Difficulties We Will Encounter While Building A Distributed Unmanned Air Vehicle Network

Berton Huang

RDF International School

Author Note

Berton Huang, Honors Thesis Class, RDF International School.

This research was supported by Dr. Lee Carroll, the teacher of Honers Thesis Class. and Ms Laurie Haupt, the final proofreader. This research was made possible by their support.

Contact: hxb@mws.site

Introduction

Have you ever seen those drone advertisements or science magazines that claim they could use drones to construct a distributed system and provide a gamut of intriguing services like high coverage Internet? There is no doubt that everyone would like to live in a world with instant Internet coverage and enjoy a whole range of convenience brought by the drones, including instant landscape mapping, automatic object delivery and accurate location service. In fact, research shows that comparing to satellites, drones have significant advantages. For example, data links provided by drones are much shorter, thus are much better in quality and speed than those provided by the satellites. Also, drones are much more flexible than satellites, while also cheaper in individual prices. (Kakaes, Greenwood, Lippincott, Meier, & Wich, 2015)

All these conclusions are leading us to a reality totally opposite to the current one, in that drones are supposed to be one of the most important device in the world and are supposed to be everywhere, forming interconnected networks and clusters flying all over the sky—just like what is introduced in the advertisements, but that is not today's reality.

Why is that? The question has been asked and needs to be answered. In this article, the difficulties we have been encountering when building a drone network are discussed from three aspects: the software, hardware, and regulatory aspects, which are proven to matter a lot. Then, we also gathered a series of revolutionary solutions oriented to those difficulties that might be the solution of them in near future. At last, it is envisaged what it would be like if a drone network is designed in the future, with both previously collected solutions and a few new ideas. Since drones are still under development and still having a bright future, it is not impossible that this system might become a reality.

Difficulties We Will We Encounter While Building A Distributed Unmanned Air Vehicle Network

Literature Review

What are the software challenges?

First of all, the list of challenges from all aspects should be acknowledged. In order to better approach the problem, we decided to start from the biggest source of challenges, according to our research, which are the software challenges. In terms of software, there are three main areas that are most worth our concerned. First of all is how the system should be constructed, including the protocol it uses and the way the devices are organized. The second area, is how will the system react to all kinds of expected and unexpected situations, in other word, emergency handling. The third area is the system's stability and resistance to environmental factors like attacks.

Imagine the system operated completely without order, and how chaotic would that be. So, we should start from the software construction of this system. Drones need a reliable order to stay in the sky so that they will not fall from the sky and hurt anyone. Thus, they must be able to connect to each other to cooperate through certain data links. Their actions should be regulated based on a series of protocols. One of the basic features of these protocols is that they should be able to cover everything from transmission errors to link instability. Also, since the system is in large-scale and distributed, which will require a large amount of data flow and will be under heavy development, the protocol will be better if it is based on some of the pre-existed ones and could be easily extensible. (Allcock, Foster, Tuecke, Chervenak, & Kesselman, n.d.)

Another issue to be worried about is the emergency handling algorithm of the software when an accident happens. These include emergency landing without human control, even under

a damaged situation. Quadcopters are relatively dangerous than those fixed wing drones because of their lack of static stability, which means once the engine stops, it falls on the ground immediately.

Problems may also come from the external environment, in that there might be several other attack factors directed at drones. According to Ablon (2017), remote attack to one of the drones' physical architectures is considered a possible threat to drone systems. He provides the vulnerabilities of each part of the drone system and possible attacks using the vulnerabilities. The first attack is called Sensor Spoofing, which allows sensors to return false information mainly regarding to the Global Positioning System(GPS) module. The second attack method is called Sensor Jamming, which is like the first one but instead of returning false information, sensors will be disabled because of jamming of their frequency used to communicate. The third and the fourth ones are called C2 data link spoofing and C2 data link jamming. From the name we know that the former one connects the drone to a pseudo ground station, and the latter one disconnect the drones and the ground station. The fifth one is called C2 data link radio interception. The last two are C2 data link radio attack on the flight control firmware and C2 data link radio attacks on ground control station software. In conclusion, the vulnerabilities of drones are mainly focused on their sensors and communication links.

Besides safety issues caused by direct external attacks, the internal software might contains vulnerabilities that could cause crashes under certain attacks or even without an attack. This might be caused by multiple reasons, from unstable communication links to the defects in chips or firmware (Sneiderman, 2016) plus weak encryption and even those so-called professional drones cannot escape. (Hartmann, & Steup, 2013)

As I mentioned regarding software safety of the drones, one large weak point for most of the drones is their data links to the ground stations or other drones. Murdock (2016) claimed that vulnerabilities are confirmed by drones security research experts in from San Francisco and the Netherlands. They did a demonstration to show that vulnerability even through the simple apparatus of a laptop and a USB-connected chip. This test is directed to a communication chip called “Xbee”, which uses a low encrypted data link to connect the drone and the controller. According to other experts, the vulnerabilities of this chip can also occur in other models. It’s inferred that there are more manufacturers that produce products with similar vulnerabilities that remain nonpublic. It’s possible that more professional drones might have relatively safer data links but the problem is still there and can be seen through this demonstration. In conclusion, the data links that current drones are using is not safe enough and are at risk of being hacked.

