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

Berton Huang

RDF International School

Author Note

Berton Huang, Honers Thesis Class, RDF International School.

This research was supported by Dr. Lee Carroll, the teacher of Honers Thesis Class. Thanks for her support so that this research was made possible.

Contact: hxb@mws.site

Introduction

Have you ever seen those drone advertisements or science magazines, which claimed that they could use drones to construct a distributed system and provide a gamut of intriguing services like high coverage Internet with it? 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, it is indicated that comparing to satellites, drones have motley amount of advantages over the another. 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 way more flexible than satellites while cheaper in individual prices. (Kakaes, Greenwood, Lippincott, Meier, & Wich, 2015)

All that 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 propagandas--which today's reality is not.

Why is so? The question has been asked and need to be answered. In this article, the difficulties we have been encountering when building a drone network are researched from three aspects, which are the software ones, hardware ones and regulatory ones, which proven to be 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 those solutions previously provided and a few new ideas. Since drones are still under development and having a bright future, it is not impossible that the system might come true one day.

What Difficulties 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 to the problem, we decide to start from the biggest challenge source according to our research, which are the software challenges. In terms of that, there are three main fields that worth to be concerned the most. First of all, it is how the system should be constructed including the protocol it use and ways the devices are organized. The second fields is how will the system react to all kinds of expected and unexpected situations, in another word, emergency handling. The third field is the system's stability and resistance to environmental factors like attacks.

Imagine the system operates completely without order, and how much mess would there be. So we should start from the software construction of this system. Drones need a reliable order to stay in the sky so they will not fall from the sky and hurt anyone. Thus they must be able to connect to each other to cooperate through a certain link. Their action should be regulated based on a serious of protocols. One of the basic features of these protocols is that they should be able to cover from transmission errors to link instability. Also, since the system is large-scaled and distributed, which consist 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 includes emergency landing without human control even under a damaged situation. Quadcopters are relatively way more dangerous than those fixed wing ones

in that it lack of static stability which means once the engine stops, it falls on the ground immediately.

Problems may also coming from the external in that there might be several other attack factors pointed to drones. According to this Ablon (2017), Remote attack to one of the drone's architectures is considered a possible threat to drone systems. H is provide vulnerabilities of each part of drone system and also provide a few ways seeking to solve those threats. The first one is called Sensor spoofing which allows sensors to return false information mainly oriented to the Global Positioning System(GPS) module. The second method is called sensor jamming which is like the first one but instead of returning false information, sensors will be disabled because of jamming frequency. The third one and the forth one is called C2 data link spoofing and C2 data link jamming. From the name we know that the former one connect the drone to a pseudo ground station and the latter one disconnect the drone 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 attack 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 might cause crash under certain attack of even without 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 ones cannot escape. (Hartmann, & Steup, 2013)

As I mentioned 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 vulnerability are confirmed by experts in security research of drones from San Francisco and

Netherlands. They did a demonstration to show that even through simple apparatus which is a laptop and a USB-connected chip. This test is 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. It's inferred that there are more manufacturers produce products with similar vulnerabilities that remains nonpublic. It's possible that more professional drones might have relatively safer data link but the problem is still there and can be seem through this demonstration. In conclusion, the data link current drones are using is not safe enough and have a risk to be cracked.

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 with what Hartmann and Steup's research (2013): A test was conducted to measure the security level of three sample UAVs now using by the U.S military for the purpose of improving it. 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 use information flows connected to the drone. There are two external flows are considered the most important which are the data link between drones and the ground station and the data link between drones' sensors and the environment. Recently, Iranian captured a drone, RQ-170 Sentinel, without using force. There are two theories one how could this 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 uses a few vulnerabilities on the Transmission Control Protocol(TCP), which have been publish a long time ago but still being actively used. Recent years, this attack has been evaluate to become more and more frequent and complicated in that this attack is unequally effective and the lack of a good and cheap way to defense from this attack. According to this article, this kind of attack is now used to coerce others for a certain purpose and its relatively easy and cheap to perform such attack. These attacks changes their forms quickly and they are hard to defense. (Citrix NetScaler: A Powerful Defense Against Denial of Service Attacks, 2017)

Also, according to my field experience, the DOS attack is hard to tell as because it is hard to separate attackers from normal users from large amount of requests, which are all trying to access the same server and use the same services. It is more like a flood of users and junking the bandwidth or memory, which is hard to defend especially when attackers have copious amount of resources—any on-line devices are usable to start an attack and the device 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 the software, the hardware, where the software lies and runs, is also another important factor to this drone system. Since drones are usually operated under multiple conditions, it 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 ideas of solar

power drones according to Versprille(2015) but their performances are fairly limited by weather and its effective payload. Also, other similar solutions contain different restrictions which block the drones from being operated freely.

