

NALYSIS OF CYBER ATTACKS ON DRONES

Rivojiddinov D.B.

Assistant, Kimyo International University in Tashkent, Namangan Branch.

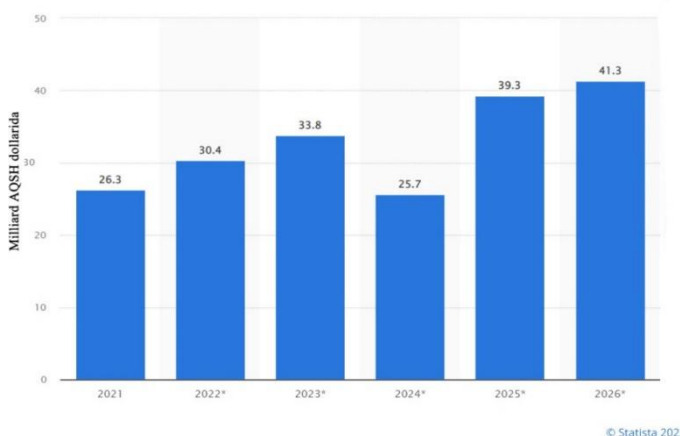
[E-mail: doniyorrivojiddinov@gmail.com](mailto:doniyorrivojiddinov@gmail.com)

Abstract: *This paper examines the rapid growth of drone technology and its increasing use in various fields worldwide. It analyzes major security challenges in drone communication systems, including DoS attacks, Man-In-The-Middle attacks, GPS spoofing, jamming, and wormhole attacks. The study highlights the limitations of drones due to limited resources, which make security implementation more difficult. It also discusses key methods for improving drone security such as encryption, antivirus use, and system updates. The research emphasizes the importance of developing effective solutions to ensure safe and reliable drone operations.*

Keywords: *Drone security, cyber threats, DoS attack, Man-In-The-Middle attack, GPS spoofing, jamming, wormhole attack, UAV communication, information security.*

Nowadays, the development of drones and their widespread use across various fields have led to an increase in demand for drones. This, in turn, has contributed to the growth of the global drone market size [1]. According to data from [statista.com](https://www.statista.com), the global drone market size is projected to develop as follows from 2021 to 2026 Figure 1

Figure 1. Global drone market size from 2021 to 2026. Drone security is a key topic of discussion among researchers and industry professionals



worldwide. Although drones have numerous applications, without addressing security issues and implementing necessary architectural changes, drone applications may not be able to fulfill their intended purposes in the near future. Therefore, it is essential to resolve security challenges in drone communications and to develop new architectural solutions.

Before studying the issues of information security in drone communications, let us consider the basic process of communication with a drone (Figure 2). A drone operates through a simple procedure [2]. It includes transmitting a data link from the controller to the drone and sending data from the drone to the satellite.

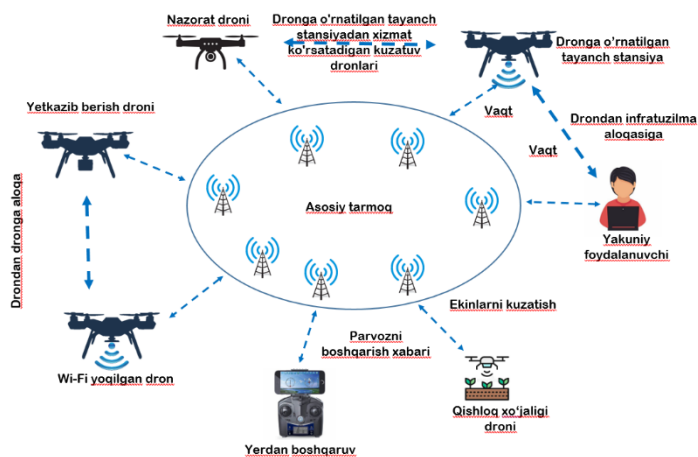


Figure 2. The main process of communication with a drone.

In drone communication, apart from general cyber threats, there are also several specific security issues. One of these issues is that drones are unmanned, which makes it difficult to dynamically and flexibly solve unexpected problems. In drone security, there is a need to apply

advanced solutions for authentication, access control, and ensuring data confidentiality in information protection. The reason for this is that resources in drones are very limited. In addition to the specific security issues mentioned above, the following security threats in drone communication must also be addressed. Some of these attacks are described below:

Denial of Service (DoS) attacks – A DoS attack restricts access to legitimate users by overwhelming shared resources with a large number of unnecessary requests sent by the attacker in order to stop the normal operation of the drone. This leads to system overload and may result in the rejection of some or all legitimate requests.