Also, research shows that these kinds of vulnerabilities do not only occur in toy drones, but also those professional ones. This point can be best illustrated by Hartmann and Steup’s research (2013): A test was conducted to measure the security level of three sample UAVs now in use by the U.S military for the purpose of improving them. The samples are the MQ-9 Reaper, RQ-170 Sentinel and the “AR Drone”. In order for information in the drone to be leaked, an essential method is to use information flows connected to the drone. There are two external flows that are considered the most important, which are the data link between drones and the ground station and the data link between the drones’ sensors and the environment. Recently, Iranian captured a drone, RQ-170 Sentinel, without using force. There are two theories as to how this could be done. No matter which one is the right theory, the RQ-170 Sentinel has at least one potentially fatal vulnerability that might be used by the attackers and probably so do the other drones.

Since this is a system connected to the Internet, another important quality of it is its defense toward network attacks over Internet. While other attacks could be solved through patches and updates, there are some attacks that could not. For example, the Denial Of Services (DOS) attack. According to this paper, the DOS attack is an attack that uses a few vulnerabilities on the Transmission Control Protocol(TCP), which were published a long time ago but are still being actively used. Recent years, this attack has been evaluated and become more and more frequent and complicated in that this attack is extremely effective and owning to the lack of a good and cheap way to defend against this attack. According to this article, this kind of attack is now used to coerce victims for a certain purpose, and it's relatively easy and cheap to perform such attack. These attacks change their forms quickly and they are hard to prevent. (Citrix NetScaler: A Powerful Defense Against Denial of Service Attacks, 2017)

Also, according to my field experience, the DOS attack is hard to identify as because it is hard to separate attackers from normal users in a large amount of requests that are all trying to access the same server and use the same services. It is more like a flood of users and clogging up the bandwidth or memory, which is hard to defend against, especially when attackers have copious amount of resources—any online devices are able to initiate an attack, and the device user may not even notice.

In conclusion, the software problems of drones include the construction of the distributed system, the safety of the system itself and the safety toward external factors.

What are the hardware challenges?

Besides software, the hardware, where the software lies and runs, is also another important element of this drone system. Since drones usually operate under various conditions, they will be challenged by the environmental factors and physical obstacles.

The first main problem is power. Drones require a large amount of power to stay in the sky. None of the current traditional power sources like gasoline or batteries could effectively support all-weather or full-time flight—not even close. There are solutions like the idea of solar-powered drones according to Versprille(2015) but their performance are fairly limited by weather and their effective payload. Also, other similar solutions have different restrictions that prevent the drones from being operated freely.

The second main problem is the stability of the system's data links. An unstable data link between drones or between drones and the ground stations might cause unpredictable consequences. Also, some inappropriate data links might be easily interrupted by peers or attackers, while others might be largely affected by the weather.

For example, common data links used by regular drones are easily interrupted. According to Goodin (2016), in addition to a few old methods that may disable or destroy a drone remotely, there is a new way to override the controller and take control. This method is claimed to be different from a jammer and works on most drones. This technology also allows others to remotely generate a unique fingerprint for each drone for the sake of identification. Currently, this technology was just released, but there has already been research on this topic for a long time. It is still not accessible to the public. This is a tool that might bring down the whole drone system by controlling them, which makes it a critical concern. According to Goodin, a firmware update could fix this problem, but not all the hardware supports the update. New devices and updates should be able to avoid this problem now that is has been revealed. In conclusion, the current data links are easily interrupted and need software aid to maintain its stability.

Also, the problem of data link infections also occurs in military drones. Hartmann and Steup (2013) assessed two Unmanned Air Vehicles (UAVs) used by the U.S military, the MQ-9 Reaper and the AR Drone based on their possible vulnerabilities and the occurrence of those vulnerabilities in terms of keeping information safe. The higher the value is, the more susceptible the module is, meaning the easier it is to be attacked. A few aspects have been taken to approach the modules. The first one was environment, and the results show that a mountainous environment will strongly affect availability of drones. The second aspect is on the communication links, which are Tactical Common Data Link (TCDL), Line of Sight (LoS) C band and los WiFi a/b/g/n. According to the results the RCDL link is the safest of all (since it is developed by the U.S military), hard to intercept, but easy to be interrupted by environmental factors like weather. The C band is relatively easier to be intercept but it is less likely to be affected by the environment. However, it might be interrupted if multiple links are present. The third one, which our regular WiFi uses, has the best availability and is less likely to be interrupted. However, this makes it the easiest to be intercepted.

Besides the data link, another problem is which type of drones should be used: fixed-wings or quadcopters. Each one has its own advantages and disadvantages.

The former one, fixed-wing, has a better static stability, and thus has a higher security level in an emergency. But it needs to remain moving to stay in the sky, which means it will not hover in a static place. The latter one is relatively more vulnerable to the emergencies like power loss, but it is able to take off vertically even in dense cities.

For in-flight emergencies, specifically on power loss, D.Atherton, from Popular Science in 2015, classified drones distress events into three types, which are pivotal as reference when drones are making decisions. The first scenario is when drones don’t have enough fuel to stay in

the sky for long. The second scenario is when the drone's engines are not working in the correct conditions and not performing normally. The third is a complete loss of engine power. Solutions must be made to address different scenarios.

