A Comprehensive Review of Anti-Drone Jamming Technology

Mr. Deepak Kumar Das[1]
Amity Institute of Defence TechnologyAmity University, Noida
India kumardeepakdas44@gmail.com

Dr. Manish Kumar Chauhan[2]
Ph.D. (IITR), M.Tech. (NITH)
Amity Institute of Defence TechnologyAmity University, Noida
India mkumar17@amity.edu

Abstract
Drones were originally intended for military purposes, but as technology advances, they might be considered the next industrial sector of the Fourth Industrial Revolution, with limitless potential. The first was a hot air balloon, which was utilised in the Battle of Austria in 1849 and later as a vital fighting weapon in World Wars I and II. Furthermore, a drone is an unmanned, remote-controlled aircraft device. It's extensively utilised for entertainment, but it's also employed for military uses like reconnaissance and surveillance, as well as transportation like Amazon Prime Air. Drones are vulnerable to hacking techniques such as GPS spoofing, control extortion, and jamming since they are operated wirelessly. There are numerous anti-drone technology available.

Index Terms

Drone, GPS Spoofing, Jamming, Anti-drones, Wireless countermeasure

I. INTRODUCTION

A drone is a gadget that is now perceived as being weird by most people. It's more of a toy now than a professional instrument utilised solely by pros. Perhaps this is due to the increased popularity of RC multicopters among the general population.
Drone technology has been identified as a critical technology. When the drone initially appeared, it had the benefit of being able to operate remotely as an autonomous device, but its operational range was limited. However, as technology progresses, motor efficiency and battery capacity rise, leading in improved flying duration and range, culminating in new movements using drones. Large corporations, such as Amazon and Google, are planning a drone- based transportation industry, implying Drones are ushering in a new era. Drones are vulnerable to physical external assaults. It is much more important that the body be lighter in order to fly through the sky. There are several external risks, including as colliding with drones, birds, electricity wires, and winds.

Something more significant than the external environment is required for the realisation of drone-enabled technology. It is a matter of security. Even if drones engineered to go farther, longer, and heavier are built, if they crash due to malicious hacking, they will cause little property damage and significant human injury.
When military drones are hacked, more significant issues develop. Drones capable of carrying explosives or fire rockets will not be hacked, and there will be no civilian terrorism.
Chapter 2 discusses drone technology and how to use it, while Chapter 3 analyses and describes how drones are hacked and their remedies. This report comes to a close with the last chapter, Chapter 4.

II. DRONE TECHNOLOGY

A. What is a drone?

Drone refers to an unmanned remotely controlled flight that is not piloted by anybody. Unmanned Aerial Vehicles (UAVs), which are also utilized in the military, are also classified as drones. Nowadays, most drones are RC multicopters. [1].

B. Drone Driving Principle

Drones fly via rotating propellers powered by a motor. The motor requires electricity to function and is powered by a rechargeable battery. The majority of RC multicopters have four propellers, and the motor likewise has four propellers to drive each propeller. These propellers may alter direction or angle of flight by adjusting their rotational speed. [2].
Electronic speed controls (ESC) control this rotation speed. This part decides the rotation speed by adjusting the power of the motor. There is also a flight control (FC) that transmits signals to control it. There is also a transceiver that can accept user commands. These essential components are included in the drone and may be controlled by the operator via the transmitter.

C. Usages of Drone

1) Security and Surveillance

Drones have become increasingly valuable in security management due to their versatility, versatility and access to hard-to-reach areas Here are some common uses of drones in security management

i. *Surveillance and Patrol*: Drones equipped with thermal cameras or images can provide real-time surveillance and allow security personnel to cover large areas of surveillance, such as borders, strategic infrastructure or rapidly expanding civic events, gather and produce visual data the answers are understandable

ii. *Perimeter Security*: Drones can be used to enhance perimeter security by flying over borders, fences, or sensitive areas. They can detect violations, unauthorized access, or suspicious activity, and provide early warning signals to security teams. Drones equipped with motion detection technology or advanced computer systems can automatically detect and track attackers.

iii. *Crowd surveillance*: Drones can be used at public events, protests, or rallies to monitor crowd movement, estimate crowd size, determine security threats or potential security threats that provide aerial views, enabling security personnel to make appropriate decisions, Work and behave well in crowd control as they do.

iv. *Search and rescue*: Drones equipped with cameras, thermal imaging, or infrared sensors can help with search and rescue. They can quickly cover large areas, locate missing persons or survivors in disaster areas, and notify rescue teams of their location. Drones can reach dangerous or inaccessible areas, providing valuable information to guide rescue efforts.

