Christoph von Braun

Writing 3 – Business Proposal and Social Impact

CS 4243 – 12/8/15

Outline

For our capstone senior design project, we are designing a drone recognition and tracking system that will identify errors in a drone's pilot program, and correct those errors during runtime. A drone will be detected using a pattern recognition algorithm performed on webcams, and the information will be corroborated to generate one three-dimensional coordinate for the location of the drone. Using historical information, it can then determine the approximate flightpath of the drone over a period of time. With an expected pilot program known, we can then easily identify if the drone is performing as it should; that is, if the drone is flying along its expected path. From there, if the drone is found to be flying incorrectly, a live swap of the drone control program can be performed, using a custom method of transferring over memory from one host to another and instantly booting up that new machine to resume execution.

For our early prototype, four webcams will be placed around the corners of a room. The four cameras will all be monitoring the same space in the same room, but from different angles. Using the open source computer vision library OpenCV, each camera will run a modified version of the Speeded Up Robust Features (SURF) algorithm to detect the drone. SURF operates with two inputs: the live camera stream itself and a still image of the object it is trying to detect. The algorithm will then process the still image for finding specific features. This can be done before runtime to cut down on delay once the feeds have been started. For every incoming camera frame, SURF will run the same processing for patterns and then run a matching analysis to find matches between the patterns in the video and patterns in the photo. After some cleaning up of the data, a final assessment can then be made whether or not sufficient matches have been found to consider the object found. The matched points can then be averaged to generate one three-dimensional coordinate representing the drone's position relative to the camera's view.

With SURF performed on four cameras separately, there will then be four sets of x/y coordinates to work with. These points will be sent off to an original algorithm that knows the relative positions of the cameras and their viewing angles. While mathematically possible to derive a formula for computing a three-dimensional coordinate from this data, the algorithm will use a less refined solution using flow control. The output will be an x/y/z coordinate for every set of for x/y coordinates. This assumes that all three cameras have detected the drone. If only three detect it, a modified version of the algorithm can still be performed, albeit with some loss in clarity. With only two cameras detecting a drone, however, the loss of resolution would be too great, so that particular frame would be discarded. With a full spatial location of the drone determined, we then move on to the second phase of the system.

The drone will be operating autonomously via some known pilot program. The expected movement patterns of the drone through the room will therefore be known at launch. Given some parameters, the next location of the drone at any given time will be deterministic. Therefore, with the current location data from the drone and the expected location data, it is possible to determine whether or not the drone is performing as expected. Of course, there will be a moderate margin of error on this comparison, as the drone can drift off course simply due to drafts in the room. If the general pattern holds, it will be assumed to be flying correctly and therefore no further action is taken. Multiple sources could cause a disruption in the pilot program, however, thus throwing the drone off course. Bugs might occur, causing an unexpected outcome. There might also have been a malicious alteration from some outside source. If an attacker were to completely override the drone and send it on some other mission, the cameras could detect that deviation and call for its correction.

Once an error has been detected, the program can send a call to immediately start up a backup machine that transfers pilot control over to the drone and resumes execution. The backup will have stored a known correct state ready to go in the event of an error. The drone will then be free to continue with its current task, with the error detected and corrected.

Business Proposal

The profit opportunity in this venture comes not just from a product to sell to consumers, but also from government contracts. The system I am proposing is a prototype for a massive distributed network of drone defense countermeasures that can be employed in every town, city, and country on the planet. If expanded to utilize satellites for identification and tracking of the drones, the market is endless. Drone use within the military and the intelligence community is the most logical use, but within the next several decades, drone usage is going to explode.

It is not hard to imagine a world in which fire suppression, medical services, garbage collection, and even shopping are all performed by autonomous drone. Amazon Prime Air is already a well-publicized application. Within thirty minutes, a customer can have a modestly-sized item or smaller delivered to their front lawn without the use of any intermediate package carrier. The Federal Aviation Administration (FAA) currently has no solution in place for regulation of such drones. They need to consider a multitude of factors, perhaps the most disturbing of which being security. Some malicious individuals would see an Amazon drone not as a convenient delivery method, but as a package ripe for the taking. With a few lines of code, they could perhaps reroute the drone to their destination of choice. In the case of fire suppression, lives could be at stake and dependent on a drone’s timely arrival. What if that drone never arrives? Medical applications can easily see the same critical issue. This solution is exactly what the FAA has been looking for.

