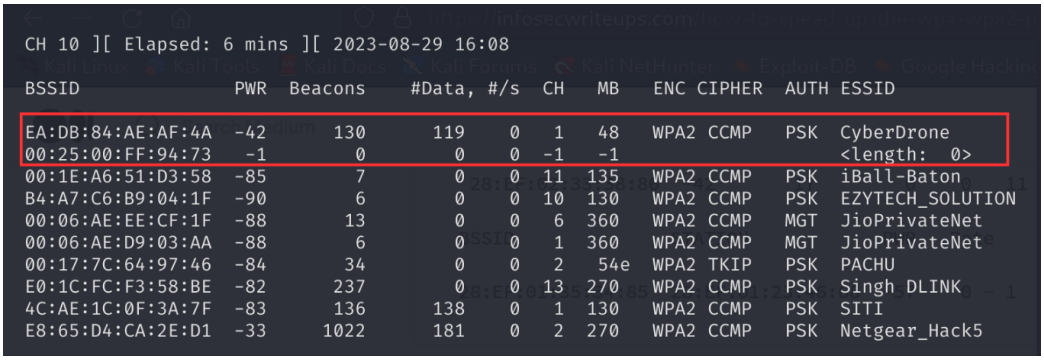
Countless defense mechanisms have been proposed in regard to attacks on drone communication systems. The risks associated with Unmanned Aerial Vehicles (UAVs) include collision hazards, potential aircraft interference, and the looming threat of cyber-attacks that can compromise data or unauthorized control. This concern has spurred extensive research into enhancing UAV security. Initial exploration in UAV security is documented by Mansfield et al. [7]. This work examined cybersecurity vulnerabilities in communication lines, smart device hardware, notably smartphones, tablets, and software applications in order to construct a risk model of the GCS networking hub's danger profile. Another work on Flying Ad-Hoc Network (FANET) [2], which is essentially an ad hoc network between UAVs, has been identified as a new network family. The contrasts between Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET), and FANET are discussed, as well as the most important FANET design problems [2]. In their work [9], Rodday et al. advocated robust encryption for Wi-Fi access points to fortify wireless network security. Another approach [1] demonstrates One-Time Pad (OTP) encryption for wireless networks, adding security layers to resist unauthorized access and cyber-attacks. In [5], Bhatiya et al. analyzed UAV firmware vulnerabilities and suggested secure update measures. Similarly, in the work [3] Reddy et al. explored blockchain for UAV security, aiming at decentralized, tamper-resistant protection of UAV data and secure communication. Together, this research aims to provide a practical approach to prevent possible communication targeting of drones in a secured flight path.

3 Experimental Setup

This section details the experimental setup of our Pi-based drone in order to cater to cost, but the methods are equally effective on any basic commercial UAV. The study uncovers vulnerabilities that attackers exploit using CIA principles in drone networks. For instance, Denial of Service (DoS) attacks disconnect the remote control, risking crashes. These demos explore communication vulnerabilities [5], aiming to enhance security through Kali Linux, a virtual environment,

and the Aircrack-ng toolkit. These actions are research-oriented, understanding drone vulnerabilities to strengthen security.

When a data capture attack is launched on the wireless network, beacon frames with both the origin and endpoint MAC addresses are gathered. As a station in charge of operating the drone, the remote-control device and the drone's MAC address are represented by the MAC addresses shown in Figure 1.



```
CH 10 ][ Elapsed: 6 mins ][ 2023-08-29 16:08

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

EA:DB:84:AE:AF:4A  -42      130       119    0   1   48   WPA2 CCMP   PSK  CyberDrone
00:25:00:FF:94:73   -1        0         0    0  -1   -1                    <length:  0>
00:1E:A6:51:D3:58  -85        7         0    0  11  135   WPA2 CCMP   PSK  iBall-Baton
B4:A7:C6:B9:04:1F  -90        6         0    0  10  130   WPA2 CCMP   PSK  EZYTECH_SOLUTION
00:06:AE:EE:CF:1F  -88       13         0    0   6  360   WPA2 CCMP   MGT  JioPrivateNet
00:06:AE:D9:03:AA  -88        6         0    0   1  360   WPA2 CCMP   MGT  JioPrivateNet
00:17:7C:64:97:46  -84       34         0    0   2   54e  WPA2 TKIP   PSK  PACHU
E0:1C:FC:F3:58:BE  -82      237         0    0  13  270   WPA2 CCMP   PSK  Singh DLINK
4C:AE:1C:0F:3A:7F  -83      136       138    0   1  130   WPA2 CCMP   PSK  SITI
E8:65:D4:CA:2E:D1  -33     1022       181    0   2  270   WPA2 CCMP   PSK  Netgear_Hack5
```

