ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Bachelor (B.Sc.) Thesis

Study of communication issues for Autonomous Vehicles and UAVs/drones

Student

STAVROS THEODOROU

Reg. number: 133986

Supervisor

Dr. Periklis Chatzimisios

Associate Professor

Department of Informatics

Alexander TEI of Thessaloniki (ATEITHE)

September 2018

Thessaloniki

ΠΕΡΙΛΗΨΗ

Η χρήση των Unmanned Aerial Vehicle(UAV) έχει αυξηθεί πάρα πολύ τα τελευταία χρόνια. Πέρα από την ευρεία χρήση τους από το στρατό, έχει εξαπλωθεί η χρήση τους σε νέες καινοτόμες κατηγορίες: η εναέρια επιτήρηση, η προστασία και η επιβολή του νόμου, η έρευνα και η διάσωση, αλλά και σε άλλες πολλές εφαρμογές.

Έτσι ολοένα και περισσότερο η τεχνολογία των drones λαμβάνει μεγάλη εξέλιξη. Η έρευνα και η ανάπτυξή τους, έχει οδηγήσει στην ραγδαία εξάπλωσή τους, μειώνοντας σημαντικά το κόστος παραγωγής τους. Οι δυνατότητές τους να συλλέγουν δεδομένα, να μεταφέρουν φορτία και να μπορούν να εξοπλιστούν με πολλών ειδών αισθητήρες, έχει ως αποτέλεσμα να χρησιμοποιούνται συνεχώς σε όλο και περισσότερους κλάδους, κατέχοντας πρωταγωνιστικούς ρόλους. Γι αυτό είναι καλό να γνωρίζουμε την δυναμική που έχουν αποκτήσει και το τι μπορούν να κάνουν και τι όχι για να έχουμε μια εικόνα σε ποιο σημείο τεχνολογικά μπορούν να φτάσουν στο μέλλον.

Η παρούσα πτυχιακή εργασία εστιάζει στη μελέτη και αξιολόγηση των τεχνολογιών ασύρματης δικτύωσης. Η προσέγγισή μου περιλαμβάνει ένα πείραμα στον Network Simulator 3 (NS3) χρησιμοποιώντας τη γλώσσα C++. Έγινε προσομείωση δικτύου drones και χρησιμοποιήθηκαν δύο διαφορετικά πρωτόκολλα: IEEE 802.11n Standard και IEEE 802.11ac Standard

ABSTRACT

The use of Unmanned Aerial Vehicle (UAV) has increased very much in recent years. Beyond their widespread use by the military, their use has spread to new innovative categories: air surveillance, protection and law enforcement, research and rescue, and many other applications. This thesis focuses on the study and evaluation of wireless networking technologies.

Thus, the drones' technology is getting bigger. Their research and development has led to their rapid expansion, significantly reducing their production costs. Their capabilities to collect data, carry loads and be able to be equipped with many kinds of sensors, has been used continuously in more and more disciplines, with leading roles. That's why it's good to know the dynamics they have gained and what they can do and what not, to have a picture of where they can be technologically in the future.

This approach includes an experiment on Network Simulator 3 (NS3) using C++. Drones network simulation was used and two different protocols were used: IEEE 802.11n Standard and IEEE 802.11ac Standard.

ACKNOWLEDGEMENT

At this point, I would like to warmly thank my thesis supervisor Dr. Periklis Chatzimisios, Associate Professor, both for the assignment of this thesis and for the unbiased understanding he has shown, but also for his time he devoted throughout this journey.

TABLE OF CONTENTS

Index of images

Index of tables

CHAPTER 1 - Introduction

1.1 –Introduction to the main subject of the B.Sc. thesis

In the present time, the term Unmanned Aerial Vehicle (UAV) refers to an innovative technology that will be significant in the near future presence in everyday life of people. The development of this technology and its transition from military to more commercial use, began in the early 21st century. Today (2018), the evolution of their technology has reached a satisfactory level to be used for practical applications; for this reason the scientific community views drones as one of the technologies of the future because of the plethora applications in industry as well as private use. Starting from simple air surveillance of large sites, such as factories, inspecting inaccessible from plant man and cinematographic landscaping; up to and including detection victims in fires, first aid in emergency situations or even drugs in war zones, UAV are an important factor in the effective implementation of the above.

Figure 1: Swarm of drones

UAVs are often referred to using the English word drones to indicate that each aircraft is autonomous or simply unmanned. There are, however, various categories of drones, which differentiate according to their structure and use, as well various ways of controlling a UAV.

The main categories in which The drones can be divided are three are based on their construction and the different flight and lifting techniques [1] [2].

- Fixed-Wing

  This kind of UAV has the familiar shape of the airplane. Its wings of the vehicle are stationary in its trunk, and as a whole they create the necessary buoyancy to take off drone but also contribute to its maintenance flight height. Still, due to its structure, the present drone obeys to natural laws of aviation, making it more controllable than one operator and more flexible on any handling and technical problems. Also because of its construction, these drones have the ability to carry more heavy equipment and for longer distances; which makes them ideal for packet distributions, especially in remote locations. Finally, the major drawback this kind of UAV is the inability to steady flight over a point - the known helicopter hover - which drives the drone in the lack of precision position.

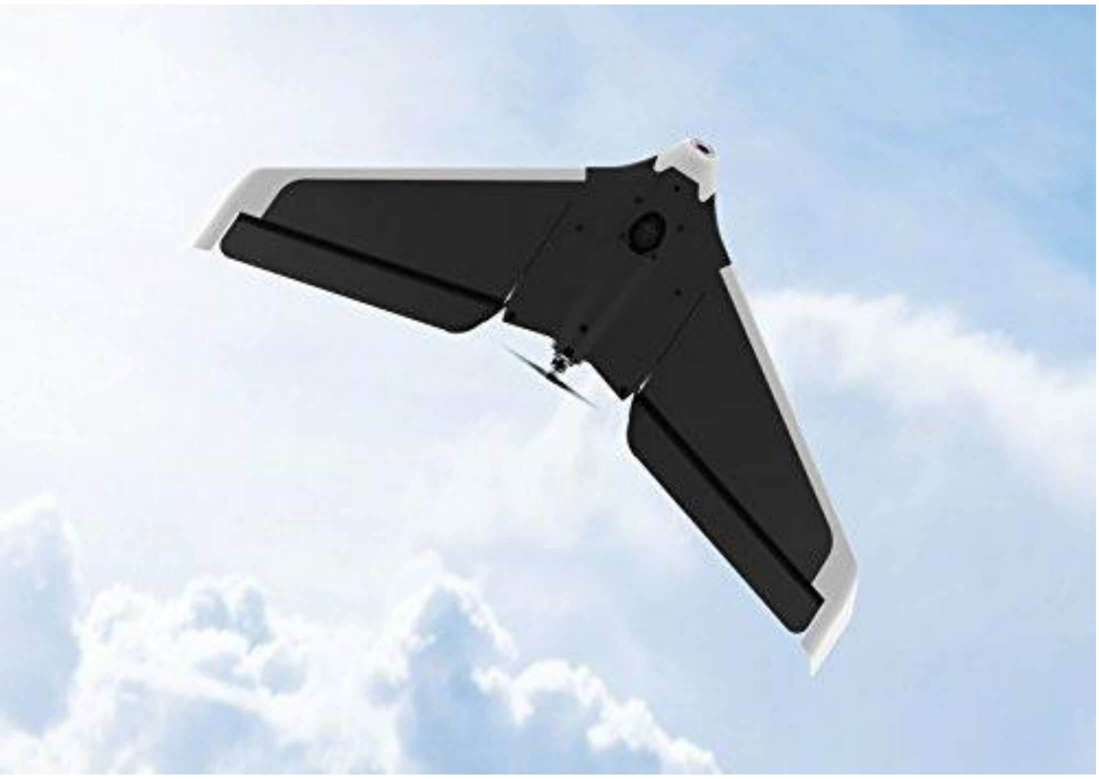

Figure 2: Fixed-Wing drone

- Rotary-Wing

This type of UAV has the structure of the conventional helicopter, with a master rotating propeller, with the only difference being that it is smaller and unmanned aircraft. Its significant advantage over the first category, is the vertical take-off and landing capability which provides the user with easier handling even in small spaces. A basic feature of this kind is the ability to fly over a point - hover - which is ideal for applications such as cinematic photography and video recording landscapes.

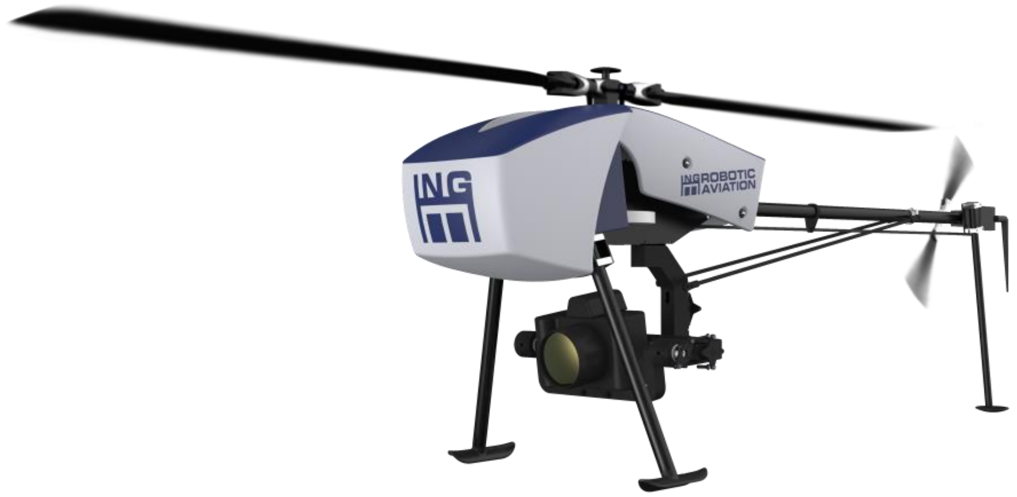

Figure 3: Rotary-Wing drone

- Multi-Rotor

This category is the most common in terms of commercial micro UAV. Their structureconsists of many propellers located perimetrically fromthemainbody. These drones are divided into different species depending on the number of their propellers.

- 3 propellers (tricopter)
- 4 propellers (quadcopter)
- 6 propellers (hexacopter)
- 8 propellers (octocopter)

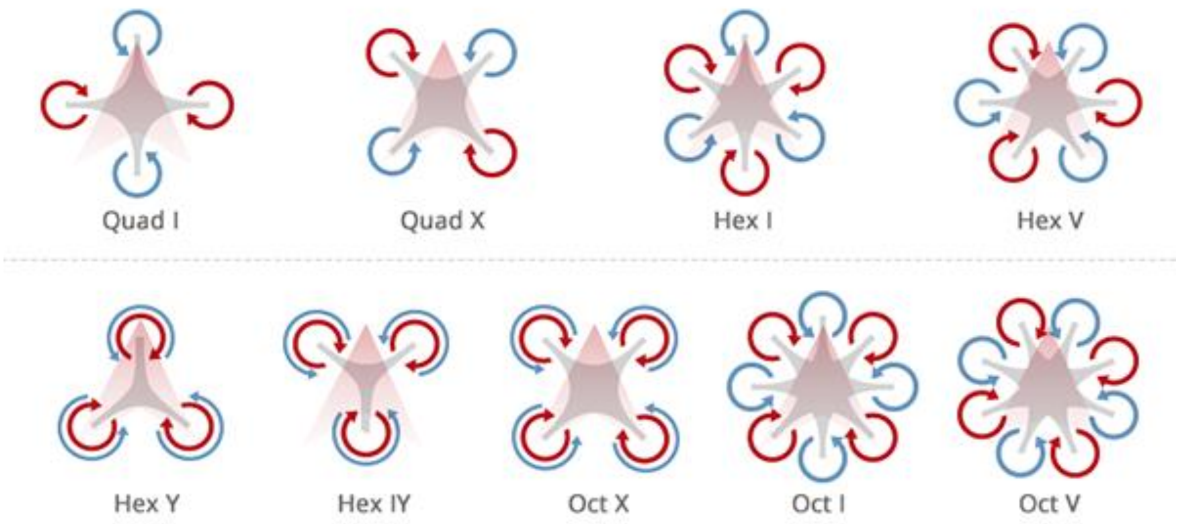

Figure 4: Multi-Rotor drones

In addition to the above main categories, there are also rarer cases such as drones with 12 or 16 propellers or 8 propellers forming the Latin letter V. Generally, with the continuous development of this technology the configurations of the structure of drones are constantly changing so that each time they serve their purpose as efficiently as possible. Multi-rotor drones have similar flight characteristics to UAVs rotating propeller, which is even more efficient. In other words, in particular drones have significantly greater air stability when they make a hover. It is also easier to remote control via operator, as well as automatic control. For this reason, they are used for applications requiring positioning accuracy and smooth motion, such as professional video recording, site surveillance and inspection, aerial mapping and infrastructure tracking.

1.2 – Objectives and aims of the B.Sc. thesis

This B.Sc. thesis is an attempt to study and evaluate the wireless networking technologies implemented within the framework of UAV systems. In particular, IEEE 802.11n and 802.11ac standards are going to be analyzed. Beyond telecommunication issues there is an attempt to approach other issues related to drones. These issues concern the characteristics of drones, various drones use cases, the drones legislation in Greece, and others.

Thus, the purpose of the work is to study, analyze as well as to understand what has been mentioned above and generally let the reader to be initiated in the sense of drones.

1.3– Structure of the B.Sc

The structure of the thesis is as follows: Chapter 2.1 is an introduction to what is to be written in Chapter 2 and 2.2 gives the features and characteristics of the drones. At 2.3 follows the Chapter conclusion and a few words about what we are going to see in Chapter 3.

Next follows the Chapter 3 where, in 3.1, an introduction to what is to be written in Chapter 3 is made and 3.2 analyzes the application areas of the UAVs. In 3.3 it is given a specific usage case for Wireless Sensor Networks. In 3.4 there is a conclusion and a few things about the next Chapter.

Then follows Chapter 4 dealing with the considerations and the simulation setup, in which 4.1 there is an introduction to the subject of the Chapter. In 4.2 there are the considerations that should be considered for the experiment. In 4.3 an analysis of the simulation setup of the experiment is made. In 4.4, it is analyzed what metrics were taken in consideration to build the diagrams. In 4.5 there is a summary of Chapter 4 and in a few words the Chapter 5 is described.

Chapter 5 deals with the performance and evaluation of IEEE 802.11n and IEEE 802.11ac. Specifically in 5.1 there is an introduction into the Chapter. In 5.2, all the charts obtained as a result of the experiment for the IEEE 802.11n Standard are analyzed. In 5.3 we analyze all the charts obtained as a result of the experiment for the IEEE 802.11ac Standard. In Chapter 5.4 there is a conclusion of Chapter 5 and some things are discussed for the sixth and final Chapter of the thesis.

Chapter 6 summarizes thisB.Sc thesis, refers to the open challenges, and draws conclusions from the experiments that preceded it. Specifically, in 6.1 is the review of the thesis. In 6.2 there are the conclusions of the experiment and in 6.3 are the open challenges and future research.Finally, there is the corresponding bibliography used and the appendix.

CHAPTER2 – Features and Characteristics of UAVs

2.1 – Introduction

In Chapter 2 we will look at the features and characteristics of drones. The development of a fully autonomous and collaborative multi-UAV system requires strong communication between the UAVs. Not enough research has been done to make sure which plan would work best. There are certain aspects of UAV networks that are not precisely defined and clarification of which will help characterize UAV networks. Below these aspects will be thoroughly analyzed.

2.2 – Features and Characteristics of UAVs

The basic features and characteristics of UAVs can be categorized as follows:

(a) **Infrastructure or ad hoc**

The majority of the available literature treats UAVs as ad hoc networks. Research on Mobile Ad hoc Network(MANET) and Vehicular ad hoc networks(VANET) has often been reported in relation to UAV networks, but they do not fully address the unique features of UAV networks. Depending on the application, the UAV network could have stable, slow or very mobile nodes. Many applications require UAVs to act as base stations in the sky to provide communication coverage in a region. Thus, unlike the ad-hoc networks MANET and VANET, UAV networks could behave more like infrastructure-based networks for these applications. Such a network will resemble a fixed wireless network with UAV as base stations except that it is overhead. There is, however, a category of applications where the nodes will be very mobile and will communicate, collaborate and install the networks dynamically in an ad hoc manner. In such a case, the topology can be determined, and the nodes involved in the data transmission decide dynamically. There are many issues that affect both UAV infrastructure and UAV ad hoc networks. For example, replacing nodes with new nodes when they fail or run out.

(b) **Server or client**

Another point of distinction is whether the node acts as a server or client. Vehicle networks are usually customers, often on mobile networks, they may, in addition to customers, also provide data transfer services to other customers. In UAV networks, UAVs are usually servers.

(c) **Star or Mesh**

The architecture of UAV networks for communication applications is an area that is unintelligible. The simplest configuration is a single UAV associated with a ground command and control center. In a multiple UAV setting, the common topologies that can be implemented are star, multi-star, mesh and hierarchical mesh. In the case of star topology, all UAVs will be connected directly to one or more ground nodes and all communication between UAVs will be routed via ground nodes. This may result in the hindering of connections, the higher latency and the demand for more expensive downlink high bandwidth links. Furthermore, as the nodes are mobile, the guiding antennas may need to remain oriented towards the ground node [1].

The multi-star topology is quite similar except for the UAVs that form multiple stars and a node from each group is connected to the ground station. Figures 5a and 5b illustrate star and multi-star configurations. Star configurations suffer from high latency as the downlink length is greater than the UAV distance and all communication must pass through the ground control center. Furthermore, if the ground center fails, there is no communication between the UAV. In most political applications, however, normal operation does not require communication between UAVs to be routed through the ground node. An architecture that supports this would result in decreased downlink bandwidth requirement and improved latency due to shorter UAV connections.

In the case of mesh networks, the UAVs are connected to each other and a small number of UAVs can be connected to the control center [2]. Figures 5c and 5d show flat and hierarchical mesh networks. Some authors believe that conventional network technologies cannot meet the needs of UAV networks. Usually there are multiple links to one or more radios, interference between channels, changes in power transmitted due to power constraints, changes in the number of nodes, changes in topology, terrain and weather effects. In ad hoc networks the nodes may be removed, the formations may break, and therefore the joints may be interrupted. Networks of wireless networks, suitably tailored, can take care of some of these problems. To address these issues, the network must be self-healing by constantly linking and rearranging around a broken path.

Compared to star networks, mesh networks are flexible, reliable and offer better performance features. In a network of wireless networks, the nodes are interconnected and can usually communicate directly on more than one link. A packet can pass through the intermediate nodes and find its way from any source to any destination. Fully connected wireless networks have the benefits of security and reliability. Such a network can use routing or flooding techniques to send messages. The routing protocol should ensure the delivery of packets from the source to the destination through the intermediate nodes. There are many routes and the routing protocol must choose the one that meets the specific goals.

Routing devices can be organized to create an ad hoc backbone mesh infrastructure that can transfer user messages over the coverage area. In addition, they can also run commands from the command and control center and are addressed to emergency handlers and vice versa. The control center can process data for posting information and to support decision-making during an emergency [3].

Because of the unique features of the UAVs described above, sometimes the existing network routing algorithms designed for advertisements for mobile hoc networks (MANET), such as BABEL or the Optimized Link-State Routing (OLSR) protocol, do not provide reliable communications [4], [5]. The main differences between star networks and networks are given in Table I.

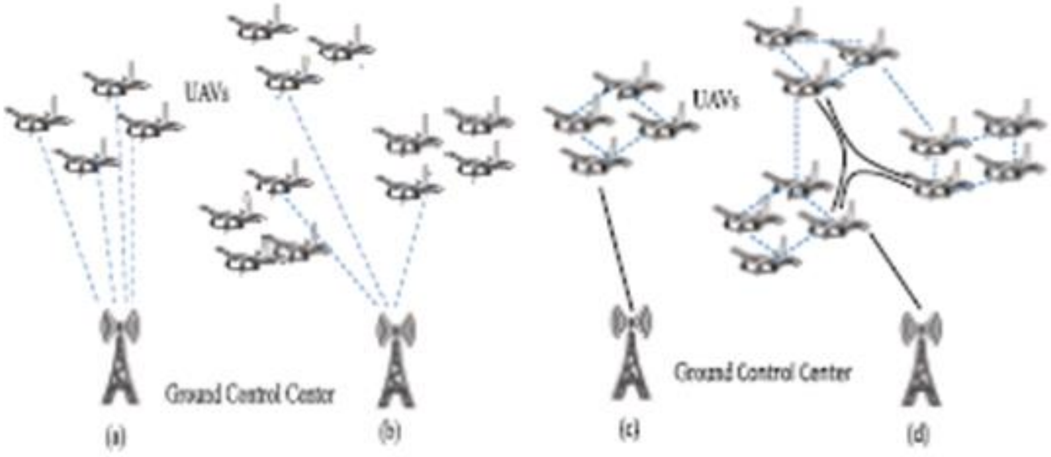

Figure 5: (a) Star Configuration (b) Multi-star Configuration (c) Flat Mesh Network (d) Hierarchical Mesh Network

Table I Comparison of star and mesh networks properties

	Star Network	Mesh Network
Topology	Point-to-point	Multi-point to multi-point
Control Center	Central control point present	Infrastructure based may have a control center, Ad hoc has no central control center
Structure	Infrastructure based	Infrastructure based or Ad hoc
Configuration	Not self configuring	Self configuring
Hop	Single hop from node to central point	Multi-hop communication
Mobility	Devices cannot move freely	In ad hoc devices are autonomous and free to move. In infrastructure based movement is restricted around the control center
Links	Links between nodes ad central points are configured	Inter node links are intermittent
Node communication	Nodes communicated through central controller	Nodes relay traffic for other nodes
Scalability	Scalable	Not scalable

(d) **Delay and disruption to prone networks**

All wireless mobile networks are prone to interrupted connections. UAV networks are no exception. The extent of the disorder depends on how mobile the UAVs are, power transmittance, UAV distances and noise. In applications where UAVs provide communication coverage in a region, the UAVs hover-over and therefore the probability of interruption will be low. On the other hand, in applications requiring rapid UAV mobility, there is a greater probability of downtime. Delays in transmission are due to poor connection quality or because one or more UAV nodes are not available. We will see more details about this in Section III.

(e) **Categorization of UAV networks**

So how do UAV networks categorize, whose applications require a different degree of mobility of nodes, different network architectures, routing and control? Like Internet delivery, there are many applications in which a wireless UAV-supported infrastructure needs to be deployed to cover the entire area. Affected areas, remote villages or oil tankers would require a rapid deployment of a UAV-based network that could provide voice, video and data services. In these applications, UAVs hover-over an area and are essentially immobile. These can be considered as cellular towers or wireless access points in the sky. Instead, detecting applications, such as forest fire detection or crop research, would require mobile UAVs.

There are other applications, especially military, that will require fast-moving UAVs to reach the enemy territory. Gravity will be given to the first category of applications and to some extent to the detection applications. When UAVs are used to build a wireless communication infrastructure, depending on the application, all UAVs could be directly under the control of the ground control center or could form a wireless mesh network with one or two UAVs communicating with the center control. In these applications, UAVs act as servers for routing user communication and control information. This is distinguished in cases where the UAVs carrying the sensors are used to collect information or those sent for an attack. In these cases, UAVs act as customers. The likelihood of delay or disturbance in the distribution category is much smaller than in other applications. When a UAV fails, the network is expected to be reshaped and current sessions should be seamlessly transferred to other UAVs. In other applications where the nodes are more dynamic, the connectors can work continuously and special routing, reconnection, and handling operations may be required.

(f) **Self-organization in networks**

One of the reasons why mesh networks are considered suitable for UAV based networks is due to their features: autonomy and reorganization. As soon as the nodes are configured and activated, they automatically form a mesh structure or are guided by the control center. When this happens, the network becomes resistant to failure of one or more nodes. There is inherent error tolerance in the mesh networks. When a node fails, the other nodes reshape the network between them. In the same way a new node can be inserted. Support for ad hoc networking, self-formation, self-healing and self-organization improves the performance of wireless mesh networks, makes them easily deployable and fault-tolerant [6], [7].

Self-organization studies in the context of ad hoc sensor networks and wireless networks can help to understand the requirements of UAV networks. Self-organization consists of the following steps: When a node fails or a new node appears, its neighbor(s) discovers the available nodes through the neighbor's localization process. Network changes, in the form of removing or adding devices on the network, cause a number of nodes to exchange messages for reorganization. This could cause conflicts in access to medium and impact network performance. Mid access control deals with access control and minimizes collision errors.

The next step is to establish the connection between the nodes during self-organization through the local connection and the creation of paths. Once the connection is complete, the service recovery management process takes care of avoiding and restoring network recovery from local failures. Finally, energy management balances the burden of data transmission responsibilities on the self-organized network and also processes related to reducing energy consumption on battery-powered devices. The goal in UAV networks would then be to ensure the connection of all active nodes in the network so that the mesh network is maintained via multi-hop communication in order to provide better access for users [8].

Wireless networks are prone to connection failure due to interference, mobility, or bandwidth demand. This will lead to a downgrade of network performance, but it can be effectively addressed by making the network redefining. The nodes monitor their links and any failures trigger the remodeling process. There are cases where certain UAVs could be shut down due to battery drainage or communication failure. In such cases, the other nodes in the network reorganize and restore communication. While the benefits of self-organization are enormous and encouraging, the challenges to self-organization are greater, making it an exciting research problem [9].

(g) **Software Defined Networking (SDN) -Automating UAV Network Control**

UAV networks are limited to communication resources. The nodes are non-permanent, the connectivity is intermittent and the channels may be reduced. This translates into implementation challenges in programming and resource allocation. Different networks use different routing protocols and therefore even nodes that use the same access technology may not work on another network due to differences in the higher levels of the protocol stack. But in both environments, there is no consensus on the routing protocols to be used, and most of the network management tasks to be performed.

Consequently, nodes that use a particular access technology on a network may not work on another network with the same access but on different higher-level protocols. The above problems could be addressed by building the protocols stack definition capability in the software. In this way UAVs could be programmed to operate flexibly in different environments. However, this is not the only reason why it is desirable to test the network software.

There are some other requirements in networks such as MANET, VANET and UAV networks. They must support dynamic nodes and frequent topology changes. Nodes may fail, for example, due to drainage of the battery and must be replaced by new nodes. The joints are interrupted and must be treated accordingly. SDN provides a way to programmatically control networks by facilitating the development and management of new applications and services, as well as coordinating network policy and performance [10], [11]. The development of SDN has been extensive in fixed infrastructure networks.