The second main problem is the stability of its data links. An unstable data link between drones or between drones and the ground stations might cause unpredictable consequences. Also, some bad 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 this Goodin(2016), besides a few old ways 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 for most of the drones. This technology also allows others to remotely generate a unique finger print for each drone for the sake of identification. Currently, this technology is just released but there are already researches on it long ago. It is still not accessible to the civil. This is a tool that might bring down the whole drone system by controlling them, which make it critical. 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 since it's revealed. In conclusion, the current data links are easily interrupted and need software aid to maintain its stability.

Also, the data link infection problem also occurs in military drones. Hartmann and Steup (2013) assessed two Unmanned Air Vehicles (UAVs) used by the U.S military which are "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 for it to be attacked. A few aspects have been taken to

approach it. The first one was environment and the result shows that environment with a lot of mountains 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 result the RCDL link is the safest of all (since it is developed by the U.S military), hard to overhear, but easy to be interrupted by environmental factors like weather. The C band is relatively easier to be overheard 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 daily wifi uses, has the best availability and 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 between fixed-wings and quadcopters. Each one has its own advantages and disadvantages.

The former one has a better static stability thus has a higher security level when facing 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 distress event of drones into 3 types, which is pivotal for drones to make decisions. The first scenario is when drones don’t have enough fuel to stay in the sky for long. The second scenario is that the engines of the drone are not working in the correct conditions and not performing normally. The third is the complete loss of engine power. Solutions must be made orienting to different scenarios.

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

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

What are the regulatory challenges?

Besides the technical challenges of drones, the regulations of them also play a pivotal role in system constructions 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.

In spite of the U.S law, there are already some regulations on UAVs, which is part 107, oriented to smaller drones. It requires certain registration for drones and drone operators. Also, drones with limited heights and areas were allowed. (NAVIGATING PART 107, 2017) This might work for usual drones usage but probably won't work for the system. The regulation for this system could be broken into 3 parts which are qualification of operators, trace of usage, and the distribution of responsibilities so that they 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 mean time, accident happens and they attract most of the attention of the public, which means the public will not be satisfied with this system at the beginning. The system must be kept safe from human, especially those who detest it, which could be done through a strict qualification of system operators.

At the same time, the regulations must keep human safe from the system, which refers to the monitor of system usage and the responsibility distribution for whatever accidents happen, since accidents will happen even with the best exception handling precautions.

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

What are the revolutionary solutions?

After listing all kinds of difficulties, it is time to wonder how should we solve them. Since there are a few current solutions, we will discuss some of the most revolutionary ones oriented to solve each problem mentioned in the previous paper, where difficulties were classified into three parts, 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 structure of achieving this (See appendix A for more information). As claimed, this system uses the High Altitude Platforms(HAPs) as the main construction material , as Mobile Base Stations(MBSs), to connect different devices into a complete network. The placement of each node will be controlled by a algorithm called K-mean clustering algorithm which may have better substitutes. As this article concludes, one main infection of such structure is that those HAPs are moving too fast which might cause instability of the data link.

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

According to an article, most of the stable data transfers are based on the file transfer protocol(FTP) protocol which mainly based on the transfer control protocol(TCP) protocol but also allows extension so it is a good choice for the base of data transfer in distributed system since it is friendly to programmers while keeping reliable connections.(Allcock, Foster, Tuecke, Chervenak, & Kesselman, n.d.) In conclusion, FTP does look like a great choice for a data

intensive distributed system, however, more extension need to be made by the developers to the system accordingly.

Besides the basic structure of the system, the security of it also plays a big role in assessing it.

First, we shall find out the weak points–vulnerabilities–the drones have under software attacks and fix them. Murdock claimed that vulnerability are confirmed by experts in security research of drones from San Francisco and Netherlands. They did a demonstration to show that even through simple apparatus which is a laptop and a USB-connected chip, 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 it is so insecure is that the chips encrypt their data link with only two addresses--Device High Address (DH) and Device Low Address (DL)--to encrypt their communication. Since both of them are not long and written on the device itself, it is possible to crack it even if the encryption method itself is irreversible and contains no visible obvious vulnerability.