Figure 1: Data packet capture showing MAC addresses of drone & remote controller device.

Using the Aircrack-ng suite's "aireplay-ng" tool, the attacker initiates a de-authentication attack by flooding the drone's MAC address with crafted de-authentication packets. These packets mimic legitimate disconnection commands, tricking the drone into thinking its operator is intentionally disconnecting it. This flood overwhelms the communication channel, cutting off the drone's link to the remote-control device.

```
root@kali: ~# aireplay-ng -0 <number of packets>
-a <bssid of target network> -c
<target client> <interface name>
```

For disconnecting, input <number of packets> (enter 0 for continuous), <target network BSSID>, <target client MAC> (optional), and <interface name>.

```
root@kali: ~# sudo airodump-ng --bssid
<bssid of target network> -w handshake wlan0mon
```

Results include crashing the drone or allowing unauthorized control, known as "drone hijacking." Attackers exploit drone vulnerabilities to manipulate it for malicious goals.

4 Our Approach

To bolster the security of drones against potential cyber threats, we introduce an array of proactive defense techniques aimed at fortifying their resilience and safeguarding their operations. These strategies encompass a long-distance data link using WiFi in raw mode, an intrusion detection system, and moving target defense.

We developed a security-enhanced base station control system for Raspberry Pi drones, integrating the outlined security measures. This system ensures encrypted communication, real-time

intrusion detection, moving target defense, and physical safeguards to fortify drone operations against cyber threats. The base station model is shown in Fig 2:

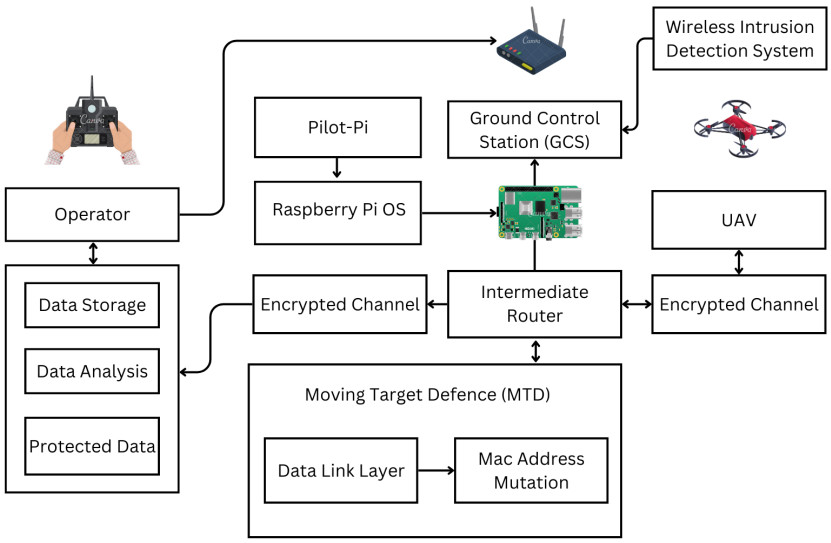


Figure 2: Illustration of secure Base Station Model.

The Raspberry Pi 3b, an affordable and versatile computer, acts as a secure router connecting the drone and remote control. It operates as a hotspot, linking the laptop and drone for efficient communication. Commands from the laptop reach the drone through the Raspberry Pi, and real-time video is sent back. This setup ensures uninterrupted data exchange and better pilot awareness. Libsodium encryption secures this communication. Raspberry Pi OS aids in robust IoT development. Raspberry Pi OS and Pilot-Pi enable communication with the Raspberry Pi Zero W on the drone for autonomous functions. Using Raspberry Pi OS, the drone shifts to autonomous piloting, enhancing efficiency and responsiveness to tasks and surroundings.