However, much of this extension was in data centers, as it was considered that SDN was suitable for centrally controlled networks and that ad hoc mesh wireless networks were decentralized. Separation of promotional devices and controller has also raised concerns about security, balance of control and flexibility. There are several policy issues concerning the balance of control and the co-operation between the auditors to be addressed. Due to the benefits it expects to offer, the interest of the academic world and the industry is growing in the implementation of SDN in dynamic wireless mobile environments.

In networks like VANET, using SDN can help in selecting a route and selecting a channel. This helps reduce interference by improving the use of wireless resources, including channels and routing in multiple mesh networks. Despite growing interest, there is no clear and complete understanding of the benefits of SDN in wireless infrastructure without infrastructure and how the SDN concept should be extended to meet the characteristics of wireless and mobile communications [10], [12]. One of the commonly used protocols for SDN on wireless networks is OpenFlow.

OpenFlow claims to provide substantial benefits for mobile and wireless networks. It helps to optimize the use of resources in a dynamic environment, provides a way of automating work, allows for better control and easier implementation of global policies and faster introduction of new services [13]. The OpenFlow protocol separates the forward and control functions. OpenFlow switches are programmable and contain flowcharts and communication protocol with controllers [14].

Figure 6 shows the separation of control and forwarding functions with the OpenFlow interface between control and data levels. Such a network can be configured by positioning the data layer or OpenFlow switches on the UAV and controlling a central ground controller or distributed UAV control. Promotion elements, which are simple OpenFlow switches rather than IP routers, contain the flow tables that are handled by the controller to determine the rules. The actions in the flow tables define the processing that would be applied to the specified set of packages. Actions could be filtering, forwarding a particular port, rewriting a header, etc. The control level of the SDN network can be centralized, distributed, or hybrid. The controller has an overview of the network and can effectively route traffic. Updates the OpenFlow switchgear flow tables with the corresponding criteria and processing steps [15]. The controller, who defines all actions taken by wireless switches on the UAV, has been proven to be on the ground. It could also be by air. In Distributed Control mode, control is distributed across all UAVs and each node controls its behavior. In hybrid mode, the controller passes control of packet processing to the local agent and there is traffic control between all SDNs.

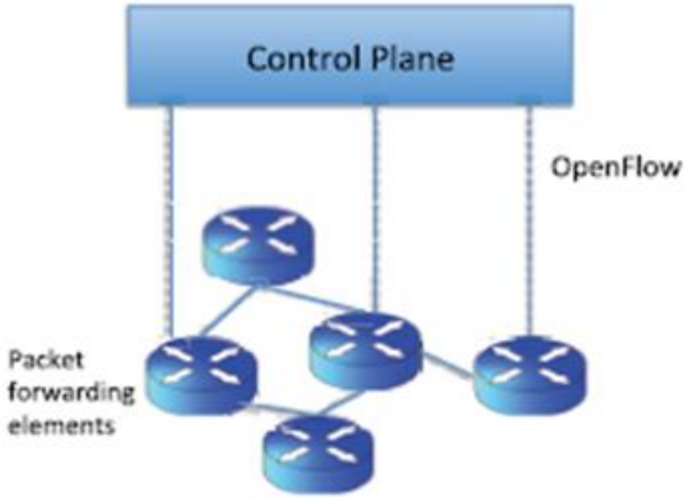

Figure 6: Software Defined Networking elements

(h) **Energy-effectiveness tradeoffs**

Available UAVs available can stay in the air for about 15-20 minutes at a time. Their mission must be highly optimized, and suboptimal topologies with reduced traffic could actually lead to longer and more successful missions.

(i) **Dynamic topologies**

Theoretical or a priori placement optimizations carried out centrally may not translate into the same exact positions in the corresponding 3D airspace. Unpredictable air currents, inaccuracies in 3-D model models and changing field conditions may require sudden and unpredictable changes to UAV detection. Protocols based on link-layer retransmissions and error control, among other approaches, should be adapted to these situations in real-time.

(j) **Multi-objective downtimes**

Given the energy needs, UAVs involved in SAR functions require multiple recharge cycles. Any such interruption recalls the UAV at the nearest charging center, which raises interesting questions as to whether the same network can be maintained (by introducing redundancy) or that the whole topology should be proactive (at the cost of execution). Due to the nature of the devices used, certain features are emerging especially for overhead networks that differ from other wireless networks such as MANETs, VANETs and traditional wireless sensor networks (WSNs). The characteristics of the air network in terms of traditional communication and networking are the energy consumption and network lifetime.

(k) **Mobility**

In many application scenarios, airborne devices can facilitate time efficiency due to their high mobility [16], [17]. Because of this high mobility, however, the ground on which UAV flights are expected to change very often, for example, from forest lands in lakes to buildings during a single flight. Not only the blind spots caused by the ground affect the wireless channel but can also introduce frequent topology changes between many devices that require connectivity.

High mobility is also a feature of VANET, however VANET mobility models follow limited 2D routes, for example, motorways and roads, while airborne devices are characterized by the demand for mobility in 3D space. So, not only can the ground on which UAVs move frequently change, but also the altitude of the flight can vary to avoid obstacles and collisions. The limitations set at the altitude of the UAV flight are underlined in [16]. It is reported that although large altitudes correspond to a larger field of view, the current available sensors are limited to their precision and therefore prevent UAVs from flying beyond certain altitude levels. Thus, for higher detection probabilities, UAVs can be limited to heights and flight speeds.

Wind speed at higher altitude is also a limiting factor since commercially available UAVs are currently unable to maintain steady operation during strong winds and other adverse weather conditions. Taking these features into account, communication protocols developed for an overhead network should allow strong networking of high mobility devices. The overall objective, however, is to maintain connectivity through controlled mobility and to achieve specific mission objectives. Since on air networks, mission objectives and network conditions vary, mobility is controlled taking into account many network parameters. This includes node density, terrain, connectivity range, communication technology, and shipping requirements, e.g. type of traffic, frequency and traffic priority.

In addition, as in other networks, mobility can be used as an advantage in overhead networks where the network may not be fully connected at all times. In this case, highly mobile devices can be placed in optimized locations in a time-efficient manner so that a certain QoS network can be supported [18], [19]. Also, controlled mobility in 3D space can be used to amplify the range using directional antennas [20]. Mobility can therefore play an important role in designing overhead networking protocols.

More about of what we discussed above can be found at [21], [22], [23], [24], [25].

2.3 – Summary of the chapter

In this Chapter we have seen the characteristics of drones. We analyzed extensively all the different features of the drones we can find. This means that depending on the project, you also choose the corresponding features that each user wants for the drones network, for example, in the event of a disaster, surveillance of public events for the security of the world, monitoring of road transport, where drones can be used as rescue services. In the next Chapter we will present various cases of use of drones. A specific use of drones will also be analyzed in detail.

CHAPTER 3–Application areas and use cases

3.1 –Introduction

The purpose of Chapter 3 is to analyze the application areas of drones in the event of an earthquake, for the monitoring of major events and the monitoring of the road network in order to deal with traffic or accidents.Moreover, we analyze the usage of WSN for helping in rebuilding a network of drones, depending on the destruction scenario. Emphasis is also placed on the important role of actions in the study of areas that have been destroyed for the immediate assistance of the victims. Road traffic monitoring provides additional evidence to prevent accidents.

Figure 7: Drones applications

3.2 – Applicationareas of UAVs

UAVs affect different areas of our daily lives. Due to their wide use, it is difficult to analyze all possible cases, we focus on certain representative use cases.

(a)**Earthquake use case**

In the event that an earthquake affects a particular area, UAVs equipped with appropriate IoT devices (sensors / cameras) can be trained to fly over this area to record for damage assessment in video. They can also detect parameters such as wind speed, temperature and the level of air pollution. The information they provide can help rescue teams avoid areas that threaten people's lives or equip them appropriately. Flying over an area, UAVs can be linked to each other to facilitate tuning and surveillance of the area. In order to precisely identify the areas with the greatest needs and to evaluate the people who need help, a team of experts process the data collected by the drones. If these areas are identified, UAVs can deliver drinks, foods and medicines to people in urgent need until the rescue teams arrive. UAVs can also help rescue teams to identify the exact geographical locations of the victims and guide the rescue teams as well as how to approach them. In such a case of earthquake and even if the communications network is damaged, partly or totally, the UAVs can act as hotspots or BSs to collect short messages of those that caught in the debris of the earthquake. Small UAVs, e.g. nano-UAV can also be used to check if victims are locked in buildings.

Figure 8: Drones in an earthquake scenario

(b)**Surveillance monitoring**

During major public events (e.g. sports tournaments and music parade) instead of sending large security staff to monitor every public space, drones that fly over the event areas and are equipped with the appropriate IoT devices can monitor these public spaces. As a result, security agents can control the safety of public spaces from a central location near the event and would only intervene when an incident was identified. Until agents reach that point, drones can watch the move or even shoot photos / videos for any suspicious moves. Therefore, with the use of drones, crowd surveillance and security will be improved, while at the same time reducing the cost of large-scale security teams and saving a lot more people.

Figure 9: Drones in surveillance scenario

(c)**Tracking the road network**

Flying in a location, drones can send real-time traffic information. These data can be collected and used by pedestrians and vehicle drivers to decide on their shorter and safest routes. As another application, drones can be used in the same way in meteorology. A drone flying over a city can collect the desired information e.g. temperature, wind speed and humidity and send it to a central server. Based on this "drone-sensing" approach, precise weather forecasting can be made easily and at a lower cost. Drones can also be used as rescue providers. In case someone has an accident, any drone flying over the area can take photo / video for the incident and send it to the monitoring center. Until the rescue team arrives, a drone equipped with a first aid kit can get to the position. Subsequently, suitable passers-by can be selected, from whom they may be asked to use this box to provide first aid to the wounded.

Figure 10: Drones in road tracking scenario

(d)**Disaster management**

When a natural disaster occurs in an area, coordination of actions is vital. Actions need to be done quickly and effectively to help people, but also to reduce the number of victims as much as possible. Therefore, information plays an important role in disaster management. UAVs can effectively help in raising awareness and assessing the situation. UAVs can effectively help in raising awareness and assessing the situation. They can assist in communications and coordination of functions, ground coverage and search procedures. With regard to the latter, UAVs can support the identification of people with disabilities and can also help detect electromagnetic emissions of personal belongings of victims who were buried under damaged buildings or hiding in dense forests. For example, UAVs used during the great earthquake in eastern Japan helped to relieve earthquake and tsunami disasters. They also recorded images of damaged reactors at the

Fukushima nuclear power plant. In another case of disasters, the UAVs were implemented in Port au Prince, Haiti in 2013, for an on-site inspection of 45 km2 in order to map urban hideouts to measure the number of scenes and to organize a census of the population. In addition, UAVs were used to provide food, medicine and other needs in developing regions and areas that were not accessible.

Figure 11: Drones in disaster management scenario

More specific UAV applications for disaster managementare presented below:

- Merge and exchange information on disasters: By combining different sources of available information or by providing a bridge between different information technologies, UAVs can support other applications in disaster management.

- Situation awareness, logistical support and evacuation support can help in gathering information during the disaster phase, particularly with regard to the movement of affected people and rescue teams.

- Autonomous communication system: UAVs can temporarily restore the damaged communication infrastructure.

- Damage assessment: UAVs can help assess damage by various methods, such as structural health monitoring and video inspection.

- Cover the media: UAVs could help provide early information to viewers for informational purposes.

- Medical applications: Although limited to payload means, specialized drones could automatically deliver the supplies necessary to keep the world alive, even in the case of a damaged road network.

3.3 – Usage of Wireless Sensor Network (WSN)

In a UAV usage scenario for disaster tracking, a fixed UAV can be used to see the disaster area. Once individuals or vehicles have been detected, 7 quad-copters can be sent to these critical points to gather the information in real time. A quad-copter with 20-25 minutes of airborne operation and 60-80 minutes of battery charging time, is used for the monitoring task. Additional UAVs could be added for sufficient backup to continuous surveillance. Therefore, a fixed or mobile first-response UAV station should be a vehicle that can store at least five quad-copters and a fixed-wing UAV. It is also equipped with a long-distance communication antenna, power generator and automatic recharging UAV system.

The UAV mobile station could be operated by a single operator, mainly for the maintenance of the station and to act as a security monitor in case something goes wrong during the operation of the UAV network. This kind of UAV station could also implement an automatic battery replacement approach along with an approach to visual-based formation control. This allows a simplified but effective control of a UAV group. Assuming the system can rely on GPS placement, the operator can manually correct the location of the UAV based on the multimedia input. Commercial UAVs should be used for disaster management because of their availability, economic value and ease of use.

Once the proposed disaster management approach involving commercial UAVs is implemented, future applications are likely to use even more robust and durable quad-copters and fixed-wing UAVs. Although the cost of such applications may be significantly higher, this justifies improving reliability and robustness.

Destruction stages

The life cycle includes three stages:

(a) Preparation before the disaster

(b) Disaster assessment

(c) Disaster management and recovery

Each stage imposes a set of UAV tasks with different time limits and different priority levels. A single optimized but static network for all three stages is no longer viable. As the destruction stages progress, static WSN deployments become less effective. Below we provide a classification of these disaster scenarios and possible related activities based on disaster types:

- Type A: geophysical (earthquake, tsunami, volcano, landslide, avalanche) or hydrological (flames and debris flow)

- Type B: climatic (extreme temperatures, drought, fire), hydrological (floods) or human-induced (industrial hazard, structural collapse, power failure, fire, contamination of hazardous materials)

- Type C: meteorological (tropical storm, hurricane, sandstorm, intense rainfall).

It should be noted that Type A disasters render the existing WSN infrastructure for monitoring non-functional. Estimation, reaction and recovery phases are mainly performed by UAV. Type B disasters partly affect the existing WSN infrastructure. In this case, the role of the UAVs is twofold: to reconnect the WSN functional sections and perform other special tasks. Type C disasters are mainly focused on meteorological events because the UAV cannot function reliably during the assessment phase and has limited operational use in the disaster recovery and recovery phase due to unstable weather conditions. In this case, WSN should play a leading role, with partial support being provided through UAV.

Stage 1: Preparing for disasters

The standby phase has no predetermined duration and could begin several years before the expected disaster, culminating in its actual appearance. For all three types of disaster, WSN plays the lead role, receiving limited UAV support. Many developed sensors collect physical information and transmit them to a central location where the information is recorded. Here, the simplest option is to use cellular modem technology, other than radio stations, on sensors, although this increases the weight and cost of sensors. Simone Frigerio and his colleagues presented a scenario for the development of the tracking of landslides in the Italian Alps, where WSNs incorporated several sensors to track shifts caused by landslides and trigger an alarm in the case of debris flow. Air traffic monitoring via UAVs has limited use to such disasters, which require ground measurements. Instead of scanning, UAVs can play a role by taking on the burden of delivering data from sensors with limited resource.

Stage 2: Disaster Assessment

This stage occurs when a disaster is in progress, making parts of the topographic area unsuitable for vehicle traffic or human residence. The focus of the wireless network is shifted from tracking to accurate assessment of the situation. The main task here is to review land for available resources and relay this data to the control center, all in real time. For type A disasters, the UAVs must form an independent network without support from the ground sensors. When work assignment is fully concentrated, it is possible to allocate the physical space to known areas and to assign one or more UAVs per region. Many UAV stations, which are strategically deployed in a broad geographical area, can guarantee that at least some UAV infrastructure components are operating even after the disaster. Consequently, for Type A disasters, heterogeneous UAV networks that include a fixed-wing UAV should be used to scan the area and identify significant points. In the case of Type B disasters, the WSN infrastructure is partially operational, so it can be used in conjunction with the developed UAV network, which can serve as a bridging node and maintain the overall WSN topology.

GurkanTuna, V. CagriGungor and KayhanGulez presented an interesting network model in the context of mobile robots that can also be considered for UAVs. [26] In their work, because WSN is still functional and can route packets to the remote sink, mobile units perform more of the exploratory work but then use WSN as the backhaul of data forwarding. For Type B disasters, it is recommended to exploit the existing WSN infrastructure. WSN can not only obtain environmental data but also help to reconnect separated segments of the UAV network. Given the particular nature of Type C disasters, there are cases of violent turbulence, strong winds and other weather-related objects and do not allow the safe air movement of UAVs.

A viable approach appears to be the use of applications such as DistressNet, an ad-hoc wireless architecture that supports disaster response with distributed collective detection, topology routing using a multichannel protocol and accurate resource identification [27].DistressNet is implemented in a set of available sensors and on a set of servers that provide network services, data analysis and decision support. For type C disasters, therefore, focus on the data provided by WSN and other available sources of information is needed.

Stage 3: Disaster response and recovery

The UAV will play an important role at this stage, first by defining cellular short-distance connectivity with affected users and then transferring data to the cellular backbone infrastructure. The network can also provide feedback to users on safe areas and evacuation routes, based on the information gathered after the disaster assessment phase. For a Type A disaster, the air link level includes the creation of a multiple UAV station relay network ranging from individual user blocks to the closest functional RAN. This creates a problem for many optimization objects to maintain the mid-roll feature and end-to-end connectivity for users. [28] An interesting example will occur in WSDN-defined wireless networking and the need for installing the drone overhead connection. This scenario can be seen as a set of UAV open-ended switches whose routing functions can be dynamically changed by commands issued by a remote control. [29] For type A disasters, it is necessary to focus on the use of different camera types and specialized sensors and actuators assembled in UAVs for rescue missions and supply of supplies. For type B destruction, when the WSN support is fully operational, it can be used to support UAV mode by unloading some of the non-critical times. For example, when two major earthquakes occurred in the Emilia-Romagna region of Northern Italy, the UAV operators were overwhelmed with information retrieval tasks. [30] Here the careful monitoring of the information flowing from the disaster shows that the controller's errors in the operation of the UAV adversely affected his rescue mission performance. An existing WSN can also help create multi-station wireless access networks on the ground. For type B disaster, it is necessary to maximize the data provided by WSN to improve the effectiveness of SAR missions performed by UAVs. In a C-type scenario, UAVs are limited in their ability to collect useful information from the site of destruction, but they can operate from the periphery. Assuming destruction involves a major disaster in the communications infrastructure where cell towers or stationary base stations are rendered ineffective, the only solution is for the sensors to advance their data using low power, forming multi-waste relay chains at the edge of the affected area. The advantage of using UAVs is that the collection point at this end can be decided dynamically based on the surviving elements of the original architecture. The use of the UAV mobile stations proposed can ensure the rapid UAV development and the preparation of the UAV network installation, thus reducing the response time and increasing the disaster recovery rate. Therefore, the fully functional WSN should be used to reconnect problematic UAVs.

More applications and use case scenarios can be found at [31], [32], [33], [34], [35]

3.4 – Summary of the Chapter

In conclusion, it is fully understood that the use of drones is vital in all areas of everyday life as they help in monitoring, early warning and logistic support. Also, the need for WSN to improve UAV networks seems to be conclusive. In the next Chapter it will be analyzed the simulation setup of this thesisand some considerations will be taken into account. Specifically, the way in which the code was constructed will be analyzed and the way the code works and its limitations will be extensively studied.

CHAPTER 4 – Considerations and simulation setup

4.1 – Introduction

Chapter 4 will analyze the simulation setup of the experiment. It will be mentioned how the code was built from the beginning and some considerations will be taken into account (e.g. random establishment of node position, node sender and receiver, node speed and duration of each connection), to understand how this code works and its limitations.The ns3 experiment will use the C ++ language. A drone network simulation will be done with two different protocols: IEEE 802.11n Standard, IEEE 802.11ac Standard.

4.2 – Considerations

Four different aspects were considered for random establishment in simulations:

_ Node position

_ Node sender and receiver

_ Node speed

_ Duration of each connection

In ns-3 a global seed and its run for simulation use can be selected.Thus, when different protocols or variants of one are compared,it ensuresthat the comparison is fair since they use exactly the same values of the four pointsstated before.If we set one seed, then it allows us to generate 2.3 x 10^{15}independent replications, more than enough if we consider that we usually use around20 foreachscenario.

4.3 – Simulation setup

For the simulation purposes, NS-3 network simulator has been used. NS-3 is a discrete-event simulator with a special focus on Internet-based systems, consisting of different library components (core, simulation, node libraries, physical and channel models, network routing protocols implementations, etc.) written in C++. Such structure allows researchers to modify, adjust and simulate various networking scenarios. More papers about ns3 projects can be found at [36]-[41].

The code for my thesis works as it follows:

A)First all nodes have to be created before the simulation starts. Nodes can be considered as stationary pcs without the capability of internet connection or communication. They are just computational units. Nodes are created in a random spot using the seed that was generated in the beginning.

B) We then install Wi Fi in the nodes using WifiHelper library to set the wifi standards that in our example are 802.11n and 802.11ac.

A few words about the standards we have used in our experiment:

-IEEE 802.11n Standard

802.11n is a wireless-networking standard that uses multiple antennas to increase data rates. Sometimes referred to as MIMO, which stands for "multiple input and multiple output". Its purpose is to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum net data rate from 54 Mbit/sec to 600 Mbit/sec with the use of four spatial streams at a channel width of 40MHz. More specific, the idea behind the IEEE 802.11n standard was that it would be able to provide much better performance and be able to keep pace with the rapidly growing speeds provided by technologies such as Ethernet. The new 802.11n standard boasts an impressive performance, the main points of which are summarized below in Table II:

Table II IEEE 802.11n Standard Salient Features

IEEE 802.11N SALIENT FEATURES	
PARAMETER	**IEEE 802.11N STANDARD**
Maximum data rate (Mbps)	600
RF Band (GHz)	2.4 or 5
Modulation	CCK, DSSS, or OFDM
Number of spatial streams	1, 2, 3, or 4
Channel width (Mhz)	20, or 40

- IEEE 802.11ac Standard

IEEE 802.11ac is a wireless networking standard in the 802.11 family, providing high-throughput wireless local area networks on the 5GHz band. The specification has multi-station throughput of at least 1 gigabit per second and single link throughput of at least 500 megabits per second. This is accomplished by extending the air-interface concepts embraced by 802.11n: wider RF bandwidth, more MIMO spatial streams, downlink multi user MIMO, and high-density modulation. More specific,

The IEEE802.11ac Wi-Fi standard has been developed to raise the data throughput rates attainable on Wi-Fi networks up to a minimum of around 1 Gbps with speeds up to nearly 7 Gbps possible. As a result of these speeds, one manufacturer is marketing the products as 5G WiFi.

The implementation of Gigabit Wi-Fi is needed to ensure that Wi-Fi standards keep up with the requirements of users.With users requiring ever higher data rates, the IEEE developed their 802.11ac Gigabit standard also known as VHT, Very High Throughput the system enables absolute maximum data rates of nearly 7 Gbps with all options running.This will enable those wanting to stream high definition video and many other files to be able to achieve this at the speeds they require.Some of the key or highlight features are tabulated below in Table III:

Table III IEEE 802.11ac Standard Salient Features

IEEE 802.11AC SALIENT FEATURES	
PARAMETER	**DETAILS**
Frequency band	5.8 GHz ISM (unlicensed) band
Max data rate	6.93 Gbps
Transmission bandwidth	20, 40, & 80 MHz, 160 & 80 + 80 MHz optional
Modulation formats	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM optional
FEC coding	Convolutional or LPDC (optional) with coding rates of 1/2, 2/3, 3/4, or 5/6
MIMO	Both single and multi-user MIMO with up to 8 spatial streams
Beam-forming	Optional

C) We also use the YansWifiPhyHelper library to instantiate and configure the PHY layer as well as the YansWifiChannelHelper library to instantiate and configure the WifiChannel. Also we use the WifiMacHelper library to add an upper mac and set it to adhoc mode. A few words about adhoc mode:
- Adhoc mode is an 802.11 framework in which devices or stations communicate directly with each other, without the use of an access point. Adhoc mode is also referred to as peer-to-peer mode. Adhoc mode is useful for establishing a network where wireless infrastructure does not exist as in our example.

D) Then we have to install mobility in the nodes. Mobility models specify how nodes will move (constant position, constant velocity / accelaration).
The Position Allocator library, that is used, is only used to initialize the mobility model. Position allocators set up initial position of nodes (list, grid, random position, etc);they do not perform the node movement. In our code we create a cube of 1km side. Also it is automatically retransformed if it is needed (in case numerous drones are used so that they can fit in the cube).
The SetMobilityModel method is used to make the nodes perform a random walk within the bounds of the cube with random speeds that are also in bounds for the nodes to be drones.

E) Then we have to install routing protocol. We use the OlsrHelper library to enable oslr: The optimized link state routing protocol is an ip routing protocol for mobile adhoc networks.

F) We then give the nodes internet connection with the InternetStackHelper library andwe give ipv4 ips to the nodes using the Ipv4AddressHelper library.

G) At last we install applications if needed. In our example we use CollisionAvoidanceHelper library for drones to avoid collisions.

In our code we have 3 variables that we change with every given possibility so we can take a look at our system and get the metrics we want so we can see how our network behaves.

-packetsize : measured in megabytes, we get from 1 mb to 5 mb with a step of .5 mb
-packetfrequency: measured in seconds and it is the time that passes until a new packet is created. We get from 1 to 10 seconds with a step of 1 second.
-number of drones: is the number of nodes that we create and we get from 2 to 30 drones so we can have a reality test sample

For the calculation of our results we use the flow monitor module for calculating the jitter and the delay. The flow monitor module goal is to provide a flexible system to measure the performance of network protocols. the module uses probes, installed in network nodes, to track the packets exchanged by the nodes and it will measure a number of parameters. Packets are divided by, according to flow they belong to, where its flow is defined according to the probe's characteristics (e.g. for ip, a flow is defined as the packets with the same protocol, source ip/port, destination ip port). The statistics collected for each flow can be exported in XML format. Moreover, the user can access the probes directly to request specific stats about each flow. Each probe will classify packets in four points:
-When a packet is sent
-When a packet is forwarded
-When a packet is received
-When a packet is dropped
Since the packets are tracked at ip level, any retransmission caused by L4 protocols will be seen by the probe as a new packet.

The throughput is calculated by the formula below:
throughput(bits/sec) = sum((number of successful packets)*(packet_size)/total time spent in delivering that amount of data)

The packetloss is calculated by the formula below:
packetloss(%) = (packets_sent - packets_received)/packets_sent*100

4.4 – Figures of merit

For the two protocols tested, the metrics thattaken into account for the Figures of merit are the followings:

_ Average throughput: rate of successful message delivery over a communication channel.