As an all-encompassing solution, this system can provide a defense mechanism against rouge drones of any type. Domestic and foreign governments are prime customers, as well as state or municipal governments, depending on how such services as fire and healthcare are organized. Hospitals, future delivery services, and retail companies are all potential customers as well. As drone usage rises, which it most certainly will, so will the need for security measures. While in relatively small numbers now, the drone population is set to explode in the coming years. All it takes is one government agency giving the green light on the contract, writing the legislation, and establishing a precedent for wide-spread drone usage in commercial applications. Even today, however, demand is certainly present. Our nation’s military has been extensively using drones in surveillance and offensive roles and have been actively looking for a solution to the security problem. This system is the prototype for that solution.

This is the first such system of its kind, and as such, will be able to gain a huge leg up on the market. Demonstrated to the FAA, we are confident they will realize its potential and request a non-contested proposal. This document will have the technical details to bring the prototype from its infancy into full distribution via satellite to a large geographic area. Upon completion and awarding of the contract, this massive distributed system can be the world’s introduction to a drone monitoring suite, which will inevitably lead to many more customers, both foreign and domestic. In time, the company will grow to a multinational effort, and become a household name, known for keeping countries and their respective vital infrastructure safe for us all.

Social Impact

Drones will change the world, but they will only have the widest spread of social impact with a well-implemented security system in place. The safer this system can make them, the higher the adoption rate across the globe, from inner cities to rural sub-Saharan Africa. Drones can have the capacity to bring internet to the remote parts of the world, provide vital supplies such as food and water to the inaccessible, and provide safer inner cities with cheaply increased police protection. With circumventing carriers for item delivery from companies like Amazon, costs for shipping will decrease dramatically, enabling more people to share the wealth of goods that such companies can provide.

So how could a remote region on the coast of Africa benefit from a drone security system, assuming the drones are already in place? Let us assume that the drones are bringing fresh drinking water that the area would not otherwise have. The drone gets 90% of the way to its destination, when its signal becomes hijacked by a band of pirates sitting off shore. They could rather easily reroute the drone from the remote village a few miles offshore to their vessel. However, with our proposed security system, this path deviation would be easily detected and rectified, thus preventing the theft. In another scenario, a drone might be supplying armaments to a group of soldiers that have been cut off from reinforcements. If intercepted and sent to the wrong individuals, this could have devastating consequences and lead to loss of life. In an inner city, on the other hand, a drone might be serving as a police monitor, flying above the streets looking for gang activity. If a band of thieves are looking to rob a particular jewelry store, they might seek to first reroute the drone to a different street to avoid detection. This too can be prevented with a security system in place.

The prototype described above only operates with security cameras. How then could it be expected to be rolled out to the entire globe? It would be absurd to attempt to deploy security cameras in every location that needs monitoring. Even if an entirely new piece of technology was invented with a massive range, the environmental effects of installing those might be drastic and unpredictable, not to mention the cost. Fortunately, there already exists a solution that is used by all of us every day. Satellites in the Global Positioning System can identify receivers from anywhere and provide a user with accurate location data. If also applied to the drone security network, the same satellites could connect with each drone to broadcast its position and location data. This information would be sent independently from the pilot program itself, otherwise it too could be spoofed during an attack. With accurate location data being broadcast back to a central hub, it can then be analyzed for faults and corrected.

What is described would cause a major security issue if all were implemented with one central hub, however. With each individual use case, there would be a separate hub for that application. There might only be one drone communicated with on any network, which is not a problem. Each admin has total control over their own security system. With no one central source, there is no centralized point of failure. A malicious user might still attempt to break into the security system as well as the drone itself, but that increases in complexity dramatically from a simple drone hack. With a physical server environment, more resources can be easily deployed to secure that hub, while securing a small pilot program on a drone is more difficult due to limited physical resources.

The system will not use any more physical assets than are already in place, resulting in its footprint being only what the datacenters will consume. Regarding malicious use of the system, there will always be uses that oppose the greater good. There will always be an enemy that build their own system that deploys it for the exact same military use on the opposite side. With the system’s numerous social benefits to healthcare, commerce, and many more however, there is no doubt that the proposed drone recognition and tracking suite is a force for good.