Reconnaissance is also possible. Drones are not only used for outdoor work, small drone or nano-drones are widely used for recon operations by armed forces in many countries. It can be used to search for jungles, high hills or places where human can't communicate.
In the defence sector, armed forces are operating UAVs as well as Unmanned Combat Aerial Vehicles (UCAVs). Although the use is slightly different, the principle is the same as that of UAV, but UCAV has a clear purpose, such as shooting missiles or dropping bombs [4].

v. *Traffic management*: Drones can help monitor and manage traffic. Real-time traffic images can be captured, traffic jams or accidents analyzed, and information shared with authorities to facilitate faster response and more efficient traffic management

vi. *Facility inspection*: Drones equipped with high-resolution cameras or sensors can conduct aerial inspections of large facilities such as industrial plants, power plants, or oil refineries to detect problems in buildings, detect leaks, check the condition of the equipment Or can, provide cost-effective and efficient inspection without the need for manual operation or specialized equipment

vii. *Counter-Drone Measures*: Drones can also be used in security surveillance to counter unauthorized or malicious drone activities. An anti-drone system or special anti-drone system is capable of detecting, tracking and neutralizing incoming or threatening drones, helping to protect critical areas from potential security breaches

2) Transportation

The use of drones in the transportation industry is on the rise, changing aspects of the industry. For deliveries, drones enable faster and more efficient last-mile delivery, especially in remote or hard-to-reach areas aided by drones equipped with cameras and sensors maintain inventory, optimize warehouse efficiency and facilitate inventory management. They also play an important role in the control of the transportation system, helping to detect errors and reducing the need for manual inspection. The drone provides real-time flight monitoring for traffic management, improving traffic management and routing. Additionally, they help research and map areas for transportation planning and development. Urban skylines are being researched with the goal of bringing drone-like vehicles to cities for short distances. However, regulatory and technical challenges remain, such as security, climate control, privacy concerns, and designing reliable systems for operation beyond the scope of identifying and overcoming these challenges is critical for the successful integration of drones into transportation systems.

3) Agriculture

Agricultural drones are already widely used. The most widely used sector, and a significant share of drones sold are agricultural drones.

Until recently, it was assumed that it was only utilised for farms the size of the United States. The field is so huge that pesticides are difficult to apply, yet they are not widely utilised in Korea. This is because they assumed drones were only used to spray medication.
These days, agricultural drones are highly technological. The camera on the drone allows you to see how much the crops have grown in real time and use it to plan production and distribution plans.
By assessing the soil's state, you may devise a plan for planting seedlings, enhancing efficiency. Similarly, pesticide application research is feasible.

4) Fire Fighting

Drones have proven to be a valuable asset in firefighting, providing vital support, and improving the efficiency of firefighting operations. They are used in many key areas to effectively fight fires.

Fire suppression is the primary use of drones in firefighting. Drones equipped with cameras and thermal image sensors provide real-time aerial detection of fire events, allowing firefighters to monitor fire behavior, find hotspots and make appropriate resource allocation decisions ho Drones also map and plan fires by taking detailed photographs of fire zones and help develop effective strategies

The drone dramatically improves situational awareness by providing video and reporting data, allowing firefighters and incident commanders on the ground to make informed decisions and change firefighting strategies in time in person especially in hard-to-reach or dangerous areas, such as rooftops in the woods, are useful for providing possible escape routes and visual information for assessing system integrity

III. ANTI-DRONE TECHNOLOGIES

A. Drone Hack

1) GPS Spoofing

Spoofing means to cheat. Combining this with GPS means you are fooling your location information. Transport drones need to know the location of their current location and destination to fly to the destination. This requires a sensor that can receive GPS signals in Figure 1 [10].

By default, GPS signals are not encrypted. Therefore, if a GPS signal is disconnected from a drone in delivery and a signal is retrieved again, any other GPS signal can be used to deliver the drone to a desired destination instead of a conventional destination [6].