4.1 Long distance Data link using WiFi in Raw Mode

This section demonstrates the establishment of a communication link connecting the drone and Raspberry-Pi camera. This enables the transmission of the drone's video stream to a ground computer, where it's displayed in the Ground Control Station. Additionally, a two-way telemetry link and TCP/IP tunnel are established, enabling drone control during flight. If manual drone control via a Ground Control Station with a Joystick using MAVLink is preferred, WFB-ng serves as a unified link for all drone communications. This setup operates over WiFi in broadcast mode and employs software from the WFB-ng project.

The WFB-ng project offers a data transport system that utilizes low-level WiFi packets, effectively overcoming the typical distance and latency limitations associated with the IEEE 802.11 stack. This technology comes with several high-level advantages. Firstly, it delivers a low-latency video link, ensuring swift and responsive communication. Additionally, it establishes a bidirectional telemetry link through MAVLink, allowing for seamless two-way data exchange. It also

creates a TCP/IP tunnel, enabling efficient and secure data transfer. Moreover, the system supports automatic TX diversity by utilizing multiple cards on the ground, eliminating the need for antenna trackers. Security is a paramount concern, and WFB-ng addresses it comprehensively with full link encryption and authentication, leveraging libsodium for robust protection. Furthermore, it optimizes data transmission by aggregating MAVLink packets into batches before sending, enhancing efficiency. Lastly, it offers an improved OSD for Raspberry Pi or generic Linux desktops using gstreamer, enhancing the overall user experience and making it a versatile solution for a wide range of applications.

Firstly, install a preconfigured image from this source. It's essential to note that this image has been tested on RPI3b in conjunction with Alfa AWUS036NHA and the PI Camera. Ensure you utilize the native USB mini-B cable provided with this card for optimal performance. Please be aware that the OSD functionality will not be operational on RPI4 due to the lack of support for OpenVG. In order to set up your communication system, follow these commands:

```
root@kali: ~# ssh pi@<ip address>

// On the Pi used as Intermediate Router
raspberry@pi: ~# sudo systemctl enable wifibroadcast@gs
raspberry@pi: ~# sudo systemctl enable rtsp
raspberry@pi: ~# sudo systemctl enable fpv-video
raspberry@pi: ~# sudo systemctl enable osd
raspberry@pi: ~# wfb-cli gs

// On the Pi used on drone
raspberry@pi: ~# sudo systemctl enable
                 wifibroadcast@drone
raspberry@pi: ~# sudo systemctl enable fpv-camera
```

4.2 Intrusion Detection System

The Intrusion Detection System (IDS) is a vigilant protector, continuously observing wireless networks for unauthorized access. It guards against attacks and spoofing, identifying irregular patterns that may signal intrusion. Yet, IDS lacks preventive abilities, focusing on alerts to administrators. Operating as software, IDS watches network behaviors and notifies administrators of suspicious activities. In our experiment, Kismet wireless IDS actively monitors the drone's network, alerting via a tailored list of alerts. These proactive measures quickly spot anomalies, aiding timely response. Specific changes in the "kismet_uav.conf" file enable wireless network detection and monitoring, readily available within Kismet's bundled configuration.

```
root@kali: ~# cd /etc/kismet
root@kali: ~# cat kismet_uav.conf
```

In this setup, changes enable the system to alert for specific malicious activities, bolstering network security. The Intrusion Detection System becomes a vigilant guardian, raising alarms for unauthorized access and threats. Kismet wireless IDS demonstrates this dedication to defending against vulnerabilities and potential exploits.

4.3 Moving Target Defence

Three fundamental components form the foundation of Moving Target Defense (MTD) design principles: "When-to-Move," which establishes the mutation cycle; "What-to-Move," which deals

with choosing which defender fingerprint set groups to mutate; and "How-to-Move," which includes mobility functions and sampling mutation techniques. MTD may be seen in Figure 3.

