International Journal of
Advanced Science and Convergence

ISSN : 2619-8150
Volume 2, Number 1, March 2020
https://doi.org/10.22662/IJASC.2020.2.1.007

Anti-Drone Jamming Technology for Protecting Privacy and Physical Security

Sunghyuck Hong[1]

[1]Division of Information & Communication Technology, Baekseok University, Cheonan, 31065, Republic of Korea

Abstract

Background/Objectives: Drones were originally developed for military use, and as their technology evolves, they can be said to be the new industrial sector of the 4th Industrial Revolution, which has unlimited possibilities. **Methods/Statistical analysis:** The first was a hot air balloon, which was actually used in the Battle of Austria in 1849 and subsequently as an important combat weapon in World Wars I and II. On the top of that, drone is unmanned, remote-controlled flight systems. **Findings:** It's widely used as an entertainment tool, but actually it's not only used for military purposes such as reconnaissance and surveillance, but also for transportation like Amazon Prime Air. Drones are vulnerable to hacking like GPS spoofing, control extortion, and jamming because they're wirelessly controlled. There are these various anti-drones technologies and there are grave risks to drone security. **Improvements/Applications:** Therefore, it is necessary to protect privacy from unwanted drone to use anti-drones technology.

Index Terms

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

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

• Manuscript received January 28, 2020
• Revised February 19, 2020 ; Accepted March 20, 2020
• Date of publication March 31, 2020

I. Introduction

Nowadays, a device called drone has become a strange word for the general public. It's more like a hobby toy than it used to be a professional tool used only by professionals. Perhaps this is because RC multicopters have become popular among the general public.

Drone technology is recognized as a core technology. When the drone first came out, it had the advantage of being able to operate remotely as an unmanned device, but the actual range of operation was not very wide. As technology advances, however, motor efficiency increases and battery capacity increases, resulting in increased flight time and range, which has resulted in new movements incorporating drones. In particular, large companies such as Amazon and Google are preparing a drone-based transportation business, suggesting that drones are creating a new trend.

Drones are weak from physical external attacks. It is even more so that the body must be lighter to fly the sky. There are many external threats, such as hitting drones, colliding with birds, power lines and gusts. If so, can the drones be made stronger to utilize them?

In order for drone-enabled technologies to be realized, there is something more important than this external environment. It is a security issue. Even if drones designed to move farther, longer, and heavier are made, if they fall through malicious hacking, they will result in small damage to property and large damage to people.

If drones for military purposes are hacked, more serious problems arise. Drones that can carry bombs or launch missiles will not be hacked and civilian terrorism will not occur.

In order to learn about drones, Chapter 2 introduces drone technology and how to use them, and Chapter 3 considers and describes how drones are hacked and their solutions. The final chapter, chapter 4, concludes this report.

II. Drone Technology

A. What is a drone?

Drone means an unmanned remotely controlled flight that is not carried by any person. Unmanned Aerial Vehicles (UAVs), which are also used in the military, also fall into the category of drones. Most drones these days mean RC multicopters [1].

B. Drone Driving Principle

Drones fly by propeller rotation through a motor. The motor requires power to operate and uses a rechargeable battery. Most RC multicopters have four propellers, and the motor also has the same number of propellers to drive each propeller. These propellers can adjust their rotational speed and can change direction or angle of flight by varying the 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 sends a signal to the transmission and controls it, and there is a transceiver that can receive user commands. These basic parts are present in the drone and can be controlled by the user by sending commands through the transmitter.

C. How to use drones

1) Surveillance and Reconnaissance

Drones are not just recreational toys for hobbies or amusement. Indeed, drones are excellent surveillance and reconnaissance tools that are also used as military technology. The unmanned aerial vehicle (UAV) mentioned above is used, and information can be obtained by attaching a surveillance camera to the UAV. If only the optical camera is equipped, it is difficult to operate at night. It is equipped with an infrared camera that can monitor enemies at night and also features laser range finders to help with the mission.

UAV is already in operation in Korea. Look at the surveillance area along the border to see if it's suspicious. Often used in conjunction with ground surveillance equipment.