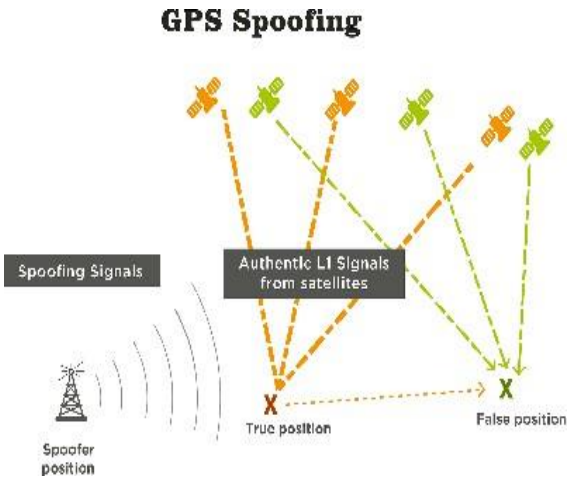

Fig 1. Drone GPS Spoofing

As you can see in Fig 1, desired path for the drone is represented as red X, but if it gets GPS Spoofing in the middle, it will refer to the wrong GPS information and change the path in the other direction such as green X [11].
There is another option. Drones must now maintain a certain altitude. You may collide with a building if your altitude is too low. If you fly too high, you may encounter severe winds or interfere with the flight path of other drones. Drones may maintain a specific height as a result of this. What if you transmit false data to the drone and it calculates that you are flying at an excessively high altitude? The drone reduces its flight height by the required altitude. This can lead the drone to fly low enough to catch and even crash.
This spoofing approach is a hack that requires the drone to have a GPS sensor. So you can use a crude way to remove the GPS sensor, but it's not a good solution because it doesn't handle issues like route modifications caused by external causes like winds or missing once drones are lost. Furthermore, creating their own GPS systems and launching satellites, like China or Russia do, is too expensive [7].
GPS spoofing has higher success rate because the GPS location and path are fed to drone at the starting of journey is not updated or transmitted during its airborne period which leads to the spoofing operation successful.. Due to battery capacity difficulties, drones now have limited flying time, therefore they can discover and transport drones in the nearest warehouse near the destination. As a result, the actual flight duration is not very lengthy, and the likelihood of a return request within that time frame is not particularly great. Spoofing, such as altering the destination, can therefore be ignored if the position is only supplied at the beginning point.

2) Hijacking

Hijacking refers to the act of acquiring control of any transportation machine unethically or forcefully. RC devices such as RC multicopters often use DSM protocols such as DSMx and DSM2 [8].

When you maneuver the drone, the transmitter transmits a signal to the drone's receiver. The signal is analysed and transmitted to the flight control system, where the gearbox changes the output of each motor to change the direction or altitude.

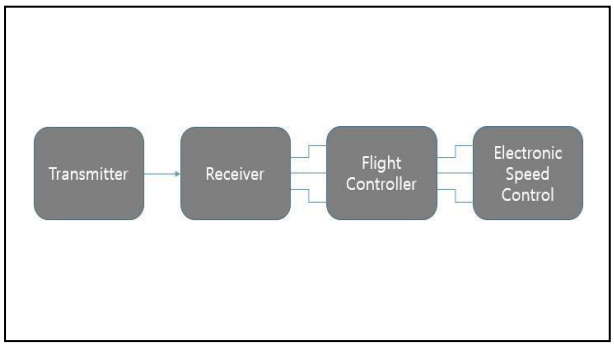

Fig 2. Signaling Process

The DSMx protocol is used when the transmitter and receiver communicate. At this time, the control right can be taken through a modulation process such as inserting and extracting secret information bits in a packet of the DSMx protocol. This is possible through a simple device and software called Icarus. This means that the hacker receives a new signal from the hacker instead of the original user's commands. [11].

To protect against hijacking, employ a proprietary protocol that is difficult to disrupt. You will be safer against outside assaults if you utilise a difficult-to-crack protocol or update the keys necessary for communication on a regular basis.

3) Jamming

Jamming technology in drones is defined as the signal disruption in between the receiver and transmitter.

Disturbance signals can be provided at high power levels to interfere with the usual signal received by the drone. When this happens, the drone loses all received signals and becomes useless. Naturally, the GPS signal is disrupted and the signal is cut off, making it difficult to know where it is, and falling on the location is rare. [10]

Fighting off jamming is challenging. The signal must be supplied at a significantly higher power than the jammer, which is challenging to do. We won't be able to live a regular life utilising radio waves if a high strength signal is transmitted about like jamming.