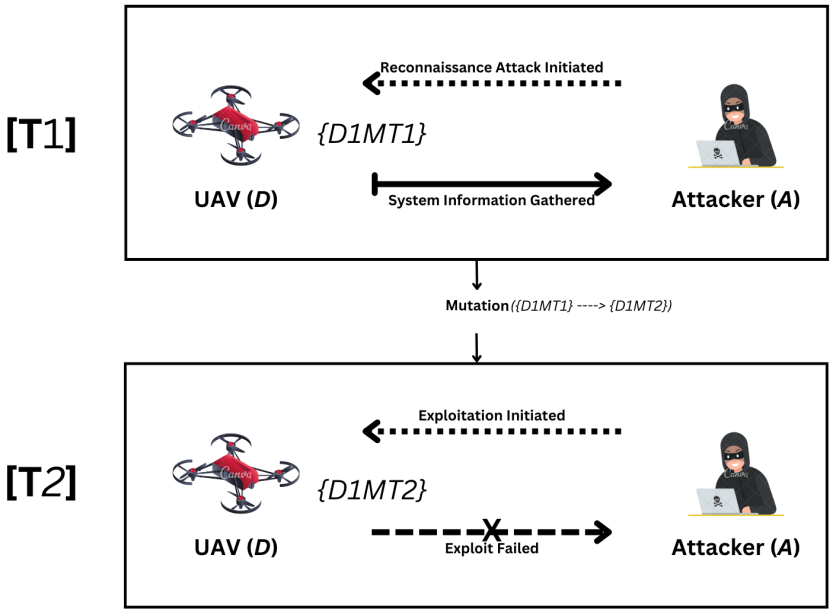


Figure 3: Mechanism of Moving Target Defence.

In 3, the attacker *A* detects legitimate network server *D's* IP address and port. When *A* acts, *D* already used MTD, maintaining a seamless connection to *Tn* via a mutation cycle parameter *MT*. *A's* attempt fails due to *D's* altered state. In MTD, MAC address mutation is employed for security, altering network identity. "Macchanger" tools on Linux modify MAC addresses to enhance anonymity and deter tracking. Executing specific commands on Pi / GCS triggers this process.

```
raspberry@pi: ~# sudo macchanger -m <desired bssid>
           <interface name>
raspberry@pi: ~# sudo service NetworkManager
           restart
```

MTD is an active-defense strategy that confuses attackers by changing network configurations while keeping services available for legitimate users. Existing MTD studies lack comprehensive evaluations, so a unique approach is needed for drones. This paper goes beyond theory, implementing MTD through experimentation. MTD enhances security by changing attack surfaces, making exploitation harder for adversaries.

5 RESULTS

The outcome of the protection strategies against cyberattacks on the drone's wireless network is shown in this section. Additionally, it draws attention to network monitoring signals from Intrusion Detection Systems (IDS). Initial data capture prepares for attacks, while security measures

like libsodium encryption deter attackers. Encryption status is already visible in Fig. 1. This integration of defense and monitoring enhances drone communication security comprehensively.

Given that the wireless network is under the vigilant monitoring of the kismet IDS, any suspicious activities within the network are promptly identified and communicated to the user through alerts. This capability is illustrated in Fig. 4, where the kismet IDS successfully detects and highlights the malicious activity occurring within the network, thereby empowering users to take appropriate defensive actions against potential cyber threats.

```
ALERT: BCASTDISCON IEEE80211 Access Point BSSID 36:7C:D9:7A:35:AC
       broadcast deauthentication or disassociation of all clients; Either
       the AP is shutting down or this is indicative of a possible denial
       of service attack.
```

Figure 4: Kismet Wireless Intrusion Detection System Alerts

Using the moving target defense technique, the router's MAC address is dynamically changed, foiling the cyber-attack designed for the old MAC. This defense is depicted in Fig. 5, where kismet IDS spots the new MAC. This strategy maintains network identity while adding complexity, deterring attackers. Thus, exploiting vulnerabilities becomes tougher, boosting system security.

```
INFO: Detected new 802.11 Wi-Fi access point E2:29:B8:5F:DB:99
INFO: 802.11 Wi-Fi device E2:29:B8:5F:DB:99 advertising SSID 'CyberDrone'
```