There are also solutions oriented to data link attacks. According to this Ablon,(2017) there are two ways to ease the sensor spoofing attack which is using anti-spoof algorithms and add more antennas and set their direction to up. Also, drones itself need a mechanism to work without sensors in order to survive the attack. Solution for the data link spoofing attack is to reinforce the safety of the connection through what’s called Public Key Infrastructure (PKI) certificates which use a public key and multiple private keys to make sure the connection is safe. Solution for the data link jamming one can only be solved by setting up a safety mechanism to

make drone survive without ground station because it's relatively hard to deal with. Data link radio interception can be solved by fixing the bugs in the firmware. One example is 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 request so it got stuck by too many of those connect requests. The second one is that the drones have not mechanism to deal with large data packages and got stuck again. The third one is that drones don't have the ability to recognize pseudo data packages and been controlled by them. In my opinion, all these three vulnerability used to occur in the early Internet system and they are now eliminated by a series of mechanisms in both wired networks and the wireless ones. So this is a possible challenge but will soon be eliminated in a few versions. In conclusion, these vulnerabilities can be easily solved as long as people realize it.

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

Also, new emergency handling techniques are now coming out for drones. There is an emergency landing algorithm for fixed-wing drones mainly focus on the emergency handling of loss of power in drones, including classified 3 types of distress event of drones. Then, there is an algorithm of emergency landing course of a drone. In order to safe power, any turning 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, dangerous areas may be avoided according to the configuration. (D. Atherton, 2015)

There is another similar emergency handling algorithm for quadcopters. It allows drones to land with broken props under controlled. This algorithm can prevent the drones from being damaged in an incomplete props failure. The failure can be due to multiple reasons including all kinds of accidents. It allows drones to land under control in this situation without extra physical modification on it.(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 cheaper because no physical change need to be made on the drones.

For the problem of limited power source stop drones from staying in the sky, there are three solutions according to Versprille, a good power source for drones much have these properties. The first one is durability which is how long the source could last per charge or how efficient it can use the energy. This makes sense because the longer the drone stays in the sky, the more they can do. The second one is reliability which is how long can it be used without malfunction. Until now there is a prototype using some of the power sources developed with the properties above called Zephyr Z8 that is huge but long-lasted which can stay in the sky for a tenth of days even in bad weathers.(2015) In conclusion, a good power source must be stable and durable in order to be used on drones.

Also, Versprille(2015) provide three possible new power sources that allows smaller drones to stay in the air longer. The first one is called thermal soaring. This is basically two algorithms which calculate how to locate and use the thermal air flows in an area and use them to raise the fixed-wing drones. This method is limited by environmental factors like wind but it don’t need any fuel to operate. The second one is a new kind of photovoltaic cell that raise the efficiency to convert sunlight into electricity from 33% to about 40%. It’s a large boost that even the first prototype stays in the sky for almost a day. The difficulty of this technology is how to

make drones survive during night and cloudy days but the good thing is it does not need any fuel, too. The third one is from a company in England which is a solid hydrogen fuel system. This system use solid hydrogen which is three times lighter than lithium batteries without any shape limit to produce electricity. This property of solid hydrogen is similar to plastic but 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 these three power sources are relatively better than the current ones in a way of more effective and more stable. In conclusion, there are three current energy source substitutes for drones that's better which are thermal soaring, a kind of better photovoltaic cells and a solid hydrogen fuel system.

For regulatory problems, laws are constantly being renewed by the government so it will self- fit the system.

In conclusion, there are several solutions for 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 add patches.

Discussion

After gathering all these materials, it is indicated that building such a drone network may not fit our current capacity range of either science or anything else. However, we can still have a view of how it might appear in the future by researching some of the future technologies as the solutions for current problems.

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

As what stated in the solution part, there is a present structure using only High Attitude Platforms(HAPs). However, their mobility needs to be suppressed to stabilize the

communication. (Yoon Song, 2009) This way, even if the structure is usable, extensions need to be made to make sure the data link is stable enough and 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 follows. High altitude balloons will act as nodes to control the smaller drones around it. 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 for them. A winch on the ground will be used to withdraw the balloons under maintenance, extreme weather condition or any kinds of emergency. Every connection area between the wire and the ground need to be strictly restricted from the public access through regulation for safety purpose.