It is also a means of making the drone invisible by employing meta-materials or mounting cameras on all sides to output the opposite side. This is also the best option because you can't select a target if you can't see the drone at all, which is often when you see it flying then drop it using jamming.

IV. CONCLUSION

Drones are clearly a technology that will garner attention. It is already employed in the transportation industry and has significant military importance. If technology advances, it may be possible to explore space using unmanned spacecraft.

People-centered technology is especially life-saving. This is because, in order to be a technology that substitutes humans to give convenience and prevent damage, it should not be detrimental to people. Drone technology is flying technology; therefore you need be extra cautious.

Drone security is thus a critical issue. Aside from the financial implications of stolen commodities in transit, it can also result in loss of life and control.

Drone security is thus a critical issue. Aside from the financial implications of stolen commodities in transit, it can also result in loss of life and control. To avoid this, the physical component must be augmented, and security issues must be avoided.

The advancement of drone technology is critical. And the thing that must be addressed is anti-drone. We have already trained white hackers to identify software security flaws. Drones are no exception. Investigate anti-drone technologies to identify and solve flaws in drone security. He aspires to develop drone technology that combines safety and ease.

REFERENCES

[1] Hong, S. (2013). The Counter Attack for Physical Attacks on Wireless Sensor Networks by Secure and Optimized Group Diffie-Hellman. International Journal of Advancements in Computing Technology, 5(11), 227–232. doi: 10.4156/ijact.vol5.issue11.24.

[2] Areias, B., Humberto, N., Guardalben, L., Fernandes, J. M., & Sargento, S. (2018). Towards an Automated Flying Drones Platform. Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems. doi: 10.5220/0006792405290536.

[3] Pascarella, D., Venticinque, S., & Aversa, R. (2013). Agent-Based Design for UAV Mission Planning. 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. doi: 10.1109/3pgcic.2013.18.

[4] Booz, J. E. (1998). Future Naval UCAV Applications & Enabling Technologies. doi: 10.21236/ada350673.

[5] Wang, C., & Lan, H. (2019). An Expressway Based TSP Model for Vehicle Delivery Service Coordinated with Truck UA`V. 2019 IEEE International Conference on Systems, Manand Cybernetics (SMC). doi:10.1109/smc.2019.8914357.

[6] Majidi, M., Erfanian, A., & Khaloozadeh, H. (2020). Prediction-discrepancy based on Innovative Particle Filter for estimating UAV true position in the presence of the GPS Spoofing Attacks. IET Radar, Sonar & Navigation. doi: 10.1049/iet-rsn.2019.0520.

[7] H.-S., & Yang, W.-C. (2006). GBAS testbed development in Taiwan with a prototype GPS/GBAS receiver. GPS Solutions, 10(3), 197–206. doi: 10.1007/s10291-006-0021- 0

[8] Wang, H.-S., & Yang, W.-C. (2006). GBAS testbed development in Taiwan with a prototype GPS/GBAS receiver. GPS Solutions, 10(3), 197–206. doi: 10.1007/s10291-006-0021-0.
[9] Hong, S. (2017). Research on IoT International Strategic Standard Model. Journal of the Korea Convergence Society, 8(2), 21–26. doi: 10.15207/jkcs.2017.8.2.021.
[10] Purwar, A., Joshi, D., & Chaubey, V. K. (2016). GPS signal jamming and anti-jamming strategy — A theoretical analysis. 2016 IEEE Annual India Conference (INDICON).doi: 10.1109/indicon.2016.7838933
[11] Shijith, N., Poornachandran, P., Sujadevi, V. G., & Dharmana, M. M. (2017). Spoofing technique to counterfeit the GPS receiver on a drone. 2017 International Conference on Technological Advancements in Power and Energy(TAP Energy). doi: 10.1109/tapenergy.2017.8397268
[12] S. Hong, "Anti-Drone Jamming Technology for Protecting Privacy and Physical Security," International Journal of Advanced Science and Convergence, vol. 2, no. 1, pp. 7- 11, 2020. DOI: 10.22662/IJASC.2020.2.1.007.