EYE FROM THE SKY:

DRONES AND URBAN SECURITY

text:
Dr. **ANTTI PERTTULA**
Principal Lecturer, Systems Engineering
Head of Aircraft Engineering Studies
Tampere University of Applied Sciences

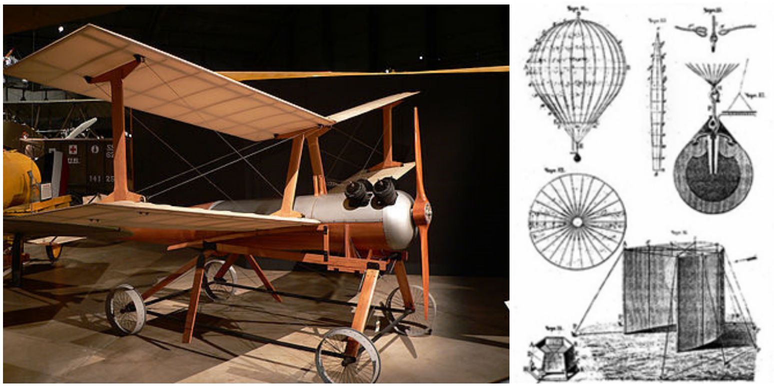
Dr. **MARKUS AHO**
Principal Lecturer, Industrial Technology
Intelligent Machines
Tampere University of Applied Sciences

In many smart cities' visions, drones have several crucial duties including logistics and security monitoring. Unfortunately, many technology applications exploiting drones have also their questionable side. Drones can be used for good and bad purposes. How drones can benefit our urban live? Can they also decrease security, and how to cope with this? We will address these important questions in this article.

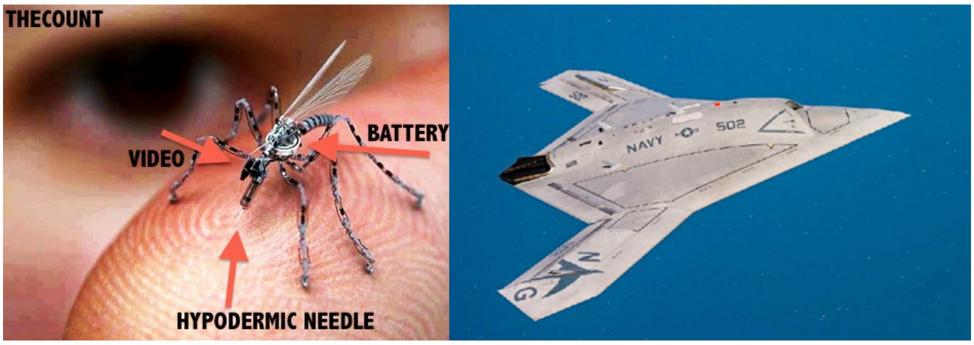
HISTORY OF DRONES

Flying drones have a long history. Probably the earliest one, Kettering Bug, was developed by US Army during the First World War in 1918. It can be defined as an aerial torpedo, a forerunner of present-day cruise missiles. It was able to reach targets up to 120 km and it flew at 80 kilometers per hour (Cornelisse, 2002, U.S. Air Force Publication). Before airplanes, balloons were used to carry out military actions remotely. In 1859, Austrians attracted Venice by pilotless balloons loaded with bombs.

Since then, the drone business has expanded hugely. Currently, sales of flying drones has reached two billion euros in a year and the amount is expected to double in five years. In addition, it has been predicted that the drone services market would reach 20 billion in 2022 (MarketWatch



Venice balloon bombs (Prof. Jurij Drushnin, Monash University) and Kettering Bug (the National Museum of the USAF)



Smallest Drone Ever (Hd Wallpaper Regimage, 2019) and Northrop Grumann X-47B (Military Machine, 2020)

2019). In military sector, these numbers are many times larger. One of the most expensive drones is Northrop Grumann X-47B with estimated price tag of USD 405 million (Military Machine, 2020). Drones are an integral part of modern warfare and currently most of the military operations utilize drones. The sizes of drones vary a lot, the largest one being bigger than Airbus A320 passenger airplane and smallest ones only some millimeter long.