_ Average Packet loss: percentage of packets lost from the total of packets sent.

_ Average delay: the sum of the delay of all received packets.

_ Average jitter: the time difference in packet inter-arrival time.

All performance figures are made using Matlab software by varying certain protocol configurations.

Because the concept of delay is more understandable than the other 3 metrics we are going to say a few words about packet loss, jitter and throughput.

Generally, packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is either caused by errors in data transmission, typically across wireless networks.However, in relation to our subject, the biggest problem is the distances between the drones and their speeds because that may occur to a weak radio signal transmission.

Jitter is the difference in packet delay. In other words, jitter is measuring time difference in packet inter-arrival time. jitter causes network congestion and packet loss. We could say that congestion is like a traffic jam on the highway. Cars cannot move forward in a traffic jam at a reasonable speed. Likewise, in congestion all the packets come to a junction at the same time. Nothing can get loaded. The second negative effect is packet loss. If packets arrive at unexpected intervals, the receiving computer cannot process the information. The result is missing information, or better called packet loss.

In general terms, throughput is the maximum rate of production or the maximum rate at which something can be processed. Factors that affect/ can affect throughput are a lot. Some of them are:

-Analog limitations

-IC hardware considerations

-Multi-user considerations

- Others

4.5 – Summary of the chapter

In this Chapter we saw simulation setup and we studied the IEEE 802.11n and IEEE 802.11ac standards. We understood the experiment from the beginning and gave some considerations that were necessary. In the next Chapter we will demonstrate and analyze the graphs that we took as result from the experiment.

CHAPTER 5–Performance evaluation of IEEE 802.11n and IEEE 802.11ac

5.1 – Introduction

Chapter 5 will show a series of graphs to understand the pros and cons against each protocol in our experiment. On the y axis we will have all the different metrics (packet loss, jitter, throughput, delay). On the x axis, we will alternate the following variables: number of drones, packet frequency and packet size. On each chart we will also see 3 different curves for the same measurement so that we get a more global view of our system.

5.2 – IEEE 802.11n Figures

In the next Figures, the results of our experiment are going to be viewed from a lot of different angles. We have separated the results into the following 6 different aspects in order to make them accessible to the reader. As it is seen below in the Figures 12-15 there are three lines:

-1 mb packet size
-3 mb packet size
-5 mb packet size
We keep constant these packet sizes in each line and we calculate the delay, jitter, packet loss and throughput from 2 up to 30 drones.

In Figure 12 we would expect to see that the bigger the packets are, the bigger the delay is but as we can see although for 1 mb and 3 mb packet size that is true, for 5 mb packet size this is not applied. So, are large packet sizes better than small packet sizes? A short answer to this question is that we want to use the largest packet size that will fit on the network. Moreover, what is also concluded from this Figure is that as the number of the drone increases, the bigger the delay grows. This is very reasonable because as the number of nodes rises, there are more collisions. Finally, we can see that the biggest delay occurs in the 3 mb packet size curve with a value of more than 7 x 10^{10} nanoseconds at thespot of about 20 and 23 drones. On the other hand, the smallest value of delay takes place for all the curves from 2 to about 13 drones with a value of almost 0 nanoseconds.

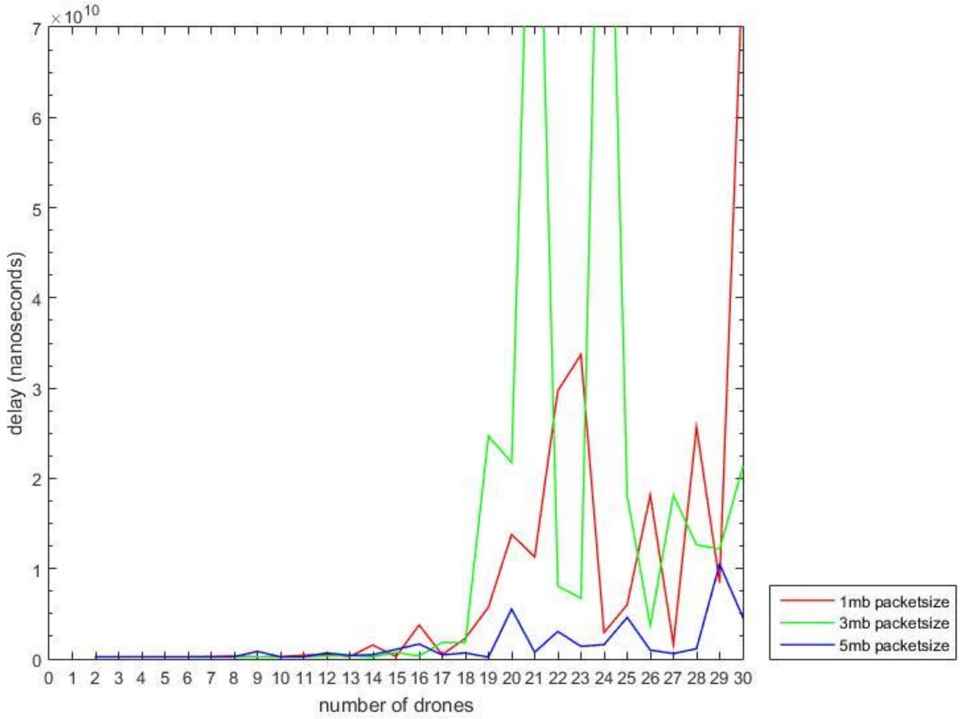

Figure 12: delay vs number of drones for 1,3,5 mb packet sizes

In Figure 13, it is observed that from 2 to 10 drones no packet loss regardless of the packet size. Nevertheless, this changes from 11 to 30 drones. From the three curves it is concluded that all packet sizes are almost identical overall but we can tell that maybe the 3mb packet size line is a little lower on the axes of y from the other two lines. This means that for 3 mb packet size there is the least packet loss percentage. The biggest packet loss percentage is presented at the 1 mb curve for 15 drones with a value of about 80% and the least value is 0% for all curves from 2 to 10 drones.

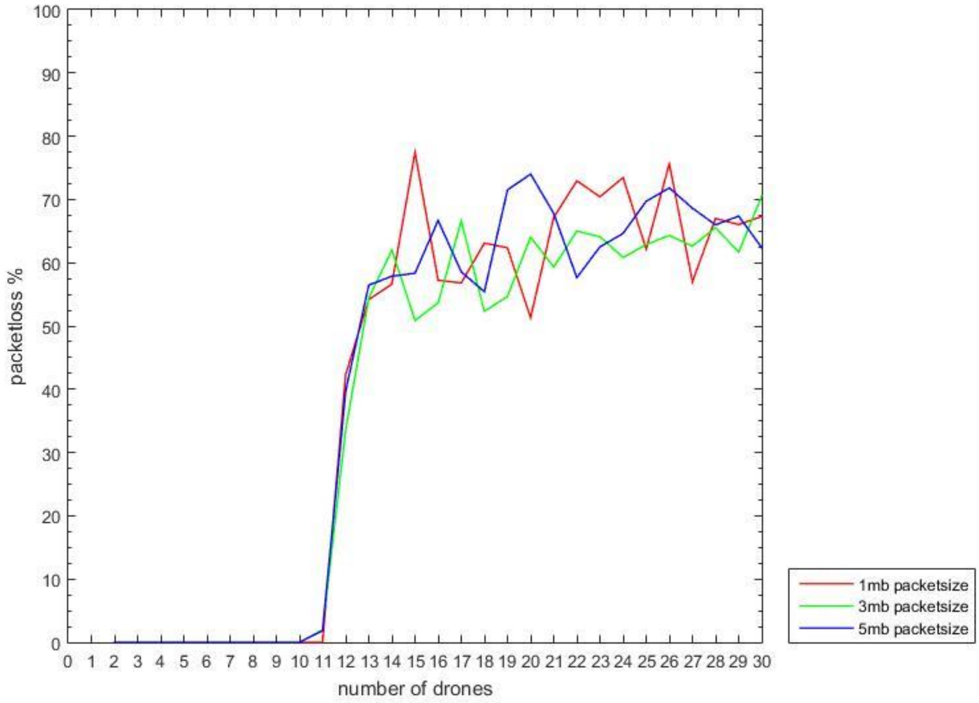

Figure 13: packet loss vs number of drones for 1,3,5 mb packet sizes

In Figure 14, it is clearly inferred that there is almost no jitter from 2 to 18 drones but then the 3mb and 1 mb lines have a lot of jitter. This is well expected since with the same amount of packet size we came across bigger delays. The biggest jitter is noticed in the 3 mb packet size curve at the spot of 21 drones with the value of more than 4 x 10 ^ 10 nanoseconds and the least value is almost 0 nanoseconds for all three curves from about 2 to 13 drones.

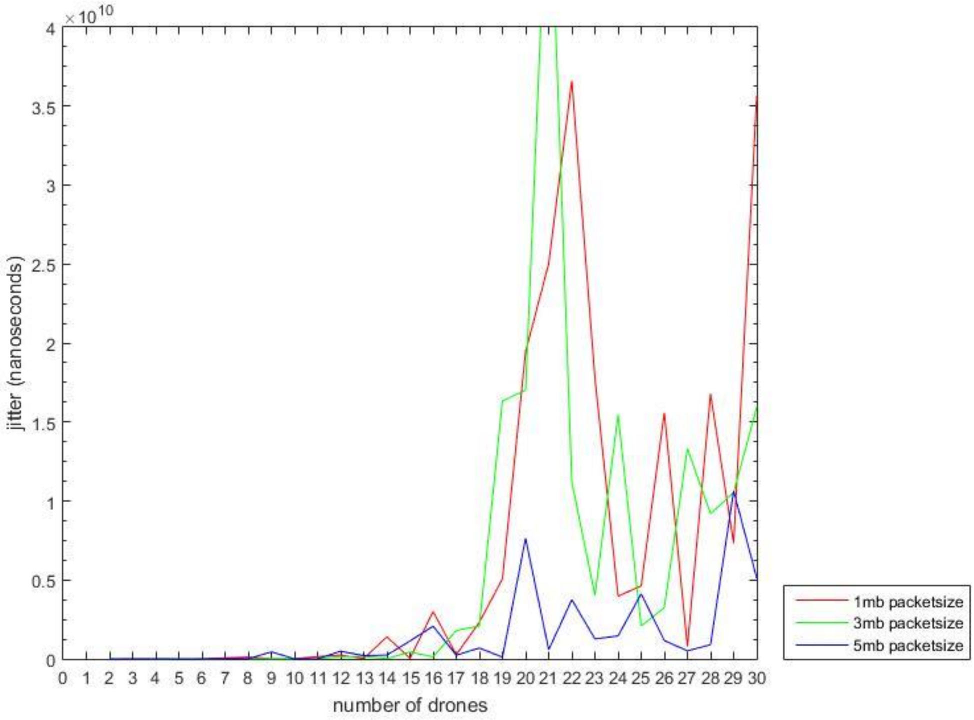

Figure 14: jitter vs number of drones for 1,3,5 mb packet sizes

In Figure 15, all three curves share the same throughput from 2 to 10 drones but then we see the 3mb line climbing up while the other two ones fall. On the whole, it is found out that at about 11 drones there have been the best possible and more stable throughput value because from 12 to 30 after the fall there have been a slow upward trading with it, at the end reaching about a little less than the biggest throughput amount we had at 10 drones. The biggest throughput is spotted in the 3 mb packet size curve with a value of 2.5 x 10 ^ 5 bps for 11 drones and the least is at 2 drones for all the curves with a value of 4096 bps.

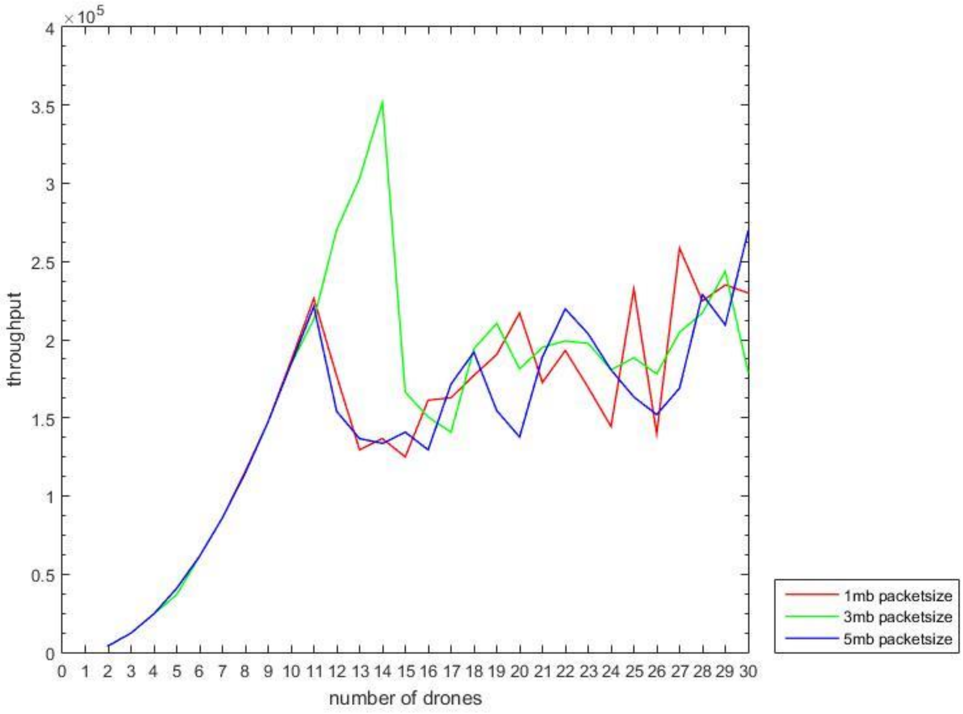

Figure 15: throughput vs number of drones for 1,3,5 mb packet sizes

It is apparent in the Figures 16-19 below there are three lines:
-1 mb packetsize
-3 mb packetsize
-5 mb packetsize
We keep these packet sizes unchanged in each line and we estimate the delay, jitter packet loss and throughput from 1 second frequency up to 10 seconds.

In Figure 16, we observe 3 lines for 1,3 and 5 mb packet size. For 1 mb packet size, the packet frequency does not affect the delay much, but for bigger packets, the smaller the frequency of packet production, the greater the delay is. This is normal because there is more traffic. The biggest value is observed in the 3mb packet size curve with a value of 10 x 10 ^ 10 at the spot of 1 second packet frequency and the least value is 0.25 x 10 ^ 10 nanoseconds that happens in the same curve at the spot of 3 seconds packet frequency.

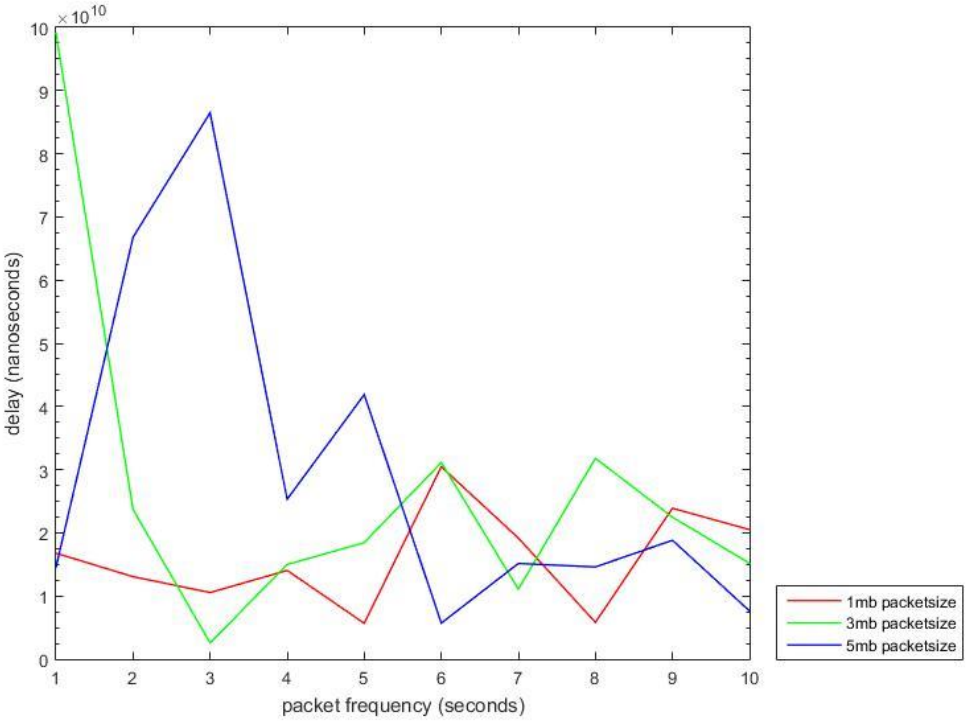

Figure 16: delay vs packet frequency for 1,3,5 mb packet sizes

In Figure 17, below it is crystal clear that frequency does not influence packet loss for all the packet sizes that much. Thus, it is directly noticed that the smaller the packet size is, the less the packet loss becomes. The biggest packet loss percentage is 80% for 4 seconds packet frequency and takes place in the curve of 5 mb packet size. The least value is at the same curve with a value of about 50% for 8 seconds packet frequency.

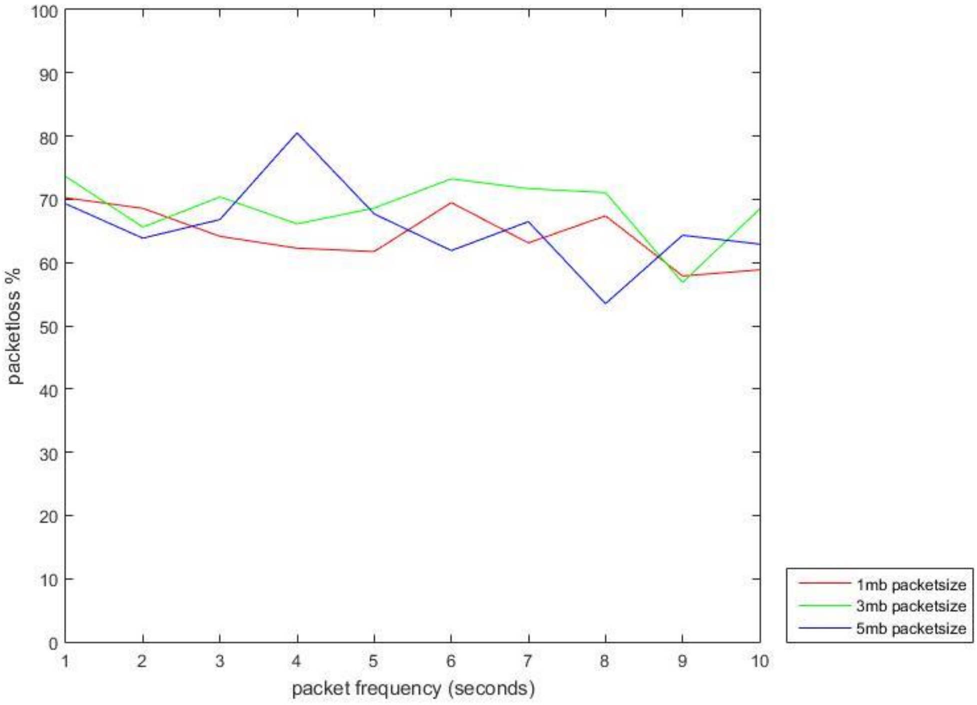

Figure 17: packet loss vs packet frequency for 1,3,5 mb packet sizes

The jitter graph for the 3 packet sizes in Figure 18 illustrates again how they get affected by the frequency. It is without question easy to infer again that the smaller the frequency is, the bigger the jitter gets. As far as smaller packet sizes are concerned there is more stable jitter over the increase of the frequency time and eventually for bigger values of frequency there is less jitter which is again normal due to the traffic which is noticed with small packet frequencies. The least value here is 0.125 x 10 ^ 10 nanoseconds and occurs in the 1 mb packet size curve for 2 second of packet frequency. The biggest jitter happens in the curve of 5 mb packet size at 3 seconds frequency and has a value of 4.375 x 10 ^ 10 nanoseconds.

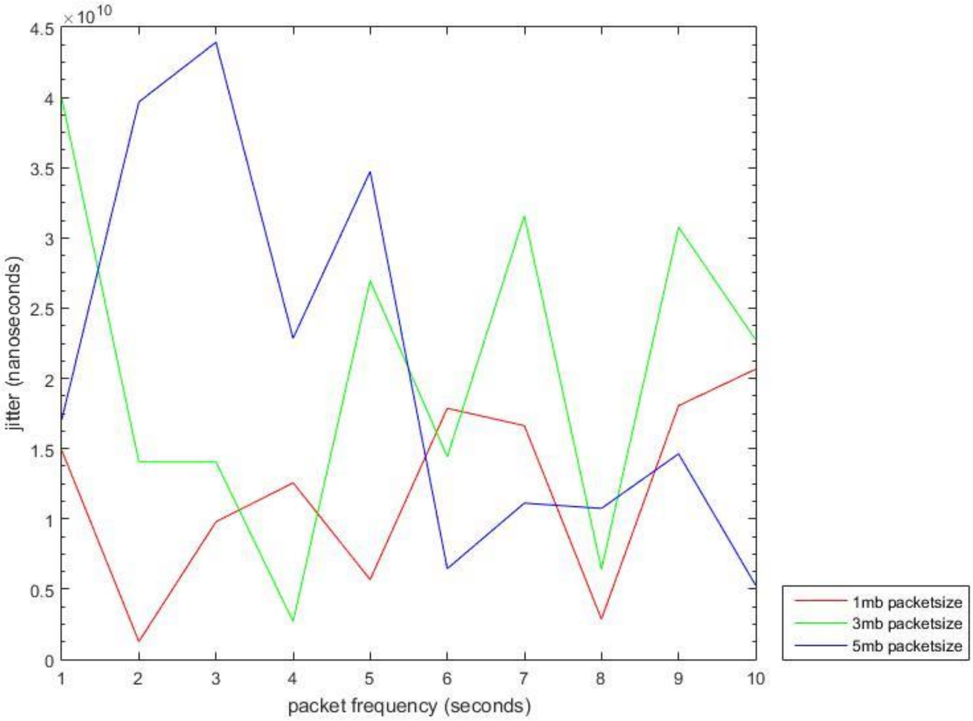

Figure 18: jitter vs packet frequency for 1,3,5 mb packet sizes

In Figure 19, on the other hand, it is revealed that the throughput remains pretty steady for the 1 and 3 mb packet sizes and in the 5 mb packet size it fluctuates. Therefore, we come to the conclusion again that the bigger the values of the frequency are, the greater the throughput becomes, except for the 3 mb curve that at about 2 seconds packet frequency there is the biggest able throughput. The highest value of throughput is 1.5 x 10 ^ 5 bps and is spotted in the curve of 5mb packet size for 8 seconds frequency and the least value is about 1.25 x 10 ^ 10 bps and occurs in the same curve for 4 seconds frequency.

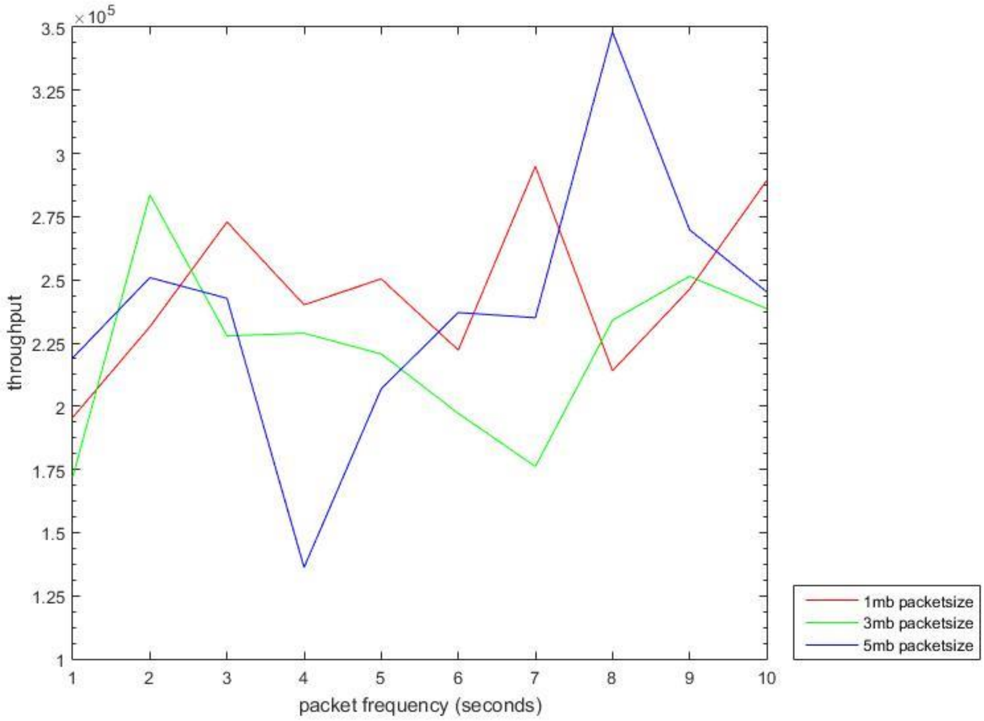

Figure 19: throughput vs packet frequency for 1,3,5 mb packet sizes

According to the Figures 20-23 below there are three lines:

-1 sec frequency

-5 sec frequency

-10 sec frequency

We keep these packet frequencies unchanged in each line and we calculate the delay, jitter packet loss and throughput from 2 drones up to 30 drones.

In Figure 20 below, 3 lines for 1,5 and 10 seconds packet frequency are shown. We can see that the bigger the value of the frequency is, the smaller the delay becomes, as we have already concluded in the previous graphs, too. In addition, for 2 to 11 drones there is almost no delay and after 11 drones until 30 the number of the delay increases. The biggest value of delay is 14.375 x 10 ^ 9 nanoseconds and occurs in the curve of 1 second frequency for 24 drones. The least value is almost 0 nanoseconds for all curves from 2 up to 11 drones.