Drones used in different areas or scenarios must be considered differently so that they will best meet what is needed in each situation.

In conclusion, drones' hardware needs to be coordinated with the most suitable software, and it needs to be stable and strong enough to survive multiple environments.

What are the regulatory challenges?

In addition to the technical challenges of drones, governmental regulation of drones also plays a pivotal role in system construction because without any regulations, it would be hard to ethically operate these drones that could easily sense private information from the public without even being noticed.

Even if the U.S law, there are already some regulations on UAVs, which is called "Part 107", regarding smaller drones. It requires certain registration for drones and drone operators. Also, drones with limited heights and areas are allowed. (NAVIGATING PART 107, 2017) This might work for usual drones usage but probably won't work for this system. The regulation for this system can be broken down into 3 parts: qualification of operators, usage tracking, and the distribution of responsibilities, so that the regulation will be easier to be designed.

Aside from this, the public attitudes toward drones may also affect the fate of this system according to Frey(2016), in that as long as there are many difficulties that could be easily imagined, it will be necessary to split them into smaller problems that need to be solved. In the meantime, accidents happens, and they attract most of the attention of the public, which means the public will not be satisfied with this system in the beginning. The system must be kept safe

from humans, especially those who are opposed to it, which could be done through a strict standard for system operators' qualifications.

At the same time, the regulations must keep humans safe from the system, meaning that regulations should monitor system usage and the responsibility distribution for whatever accidents occur, because accidents will happen even with the best exception handling precautions.

In conclusion, there are some existing drone regulations, but these will not be suitable for building a new system, so new regulations may be required to make sure things are on the right track.

What are the revolutionary solutions?

After listing all of these difficulties, it is time to consider how we should solve them. Since there are already a few existing solutions, we will discuss some of the most revolutionary ones that are aimed at solving each problem mentioned in the previous section, where difficulties were classified into three types: software, hardware and regulatory.

The most fundamental part of this system will be a combination of multiple platforms including drones, ground stations and satellites. According to Yoon Song in 2009, there is a possible method for achieving this (see appendix A for more information). This system uses High Altitude Platforms (HAPs) as the main component and Mobile Base Stations (MBSs) to connect different devices into a complete network. The placement of each node will be controlled by a algorithm called the K-mean clustering algorithm, which may have better substitutes. As this article concludes, one main defect of this kind of structure is that the HAPs are moving too fast, which might cause the data link to be unstable.

After we have determined the basic hardware structure, it is time to consider the software component of data transmission.

It is indicated that most stable data transfers are based on the file transfer protocol (FTP) protocol, which is mainly based on the transfer control protocol (TCP) protocol. This also allows for extensions, so it is a good choice to use as the base for data transfers in a distributed system because it is friendly to programmers while maintaining reliable connections. (Allcock, Foster, Tuecke, Chervenak, & Kesselman, n.d.) In conclusion, FTP seems to be a good choice for a data intensive distributed system. however, more extensions will need to be made to the system by the developers.

In addition to the basic structure of the system, the level of security also plays a large role in assessing it.

First, we need to discover the weak points or vulnerabilities that the drones have when they come under software attacks and fix them. Murdock claimed that vulnerabilities were confirmed by drone security research experts from San Francisco and the Netherlands. They did a demonstration to show that even through the simple apparatus of a laptop and a USB-connected chip, an attack could be easily initiated oriented to a communication chip called “Xbee”which uses a low encrypted data link to connect the drone and the controller. According to other experts, the vulnerabilities of this chip can also occur in other models. (2016)

However, according to Rodday (2017), the reason why the system is so vulnerable is that the chips encrypt their data link with only two addresses—a Device High Address (DH) and a Device Low Address (DL)--to encrypt their communications. Because both addresses range from 0xFFFFFFFF to 0x00000000 and are written on the device itself, it is possible to crack the

addresses even if the encryption method itself is irreversible and contains no obvious vulnerability.

There are also solutions for resolving data link attacks. According to Ablon (2017), there are two ways to reduce the sensor spoofing attacks, which are using anti-spoof algorithms and adding more antennas and appropriately setting their direction. Also, drones themselves need a mechanism to operate without sensors in order to survive the attack. One solution for the data link spoofing attack is to reinforce the safety of the connection through Public Key Infrastructure (PKI) certificates, which use a public key and multiple private keys to make sure the connection is safe. For the data link jamming attack, it can only be solved by setting up a safety mechanism to enable drones to survive without a connection to the ground station. Data link radio interceptions can be solved by fixing the bugs in the firmware. One example is by using Microsoft's Security Development Lifecycle (SDL).

But that does not mean drones are safe. According to Sneiderman (2016) , there are three vulnerabilities detected by the researchers that are relatively universal. The first vulnerability is that the drone doesn't even have the ability to handle malicious connection requests so they got overwhelmed by too many of connection requests. The second is that the drones have not mechanism to deal with large data packages and got overwhelmed again. The third is that drones don't have the ability to recognize pseudo data packages and can be controlled by them. However, these three vulnerabilities used to occur in the early Internet system, but they have been eliminated by a series of mechanisms in both wired and the wireless network. So this is a possible challenge, but will soon be eliminated after a few iterations. In conclusion, these vulnerabilities can be easily solved as long as people realize it.