By deploying those balloons scatteringly in the area need to be covered, like a city, especially those in the city, we may get smooth signal coverage not only in the surrounding area but also in the surrounding airspace that allows other devices to connect to the nodes. With the central balloon and the other devices connected to it, the basic unit of this system is formed. The unit themselves are to be managed in a centralized way rather than distributed but the interrelations between units could be different, which means, different units will be equally independent without any central managements.

This setup may not be enough if it is deployed in a population host spot. Thus this author decides to add drones connected to reinforce the service coverage. They are controlled by those balloons and may curios around the father balloon they belong to or lands at a certain ground station waiting for command. They will be consist of both quadcopters and fixed-wing drones in a ratio according to the local condition where the former one is more flexible and the latter one

stands harsher conditions. Once necessary, they will be launched automatically and be operated according to the need of the balloon station.

The placement of drones, according to Yoon Song, should be controlled by the K-mean clustering algorithm which previously used for placement of the 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 the kinds of service the users are requesting for and the current work load of the central balloon. Within the unit, the data packages will be routed across drones to get to its destination under a connection oriented protocol that makes sure all the packages are transmitted on C-band. Any transmitters in such frequency channels need to be strictly regulated to minimized jammers or replay attacks to the system. Each drone will be marked by a unique serial number with a private cipher file embedded to its chip and they will be used to encrypt connections to the central node—the balloon—who already had necessary public key in the memory.

The firmware and the software inside the system could be maintained by the government, carrieroperator or even open source communities depending on the choice of the public while each has its own disadvantages. For example, the government or carrieroperator may be wiretapping the network traffic or even using the drones to sense directly private information, and open source communities' products may not be as stable plus open source codes might cause a higher vulnerability exposure rate.

A more neutral solution for software development, suggests by this author, is to allow all the government, carrieroperator and open-source communities to contribute to such software. However, all the source code added must be made open-source and accessible to everybody. This

way, people will no longer worried about the problem of privacy while everyone can get a chance to contribute to such 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 built to ensure that every device is loaded with correct firmware.

Another important concern of us is on the emergency handling of drones. This author decides that there should be a layer of airspace in a specific range of heights, probably lower than the routine cruise height, defined as the back-up return layer. Under the issue of lost connection with central balloon, unattended power shortage, mechanical difficulties or any other exceptions that still have the ability to return for manual handling, even under the emergency landing algorithms mentioned in the previous sections, will be navigated to a specific landing area with Global Positioning System(GPS) and wait for manual repairing. Those, which fail to make its back on estimated time, will be reported and will be handled by operators. Those, which does not have such ability to return, will land on a floating platform formed by drones and then brought to the landing area. For any other situations, manual override will be required. The organization mentioned previously to regulation drone firmware could also be used to handle such emergencies.

For the case of possible GPS spoofing or jamming, this author believes that an well-encrypted data-link with enough regulations will eliminate them well enough. Also, the signal strength and acceleration sensors on the drones could also help the drone to determine its relative position. By comparing to the location provided by the satellites, it is possible to detect GPS spoofing. Events information from the GPS receiver conflicts from the other sensors or

abnormal GPS signal strength jump may be used as the indicators for possible GPS spoofing attacks.

Another thing worth to be focused on is the power source of the drones, which is a big shortage of them. There are already three alternative power sources mentioned in the previous section.(Versprille, 2015)However, neither one of them itself allows drones to stay in the sky for long enough time.

After careful consideration, this author believes that instead of choosing one single power sources , it will be better if each power source is made modularized and could be easily loaded 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 strike. Also, the thermal soaring algorithm could be put on fixed-wing drones as always. Also, it might be possible for a quadcopter could expand itself in the sky and soar as a fixed-wing drone in order to stay in the sky for longer period and changes back only when it needs to suspend itself. This way, not only the thermal soaring algorithm could be applied to it, other algorithms like the emergency landing algorithm for fixed-wing drones only could also be applied to to. This will largely reduce the risk of crashing under an power-loss emergency.