DRONES IN SMART CITY

There are many possible applications for drones in urban areas. Especially, drones offer excellent platform for city logistics and many kinds of sensors. The raising trend is to use low carbon solutions for mail and packet delivery in centers of smart cities. Drone logistics provides one solution and if done autonomously, it can also save labour costs and increase security. Large logistics related companies, such as DHL, Google, Amazon and UPS, have already shown their strategies for drone logistics. In 2019, UPS was the first company to receive from US aviation authority (FAA) a permission for autonomous commercial cargo transportation in 'beyond visual line of sight conditions' (BVLOS). At Tampere University of Applied Sciences, we have got a permission from Finnish civil aviation authority (CAA), Traficom, to carry out BVLOS flights in Tampere area for research purposes. City of Tampere in Finland, aims for innovative and sustainable smart city solutions and, among others, has provided specific test site for new drone related experiments. Drones can be used in several sensoring purposes, such as air quality and traffic congestions monitoring, and collecting data from activities of single or groups of people. Drones can quickly transport many kinds of sensors to areas, where immediate measurements are needed. The data can then be transmitted online, e.g., to Fire, Search and Rescue and Police organization. By drone, one can also inspect the conditions of infrastructure and mechanical failures in high buildings, such as antenna masts, bridges and chimneys, and measure heath losses and check assembly's quality for buildings.

SAFETY CONCERNS IN URBAN AREAS

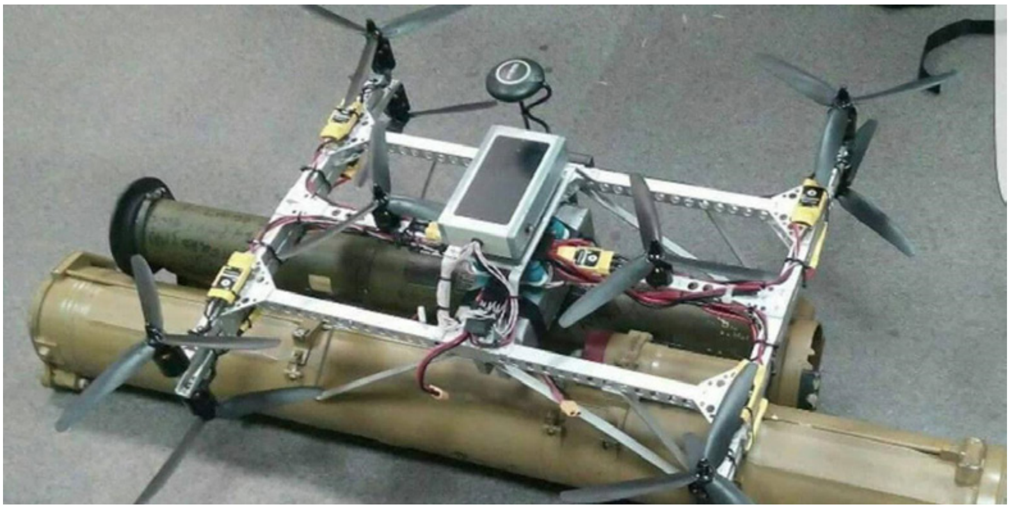
In urban areas, buildings and other infrastructures are close and drones operate in people's normal living environment. People are physically present there and apply many kinds of communication and data transfer systems, becoming more and more wireless. Same time, drone operations are based on wireless data transfer. The signal transmitting channel needs enough capacity to serve also the peak load situations with many simultaneous channel users. The coming 5G network may help here. However, there is always possibility to interfere or even block the communication system by just increasing RF noise. For this purpose, illegal jammers can be bought online cheaply. Drones are equipped with several sensors and cameras, which can cause privacy concerns. Commercial drones are built using normal consumer grade components, which are not as reliable as components in normal aircrafts. Similarly, there is not back-up systems for critical functions, such as energy sources, motors and propellers. One significant safety risk is the drone pilot. The pilot may not have enough understanding about the physical or technical constrains of drones and experience of the severe weather conditions.