Similarly, the software problems will be able to be solved by constant patching and updates to the new firmwares.

Also, new emergency handling techniques are now coming out for drones. There is an emergency landing algorithm for fixed-wing drones that mainly focuses on the emergency handling of powerloss in drones, which includes a classification for three types of drone distress events. There is also an algorithm to caculate drone's emergency landing course. In order to save power, any turns will be minimized. But always flying in a straight line will be slower, so this algorithm can balance the speed and the power loss of drones. Also, the algorithm may be coded to avoid dangerous areas (D. Atherton, 2015).

There is another similar emergency handling algorithm for quadcopters. It allows drones to land with broken propellors under the control of the algorithm. This algorithm can prevent the drones from being damaged in a incomlpete propellors failure. The failure could be due to multiple reasons including all kinds of accidents. This algorithm also allows drones to make controlled landings in this situation without extra physical modifications.(Coxworth, 2013) This method can be used with the emergency landing algorithm I mentioned above to reach the best performance. In conclusion, this method is relatively inexpansive to apply because no physical change needs to be made to the drones.

Regarding the problem of limited power source preventing drones from staying in the sky for long, there are three solutions. According to Versprille, a good power source for drones must have these properties: First is durability, which is how long the power source could last per charge, or how efficienty it can use energy. This makes sense because the longer the drone stays in the sky, the more they can do. The second property is reliability, which is how long it be used without malfunction. Currently there is a prototype using the power sources developed with the

properties above called Zephyr Z8, it is huge but long-lasting which means it can stay in the sky for more than ten days even in bad weather(2015). In conclusion, a good power source must be stable and durable in order to be used on drones.

Also, Versprille (2015) provides three possible new power sources that allow smaller drones to stay in the air longer. The first one is called thermal soaring. This is basically two algorithms that calculate how to locate and use the thermal air flows in an area and use them to lift the fixed-wing drones. This method is limited by environmental factors like wind, but it doesn't need any fuel to operate. The second one is a new kind of photovoltaic cell that raises the drone's efficiency at converting sunlight into electricity from 33% to about 40%. It's a large boost that allowed even the first prototype to stay in the sky for almost a day. The difficulty of this technology is how to help drones survive during the night and on cloudy days but the good thing is it also does not need any fuel. The third one is solid hydrogen fuel system from a company in England. This system uses solid hydrogen, which is three times lighter than lithium batteries to produce electricity plush such battery do not have a shape limit. Solid hydrogen is similar to plastic except it is flammable as gasoline. It is much less reactive than the lithium inside a traditional battery, so it's much safer. Also, it's relatively cheap. All of these three power sources are better than the current ones in that they are more effective and more stable. In conclusion, there are three current improved energy source substitutes for drones, which are thermal soaring, a better kind of photovoltaic cell and a solid hydrogen fuel system.

Regarding regulatory problems, laws are constantly being renewed by the government, so regulations will adapt to fit the system.

In conclusion, there are several solutions for creating a drone network, including a basic structure, a few extensible protocols and a few emergency handling mechanisms for different

drones. Also, software vulnerabilities have been proved fixable by updating the firmware and adding patches.

Discussion

After gathering all these materials, it is apparent that building this kind of drone network may still be outside of out current technological capacity. However, we can still have gain vision of how it might appear in the future by researching some of the future technologies that will be used as solutions for our current problems.

With those technologies introduced in the previous section, the system might work like the following.

As stated in the solution section, here is an existing structure using only High Attitude Platforms (HAPs). However, their mobility needs to be suppressed to stabilize communication (Yoon Song, 2009). Even if the structure is functional, extensions need to be made to make sure that the data link is stable enough and that the nodes are dense enough to provide a reliable and stable service, even in those area with dense populations.

With these factors in mind, after extensive research into drone networking and current state of the art, this author has designed his own solution for creating a drone network, which is as follows: High altitude balloons will act as nodes to control the smaller drones around them. This author decides that they will be tied to the ground with a cable twisted rope and electric cables to provide energy, network and motion control. A winch on the ground will be used to withdraw the balloons for maintenance, under extreme weather condition or in any kinds of emergency. For safety purpose, the entire connection area between the wire and the ground needs to be strictly restricted from public access by regulations.

By deploying those balloons across the area that needs to be covered, such as a city, we will get smooth signal coverage not only in the surrounding area but also in the surrounding airspace, which will allow other devices to connect to the nodes. The basic unit of this system is formed by the central balloon and the other devices connected to it,. The units themselves are to be managed in a centralized way rather than being distributed, but the interrelationsips between units could be diffierent, which means different units will be independent and will not be subject to central managements.

This setup may not be enough if it is deployed in a high population area. Thus this author decides to add connected drones to reinforce the service coverage. They are controlled by the balloons and may curios near the base balloon they belong to or land at a certain ground station waiting for command. They will consist of both quadcopters and fixed-wing drones in a ratio determined by local conditions (the former is more flexible and the latter can withstand harsher conditions). When needed they will be launched automatically and operated according to the needs of the balloon station.