Reconnaissance is also possible. In addition to outdoor areas, there are also drones that can navigate inside the building. These drones are usually designed to be small in size and quiet. You can use this drone to scout areas that are hard to reach, such as buildings, jungles, and mines that have been destroyed by disasters.

In the United States, which uses a lot of defense power, it is 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].

2) Transportation

Amazon is a global online shopping platform. Amazon also announced a new platform that incorporates drone technology. Amazon Prime Air, a company for drone delivery services, was founded on December 7, 2016, and was set up to allow drones to deliver their orders quickly. The drone used for this is a fully automatic driving drone [5]. There is no human intervention in the delivery drones carrying the goods ordered by the customers to their destinations. It just receives the location information of the destination and then flies to the destination by autonomous driving. Normally drones and UAVs are not human-driven, but they are often controlled by humans, and this Amazon Prime Air aims to automate even the controls. To this end, we've created intermediate hubs that hold drones around, and we're also introducing technologies such as installing a charging platform on the streetlight for a short break.

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 recognized that it was used only for farmland as large as the United States. The field is so large that it is hard to give pesticides, but it is not used well in Korea. This is because they thought drones were just for spraying medicine.

Agricultural drones have high technology these days. The camera on the drone allows you to check in real time how much the crops have grown, and use it to formulate production and distribution strategies.

By checking the condition of the soil, you can establish a strategy for how to plant seedlings, thus increasing efficiency. Similarly, research on pesticide application is possible.

4) Fire Fighting

Drones can also be used for fire fighting. Compared to fire trucks, which can be difficult to dispatch immediately depending on road conditions, drones can fly faster because they have no restrictions on flying. Of course, the amount of water that can be mounted is not very high, but it can be quite effective in the initial suppression. In addition, the extent of the fire in the air is easy to understand, which can be helpful in developing future firefighting strategies.

III. DRONE TECHNOLOGY SECURITY

A. Security Importance

Drone technology has a very important blind spot. What if Amazon's shipping drones were stolen and changed their shipping address through unauthorized outside access? Or if a drone controlled by a civilian is hacked and can't be controlled and falls on others? Or what if UCAV, a military operation, was attacked by a hack, taking control?

These hypotheses are not easily passed [6]. There is no lasting security in the world, especially IT technologies are evolving day by day, with cybersecurity threats steadily increasing. As drones move above people's heads, care should be taken because problems in flight can cause them to fall on people or buildings and cause physical damage.

B. 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 [11].

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 [7].

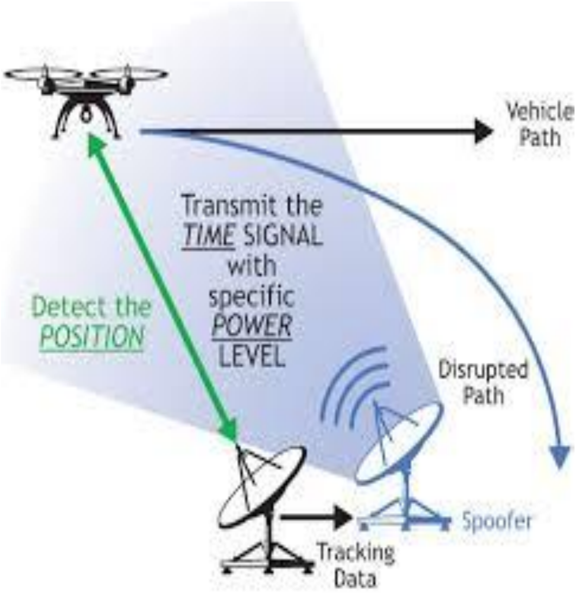

Fig 1. Drone GPS Spoofing

As you can see in Fig 1, you should move to the black line with blue GPS information, but if you get GPS Spoofing in the middle, it will refer to the wrong GPS information and change the path in the other direction.

There is another way. Altitude is important now for drones. If the altitude is too low, you may hit a building. If the altitude is too high, you may have winds that are too strong or may interfere with the flight path of other drones. Because of this, drones have the ability to maintain a certain altitude. What if you send fake information to the drone and calculate that you are flying at too high altitude? The drone lowers its flight height and lowers it by the appropriate altitude. This can cause the drone to fly low enough to capture and even fall to the ground.