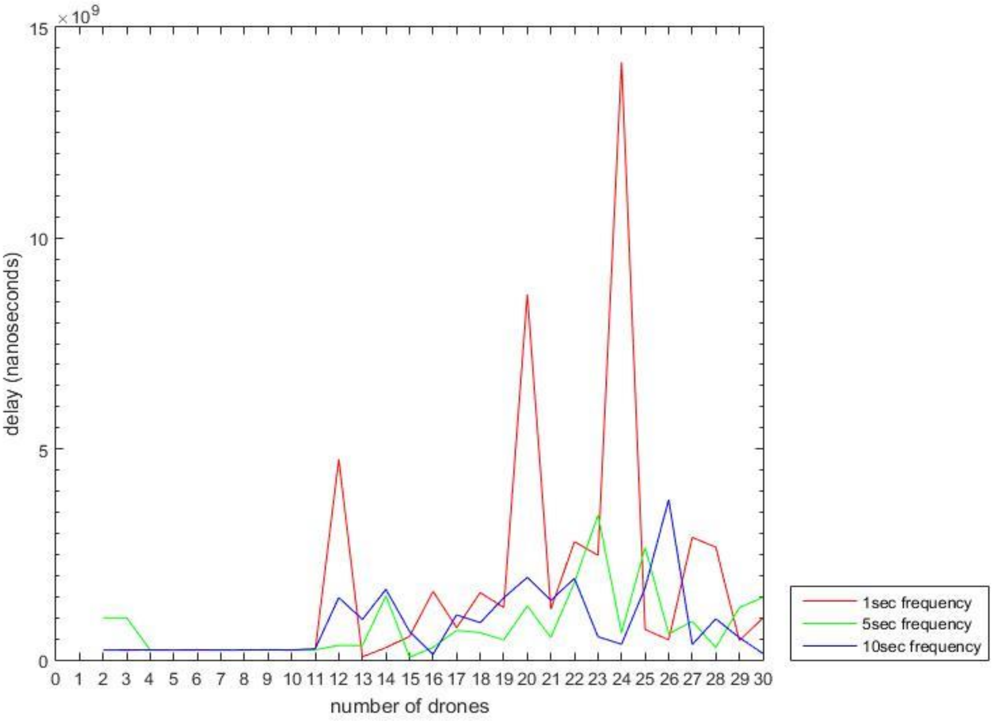

Figure 20: delay vs number of drones for 1,5,10 sec packet frequency

In Figure 21 below, we draw the conclusion that the change of frequency on the same number of drones does not affect the packet loss percentage significantly, thus, once again, we have aslightly lower packet loss percentage for bigger frequencies. Again from 2 to 11 number of drones there is almost no packet loss. The biggest percentage of packet loss is 77.5 % and is met in the curve of 5 sec frequency for 28 drones. The least percentage is 0 % and it is the same for all curves from 2 up to 11 drones.

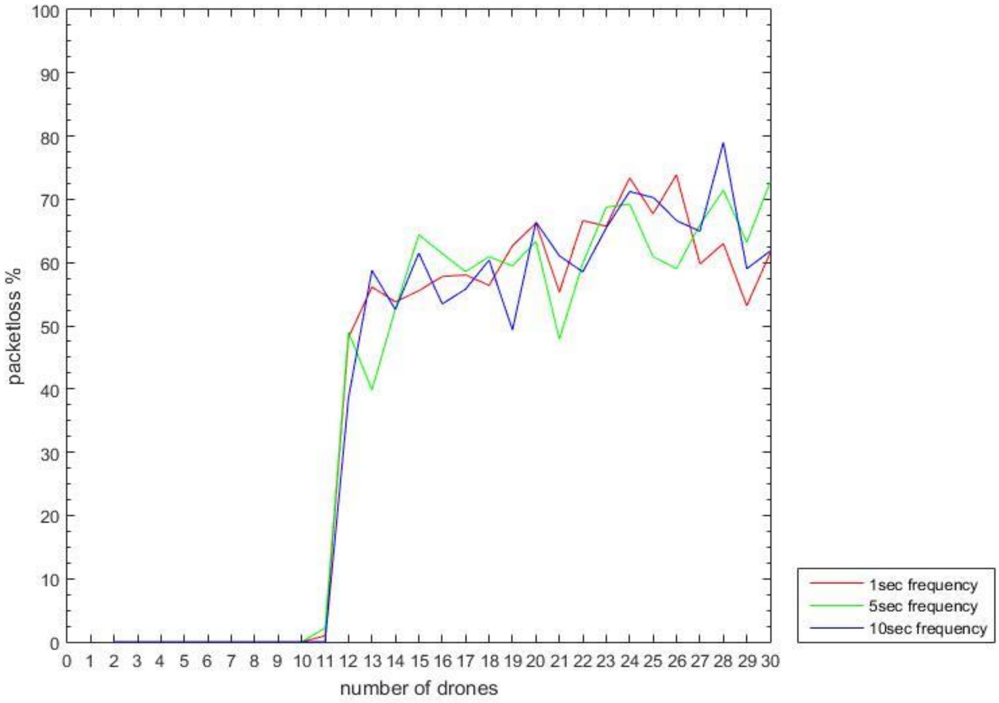

Figure 21: packet loss vs number of drones for 1,5,10 sec packet frequency

Figure 22, on the other side, suggests that jitter is influenced by the change of frequency on the same number of drones. The smaller the frequency is, the bigger the jitter grows and that is not desirable. Drones from 2 to11 have almost no jitter apart from a little jitter at the beginning of the 5 sec frequency curve. Consequently, for 30 drones the amount of jitter is lowered by a lot compared to the climbing of the curves from 12 to 27 number of drones. The biggest value of jitter is 13.5 x 10 ^ 9 nanoseconds and is met in the curve of 1 second packet frequency for 24 drones. The least value is almost 0 for all three curves from 2 up to 11 drones.

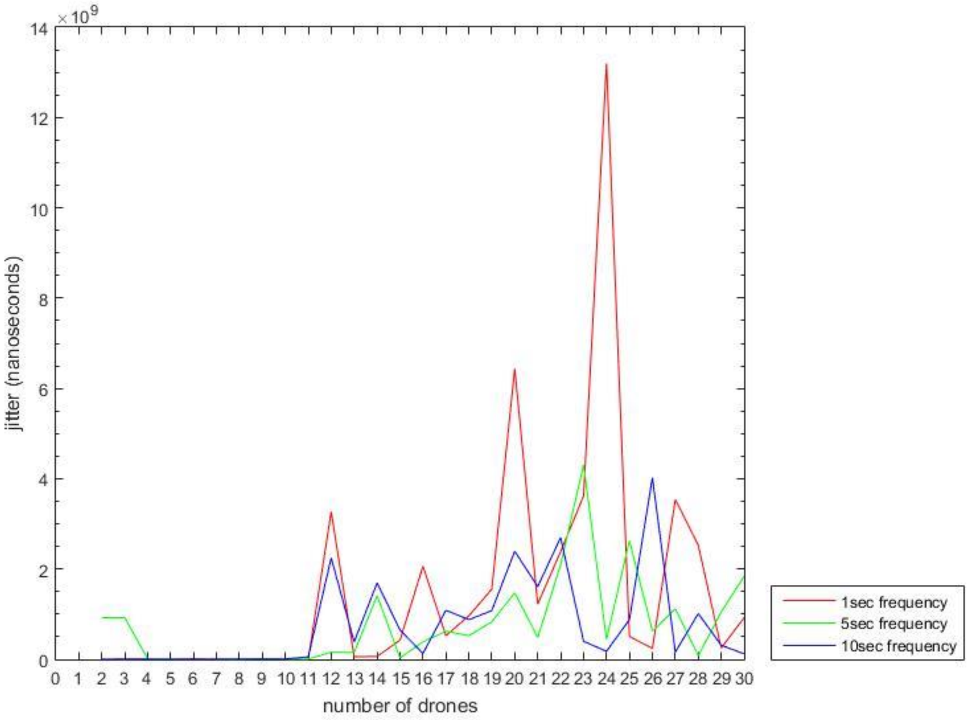

Figure 22: jitter vs number of drones for 1,5,10 sec packet frequency

Regarding the throughput in this experiment, as it is presented in Figure 23, there is an upward from 2 to about 10 number of drones, in all 3 curves of packet frequency. Thus, there are step ups after 11 drones. We come to the conclusion that there is not actual effect of the packet frequency on the same number of drones as we have said above. Furthermore the biggest value of throughput is at 10 number of drones for all curves except the 10 sec frequency curve that at 29 drones has the biggest value which is 2.875 x 10 ^ 5 bps. The least value for all curves is 4096 bps for 2 drones.

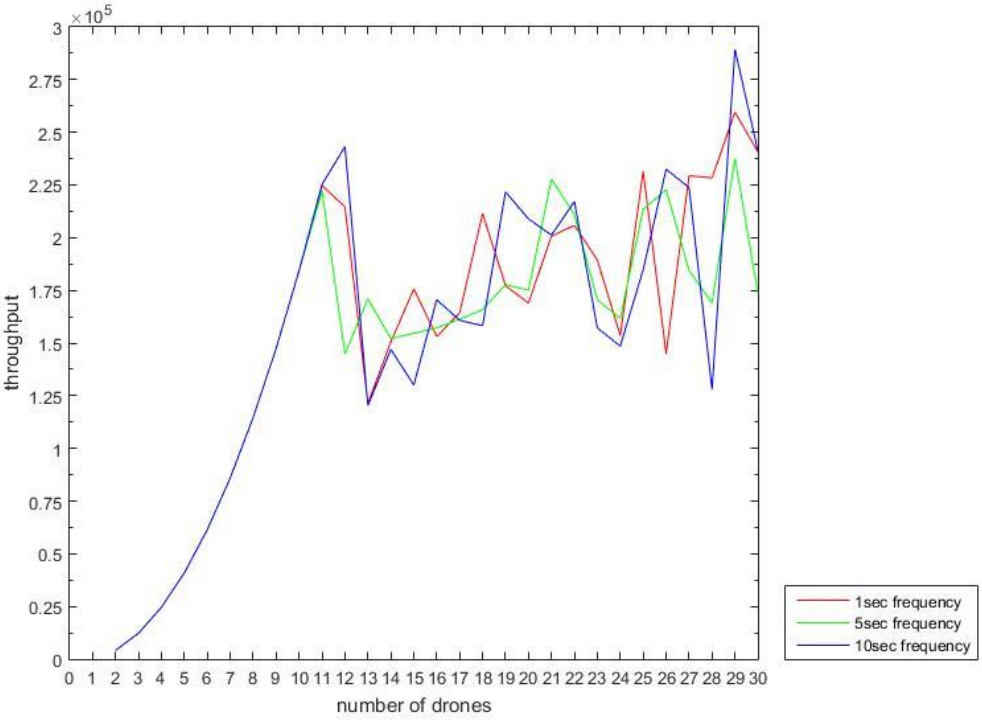

Figure 23: throughput vs number of drones for 1,5,10 sec packet frequency

As it is displayed in the Figures 24-27 below there are three lines:

-1 sec frequency

-5 sec frequency

-10 sec frequency

We keep constant these packet frequencies in each line and we calculate/ measure the delay, jitter packet loss and throughput from 1 up to 5 mb packet size.

Figure 24 illustrates the effect of the packet size on the delay, jitter, throughput and packet loss for 1,5 and 10 seconds frequency. It is inferred that we have the smallest delay for the curve of 5 seconds frequency with a value of 0.2 x 10 ^ 9 nanoseconds for 3.5 mb packet size and the biggest for the 1 second curve with the value of 5.8 x 10 ^ 9 nanoseconds at 3 mb packet size. Additionally, the smallest values of delay are at about 2.5 mb packet size and 3.5 mb packet size. Thus, we also have good results for 1 and 5 mb packet size

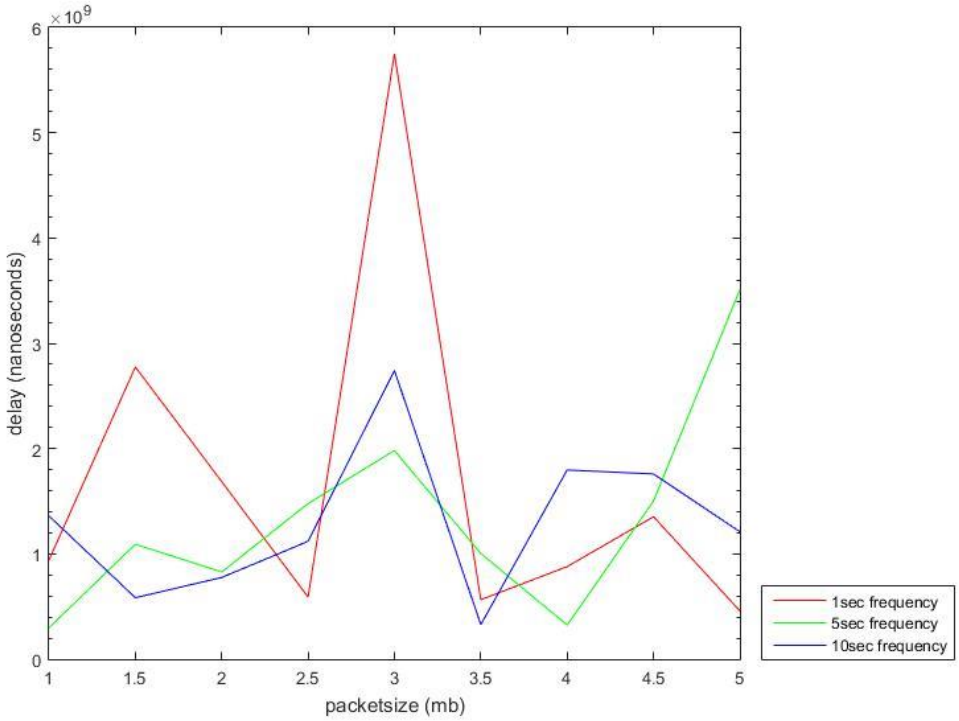

Figure 24: delay vs packet size for 1,5,10 sec packet frequency

In Figure 25 below we can see that there is minor/insignificant/slight frequency effect for the same values of packet size. We could say though that we have more stable packet loss curve for the 10 sec frequency line among all its values of packet size. The biggest percentage of packet loss takes place in the curve of 1 second frequency with a value of about 72.5 % for 2.5, 4 and 5 mb packet size. The least percentage is about 55 % and occurs in the same curve for 2 mb packet size.

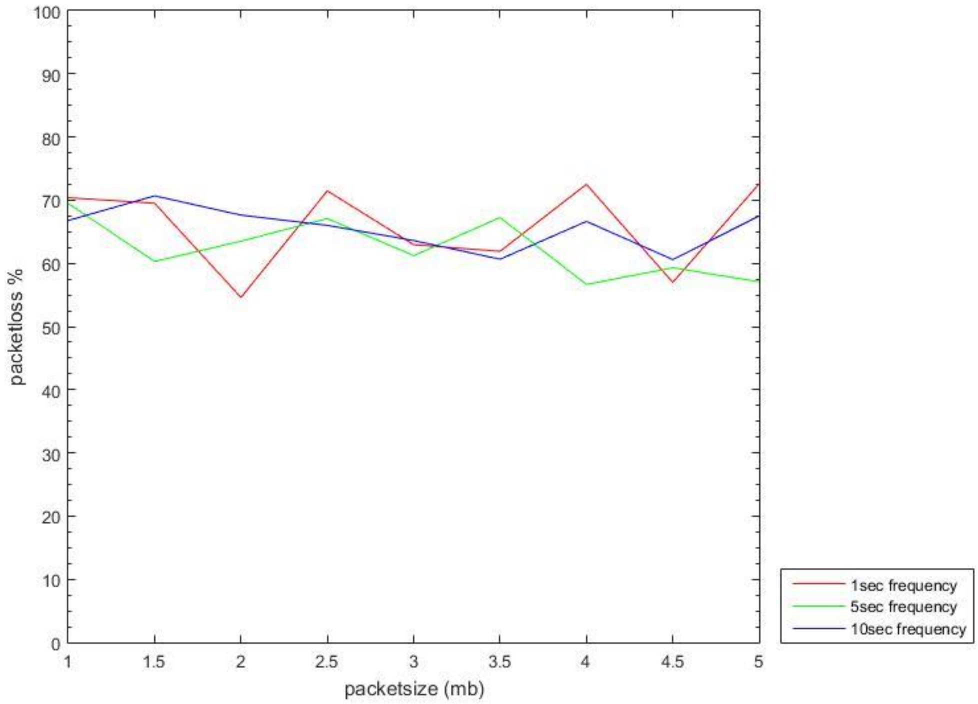

Figure 25: packet loss vs packet size for 1,5,10 sec packet frequency

Figure 26 below shows that for 5 seconds frequency there is the smallest jitter. It is worth noticing that for 2.5 and 3.5 to 4 mb packet size there are the smallest amounts of jitter for all curves. Repeatedly, for 1 and 5 mb packet size there are results for all the different frequency values. The biggest value of jitter is about 4.625 x 10 ^ 9 nanoseconds and occurs in the 1 second frequency curve for 3 mb packet size. The least value is 0.125 x 10 ^ 9 nanoseconds and appears in both curves of 5 and 1 second frequency for 1 and 4 mb packet size on the green line and at 5 mb packet size on the red line.

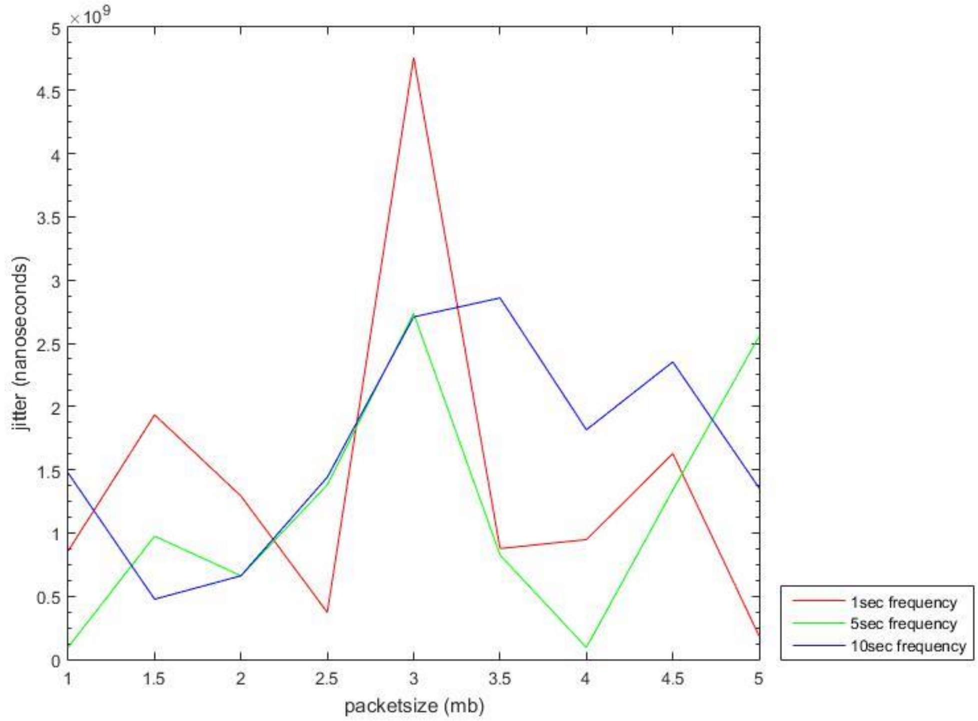

Figure 26: jitter vs packet size for 1,5,10 sec packet frequency

In Figure 27, for the line of 1 second frequency there are a lot of step ups for throughput in different packet sizes, although the biggest values are noticed here. However, the most stable is on the line of 5 seconds frequency. Overall, it could be concluded that for the most stable throughput the line of 5 seconds frequency is the best. Furthermore, as can be seen, concerning the packet size values with decimal points, there is a fall of the throughput. The biggest value is almost 3 x 10 ^ 5 bps and occurs in 1 sec frequency curve for 2 mb packet size. The least value is 1.75 x 10 ^ 5 bps in the curve of 1 and 10 sec frequency at the spot of 1.5 mb packet size for the blue line and 5 mb packet size for the red line.

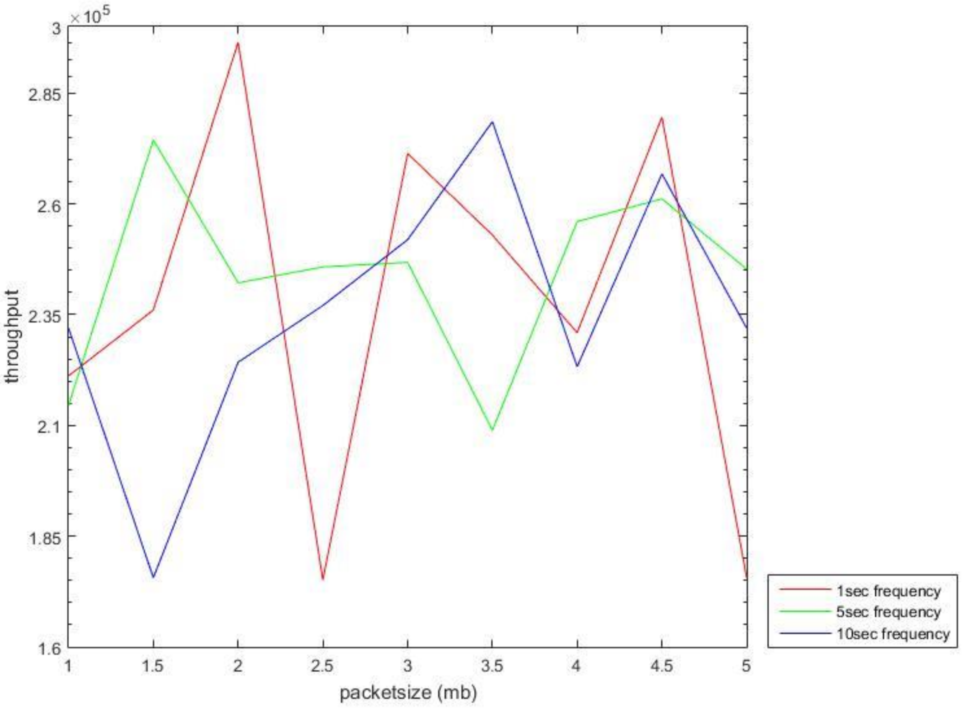

Figure 27: throughput vs packet size for 1,5,10 sec packet frequency

As it can be seen in the Figures 28-31 below there are three lines:

-10 number of drones

-20 number of drones

-30 number of drones

We keep constant/steady these numbers of drones in each line and we calculate delay, jitter packet loss and throughput from 1 up to 10 seconds packet frequency. As it was displayed in the graphs above, similarly, in the Figure 28 below for 10 number of drones there is almost no delay which is preferable. It has already been said that the more the number of drones is the more the value of the delay becomes. As far as the frequency effect is concerned, it can be said that there is a little random curve but that does not mean that it cannot be concluded that for bigger frequency values there is lesser delay. For the curve of 30 drones though we can tell that it has a lot of step ups with the least delay at 6 seconds packet frequency that is almost negligible. The biggest value is more than 10 x

10^{10}nanoseconds and occurs in the blue line at 1 and 7 seconds frequency. The least value is at almost all length of the red line that is about 0 nanoseconds.

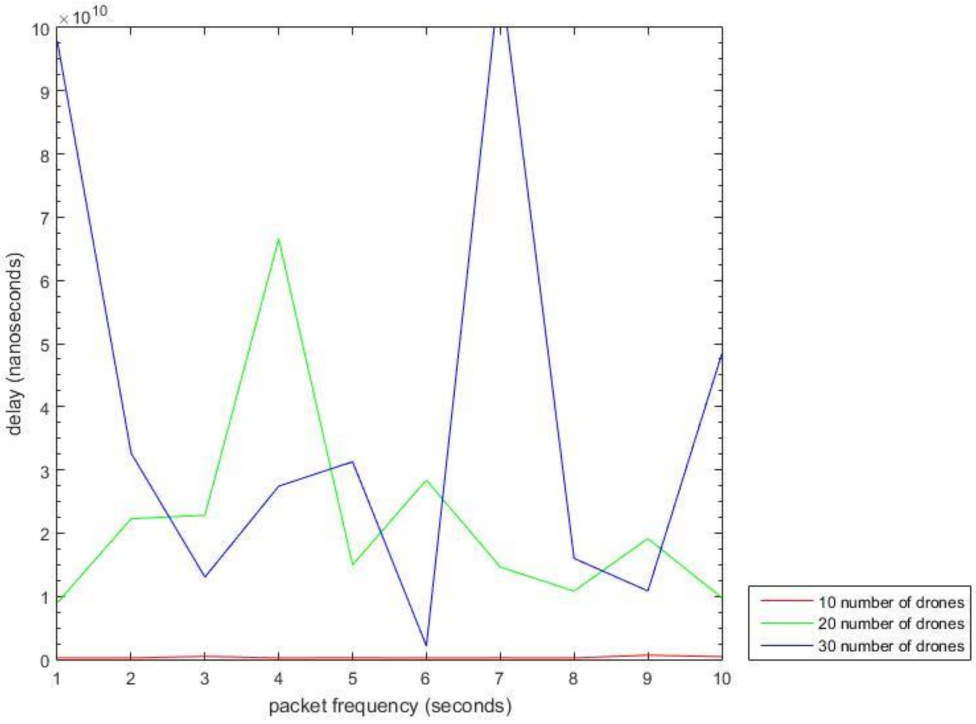

Figure 28: delay vs packet frequency for 10,20,30 number of drones

In Figure 29 for 10 drones,it is obvious that there is not at all packet loss. It can also be said that for the curves of 20 and 30 drones the packet frequency does not affect the packet loss that much, even though for both curves there are very big values of packet loss that might not be preferable, but that depends on the application we want to build.The biggest percentage is at 72% for green and the blue line at all of its top points. The smallest is 0 % for all the length of red line

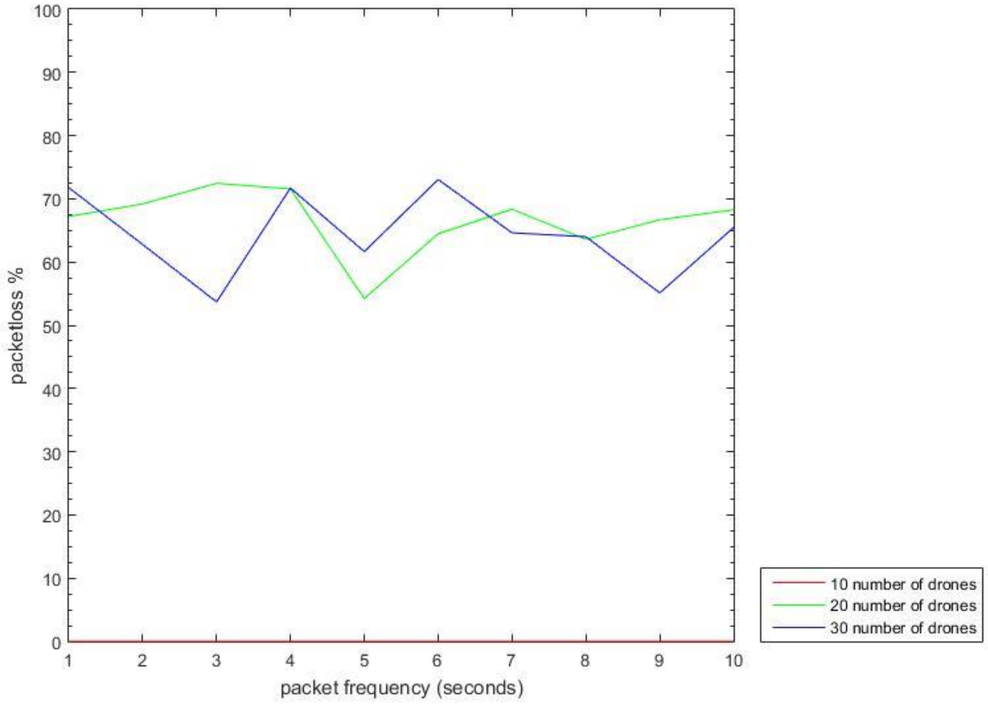

Figure 29: packet loss vs packet frequency for 10,20,30 number of drones

In Figure 30 for the curve of 10 drones again there is almost no jitter. For the other two lines we can say that the bigger the number of drones is, the bigger the jitter becomes, but also the bigger the frequency is, the better for the amount of jitter it gets .The biggest value is more than 4 x 10 ^ 10 nanoseconds for the blue line at 1 second frequency. The least value is almost 0 for all the length of red line.