Figure 5: Broadcast of mutated MAC address

The attacker's attempt to breach the wireless network using the original MAC address fails due to the dynamic MAC address mutation, evident in Fig. 6 with the message "No such BSSID available." This defense mechanism's success lies in the constant change of MAC addresses, reducing attack predictability and bolstering security against unauthorized intrusion.

```
└─$ sudo aireplay-ng --deauth 1000 -a EA:DB:84:AE:AF:4A -c EA:DB:84:AE:AF:4A wlan
0mon
01:09:12  Waiting for beacon frame (BSSID: EA:DB:84:AE:AF:4A) on channel 9
01:09:23  No such BSSID available.
```

Figure 6: Emulation of DOS attack on UAV after MTD implementation

6 CONCLUSION

Keeping drone communication safe is very important, especially in risky areas. This study introduces practical implementation of a system called Moving Target Defense (MTD) and Intrusion Detection System (IDS) to prevent cyber threats from causing communication problems. The system uses frequency changes, data encryption, and real-time detection of unusual activities to protect drones from attacks like jamming and spoofing. Tests show this system reduces security issues while keeping drones steady and data accurate. Unlike older security methods, this system is better at adapting to and stopping threats, making it ideal for crucial drone tasks. Future studies can enhance this system with machine learning to predict and respond to attacks

more effectively. The results of this research help advance drone safety and support the future of autonomous flying systems.

References

[1] Sukhrob Atoev, Oh-Jun Kwon, Chee-Yong Kim, Suk-Hwan Lee, Young-Rak Choi, and Ki-Ryong Kwon. The secure UAV communication link based on OTP encryption technique. In *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 1–3, 2019.

[2] Ilker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks*, 11(3):1254–1270, 2013.

[3] Rupa Ch, Gautam Srivastava, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Sweta Bhattacharya. Security and privacy of uav data using blockchain technology. *Journal of Information security and Applications*, 55:102670, 2020.

[4] Wesley DeBusk. Unmanned aerial vehicle systems for disaster relief: Tornado alley. In *AIAA Infotech@ Aerospace 2010*, page 3506. 2010.

[5] Fekadu Lakew Yihunie, Aman Kumar Singh, and Sajal Bhatia. Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. In *Smart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019*, pages 701–710. Springer, 2020.

[6] Geoffrey Ling and Nicole Draghic. Aerial drones for blood delivery. *Transfusion*, 59(S2):1608–1611, 2019.

[7] Katrina Mansfield, Timothy Eveleigh, Thomas H Holzer, and Shahryar Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, pages 722–728. IEEE, 2013.

[8] Vinay Pandit and Arun Poojari. A study on amazon prime air for feasibility and profitability: A graphical data analysis. *IOSR Journal of Business and Management*, 16(11):06–11, 2014.

[9] Nils Miro Rodday, Ricardo de O Schmidt, and Aiko Pras. Exploring security vulnerabilities of unmanned aerial vehicles. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, pages 993–994. IEEE, 2016.

[10] Sonia Waharte and Niki Trigoni. Supporting search and rescue operations with uavs. In *2010 international conference on emerging security technologies*, pages 142–147. IEEE, 2010.

[11] Huifang Wang, Hongjun Cheng, and Heyuan Hao. The use of unmanned aerial vehicle in military operations. In Shengzhao Long and Balbir S. Dhillon, editors, *Man-Machine-Environment System Engineering*, pages 939–945, Singapore, 2020. Springer Singapore.

[12] Jun Xu, Pinyao Guo, Mingyi Zhao, Robert F Erbacher, Minghui Zhu, and Peng Liu. Comparing different moving target defense techniques. In *Proceedings of the First ACM Workshop on Moving Target Defense*, pages 97–107, 2014.

[13] Yueyan Zhi, Zhangjie Fu, Xingming Sun, and Jingnan Yu. Security and privacy issues of uav: a survey. *Mobile Networks and Applications*, 25:95–101, 2020.