Aside from this, this author believed that the behavior of every unit in connecting to Internet should be similar to a separate device in a local area network. However, there should be two networks, which one of them needs to be connected to the Internet, with the inner addresses well-translated. Also, there should be another dedicated network separated from the Internet for communications of the units only. This also separates the service providing part of the system from the actual dispatch part of the system, which the latter one is more protected and critical for

the survival of the system. This action will have another advantage which is that Internet attacks like the DOS attack mentioned in this paper will no longer threat the safety of the system. The attacks may cause services to malfunction until the attackers are punished with strict regulations but none of the actual operation of the system. Drones could be dispatched over units as long as the borrower unit could prove itself busy enough.

At last, this author believe that the public need to be convinced by propaganda, regulations and actual convince brought to them to accept this network and to believe it is safe and no private data is collected. This step could be done though opening the source code of the firmware and regulating certain conspiracy theorist. Just like how did people react to today's Internet—some with care and some with fear—it is acceptable if part of the press have differ on this system.

Other than all these difficulties mentioned in the previous sections, there will always be unexpected problems have not been considered or addressed and there will always be problems with the stated solutions. The actual system needs to be refined in the practice of further experimenting or testing instead of pure paperwork and researching.

In conclusion, with all these solutions to the previous difficulties found in building such a system, it should be made possible for deploying such a drone network that provide network service coverage for us, if it is using the structure and solutions this author designed in this section.

Conclusion

In the paper, we discussed three parts of difficulties from different aspects, which are software, hardware, and regulatory difficulties. They mainly occur in construction of basic levels and dealing with safety concerns. However, there are solutions like extensible transfer protocols

and alternative power sources, some readily for use, some need a lot more refinements, and the others remain on papers.

The question asked in the introduction, which is why the system has not been built yet, can be now answered by all the difficulties and unfinished solutions. However, no evidence rejects such system from existence. By looking at the trends of current solutions, it is made possible for us to imagine what such system may be like if it is built. They 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 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 are to 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 protect both the system and the people at the same time.

Also, a few new technologies need to be introduced or developed to solve the remaining problems in the system over the course of testing usage.

In conclusion, even if we have not be able to build the system with current technology, still 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 need to be focused on field experiments to build experimental systems in a much smaller scale. Also, newer technologies to support the system like better materials or power sources could be researched.

For possible future study on software, better algorithms need to be developed to make such system work in a more efficient way. The stability of drones is another field need to be researched to that the system could 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

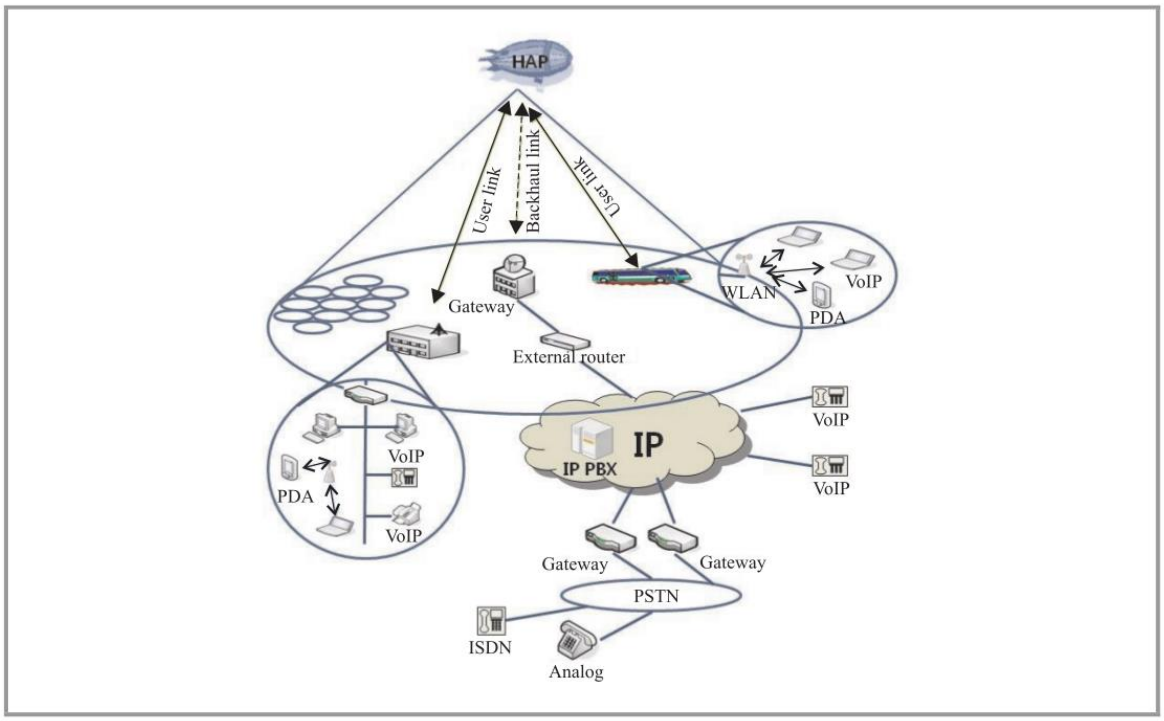
Versprille, A. (2015). Alternative Power Sources Boost Small Drone Endurance. Nationaldefensemagazine.org. Retrieved 13 April 2017, from http://www.nationaldefensemagazine.org/archive/2015/November/pages/AlternativeP owerSourcesBoostSmallDroneEndurance.aspx