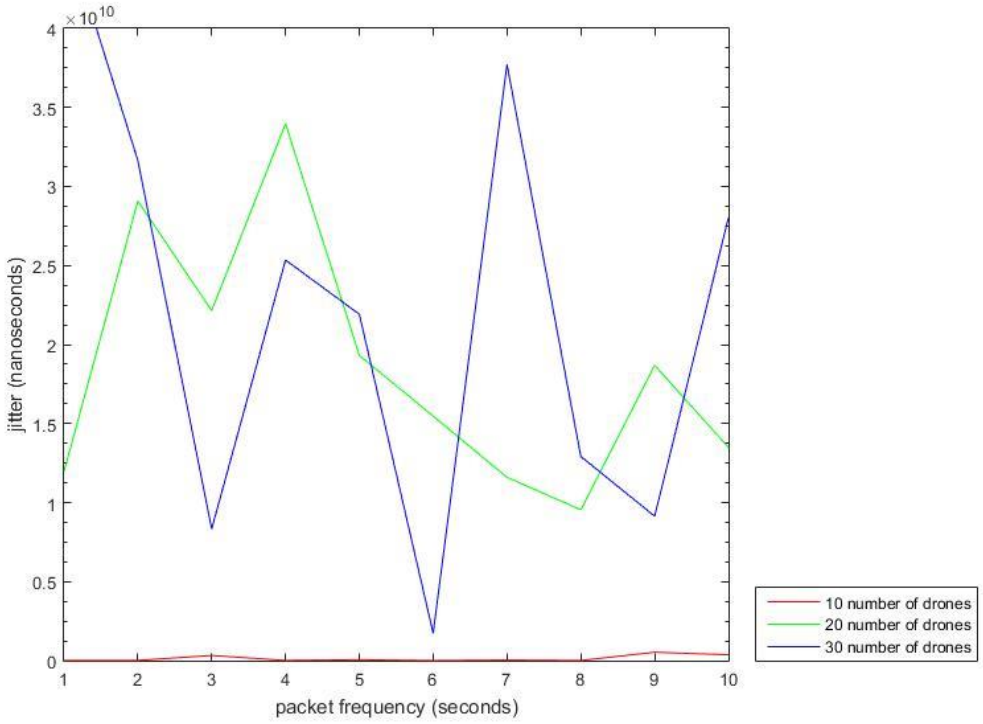

Figure 30: jitter vs packet frequency for 10,20,30 number of drones

In Figure 31 below it can be noticed that for 10 drones there is a stable curve for all packet frequencies at about 1.9 x 10 ^ 5 bps. In relation to the other two curves,we can say that for a bigger number of drones, there are more throughput values. Concerning frequency, there are the best results at about 4 to 9 seconds.The least value is 1.55 x 10 ^ 5 bps at 4 seconds frequency for the green line and the biggest value is 3.2 x 10 ^ 5 bps and occurs in the blue line at 9 seconds packet frequency.

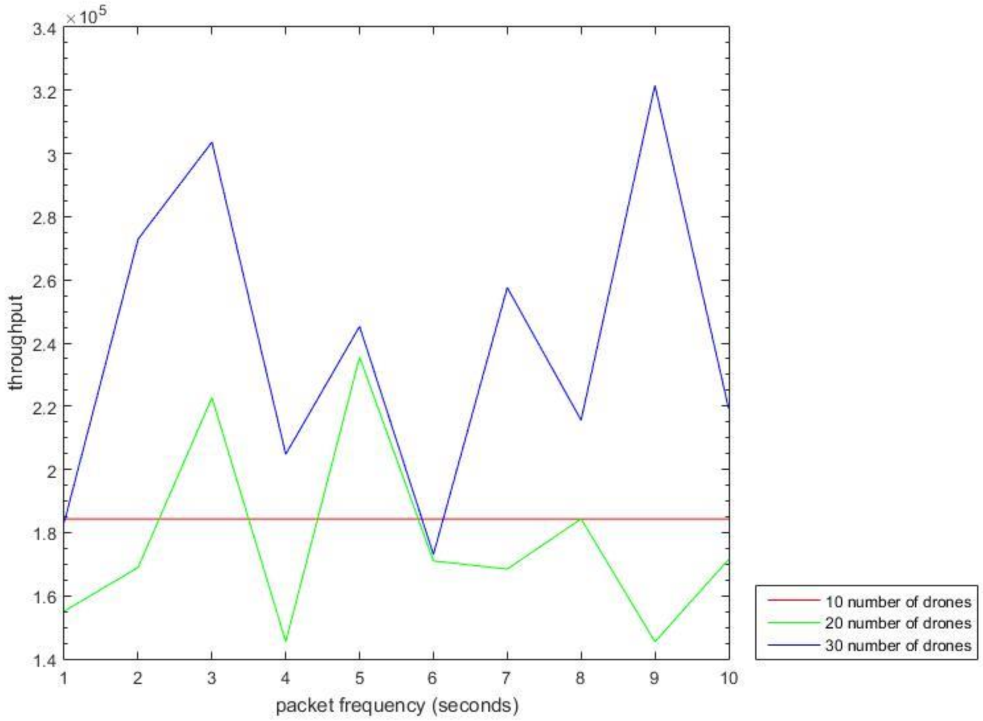

Figure 31: throughput vs packet frequency for 10,20,30 number of drones

As we can see in the Figures 32-35 below there are three lines:

-10 number of drones

-20 number of drones

-30 number of drones

We keep constant these number of drones in each line and we calculate the delay, jitter packet loss and throughput from 1 to 5 mb packet size.

In Figure 32, for 10 drones again there is almost no delay for different packet sizes. For 20 and 30 drones it can be pointed out that for smaller packet sizes there is lesser delay with the least value at about 2 mb packet size. Also the bigger the number of drones is, the more delay there is. The biggest value of delay is noticed in the blue line at 4.5 mb packet size with a value of more than 4 x 10 ^ 10 nanoseconds. The least value is almost 0 for the red line and appears almost in all its length.

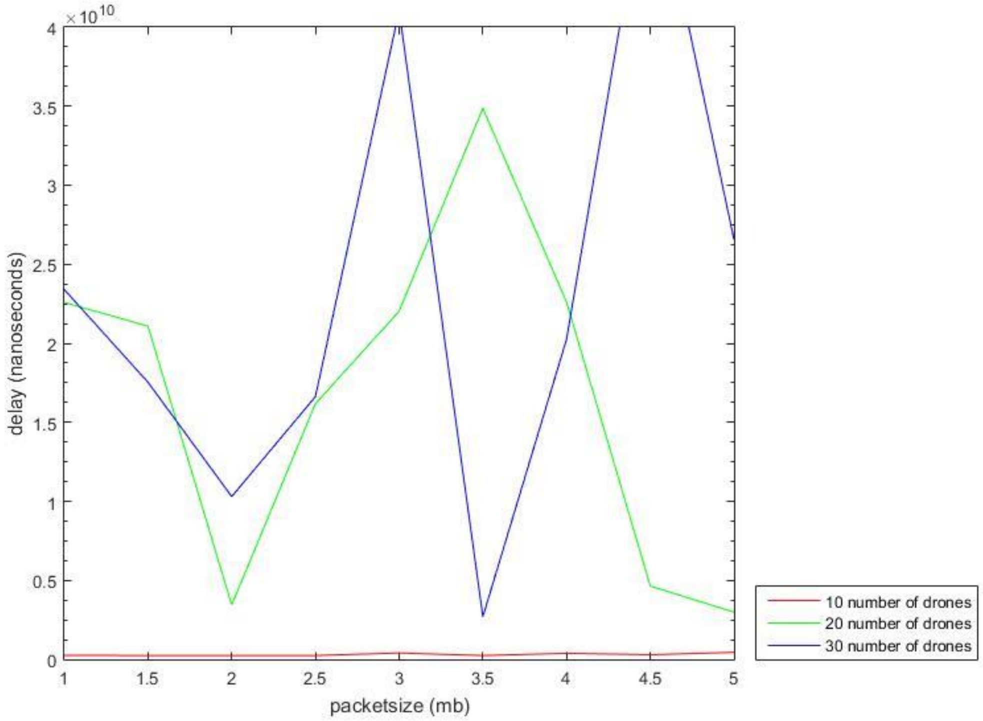

Figure 32: delay vs packet size for 10,20,30 number of drones

In Figure 33 for 10 drones there is no delay at all. For 20 and 30 drones there is a lot of packet loss but there is not much difference for the two curves. It can be inferred though that for the same number of drones, packet size does not affect packet loss that much. The least percentage is 0 for all the red line and the biggest percentage which is 70% occurs at 1.5 and 5 mb packet size for the blue line and 3.5 mb packet size for the green line.

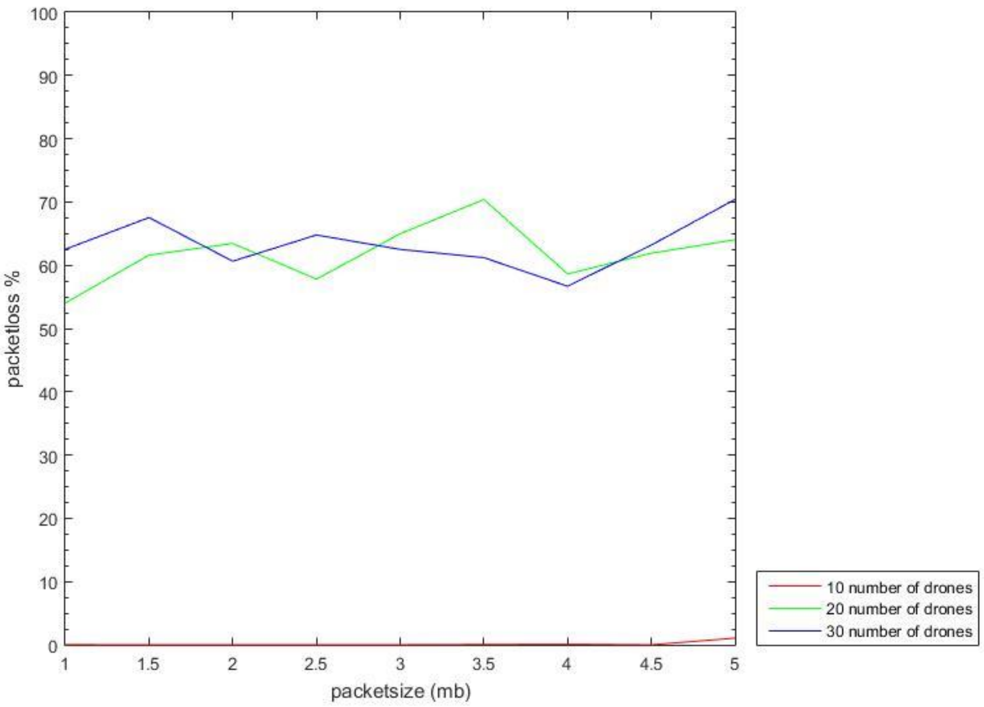

Figure 33: packet loss vs packet size for 10,20,30 number of drones

Likewise, in Figure 34, for 10 drones the least jitter is observed, and for a greater number of drones the biggest one. It is worth noticing though that for about 1.5 to 2 and 3.5 to 4 mb packet size, the least jitter for all curves is seen. The biggest value is more than3 x 10 ^ 10 for the blue curve at 3 mb packet size. The least value is almost 0 for the red line in all its length.

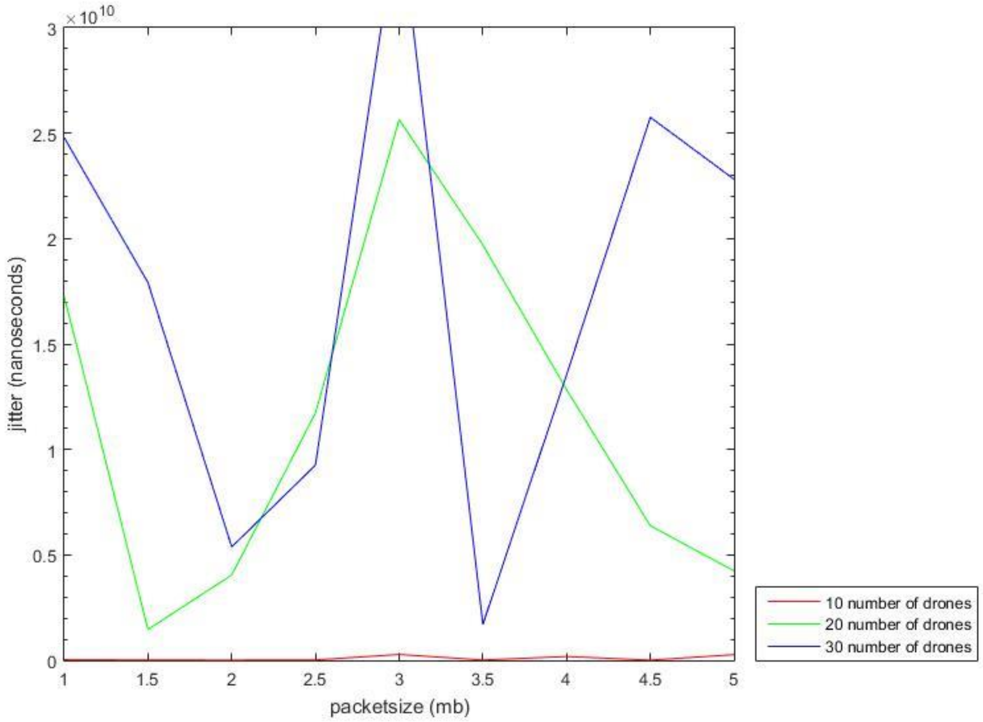

Figure 34: jitter vs packet size for 10,20,30 number of drones

In Figure 35, we can see that the 10 number of drones' curve is about 1.9 x 10 ^ 5 bps in its all length. The biggest values for throughput are in the 30 drones' curve though there are a lot of step ups. For 20 number of drones we can see that the curve is not that good because in a lot of points the smallest amounts of throughput are observed; for example, at 3.5 mb packet size. We can also conclude that the bigger the packet size is, the less the throughput becomes but not with much difference. The biggest value is about 3 x 10 ^ 5 bps for the blue curve at 4 mb packet size. The least value is about 1.5 x 10 ^ 5 bps in the green curve for 3.5 mb packet size.

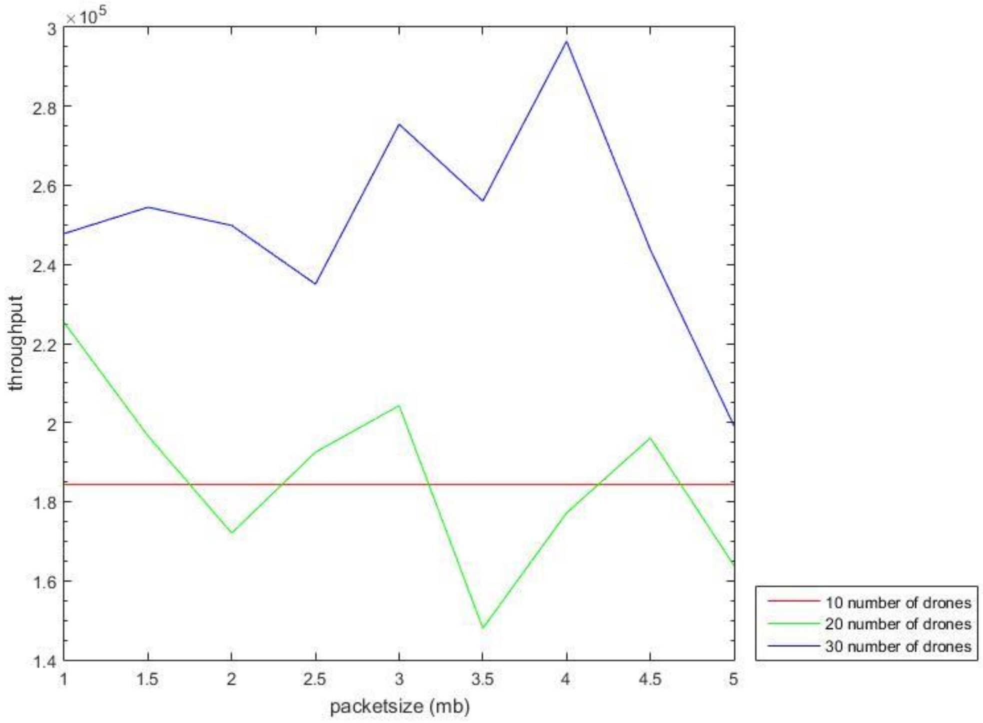

Figure 35: throughput vs packet size for 10,20,30 number of drones

5.3 – IEEE 802.11ac Figures

In the next Figures, the results of our experiment are going to be presented from a lot of different angles. We separated the results into the following 6 different aspects to make them more accessible to the reader:

As we can see in the Figures 36-39 below there are three lines:

-1 mb packetsize

-3 mb packetsize

-5 mb packetsize

We keep constant these packet sizes in each line and we calculate the delay, jitter packet loss and throughput from two drones up to 30 drones.

In Figure 36, as it is obvious at about 2 to 9 drones for all curves there is almost no delay. After that point, there are step ups for all the curves. It can be concluded though that for 5mb packet size there is a little more stable/steady delay and the second smaller one; the smallest delay that has been spotted for 1 mb packet size. It is also obviously shown that for a greater number of drones, there is bigger delay for all curves. The biggest value is almost 8.5 x 10 ^ 9 nanoseconds for the blue curve at 30 drones. The least value is almost 0.25 x 10 ^ 9 nanoseconds for all the curves from 2 up to about 9 drones.

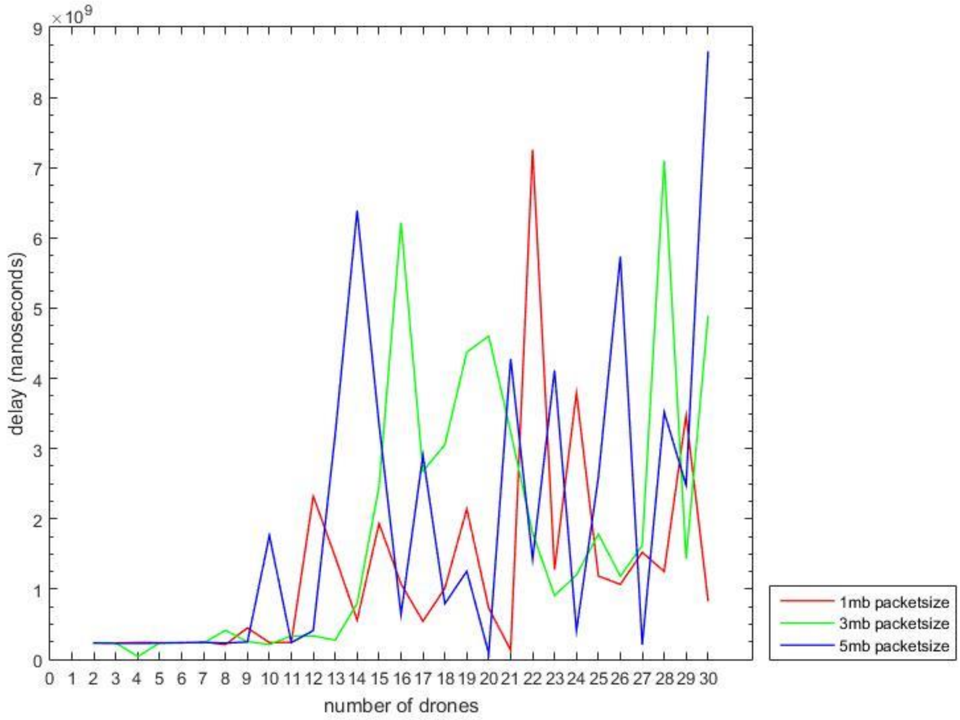

Figure 36: delay vs number of drones for 1,3,5 mb packet size

In Figure 37, it is displayed that for 1 mb packet size,the least packet loss is observed although from 2 to 9 drones there is a little packet loss but for the other two curves that is not noticed. Surprisingly, in our experiment, we can see that for 3 mb packet size there is more packet loss even more than the 5mb packet size.In addition, as it is expected, there is more packet loss with a bigger number of drones. The biggest percentage of packet loss is 75% and occurs in the green line for 22 drones. The least percentage is 0% for the blue and green curve from 2 to 9 drones.

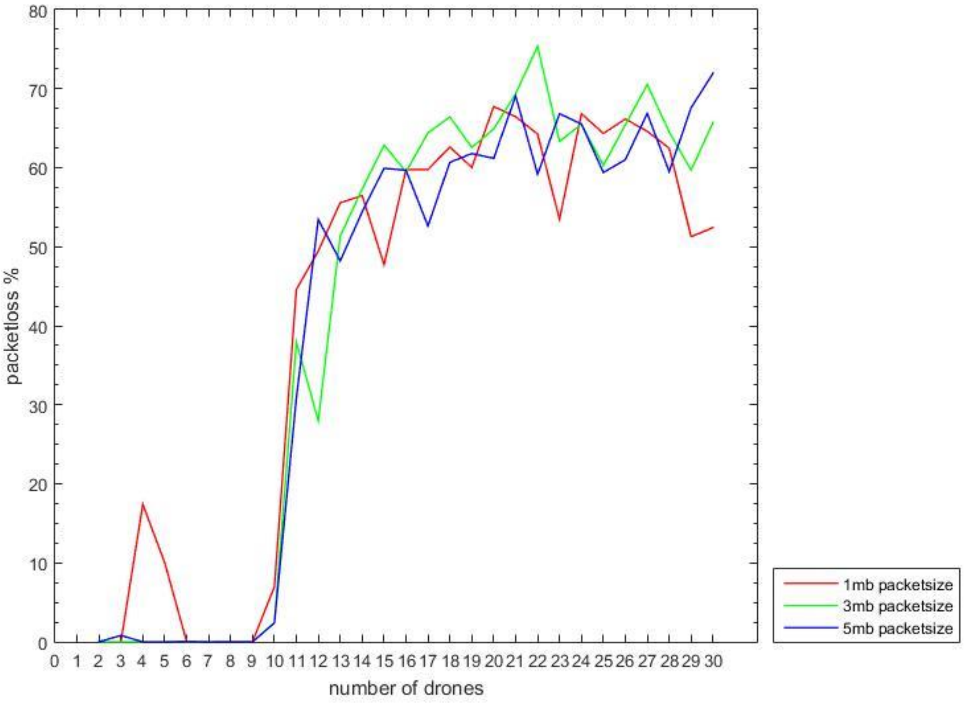

Figure 37: packet loss vs number of drones for 1,3,5 mb packet size

In Figure 38, on the other hand, as far as jitter is concerned, it is described that the 5mb packet size curve presents the most step ups even for a smaller number of drones. The smallest jitter we get is for the 1 mb packet size curve. From 2 to 9 drones there is almost no jitter and clearly/apparently the bigger the number of drones is, the bigger the jitter becomes. Nevertheless, it cannot be said that there are big differences for all the curves. The biggest value is 3.5 x 10 ^ 10 nanoseconds for the blue line at 17 drones. The least value is almost 0 for all curves from 2 up to 9 drones.

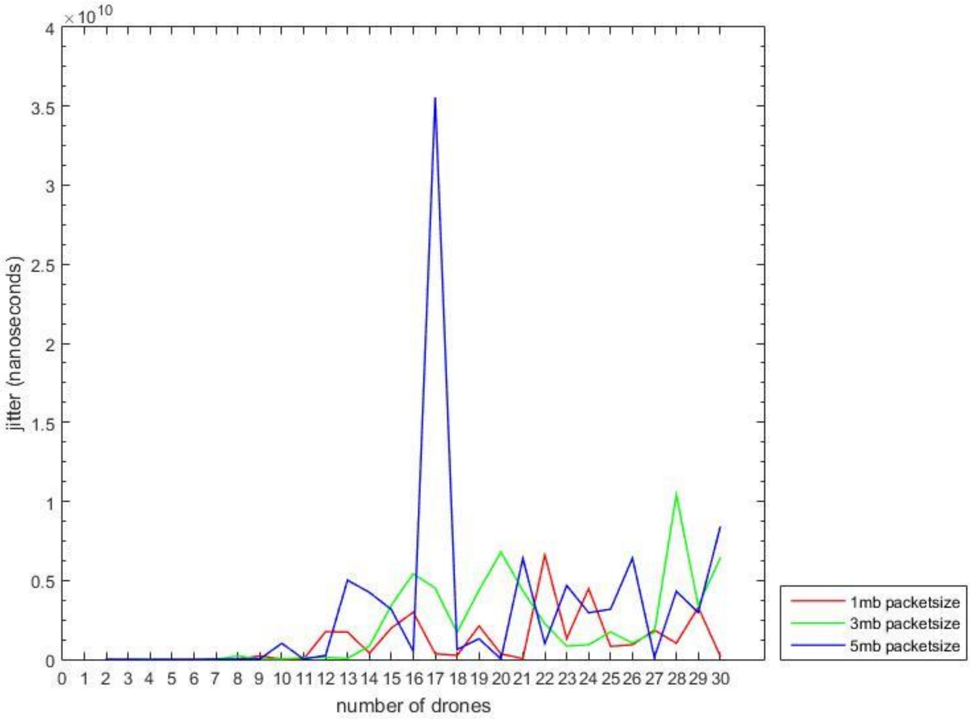

Figure 38: jitter vs number of drones for 1,3,5 mb packet size

Regarding throughput, we can see that in Figure 39 there is not a peak as early as in the 802.11n standard. As the line goes, the bigger the throughput becomes. We can say that the 5mb packet size curve has overall the biggest values of throughput but the differences are very small for all the curves. The biggest value of throughput has to do with 29 drones for 1 mb packet size with the value of about 3.5 x 10 ^ 5 bps. The least value is almost 0 for all the curves at 2 drones.