The placement of drones, according to Yoon Song, should be controlled by the K-mean clustering algorithm, which has previously used for the placement of HAPs (2009). (It may be replaced by any algorithm that works better.)

Once the drone is sent to the right place, it will act as a repeater or an individual server according to the kinds of service the users are requesting and the current workload of the central balloon. Within the unit, the data packages will be routed across drones to get to their destinations under a connection-oriented protocol that ensures all the packages are transmitted on C-band. Any transmitters on these frequency channels need to be strictly regulated to minimize jamming or replay attacks on the system. Each drone will be marked by a unique serial number

generated by inreversablly alghoithms from a unique private cipher file embedded in its chip, and the file will be used as the private key to encrypt connections to the central node—the balloon—which already had all the necessary public keys in the memory.

The firmware and the software inside the system could be maintained by the government, carrier operator or even open source communities, depending on the preferences of the public. However, each choice has its own disadvantages. For example, the government or carrier operator may be wiretapping the network traffic or even using the drones to directly collect private information, and open-source communities' products may not be as stable. Plus open source codes might cause a higher rate of vlunerabilities are exposed to the public .

A more neutral solution for software development, suggested by this author, is to allow all the government, carrier operator and open-source communities to contribute to such software. However, all the added source code must be made open-source and accessible to everybody. This way, people will no longer be worried about the problem of privacy, while at the same time everyone can have a chance to contribute to the system and make it better. Regulations and strong examination procedures need to be established in order to make sure the system remains safe and organized. Also, a third-party organization could be established to ensure that every device is loaded with correct firmware.

Another important concern for us is drones' emergency handling. This author decides that there should be a layer of airspace at a specific altitude range, probably lower than the routine cruise altitude, defined as the back-up return layer. Under the event of losing connection with the central balloon, or experencing power shortage, mechanical difficulties or any other issues that still allow the drone to return for phyical repais under the emergency landing algorithms mentioned in the previous sections, it will be navigated to a specific landing area with Global

Positioning System(GPS) and wait for manual repairs. Those that fail to return within the estimated time will be reported and will be dealed with by operators. Those that do not have the ability to return will land on a floating platform formed by drones and then be brought to the landing area. In any other situations, manual override will be required. The organization mentioned previously that will regulate drone firmware could also be used to handle such emergencies.

In the case of possible GPS spoofing or jamming, this author believes that well-encrypted data-link with enough regulations will sufficiently eliminate these problems. Also, the signal strength and acceleration sensors on the drones could also help the drone to determine its relative position. By comparing with the location provided by the satellites, it is possible to detect GPS spoofing. Event information from the GPS receiver that conflicts with data from the other sensors or abnormal jumps in GPS signal strength may be used as the indicators for possible GPS spoofing attacks.

Another thing worth this author's attention is the power source of the drones, which is one of their big limitations. There are already three alternative power sources mentioned in the previous section (Versprille, 2015). However, none one of them allow drones to stay in the sky a for long enough time if used in isolation.

After careful consideration, this author believes that instead of choosing one single power sources, it will be better if each power source is modularized and made to easily loaded on and unloaded from the drone. This way, the solid hydrogen fuel system and the lithium-ion batteries could be the regular power module for drones, while the photovoltaic cells could be loaded if the weather report shows a coming sunny streak. Also, the thermal-soaring algorithm could be put on fixed-wing drones as usual. In addition, it might be possible for a quadcopter to expand itself in

the sky and soar as a fixed-wing drone in order to stay in the sky for a longer period, and then change back only can it use when it needs to suspend itself. This way, not only the thermal soaring algorithm could be applied to it, but it could also use other algorithms like the emergency landing algorithm for fixed-wing drones. This will largely reduce the risk of a drone crashing under a power-loss emergency.

Aside from this, this author believed that the behavior of every unit while connecting to the Internet should be similar to a separate device in a local area network. However, there should be two networks, one of which needs to be connected to the Internet, with the inner addresses well-translated. Also, there should be another dedicated network separate from the Internet specificially for for communication between units. This also separates the service-providing part of the system from the actual dispatch part of the system: the latter one is more protected and is critical for the survival of the system. This strategy will have another advantage, which is that Internet attacks like the DOS attack mentioned in this paper will no longer threaten the safety of the system. The attacks may cause services to malfunction until the attackers are punished according to strick laws, but will not affect the actual operation of the system. Drones could be dispatched over units as long as the borrower unit could privide enough certificates.

Finally, this author believes that the public need to be convinced by promotions, regulations and presuation in order to accept this network and to believe it is safe and that no private data is collected. This could be done though making the firmware open-sourced and regulating conspiracy theorists. Just like how people reacted to the Internet—some with excitement and some with fear—it is acceptable that part of the public have different opinions on this system.

In addition to all the difficulties mentioned in the previous sections, there will always be unexpected problems that have not been considered or addressed, and there will always be problems with the above-mentioned solutions. The actual system will need to be refined through further experiment or test instead of pure paperwork and research.

In conclusion, with all these solutions that addresses the previous difficulties previously encountered in building such a system, it should be possible to deploy this kind of drone network that provides us with network service coverage, if it is uses the structure and solutions this author designed in this section.