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/

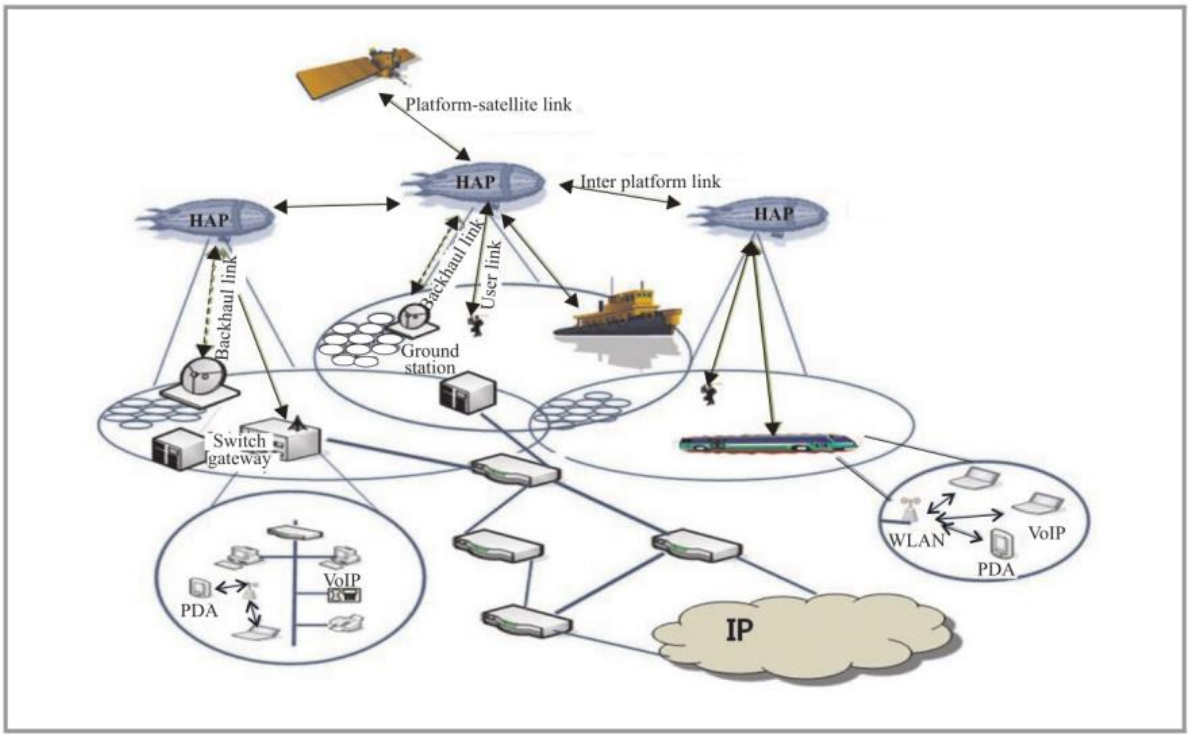
Yoon Song, H. (2009). A Method of Mobile Base Station Placement for High Altitude Platform Based Network with Geographical Clustering of Mobile Ground Nodes (1st ed.). Retrieved from http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BAT8- 0016-0015/c/httpwww_itl_waw_plczasopismajtit2009222.pdf

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.