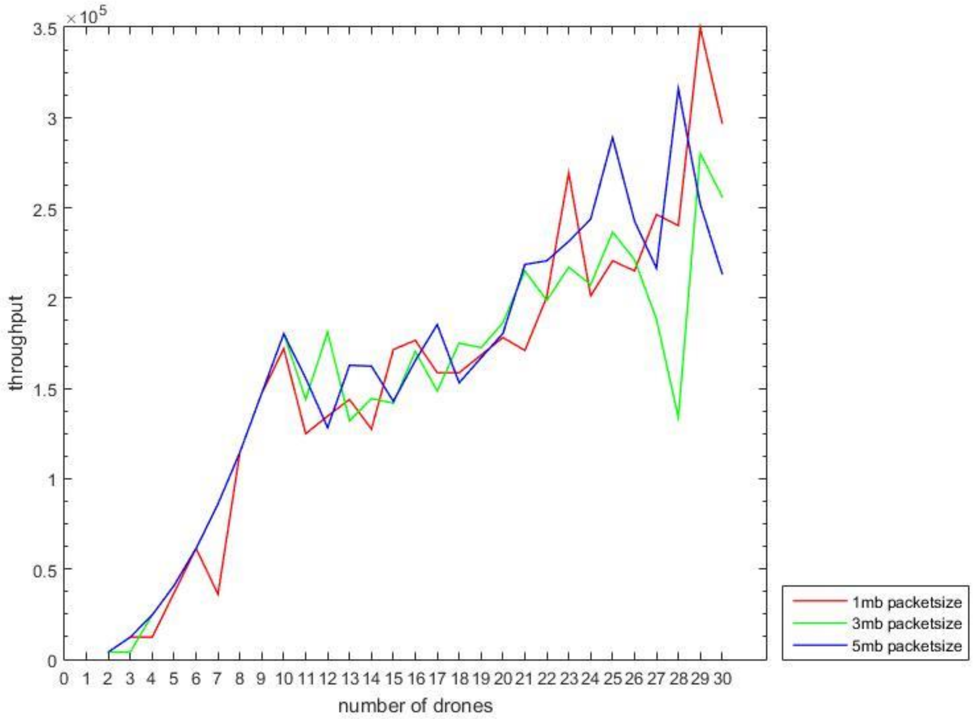

Figure 39: Throughput vs number of drones for 1,3,5 m packet size

As it can be seen in the Figures 40-43 below there are three lines:

-1 mb packetsize

-3 mb packetsize

-5 mb packetsize

We keep constant these packet sizes in each line and we calculate the delay, jitter packet loss and throughput from 1 to 10 seconds packet frequency.

In Figure 40,it is shown that for smaller frequencies, there is a bigger delay for all curves as it has beenexpected. The least delay we can see occurs at the curve of 3mb packet size. There are smaller delays as the packet size value increases, except for the spot of 2 seconds frequency in the 5 mb packet size, that we have the biggest delay. The biggest value is the one of 10 x 10 ^ 9 nanoseconds that appears in the blue line for 2 seconds frequency. The least value is a little less than 1 x 10 ^ 9 nanoseconds that is spottedat 1 second frequency and at 7 seconds frequency for the green line.

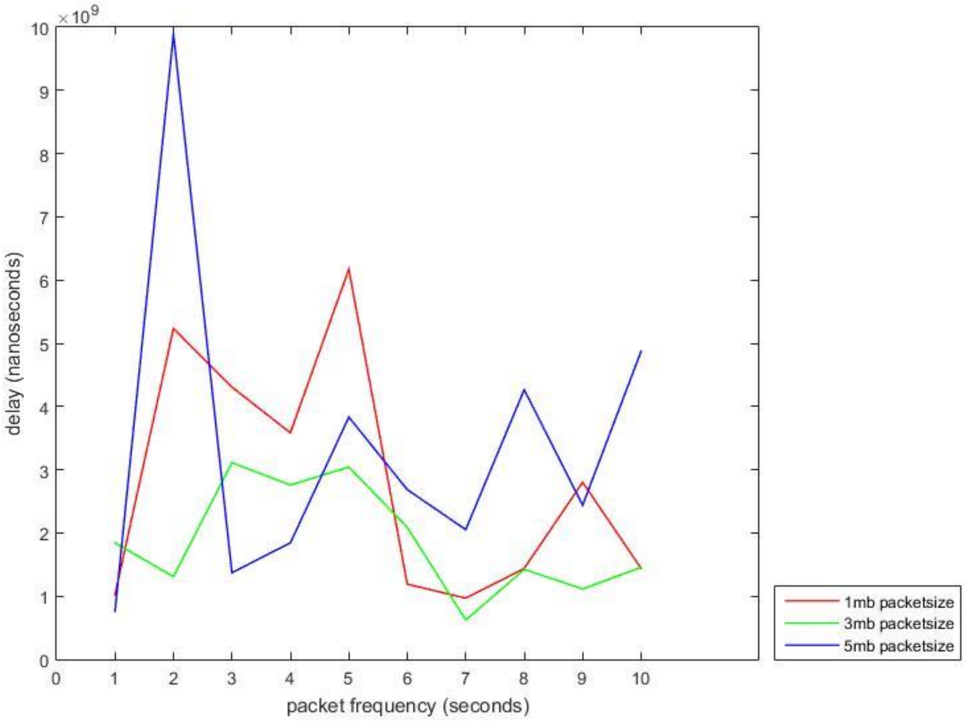

Figure 40: delay vs packet frequency for 1,3,5 mb packet size

In Figure 41, overall, the small packet loss percentages are noticed for all of our curves. We can also draw an inference that for bigger packet sizes there is less packet loss. At last, we can see that in this Figure, frequency doesn't affect the packet loss that much. The biggest value is 72.5 % at the green line for 3 seconds frequency. The least is at the same curve at 5 seconds packet frequency with a value of 50%.

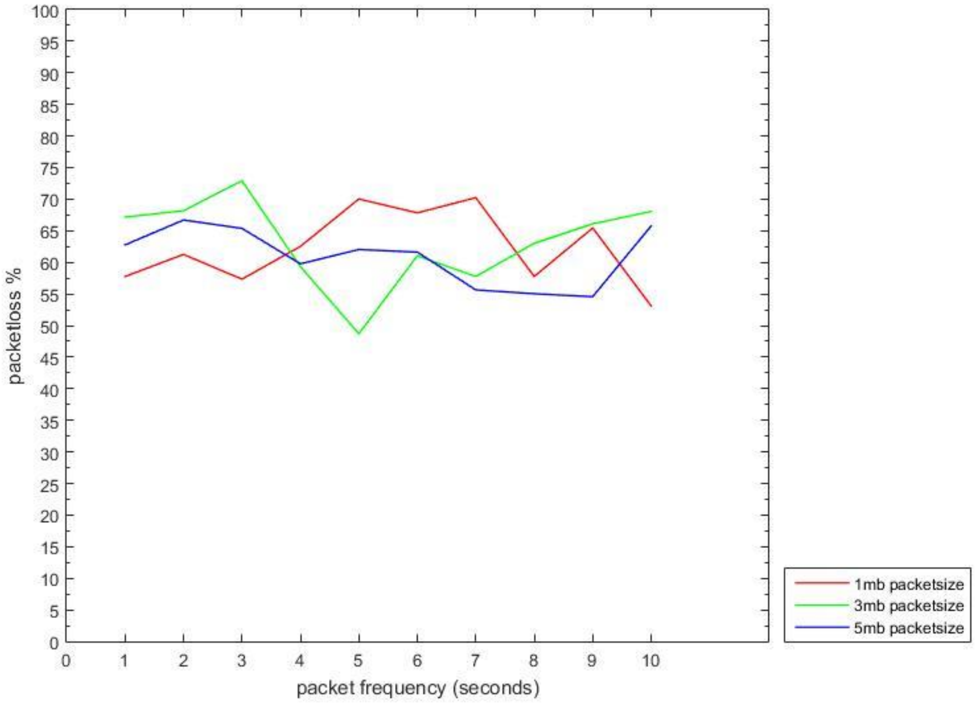

Figure 41: packet loss vs packet frequency for 1,3,5 mb packet size

In Figure 42, it is explicitly depicted that for smaller frequencies there are bigger jitter values. Moreover, for the lines of 5 and 1 mb packet sizes there are overall the biggest jitters. The 3 mb packet size curve has the smallest number of jitters with not very big/moderate step ups in comparison with the other two curves. The biggest value is 9.75 x 10 ^ 9 nanoseconds and occurs at the blue curve for 2 seconds packet frequency. The least value is 0.5 x 10 ^ 9 nanoseconds and occurs at the blue curve for 1 second frequency and at the green line for 7 seconds frequency.

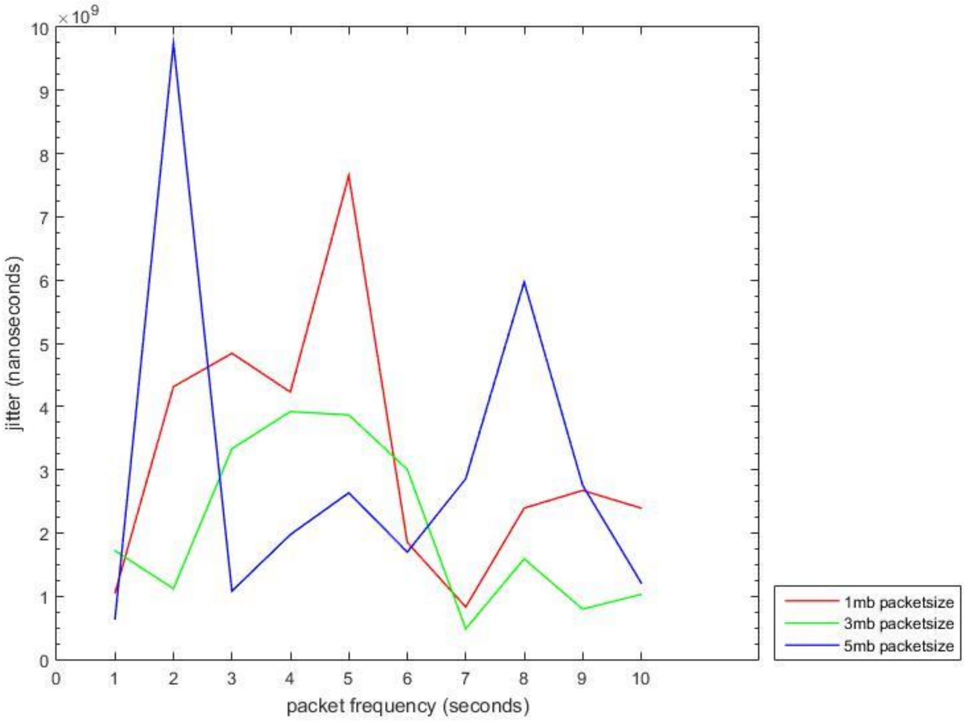

Figure 42: jitter vs packet frequency for 1,3,5 mb packet size

Concerning throughput, there are insignificantdifferences throughout the curves in Figure 43. However, at the beginning of the 1 b packet size line there is a big step up. Overall, it is concluded that the biggest throughput values occur in the 5mb packet size curve. In addition, it can be said that frequency doesn't affect the throughput graph for the different packet sizes that much and there are a lot more stable lines than the 802.11n Figures respectively. The biggest value is 8 x 10 ^ 5 bps which occurs at the red line for 1 second frequency. The least value is a little more than 2 x 10 ^ 5 bps that appears/is spotted at the green line for 3 seconds frequency.

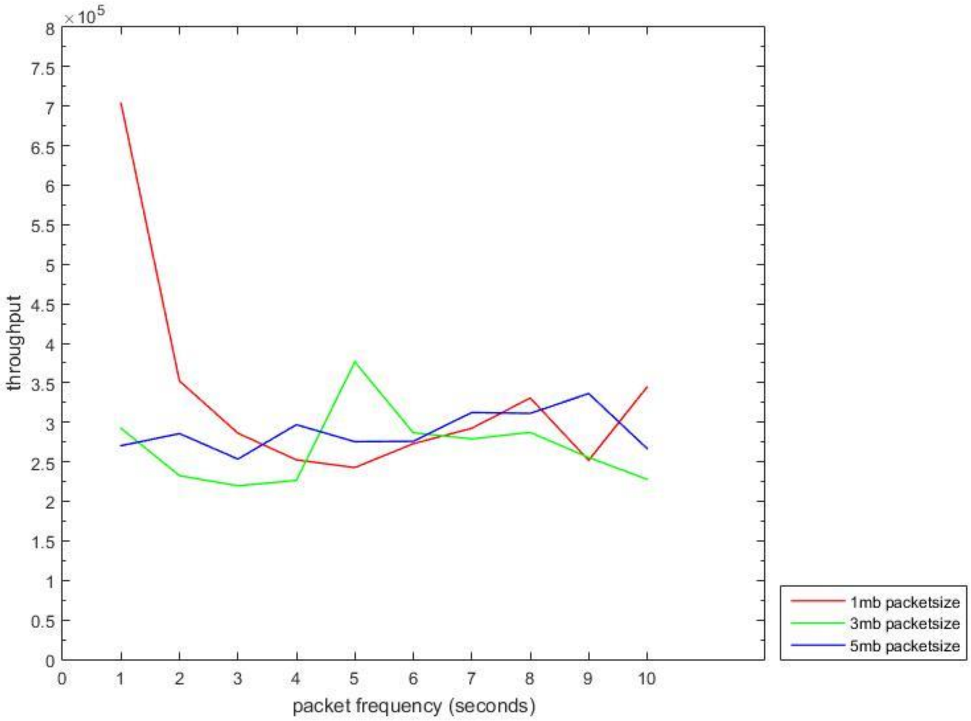

Figure 43: throughput vs packet frequency for 1,3,5 mb packet size

There are three lines in the Figures 44-47 below:

-1 second packet frequency

-5 seconds packet frequency

-10 seconds packet frequency

We keep constant these packet frequencies in each line and we calculate the delay, jitter packet loss and throughput from 2 drones up to 30 drones.

From 2 to 13 drones there is almost no delay again in Figure 44. It is obvious though that for a greater number of drones, there is less delay for bigger packet sizes. The 3 mb packet size curve presents less delay at the beginning of its length compared to other curves. The least value is almost 0 from 2 to 10 drones for all curves except some spots. The biggest value is 1.8 x 10 ^ 10 that occurs in the green curve for 29 drones.

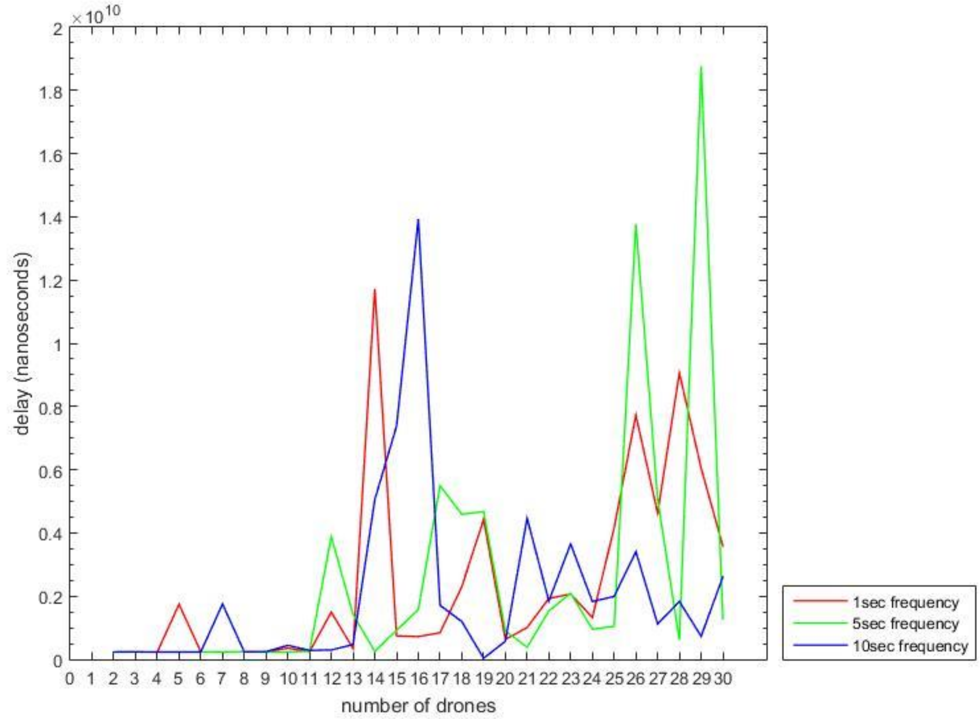

Figure 44: delay vs number of drones for 1,5,10 sec packet frequency

In Figure 45, it is found out that for 5 and 10 seconds frequency curves there is less packet loss from 5 to 10 drones, although after 10 drones there is less packet loss than the spot of 2 to 5 drones; that is not the same for the curve of 1 second frequency. It is also noticed that from 2 to 10 drones there is insignificant packet loss and then it rises bigger. It is also concluded that for bigger values of frequency there are less packet loss percentages but not with much difference from the others/being slightly different from others. The biggest value is about 72.5 % that occurs in the blue line for 4 drones. The least value is 0 and occurs from 2 to 7 drones for the red line, from 5 to 8 for the blue line and from 4 to 9 for the green line.

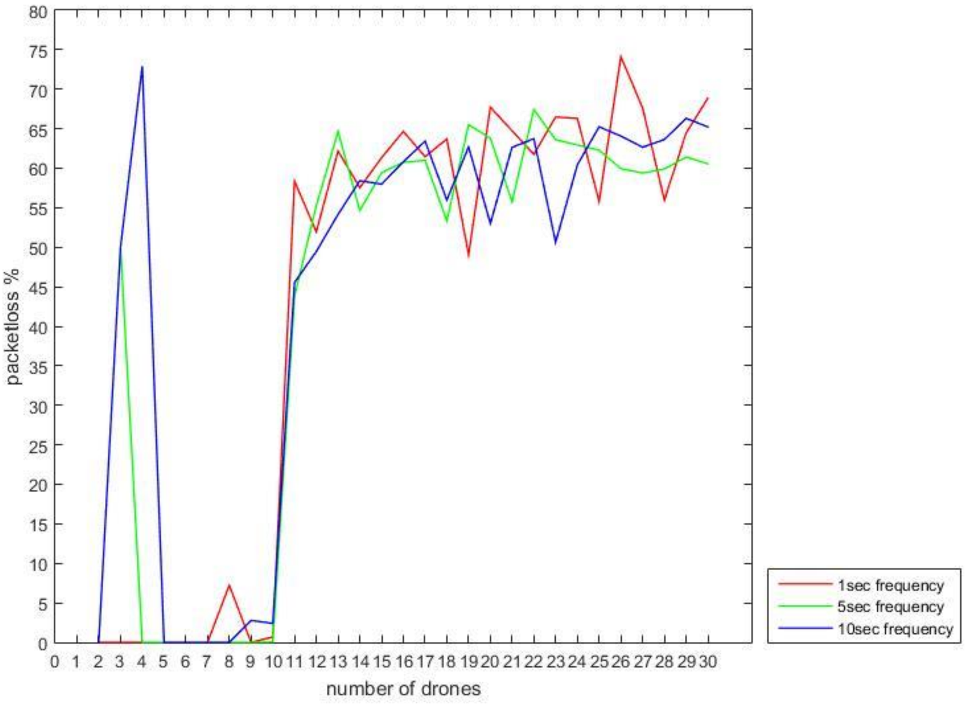

Figure 45: packet loss vs number of drones for 1,5,10 sec packet frequency

In Figure 46, it can be referred that, if we exclude the step ups in the middle of the length in 10 seconds frequency curve, there is less jitter for bigger frequency values. On top of that, as the number of drones increases, the jitter rises,too. The biggest value is 3.5 x 10 ^ 10 nanoseconds and occurs at/on the blue line for 18 drones. The least value is from 2 up to 11 drones for all curves in almost all this length.

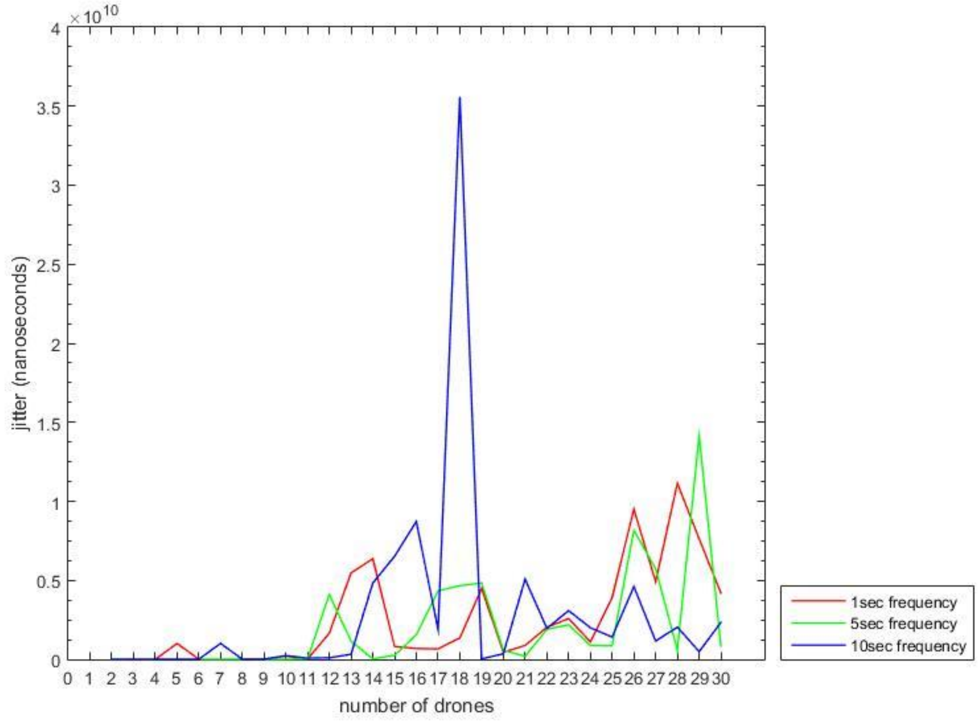

Figure 46: jitter vs number of drones for 1,5,10 sec packet frequency

In the same way, regarding 802.11ac throughput that is shown in Figure 47 below, it is derived that as the number of drones increases, the bigger the throughput value grows. For all the curves we have about the same throughput values, we come to the conclusion that there is more throughputfor bigger frequency values. The biggest value is about 3 x 10 ^ 15 bps and occurs at/on the green line for 30 drones. The least value is 4096 and occurs for 2 drones at/on the red line, from 2 to 3 drones at the green line and from 2 to 4 drones at/on the blue line.

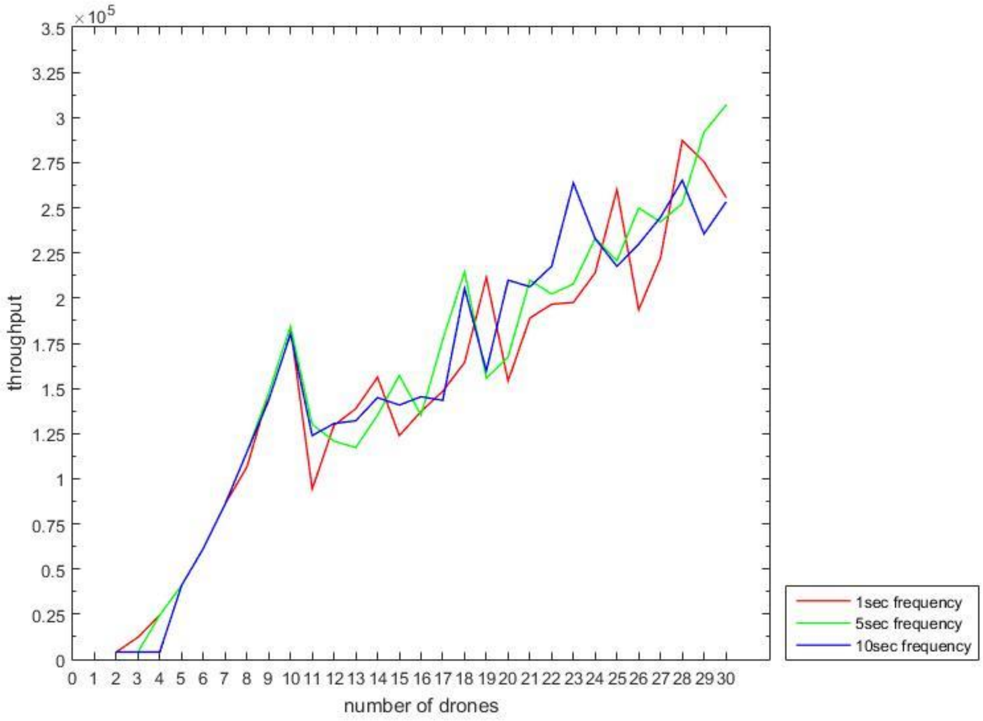

Figure 47: throughput vs number of drones for 1,5,10 sec packet frequency

As it is clearly seen in the Figures 48-51 below there are three lines:

-1 second packet frequency

-5 seconds packet frequency

-10 seconds packet frequency

We keep constant these packet frequencies in each line and we calculate the delay, jitter packet loss and throughput from 1 mb packet size up to 5 mb

.

At the beginning of Figure 48, it is displayed that the curve of 5 seconds frequency is higher on the axes of y than the curve of 10 seconds frequency, that means from 1 to about 2.8 mb packet size there is more delay for smaller frequency values. From 3 mb packet size though,there is overall greater delay for bigger frequency values. Nevertheless, it is clearly viewed that there are a lot of fluctuations for all curves, therefore the packet size matters a lot. The biggest value is about 11 x 10 ^ 9 nanoseconds which occurs at/on blue line at 4 mb packet size. The least value is about 1 x 10 ^ 9 nanoseconds which occurs at 4 mb packet size for the red curve and at 3 mb packet size for the green curve.