Conclusion

In this paper, we discussed three main difficulties, which are software, hardware, and regulatory difficulties. They mainly occur in the construction of the basic system and while dealing with safety concerns. However, there are solutions, like extensible transfer protocols and alternative power sources. Some are ready for use, some need a lot more refinement, and the others remain theoretical.

The question asked in the introduction, which is why the system has not been built yet, can be now answered by looking at all the difficulties and unfinished solutions. However, no evidence suggests that a system like this cannot exist. By looking at the trends of the current solutions, it is possible for us to imagine what such a system could be like if it is built. The system will be highly modularized for the convenience of maintenance. By separating the whole system into separate but similar units, it will be much easier to maintain and implement. Every unit will be centralized by including a central balloon as node and several devices controlled by the nodes. The relationship between nodes could be distributed, and the nodes would be connected with a private network.

Specially designed emergency handling procedures and strict regulations will be applied to such a precise system to minimize mistakes and to protect both the system and the public at the same time.

Also, during the development phase, a few new technologies need to be introduced or developed to solve the remaining problems in the system.

In conclusion, even if we have not yet been able to build the system with our current technology, and we still have a long way to go, it is possible to construct it though systematically designing the system and solving the difficulties.

Thus, possible future study on hardware needs to be focused in field experiments to build experimental systems in a much smaller scale. Also, newer system support technologies to support the system like better materials or power sources could be researched.

Regarding possible future studies on software, better algorithms need to be developed to make these systems work in a more efficient way. Drones' stability is another field that needs to be researched so that the system can be stable enough to support long-term usage.

References

Ablon, J. (2017). Security and the Drone-of-Things - AirMap. AirMap. Retrieved 13 January 2017, from https://www.airmap.com/security-drone-of-things/

Allcock, W., Foster, I., Tuecke, S., Chervenak, A., & Kesselman, C. Protocols and Services for Distributed Data-Intensive Science (1st ed.). Retrieved from https://www.globus.org/sites/default/files/ACAT3.pdf

Citrix NetScaler: A Powerful Defense Against Denial of Service Attacks. (2017) (1st ed.). Retrieved from https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-a-powerful-defense-against-denial-of-service-attacks.pdf

Coxworth, B. (2013). Algorithm lets quadcopters keep flying on three or less propellers. Newatlas.com. Retrieved 13 April 2017, from http://newatlas.com/quadcopter-failure-algorithm/30031/

D. Atherton, K. (2015). Calculating Safe Emergency Landings For Drones. Popular Science. Retrieved 13 April 2017, from http://www.popsci.com/calculating-safe-emergency-landings-drones

Drones In Construction (1st ed.). Retrieved from http://go.skyward.io/rs/902-SIU-382/images/DronesInConstruction_SkywardGuide.pdf

Fingas, J. (2017). Anti-drone gun takes down targets from 1.2 miles away. Engadget. Retrieved 13 January 2017, from https://www.engadget.com/2016/11/28/droneshield-anti-drone-gun/ http://www.popsci.com/drone-gun-downs-drones-with-radio-waves

Frey, T. (2016). 37 Critical Problems that need to be Solved for Drone Delivery to become Viable. DaVinci Institute – Futurist Speaker. Retrieved 13 April 2017, from

http://www.futuristspeaker.com/business-trends/37-critical-problems-that- need-to-be-solved-for-drone-delivery-to-become-viable/

Gettinger, D. (2014). What You Need to Know About Drone Swarms. Center for the Study of the Drone. Retrieved 13 April 2017, from http://dronecenter.bard.edu/what-you-need-to-know-about-drone-swarms/

Goodin, D. (2016). There's a new way to take down drones, and it doesn't involve shotguns. Ars Technica. Retrieved 13 April 2017, from https://arstechnica.com/security/2016/10/drone-hijacker-gives-hackers-complete-control-of-aircraft-in-midflight/

Hambling, D. (2016). Drone swarms will change the face of modern warfare. WIRED UK. Retrieved 13 April 2017, from http://www.wired.co.uk/article/drone-swarms- change-warfare

Hartmann, K., & Steup, C. (2013). The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment (1st ed.). Magdeburg, Germany. Retrieved from https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf

J. VanDoren, V. (2000). Understanding PID Control | Control Engineering. Controleng.com. Retrieved 13 April 2017, from http://www.controleng.com/single-article/understanding-pid- control/ebf9ab7fe3e5571f83901e0b8f3d8f07.html

Kakaes, K., Greenwood, F., Lippincott, M., Meier, P., & Wich, S. (2015). DRONES AND AERIAL OBSERVATION: NEW TECHNOLOGIES FOR PROPERTY RIGHTS, HUMAN RIGHTS, AND GLOBAL DEVELOPMENT A PRIMER (1st ed.). New America.