Man-In-The-Middle (MITM) attack – In this attack, the attacker positions themselves between the client and the drone. The attacker uses a device known as a Wi-Fi Pineapple.

Geolocation spoofing (GPS spoofing) – In GPS spoofing attacks, the attacker transmits incorrect signals. During the process of obtaining the drone's GPS coordinates, the drone uses fake geolocation data based on GPS manipulation.

Radar systems – Monostatic radar is one of the most traditional methods for detecting important objects. Radars emit electromagnetic signals that can travel long distances. These signals spread in all directions and are reflected from the surface of the drone when it is detected.

Jammers (signal jamming attacks) – Jammers are electronic devices used by attackers to block signals at the receiver side using electronic interference equipment.

Wormhole attack – In a wormhole attack, two malicious drones strategically position themselves within the network to intercept communication between drone networks. A tunnel is created by the attacker, allowing them to launch attacks from any point in the network [3].

To counter the above threats, several recommendations are proposed:

- regularly update drone software;
- use updated antivirus software on drones;
- use VPN (Virtual Private Network) to encrypt connections;
- limit the number of devices that can connect to the main station;
- use the "Return To Home" (RTH) mode in case the drone is stolen.

Conclusion: This article analyzed several drone-related attacks such as DoS attacks, deauthentication attacks, Man-In-The-Middle, GPS spoofing, jamming attacks, and other location-related threats such as radar-based detection.

REFERENCES:

1. www.statista.com
2. Ganiyev, A. A., et al. "Kompyuter tarmoqlarida uzatilayotgan axborotni kriptografik himoyalash usuli." *Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий* 7.1 (2024): 73-79.
3. Ganiyev, A. A., Mavlonov, O. N., Shodmonov, D. A., & Maxmudov, J. I. (2024). Kompyuter tarmoqlarida uzatilayotgan axborotni kriptografik himoyalash usuli. *Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий*, 7(1), 73-79.
4. Umarov, Muzaffar, et al. "Yashil Iqtisodiyot Sharoitida Kichik Biznes Va Xususiy Tadbirkorlikni Rivojlantirishda Davlatning Roli." *Green Economy and Development* 3.4 (2025): 665223.
5. Muradovich, Rustamov Rakhmatali, et al. "Methodology of development of technical and economic model of agricultural machinery dealer point." (2021): 2649-2655.
6. Toshboltaev, M. T., and Z. A. Seytimbetova. "Multichannel System State Graph of Combine Harvesters Branded Technical Service in Uzbekistan." *Agricultural Machinery and Technologies* 14.1 (2020): 46-49.
7. Эгамназаров, Бехзод Бахромжон Ўғли. "Шоличилик кластери бош модели ва машина парки таркибини асослаш." *Илм-фан ва инновацион ривожланиш/Наука и инновационное развитие* 6.3 (2023): 106-114.
8. Sobirjonovich, Isoqov Saydullo. "Considerations of Education as a factor of social mobility in Uzbekistan." (2023).
9. Жураев, Жамшед Рахматиллоевич, Сайдулла Собиржонович Исоков, and Шавкат Куранбаевич Яхшибоев. "Фалсафа доктори (PhD) илмий даражасини олиш учун ихтисослик буйича малакавий имтихон топширувчи талабгорлар РУЙХАТИ." *Социология* 22: 01.
10. Sherzodbek, N. (2025). Til o'rganishda motivatsiyaning roli: ichki va tashqi omillar. *yangi o'zbekiston, yangi tadqiqotlar jurnali*, 2(5), 470-474.
11. Tokhirova, S. The Influence OF Physical Culture on Personality Development. *Maktabgacha va Maktab Ta'limi Jurnali*, 674367.
12. Khayrullayeva, N. N. "The Influence of Persian Classical Literature on English Literature." *International Journal of Language Learning and Applied Linguistics* 3.4 (2024): 107-111.

13. Jamolxonovna, Xayrullayeva Nigora. "Gender tolerantlikni rivojlantirishda etnopedagogik metodlarning ilmiy-pedagogik ahamiyati." *Fergana methodical school 3* (2025): 108-114.

14. Kamalova, Gulnara Gulyamovna, Tulagan Agzamovich Sagatov, and Nizom Jumakulovich Ermatov. "Studying the individual modification of the ovaries of the women during intensive body height of genitals." *European research: innovation in science, education and technology*. 2018.

15. Kamalova, Gulnora, and Kassym-Khodzhaev Ibrokchim. "Age features ehoparameters uterus before menstruation with ovulation in a left-handed girls aged 13 to 23 years." *The Twelfth European Conference on Biology and Medical Sciences*. 2016.