This spoofing method is a hacking method that the drone needs to have a GPS sensor. So you can use a primitive solution to remove the GPS sensor, but it's not a good solution because you can't solve problems such as route changes caused by external factors such as gusts or missing after drones are lost. Also, developing their own GPS systems and launching satellites like China or Russia requires too much budget [8].

My personal solution is to have destination location information entered only at the first departure point. This is a problem that cannot accept the request of return or change of destination due to customer remorse, but this is not a big problem. Currently, drones have limited flight time due to battery capacity issues, so they can find and ship drones in the nearest warehouse near the destination. Therefore, the actual flight time is not very long, so the probability of return request within that time is not very high. In this way, if the location is input only at the starting point, spoofing such as changing the destination can be ignored.

2) Hijacking

Hijacking refers to the act of kidnapping a vehicle such as an airplane. RC devices such as RC multicopters often use DSM protocols such as DSMx and DSM2 [9].

When manipulating the drone, the transmitter sends a signal to the receiver in the drone. The signal is analyzed and sent to the flight control system, and the transmission adjusts the output of each motor accordingly to adjust the direction or altitude.

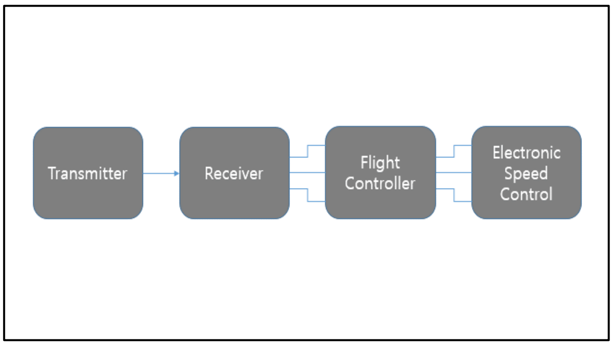

Fig 2. Signaling Process

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 command.

To defend against hijacking, you can use a proprietary protocol that is difficult to interfere with. If you use a protocol that is difficult to crack or periodically change the keys required for communication, you will be safer from outside attacks.

3) Jamming

Jamming means jamming technology. Disturbance signals can be sent at high outputs to interfere with the normal signal the drone is receiving. If this interference occurs, the drone loses all received signals and becomes inoperable. Naturally, the GPS signal is interrupted and the signal is cut off, so it is impossible to know where it is, and it is unusual to fall on the spot [10].

It's hard to defend against jamming. The signal must be sent at an output much higher than that of the jammer, which is difficult to realize. If a high power signal is sent around like jamming, we won't be able to live a normal life using radio waves.

It is also a kind of method to make the drone invisible by using meta-materials or attaching cameras on all sides to output the opposite side. This is also the way to go because you can't set a target if you don't see the drone at all because you usually see it flying and drop it using jamming.

IV. CONCLUSION

It is clear that drones are a technology that will attract attention. Already used in the transportation industry, it is also of great military value. If the technology evolves further, it may be possible to explore space with an unmanned spacecraft.

Technology that is close to people is particularly life-saving. This is because it should not be harmful to people in order to be a technology that replaces people to provide convenience and reduce damage. Drone technology is flying technology, so you should pay more attention to safety.

So drone security is a serious problem. In addition to the financial problems of being stolen goods in transit, it can also cause loss of life and loss of control. To prevent this from happening, the physical part must be supplemented and security problems must be prevented as well.

The development of drone technology is important. And the part that needs to be taken care of is antidrone. Already we have trained white hackers to find out about software security weaknesses. The same is true for drones. Research antidrone technology to find and address weaknesses in drone security. He dreams of creating drone technology that captures both safety and convenience.

ACKNOWLEDGMENT

This research is supported by 2020 Baekseok University Research Fund.

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, Man and Cybernetics (SMC). doi: 10.1109/smc.2019.8914357.

[6] Suhrke, A. (2019). The plain drone, the armed drone and human security. Handbook on Intervention and Statebuilding, 260–269. doi: 10.4337/9781788116237.00031

[7] 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

[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