DRONES AS THREATS

Drones have several sensors, antennas and cameras, which make them very useful spying devices. They can fly over physical barriers and can reach high buildings and antenna masts. Drones can capture data from WIFI hot spots, disrupt networks, carry explosives and guns. There are also cases, where drones have been used to carry illegal ware and for smuggling goods between countries. If a drone would hit on airplanes, it could destroy parts of fuselage, wings or blades in jet engines and the whole aircraft finally. Small drones are difficult to detect, because they have low acoustic and thermal signatures and low-power RF transmitters. Thus, for radar, they look like birds, and air traffic control radars ignore birds.

DECREASING DRONE RISKS

In digital trust, appropriate IT security practice is important, including checking unauthorized access points and making sure the SW updates come from a reliable partner. Transferred control data between drones and transmitter should be encrypted. Almost all drones are carrying cameras. They can look through windows without closed window blinds, which detect and disrupt drones' views. Make "What-if "-scenarios when needed: What could drone see through the window like managing director's laptop display? Drone pilot should understand when he or she has full control of drone. How to prevent an attacker hijacking the controls? If something strange happens, for example, if the positioning or control signal are jammed, the drone should land autonomously. Data transmitting channel should have enough band-with, low latency and enough speed; new 5G



ISIS jihadis planning a drone bomb attacks on England fans at Russia World Cup (The Sun 1 Apr 2018)

system may help with these issues. Drones should be designed only by highly qualified persons, who understand the reliability and stability of components and mechanical structures; know the critical functions to be duplicated; and can manage external and internal mechanical, electrical and RF interferences, including EMC. In urban areas, drones should fly only through pre-defined flying paths, which will not be located directly above people.

ATTACK TO DRONES

There are several possible levels of attack. The whole drone can be taken in control from its normal planned use mission. It is possible to interfere the flight control computer's internal processes or data transfer channel between the drone and controlling station. In addition, it is possible to change the navigation data by interfering navigation antennas and as mentioned earlier, all RF signals can be blocked completely by jammers. Also, artificial Intelligence (AI) can be used to attack drones. AI type of malware can let drone operate normally until a precise target is located. Target can be identified by facial recognition or other means from kilometers away. After identifying the target, AI takes over the control and commands the drone to complete the forced task. Sometimes, the malware is almost impossible to be found among the normal drone's SW. Marc Ph. Stoecklin from IBM says: "DeepLocker can leverage several attributes to identify its target, including visual, audio, geolocation and system-level features. As it is virtually impossible to exhaustively enumerate all possible trigger conditions for the AI model, this method would make it extremely challenging for malware analysts to reverse engineer the neural network and recover the mission-critical secrets, including the attack payload and the specifics of the target."

ANTIDRONE MEASURES

The off-the-shelf drones of the largest manufactures, DJI and Parrot, have a geofencing software, which prevent drone flies over airports or other restricted areas. However, geofencing in Parrot's drones, can be turned off. In addition, one can build a drone without any geofencing hardware or software and block the drone GPS signals. Also hacking SW is available. In some cases, guns deploying nets, birds of prey ("Eagles trained to take down drones" -BBC News 8.3.2016) and lasers are used to take drones down. However, in urban areas and in airports, it is difficult to use lasers, jammers or a sniper to shoot a drone down. To jam the signals is possible, but illegal in the major part of the West. Fortunately, also other techniques exist to take over and capture or land drones (refer, e.g., Sensofusion). |

CONCLUSION

Drones are entering our everyday lives, also in cities. They are very good and flexible for certain applications and save money and environment. However, we need to understand also the risks they may have because of unreliable components, unprofessional pilots, weather conditions or simply if someone or AI takes over the control and misuse them. Fortunately, there are many actions to decrease the risks, the hardest one being to force drones to land immediately

On the one hand, the accelerated digitalization has increased drone related research, technological development and many new practical applications for smart cities. On the other hand, further research and policymaking is needed fast to find and deploy drone technologies and practices safely.