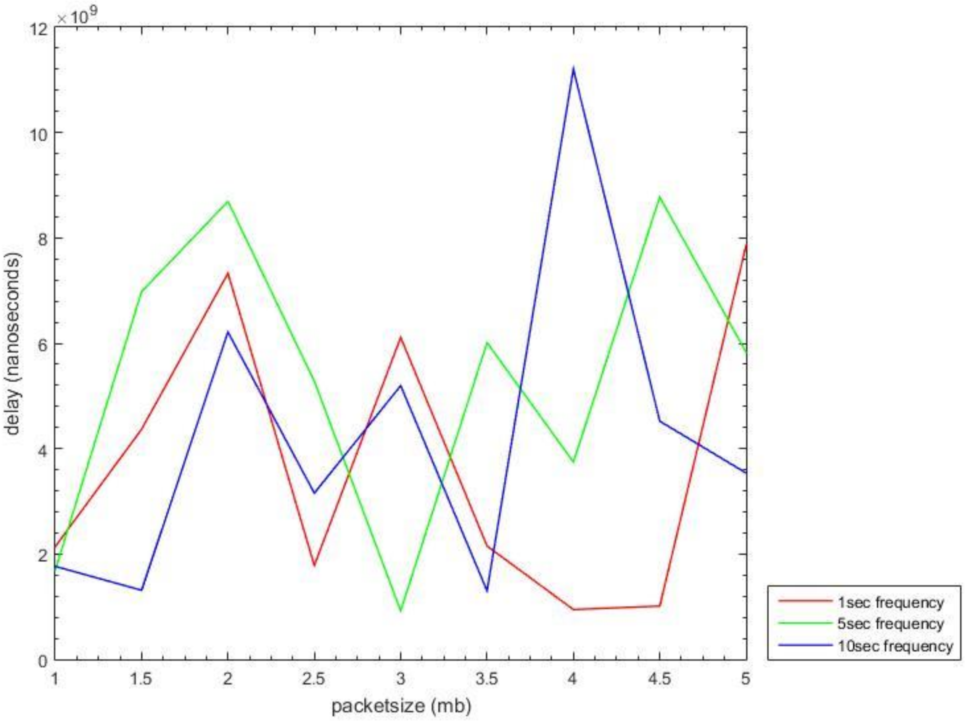

Figure 48: delay vs packet size for 1,5,10 sec packet frequency

Packet loss, on the other hand is equally distributed in all curves' length, as shown in Figure 49. We cannot draw a conclusion for which has the less overall, so we can say that the differences are negligible. Consequently, different frequencies with different packet sizes do not affect packet loss percentagesthat much.The biggest percentage is about 70% for the blue line at 3.5 mb packet size and at 4 mb packet size for the green one. The least percentage occurs at 1.5 mb packet size for both green and red curves.

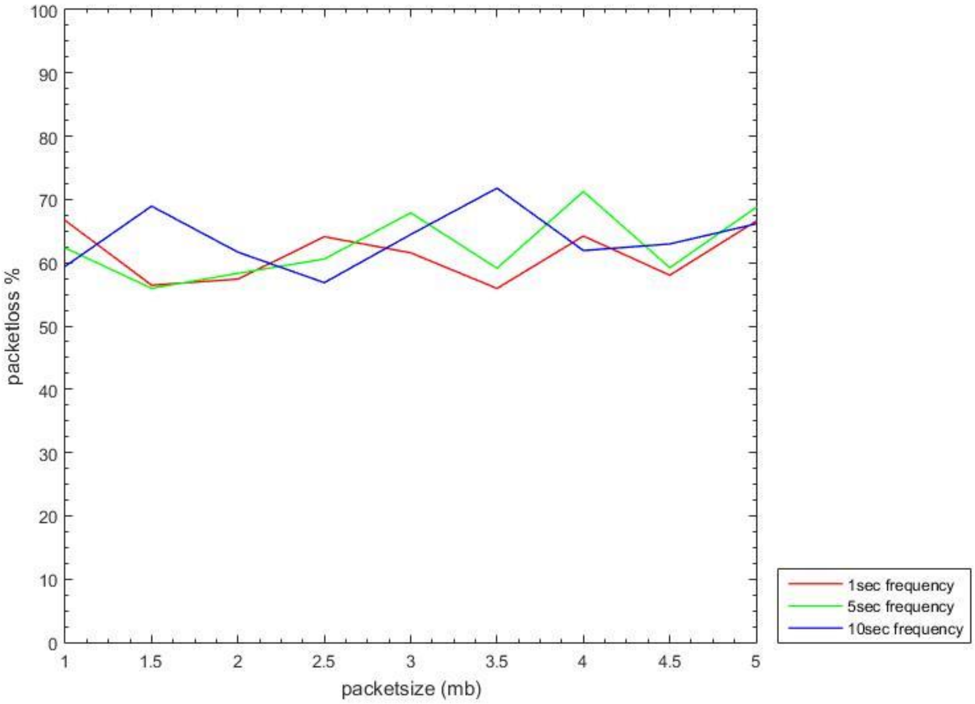

Figure 49: packet loss vs packet size for 1,5,10 sec packet frequency

In Figure 50, concerning jitter, it is indicated that at 2,3 and 4 mb packet size, there are almost the biggest jitter values. The 10 second frequency curve has a more stable jitter over its length. The 5 seconds frequency acquires more jitter as the packet size increases. The 1 second frequency curve presents less jitter for smaller packet sizes. The biggest value is about 11.75 x 10 ^ 9 nanoseconds and occurs at the green line for 4.5 mb packet size. The least amount of jitter occurs at 2.5 and 4 mb packet size for the red line and at 3 mb packet size for the green line.

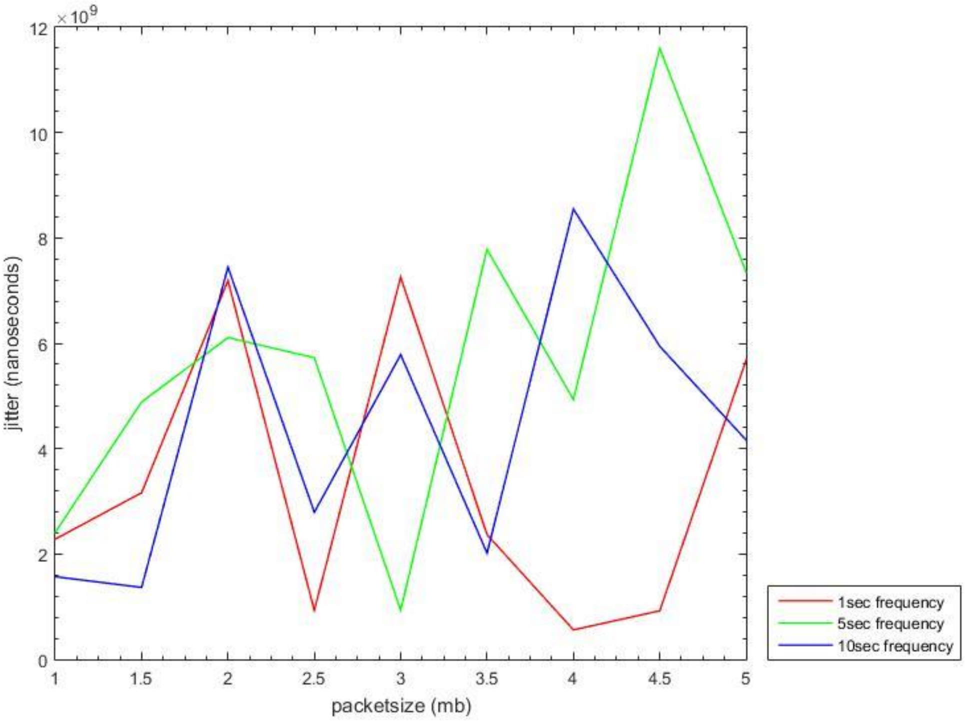

Figure 50: jitter vs packet size for 1,5,10 sec packet frequency

What is deduced from Figure 51 is that packet size has a considerable impact on throughput. On the 10 second frequency curve, it is also noticed that at 1, 2.5 and 5 mb packet size, there is the biggest throughput values in this frequency. In the 5 seconds curve there are the biggest values of throughput at about 1.6, 3.5 and 4.5 mb packet size. In the 1 second packet size the biggest values of throughput are at 2, 3.5 and 5 mb packet size. All in all, it cannot be inferred which curve produces the best result because all the lines present a lot of rapid changes .The biggest value of throughput is about 3.3 x 10 ^ 5 bps and occurs at 1.5 mb packet size for the green line and at 5 mb packet size for the blue line.

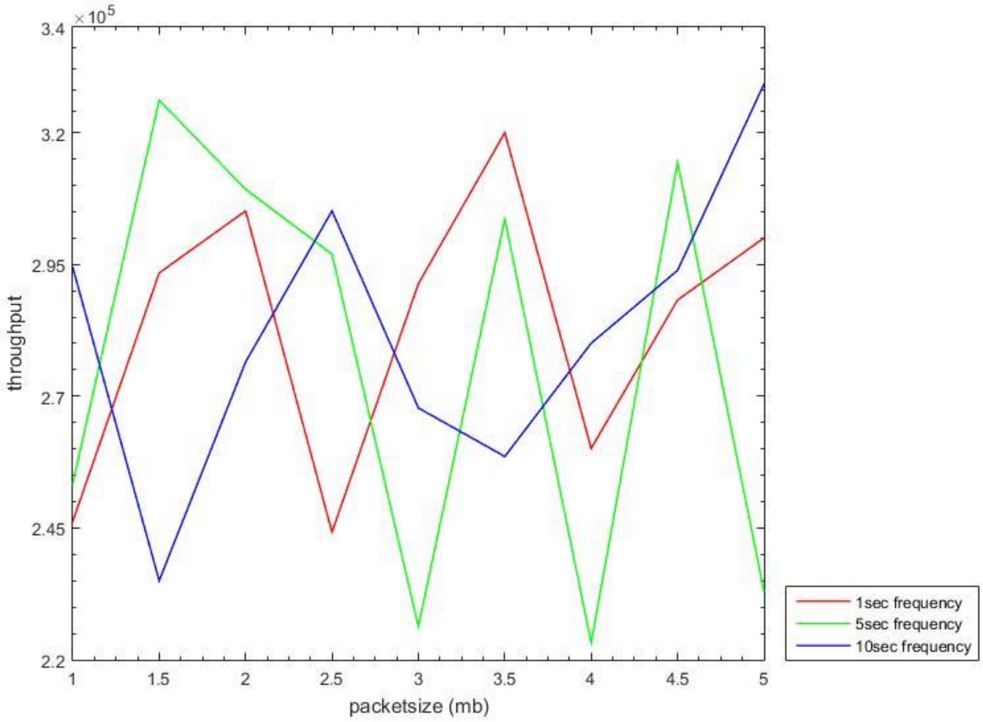

Figure 51: throughput vs packet size for 1,5,10 sec packet frequency

There are three lines in the following 43-46 Figures:

-10 number of drones

-20 number of drones

-30 number of drones

We keep constant/unchanged/steady these number of drones in each line and we calculate the delay, jitter packet loss and throughput from 1 second frequency up to 10 seconds.

In Figure 43, it is suggested that for the 10 drones' curve there is almost no delay. The 20 drones' curve has a lot of delay from 1 to 3 seconds frequency andthen there is a significant fall. The 30 drones' line presents a lot of oscillations but overall delay keeps at low levels. It is also deduced that for the 20 drones' line there is more delay for smaller values of packet frequency and for the 30 drones' line there is bigger value of delay for bigger values of frequency. The biggest value is a lot more than 12 x 10 ^ 6 microseconds and occurs at/on the green line at 2 seconds frequency. The least value is almost 0 microseconds for the blue line at 5 seconds frequency.

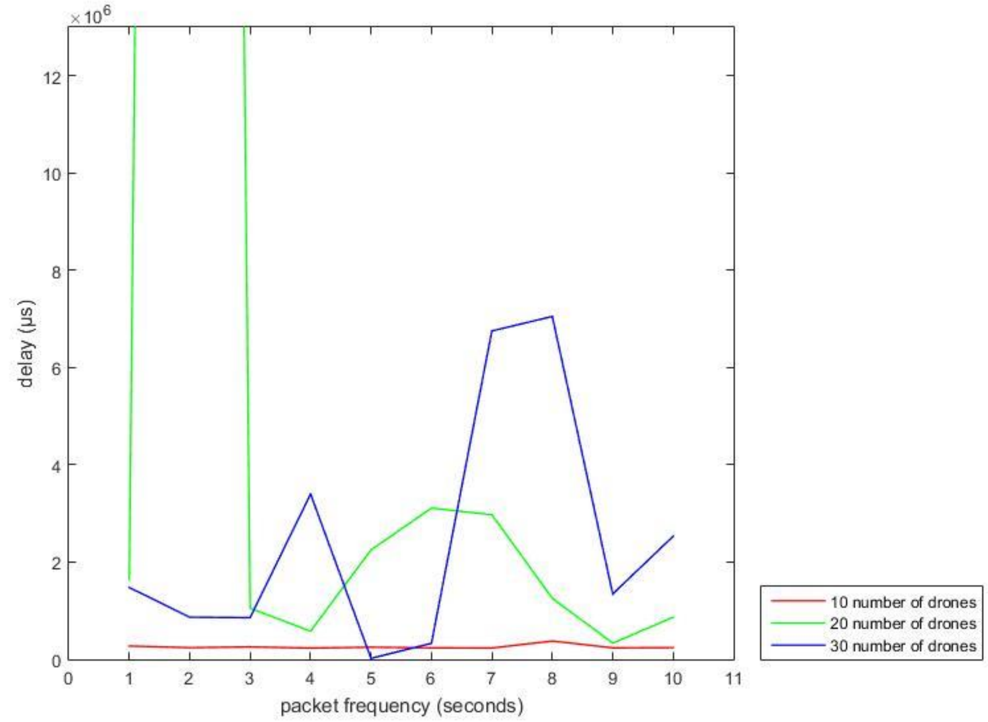

Figure 52: delay vs packet frequency for 10,20,30 number of drones

Figure 44 leads to the conclusion that frequency doesn't affect the packet loss percentage that much. For 10 number of drones, the smallest percentages of packet loss are spotted. For 20 and 30 number of drones almost no difference is noticed, although it could be said that the bigger the number of drones is, the greater the packet loss becomes. The biggest value is almost 70% for 4 seconds frequency at the blue line. The least percentage is at 0, 6- and 8-seconds packet frequency that appears at/on the red line.

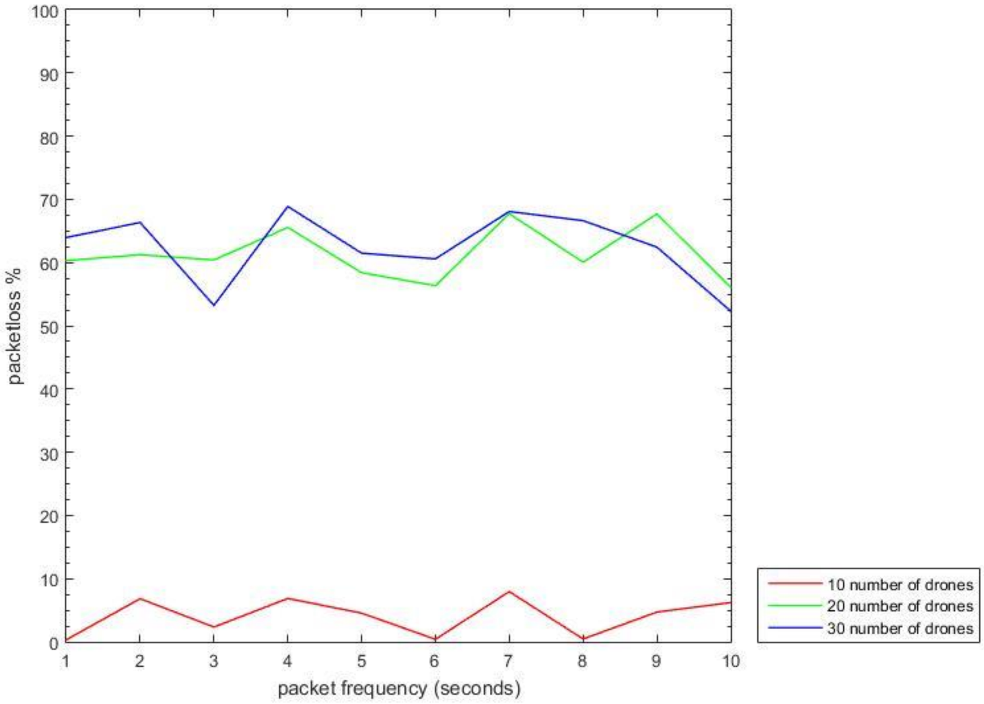

Figure 53: packet loss vs packet frequency for 10,20,30 number of drones

Likewise, in 10drones'linethere isalmost no jitter as seen in Figure 45. For 20 drones more jitteris presented thanonthe line of 30 drones.Additionally, smaller frequenciespresentmorejitter forthe20drones'curve and less jitterforthe30drones'curve.

At last,the smallestvalues for jitter in all 3 curves are at about 4 to 5 seconds packet frequency. The biggest value is a lot more than 10 x 10 ^ 5 microseconds and occurs atthegreen line for 2 seconds packet frequency. The least value is almost 0 microseconds and occurs in almost all the length ofthered line and at 5 seconds packet frequency for the blue line.

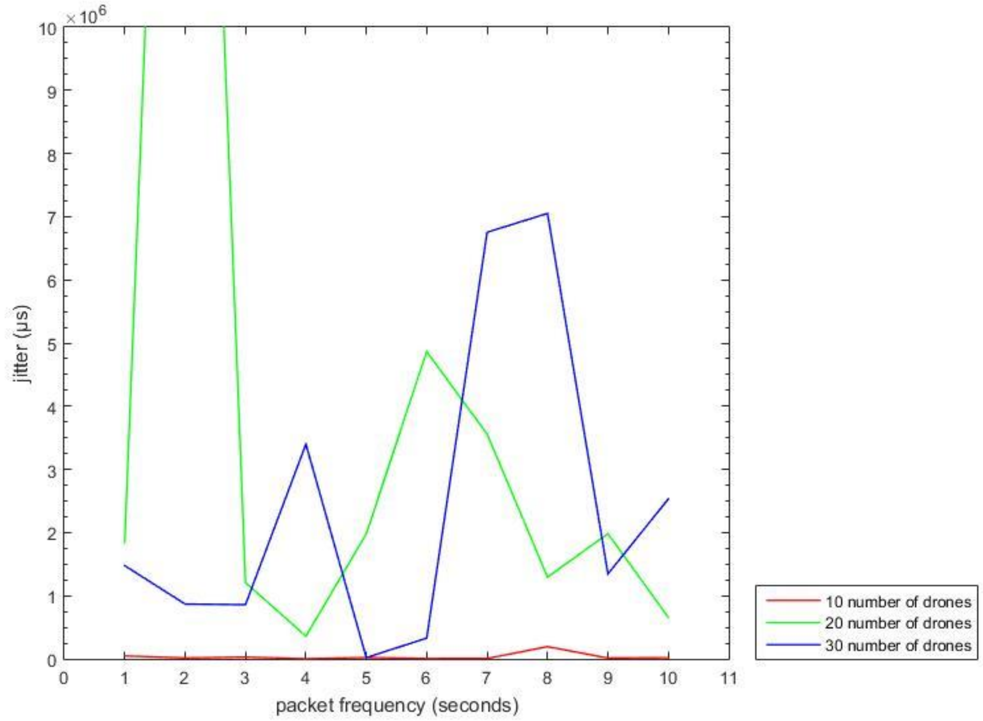

Figure 54: jitter vs packet frequency for 10,20,30 number of drones

In the Figure 46, it seems that for the curve of 10 drones there is almost steady throughput in its full length. The other 2 curves produce a lot of waves, although it is clear that for 30 drones there are the biggest values of throughput. Therefore, it is inferred that frequency affects the 20 and 30 drones' lines greatly, whereas the 10 drones' line is not influenced that much. The biggest value is more than 3.25 x 10 ^ 5 bps which occurs at/on the blue line at 3 seconds packet frequency. The least value appears in the same curve at 4 seconds frequency which is about 1.25 x 10 ^ 5 bps.

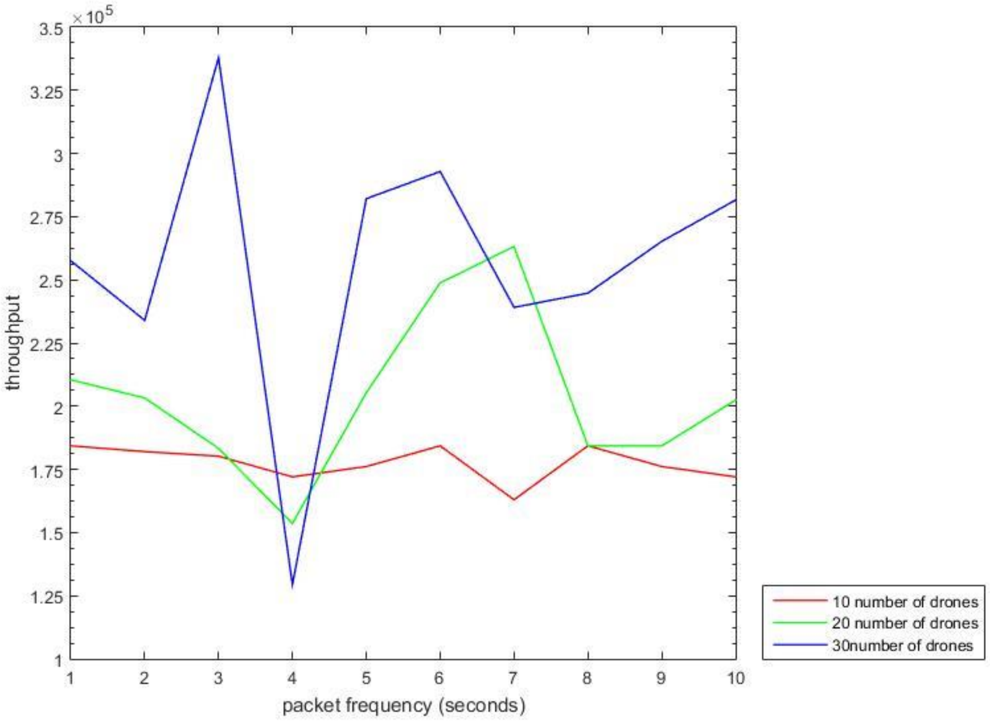

Figure 55: throughput vs packet frequency for 10,20,30 number of drones

There are three lines in the next 47-50 Figures:

-10 number of drones

-20 number of drones

-30 number of drones

We keep constant these number of drones in each line and we calculate the delay, jitter packet loss and throughput from 1 mb packet size up to 5 mb.

In Figure 47, it is noted that for 10 drones there is not considerable delay in different packet frequencies. As expected, for more drones there are bigger delay values. It is obvious that for 20 and 30 drones' curves there are a lot of palpitations, thus the packet size affects these curves significantly. At 1, 2.5, 4 and 5 mb packet sizes, the smallest delay values are observed in the 30 drones' curve. At 1.5, 4 and 5 mb packet size there are the smallest values of delay in 20 drones curve. The biggest value is at 3 mb packet size for the blue line and has a value of more than 6 x 10^ 9 nanoseconds. The least value is about 0.125 x 10 ^ 9 nanoseconds at 1.5 mb packet size for the red line.

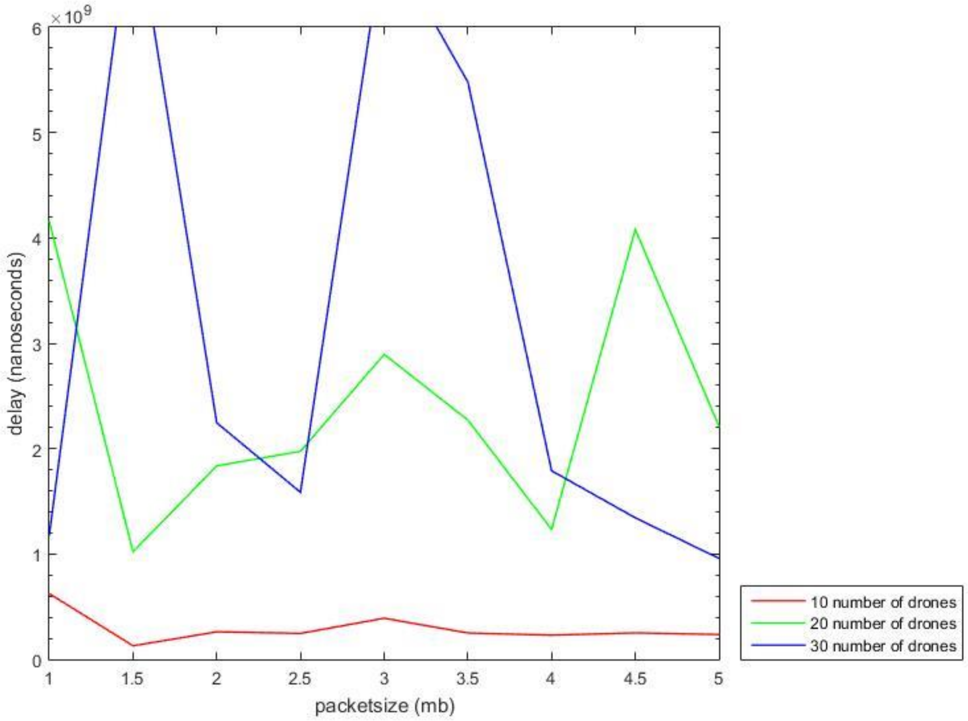

Figure 56: delay vs packet size for 10,20,30 number of drones

In Figure 48, it is deduced that packet size doesn't affect packet loss considerably, although it is seen that for greater number of drones, bigger packet loss percentages exist. Eventually, it is suggested that the least amount of packet loss is marked at the 10 drones' curve. The biggest value is about 71% and occursat the blue curve at 2 mb packet size. The least value is about 2.5 % and appears at 1.5, 3.5 and 4.5 mb packet size for the red line.