Moody, J. (2017). SkyWard Announces First Commercial Drone Network Demonstration. 3DR News. Retrieved 13 January 2017, from https://news.3dr.com/skyward-announces-first-commercial-drone-network- demonstration-f2795b7b8ed

Murdock, J. (2016). Drone hack: Weak encryption leaves high-end UAVs wide open to remote hijacking. International Business Times UK. Retrieved 13 April 2017, from http://www.ibtimes.co.uk/drone-hack-weak-encryption-leaves-high-end- uavs-wide-open-remote-hijacking-1547356

NAVIGATING PART 107. (2017) (1st ed.). Retrieved from http://go.skyward.io/rs/902- SIU-382/images/31030%20eBook%20Part107%20FIN.pdf?aliId=4470120

Nelson, P. Drones are part of the Internet of Things, drone maker says. Network World. Retrieved 13 April 2017, from http://www.networkworld.com/article/2986755/internet-of-things/drones-are- part-of-the-internet-of-things-drone-maker-says.html

Pham, H., A. Smolka, S., D. Stoller, S., Phan, D., & Yang, J. A Survey on Unmanned Aerial Vehicle Collision Avoidance Systems (1st ed.). Stony Brook, NY, USA: Department of Computer Science, Stony Brook University. Retrieved from https://arxiv.org/ftp/arxiv/papers/1508/1508.07723.pdf

Prigg, M. (2017). Flying defibrillator that can reach speeds of 60mph revealed. Mail Online. Retrieved 1 January 2017, from http://www.dailymail.co.uk/sciencetech/article-2811851/The-ambulance-drone- save-life-Flying-defibrillator-reach-speeds-60mph.html

RICHARDS, C. (2017). Will Internet Access Via Drones Ever Fly?|WIRED. Wired.com. Retrieved 13 April 2017, from https://www.wired.com/insights/2014/11/internet- access-drones/

Rodday, N. (2017). EXPLORING SECURITY VULNERABILITIES OF UNMANNED AERIAL VEHICLES (Master). University of Twente.

Rothstein, A. Why the drone revolution can't get off the ground. Kernelmag.dailydot.com. Retrieved 13 January 2017, from http://kernelmag.dailydot.com/issue-sections/staff-editorials/11575/7-problems- drone-gao-nas-regulation/

S.McNeal, G. (2016). Forbes Welcome. Forbes.com. Retrieved 13 April 2017, from https://www.forbes.com/sites/gregorymcneal/2016/10/19/key-questions-about-securing-drones-from-hackers/#1ae8af5133f3

Sneiderman, P. (2016). Here's how easy it is to hack a drone and crash it - Futurity. Futurity. Retrieved 13 April 2017, from http://www.futurity.org/drones-hackers-security-1179402-2/

Surakul, K., Sodsee, S., & Smanchat, S. (2015). A Control of Multiple Drones for Automatic Collision Avoidance (1st ed.). Information Technology Journal. Retrieved from http://ojs.kmutnb.ac.th/index.php/joit/article/view/690/644

Versprille, A. (2015). Alternative Power Sources Boost Small Drone Endurance. Nationaldefensemagazine.org. Retrieved 13 April 2017, from http://www.nationaldefensemagazine.org/archive/2015/November/pages/AlternativeP owerSourcesBoostSmallDroneEndurance.aspx

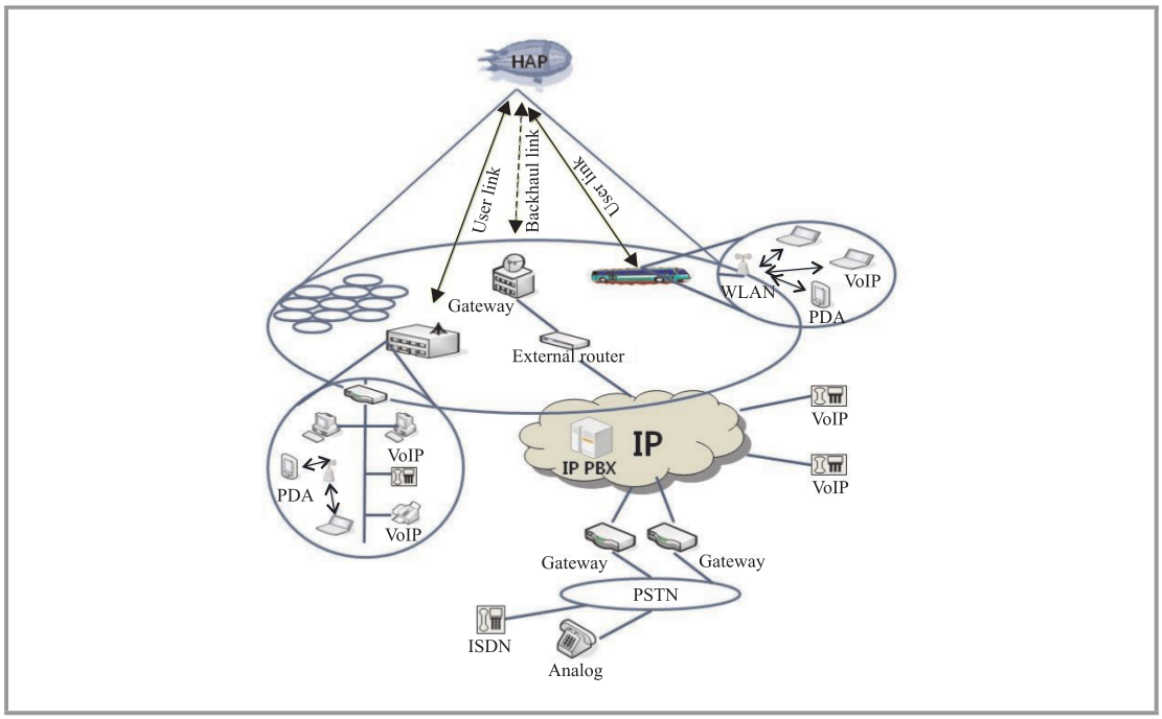
Viquerat, A., Blackhall, L., Reid, A., Sukkarieh, S., & Brooker, G. (2007). Reactive Collision Avoidance for Unmanned Aerial Vehicles using Doppler Radar (1st ed.). France.Springer: Springer Tracts in Advanced Robotics. Retrieved from https://hal.inria.fr/inria-00195933/document

Whitlock, C. (2014). When drones fall from the sky. Washington Post. Retrieved 13 April 2017, from http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/

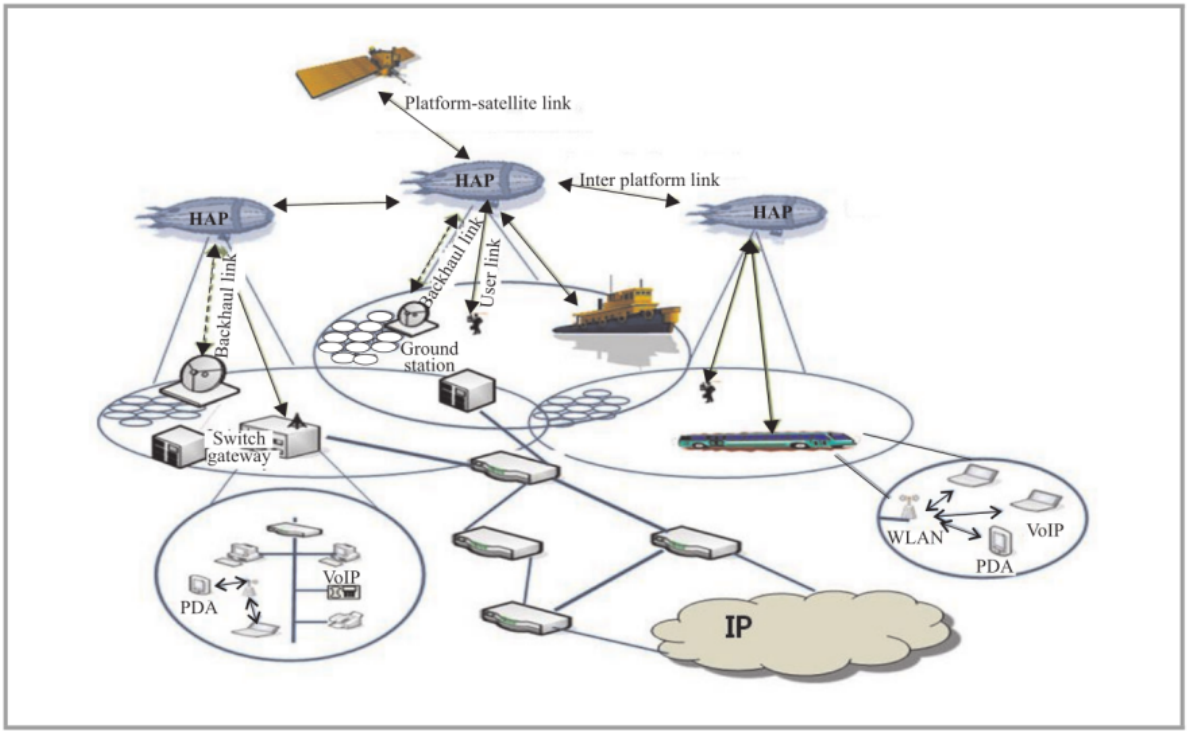
Yoon Song, H. (2009). A Method of Mobile Base Station Placement for High Altitude Platform Based Network with Geographical Clustering of Mobile Ground Nodes (1st ed.). Retrieved from http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BAT8- 0016-0015/c/httpwww_itl_waw_plczasopismajtit2009222.pdf

Appendix A

Basic configure of HAP based network-Singular HAP case(Yoon Song, 2009)



Basic configure of HAP based network-Multiple HAP case(Yoon Song, 2009)



Appendix B

Glossary

- **DH-device** high address
- **DL-device** low address
- **C2 data link**-a telecommunications link over which data is transmitted.
- **Communications protocol**-a defined set of rules and regulations that determine how data is transmitted in telecommunications and computer networking.
- **Firmware**-a type of software that provides control, monitoring and data manipulation of engineered products and systems.
- **UAV**-an unmanned aerial vehicle
- **DOS attack**-a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.
- **TCP/IP**-Transmission Control Protocol / Internet Protocol, is a suite of communications protocols used to interconnect network devices on the Internet.TCP / IP implements layers of protocol stacks, and each layer provides a well-defined network services to the upper layer protocol.
- **Public Key Infrastructure**-a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- **Photovoltaic cell**-an electrical device that converts the energy of light directly into electricity by the photovoltaic effect.