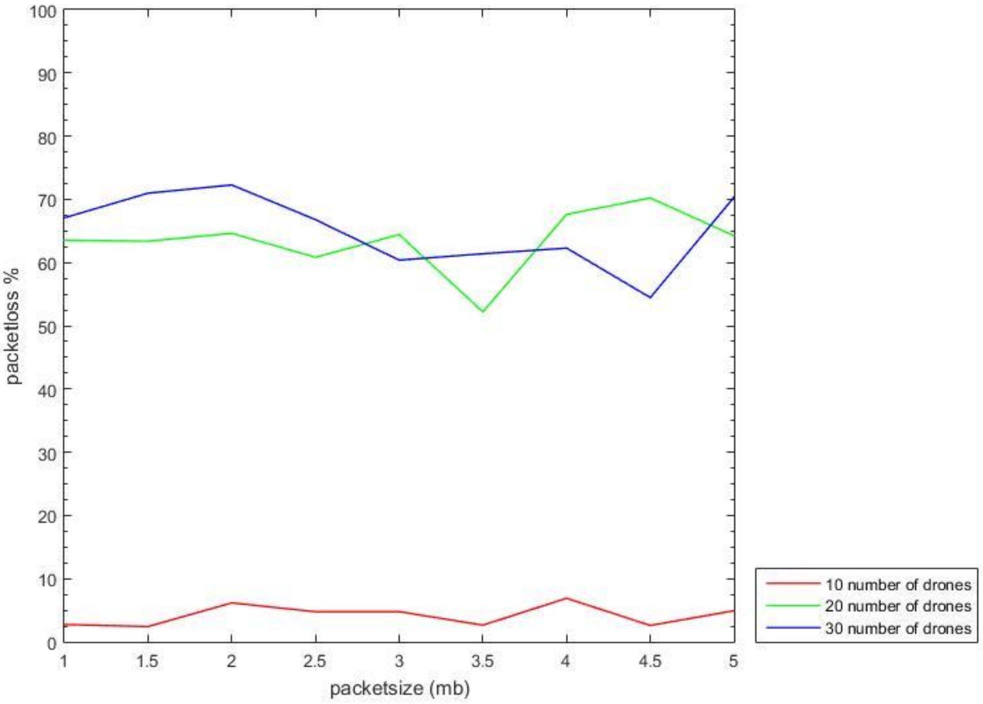

Figure 57: packet loss vs packet size for 10,20,30 number of drones

In the Figure 49, it is shown that in the 10 number of drones’curve, there is almost no jitter for different packet size values. In the 20 and 30 drones’ curve, it is seen that there are a lot of fluctuations and also that the packet size affects the jitter values greatly. In the 20 drones’ curve, the least amount of jitter is noticed at 1.5, 3.5 and 5 mb packet size. In the 30 drones’ curve the least amount of jitter is spotted at 1, 2.5 and 5 mb packet size. The biggest value is more than 10 x 10 ^ 9 at for 4 mb packet size on the green line. The least value is almost 0 from 1.5 to 2.5 and from 3.5 to 5 mb packet size on the red line.

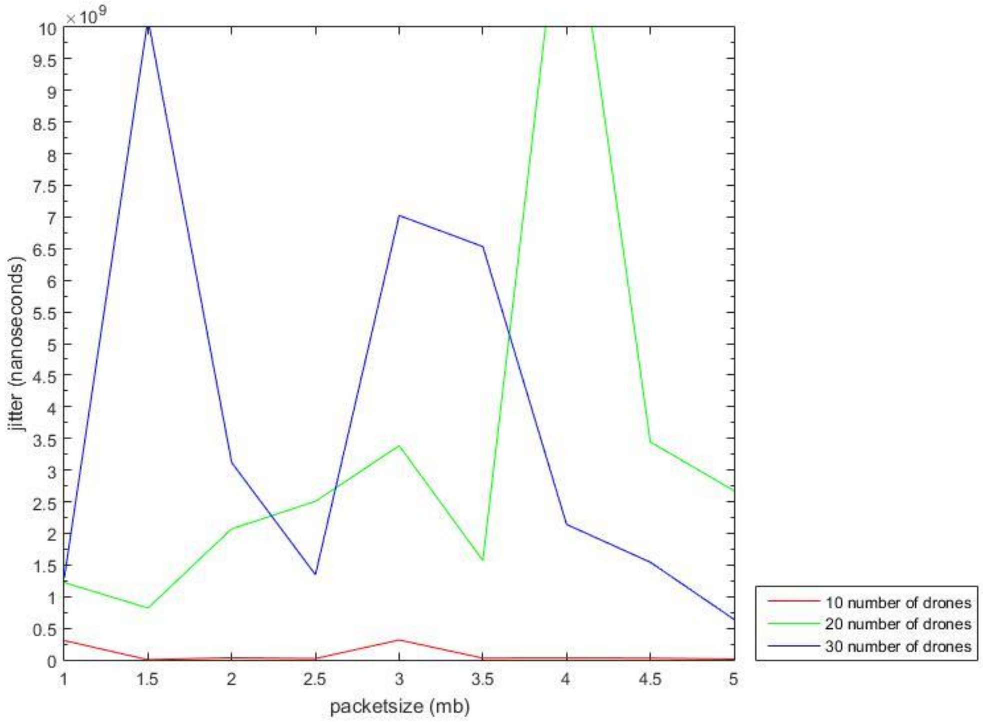

Figure 58: jitter vs packet size for 10,20,30 number of drones

In the Figure 50, packet size affects the throughput values more as the number of drones rises. For 10 drones there are almost no fluctuations and the throughput remains almost unchanged. In 20 drones' curve, there are bigger throughput values as the packet size increases. In addition, in 30 drones' curve, bigger throughput values are noticed for bigger packet size values. Overall, the biggest throughput value is 3.25 x 10 ^ 5 bps and occurs at 3 mb packet size for 30 drones. The least amount of throughput is met at 4.5 mb packet size for 20 number of drones with a value of less than 1.75 x 10 ^ 5 bps.

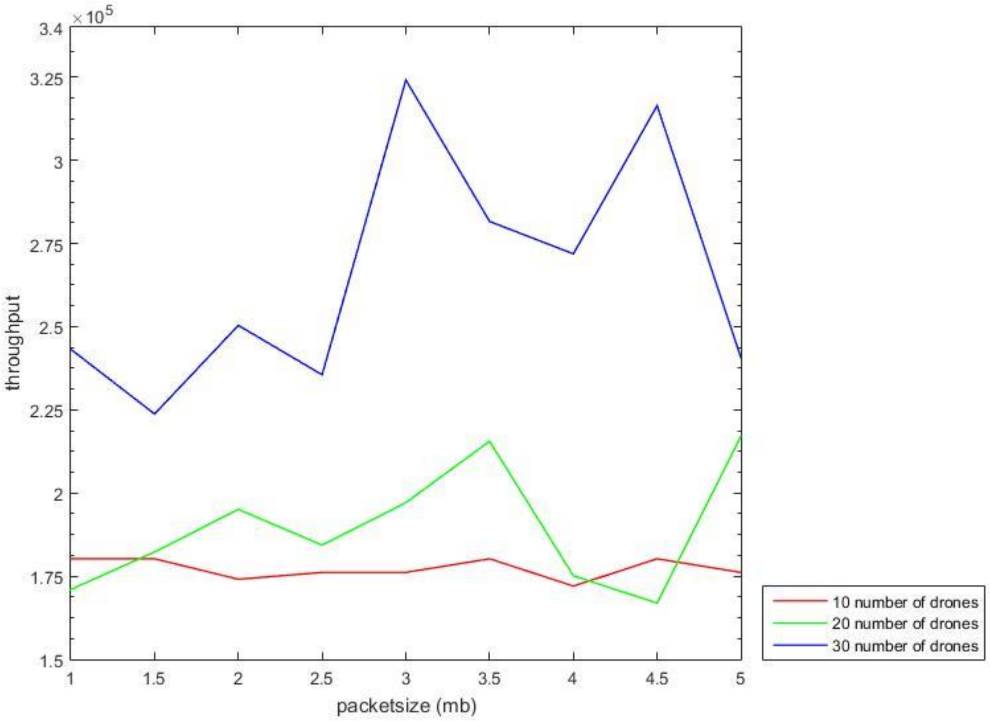

Figure 59: throughput vs packet size for 10,20,30 number of drones

5.4 – Summary of the chapter

In this Chapter we saw simulation all the graphs that we took as result from our experiment about the IEEE 802.11n and IEEE 802.11ac standards. We analyzed every single graphand thus we understood the pros and cons in every scenario for our network. In the next Chapter we will draw the conclusions from the experiment as well as we will demonstrate open issues and future challenges.

CHAPTER 6–CONCLUSION AND OPEN CHALLENGES

6.1 – Review

During this thesis, an analysis was made of the basic features of UAVs and of the applications they may have. The limitations as well as the rules governing the movement and the flight of drones in Greece and abroad were studied. Through the experiment, wireless networking technologies have been studied that can be used for corresponding IoT applications. All of this was evaluated and the research future challenges were recorded, giving importance to technological issues.

6.2 – Conclusion

Unquestionably, both standards have pros and cons. After all, scientific target determines what is regarded positive or negative. Considering 802.11 n standard, it is suggested that if a network with less amount of delay, jitter and packet loss is needed, the best case scenario has to do with taking 10 drones and creating 5mb packets every 6 seconds. These values present the least amount of the metrics which were mentioned above with the highest able throughput. On the other hand, if more throughput is wanted and more loss does not cause problems, then it's will be the users' decision how they will take advantage of their drone network. In relation to 802.11 ac standard,the best possible outcome for minimum losses has to do with 27 drones with 5 mb packet size creating these packets every 10 seconds. Nevertheless, this doesn't mean that it is highly recommended / necessary to use these values (exactly) because as we have already said it depends on the subject. To sum up, It is clearly proved that 802.11 ac has the biggest throughput values and the least delay and jitter for a bigger number of drones.

With reference to 802.11 n, it can be noted that there may be worst values at the same spots but for 2 up to 10 drones there is better performance overall with less losses than the 802.11 ac. This thesis is structured so we can have a look at these two standards and compare them. It is not aimed at recommending the one over the other. Generally, 802.11 n is older than 802.11 ac, so we should see improvement. The 802.11 ac standard has been designed to give us more throughput values as we have said above but practically this doesn't mean that we could achieve this. As far as 802.11 ac is concerned, it has the headroom to support up to 8 antennas at over 400Mbps each but the fastest router to date only has four antennas. The reason for that is the fact that antennas add cost and take up space. Last but not least, as it has already been mentioned, this thesis has been written so thatwe can evaluate the benefits in different situations and select what is suitable, ideal and affordable for our current usage.

6.3 – Future research

The growing frequency of increased use of drones in disaster management, underlines their important role. However, their use in such businesses raises a number of legal and ethical issues and reservations that need to be addressed. The great dangers in the implementation of drones systems revolve around issues of public safety and order. A key problem is the inclusion of drones in the national airspace system, as they often interfere with air traffic and create a series of dysfunctions. There is also the possibility of an accident from the use of drones (sudden drop, damage to propellers, collision of two drones or simple failure of the material). Typical is the case in San Gabriel, California in 2016, which burned more than 5,200 hectares, hundreds of residents vacated their homes and 900 firefighters attempted in the area. On 26/6/2016 the drones abandoned the firefighting operations due to the danger that existed from the uncontrolled flight of private drones in the area. At the same time, their technology is still often lagging behind in difficult weather conditions due to its low weight and low propulsion power. They are more sensitive to wind gusts, heavy rain or high temperatures, which increases the risk of an accident. Damage may also be the main purpose of drones, for example, terrorist acts or hacking.

The presence of drones brings to mind images of battle with "drones-killers" armed with missiles whose purpose is to kill and destroy. In fact, most of the technology developed for drones is designed for intelligence, surveillance and recognition.

This technology can be adapted and applied in times of peace and in emergency situations. Drones technology provides access to areas that were not accessible by law enforcement or non-law enforcement agencies. Frequently raised issues of protection of victims' personal data and questions as to whether the use of drones is permissible in disaster management operations. Finding the balance between the flexibility required for the immediate response and the protection of individual rights is difficult. A US public opinion on the use of drones by the police showed public disapproval of 65% [41]. This research is worrying, considering the prominent role of the police during a disastrous incident.

The public debate on privacy and security has led to a legislative definition of the use of drones. The use of drones in European countries is determined by the regulations established by the National Civil Aviation Authorities, which retain the responsibility and authority to issue permits for use. The European Commission has issued guidelines but does not interfere with national agencies. Some CAAs in the countries of Europe have issued the necessary instructions, others are in the issuing phase, while others have not yet raised the issue. The central directions of the majority of Europe's states is that a drone with a gross take-off weight of less than 25 kilograms should be flown by a visual contact with his operator at a height of less than 500 feet.

In Greek National Law the use of drones was regulated by the recent publication of the "Unmanned Aircraft Systems - UAS" Regulation. In practice, the implementation of the above institutional arrangements presents considerable difficulties in the management of emergency situations with the support of drones. In the US, although there have been several serious cases where drones have been used to relieve disasters in other countries, they do not like to use them due to regulatory and legislative constraints within the country [42]. For example, one of the issues with the use of a drone in dealing with disasters and recovery efforts is the legal obligation to provide a detailed description of the operation, including the classification of the airspace to be used. This information is often unknown before the catastrophe arrives. Neither the extent of the deviation services (state bodies, voluntary organizations, citizens, etc.) that are involved will be known until the advent of the event. Not knowing this information makes it unlawful to operate a drone as part of disaster relief and rehabilitation efforts. The use of this technology can easily provide vital information about services that are responsible for search and rescue and damage assessment. Issues of privacy, sensitive personal data, and privacy by the use of drone in emergency operations require clear policies.

As to the handling of public data and information collected (who has access, who they are distributed, how much they are stored, how the information is stolen, etc.). There is no doubt that not only state but also humanitarian actors will continue to use drones as technology becomes more accessible and accessible. However, to make full use of these sites, policy-makers should develop a supportive legal and regulatory framework as well as clear guidelines and rules in line with international humanitarian law.

Due to privacy concerns and the need for data security, encryption of data should be considered as a disaster management solution in order to avoid piracy by malicious actors. It must be ensured that the information collected by the drones will only be used for thepurpose they are collected. Encryption of control signals and data relayed by drones to missions is already technologically feasible. Wide consultation is required with the relevant bodies (CAA, drones pilot associations, emergency managers, research and university institutes, etc.) on the issues of privacy and property protection from the use of drones under the supervision of the General Secretariat for Civil Protection, as a coordinating body in order to develop a regulatory and regulatory framework that will encourage the optimal operational use of drones in emergencies.

BIBLIOGRAPHY

[1] E. W. Frew and T. X. Brown, “Airborne communication networks for small unmanned aircraft systems,” Proc. IEEE, vol. 96, no. 12,pp. 2008–2027, Dec. 2008.

[2] J. Li, Y. Zhou, and L. Lamont, “Communication architectures and protocols for networking unmanned aerial vehicles,” in Proceedings of IEEE Globecom Workshops, pp. 1415–1420, 2013.

[3] I. Dalmasso, I. Galletti, R. Giuliano, and F. Mazzenga, “WiMAX networks for emergency management based on UAVs,” in Proc. IEEE 1stAESS Eur. Conf. Satell. Telecommun. (ESTEL), pp. 1–6, 2012.

[4] S. Rosati, K. Kruzelecki, L. Traynard, and B. Rimoldi, “Speed-aware routing for UAV ad-hoc networks,” in Proc. IEEE Globecom Workshops (GC Wkshps), pp. 1367–1373, 2013.

[5] S. Morgenthaler, T. Braun, Z. Zhao, T. Staub, and M. Anwander, “UAVNet: A mobile wireless mesh network using unmanned aerialvehicles,” in Proc. IEEE Globecom Workshops (GC Wkshps’12), pp. 1603–1608, 2012.

[6] F. J. Watkins, R. A. Hinojosa, and A. M. Oddershede, “Alternative wireless network technology implementation for rural zones”, Int. J. Comput. Commun. Control, vol. 8, no. 1, pp. 161–165, Feb 2013.

[7] Y. Wang and Y. J. Zhao, “Fundamental issues in systematic design of airborne networks for aviation,” IEEE Aerosp. Conf., pp. 1721–1728, 2006.

[8] A. P. Athreya and P. Tague, “Network self-organization in the internet of things,” in Proc. IEEE Int. Workshop IoT Netw. Control (IoT-NC’13), pp. 25–33, Jun. 2013.

[9] P. Sharnya and J. S. Raj, “Self organizing wireless mesh network,” Int. J. Innov. Appl. Stud., vol. 3, no. 2, pp. 486–492, Jun. 2013.

[10] M. Mendonca, B. N. Astuto, K. Obraczka, and T. Turletti, “Software defined networking for heterogeneous networks,” IEEE MMTC E-Lett.,vol. 8, no. 3, pp. 36–39, May 2013.

[11] I. Ku et al., “Towards software-defined VANET: Architecture and services,” in Proc. 13th Annu. Mediterr. Ad Hoc Netw. Workshop(MED-HOC-NET’14), pp. 103–110, 2014.

[12] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, “Software defined wireless networks: Unbridling SDNs,” in Proc. Eur. Workshop Software Defined Netw. (EWSDN’12), pp. 1–6, 2012.

[13] Open Networking Foundation (ONF). (2013, Sep.). OpenFlowTM Enabled Mobile and Wireless Networks, ONF Solution Brief [Online].
Available: sdn-resources/solution-briefs/sb-wireless-mobile.pdf (accessed on Oct. 2014).

[14] N. McKeown et al., “OpenFlow: Enabling innovation in campus networks,” ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008.

[15] A. Detti, C. Pisa, S. Salsano, and N. Blefari-Melazzi, “Wireless mesh software defined networks (wmSDN),” in Proc. IEEE 9th Int. Conf.Wireless Mobile Comput. Netw. Commun. (WiMob’13), pp. 89–95, Oct. 2013.

[16] M. A. Goodrich, B. S. Morse, D. Gerhardt, J. L. Cooper, M. Quigley, J. A. Adams, and C. Humphrey, “Supporting wilderness search and rescue using a camera-equipped mini UAV,” Journal of Field Robotics, vol. 25, no. 1-2, pp. 89–110, 2008.

[17] S. Waharte, N. Trigoni, and S. Julier, “Coordinated search with a swarm of UAVs,” in Proc. IEEE Conf. Sensor, Mesh and Ad Hoc Commun. and Networks Workshops, pp. 1–3, Jun. 2009.

[18] F. Jiang and A. Swindlehurst, “Dynamic UAV relay positioning for the ground-to-air uplink,” in GLOBECOM Workshops (GC Wkshps), pp. 1766–1770, Dec. 2010.

[19] M. Asadpour, D. Giustiniano, K. A. Hummel, S. Heimlicher, and S. Egli, “Now or later?: delaying data transfer in time-critical aerial communication,” in Proc. ACM Conf. on emerging Networking Experiments and Technologies (CoNEXT), pp. 127–132, 2013.

[20] A. Alshbatat and L. Dong, “Adaptive MAC protocol for UAV communication networks using directional antennas,” in Proc. IEEE Int. Conf. on Networking, Sensing and Control (ICNSC), pp. 598–603, Apr. 2010.

[21] Samira Hayat, Evsen Yanmaz, and Raheeb Muzaffar ,“Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint”, IEEE Communications Surveys & Tutorials, Volume: 18, Issue: 4, pp. 2624-2661, 29 April 2016.

[22] Lav Gupta, Raj Jain and Gabor Vaszkun, “Survey of Important Issues in UAV Communication Networks”, IEEE Communications Surveys & Tutorials, Volume: 18, Issue: 2, pp. 1123-1152, 03 November 2015

[23] Milan Erdelj, Enrico Natalizio Sorbonne, Kaushik R. Chowdhury, “Help from the Sky: Leveraging UAVs for Disaster Management”, IEEE Pervasive Computing, Volume: 16, Issue: 1, pp. 24-32, 05 January 2017

[24] Azade Fotouhi, Ming Ding and Mahbub Hassan, “Understanding Autonomous Drone Maneuverability for Internet of Things Applications”, 2017 IEEE 18th

International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 13 July 2017

[25] Jingjing Wang, Chunxiao Jiang, Zhu Han, Yong Ren, Robert G. Maunder, and Lajos Hanzo, "Taking Drones to the Next Level: Cooperative Distributed Unmanned-Aerial-Vehicular Networks for Small and Mini Drones", IEEE Vehicular Technology Magazine, Volume: 12, Issue: 3, 28 July 2017

[26] G. Tuna, V.C. Gungor, and K. Gulez,"An Autonomous Wireless Sensor NetworkDeployment System Using MobileRobots for Human Existence Detection in Case of Disasters," Ad Hoc Networks, pp. 54–68,Feb. 2014.

[27] S. George et al., "DistressNet: A WirelessAd-Hoc and Sensor Network Architecturefor Situation Management inDisaster Response," IEEE CommunicationsMagazine, vol. 48, no. 3, pp. 128–136, 2010.

[28] M. Di Felice et al., "Self-OrganizingAerial Mesh Networks for Emergency Communication," IEEE Symp. Personal,Indoor, and Mobile Radio Communication (PIMRC), 2014.

[29] I.F. Akyildiz et al., "SoftAir: A SoftwareDefined Networking Architecture for 5G Wireless Systems," Computer Networks, pp. 1–18. 2015.

[30]G.-J. Kruijff et al., "Rescue Robots atEarthquake-Hit Mirandola, Italy: A Field Report," Proc. 2012 IEEE Symp. Safety,Security, and Rescue Robotics (SSRR), 2012.

[31] Tony Michel, Bishal Thapa and Steve Taylor, "802.11s based Multi-radio Multi-Channel Mesh Networking for Fractionated Spacecraft", 2013 IEEE Aerospace Conference, 13 May 2013.

[32] Sara Koulali, Essaid Sabir, Tarik Taleb, and Mostafa Azizi, "A Green Strategic Activity Scheduling for UAV Networks: A Sub-Modular Game Perspective", IEEE Communications Magazine, Volume: 54, Issue: 5, 18 May 2016.

[33] Jongho Won, Seung-Hyun Seo, Elisa Bertino, "A Secure Communication Protocol for Drones and Smart Objects", Proceeding ASIA CCS '15 Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp. 249-260, 2015.

[34] Aymen Jaziri, RidhaNasri and Tijani Chahed, "Congestion Mitigation in 5G Networks using Drone relays", 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 29 September 2016.

[35] Samira Hayat, EvsenYanmaz, Timothy X Brown, and Christian Bettstetter "Multi-Objective UAV Path Planning for Search and Rescue", 2017 IEEE International Conference on Robotics and Automation (ICRA), 24 July 2017.

[36] Satria, Muhammad Haikal, Muhammad Akmal Ayob, Eko Supriyanto and Jasmy bin Yunus. “Wireless Mesh Telemedicine Simulation on ns 3”.

[37] Alamsyah, Mauridhi Hery Purnomo, I Ketut Edy Purnama, “Performance of The Routing Protocols AODV, DSDV and OLSR in Health Monitoring Using NS3”, 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), 23 January 2017.

[38] “Performance Evaluation of OLSR and AODV in VANET Cloud Computing Using Fading Model With SUMO and NS3”, 2015 International Conference on Cloud Computing (ICCC), 09 July 2015.

[39] Marc Esquius, “IEEE 802.11s Mesh Networking Evaluation under NS-3”, upcommons.upc.edu/bitstream/handle/2099.1/12595/PFCE_Marc_Esquius.pdf, April 2011

[40] Kirill Andreev, Pavel Boyko, “IEEE 802.11s Mesh Networking NS-3 Model”, https://www.nsnam.org/workshops/wns3-2010/dot11s.pdf.

[41] Rasmussen “65% Oppose Use of Drones for U.S Police Work”,http://www.rasmussenreports.com/public_content/politics/general_politics/october_2013/65_oppose_use_of_drones_for_u_s_police_work (Last accessed October 28, 2013)

[42] Honig Z. 2011.T-Hawk UAV enters Fukushima danger zone, returns with video, Engadget, http://www.engadget.com/2011/04/21/t-hawk-uav-enters-fukushima-danger-zone-returns-with-video.

APPENDIX

```
int main (int argc, char *argv[])
{
  time_t currentTime;
  time (&currentTime);//Grab current time as seed if no seed is specified

  LogComponentEnable("DroneAdhoc", LOG_LEVEL_INFO);

  std::string phyMode ("OfdmRate9Mbps");

  uint32_t numDrones = 30;
  uint32_t maxX = 1000; // m
  uint32_t maxY = 1000; // m
  uint32_t collPacketSize = 1; // kilobytes (KB)
double collFrequency = 0.5; // seconds
  uint32_t imagePacketSize = 5; // megabytes (MB)
double imageFrequency = 10.0; // seconds
bool onStateChange = true;

  CommandLine cmd;

  cmd.AddValue ("numDrones", "number of drones in network", numDrones);
  cmd.AddValue ("maxY", "position of wall (top) for drone box (meters)",
maxY);
  cmd.AddValue ("maxX", "position of wall (right) for drone box
(meters)", maxX);
  cmd.AddValue ("collPacketSize", "collision detection packet size (KB)",
collPacketSize);
  cmd.AddValue ("collFrequency", "collision detection packet frequency
(seconds)", collFrequency);
  cmd.AddValue ("imagePacketSize", "image packet size (MB)",
imagePacketSize);
  cmd.AddValue ("imageFrequency", "image packet frequency (seconds)",
imageFrequency);
  cmd.AddValue ("onStateChange", "whether to adjust gains while idle.",
onStateChange);
  cmd.AddValue ("seed","seed for the RngSeedManager", currentTime);

  cmd.Parse (argc, argv);

  NS_LOG_INFO (std::to_string (currentTime));
  RngSeedManager::SetSeed (currentTime);

  std::string dimensions = std::to_string (maxX) + "x" + std::to_string
(maxY);
  std::string size = std::to_string (numDrones);
  std::string control = "";
if(!onStateChange){ control = "not-"; }
  control += "controlled";
  std::string signature = dimensions + "-" + size + "-" + control + "-" +
std::to_string (currentTime);
  Gnuplot throughput = Gnuplot ("data-throughput-"+signature+".png");
  std::vector<Gnuplot2dDataset> datasets = {};

  Ptr<DroneExperiment> experiment;

  experiment = CreateObject<DroneExperiment> ();
  experiment->SetAttribute ("NumDrones", UintegerValue (numDrones));
  experiment->SetAttribute ("MaxX", UintegerValue (maxX));
  experiment->SetAttribute ("MaxY", UintegerValue (maxY));
  experiment->SetAttribute ("CollisionPacketSize", UintegerValue
(collPacketSize*1024));
  experiment->SetAttribute ("CollisionPacketFrequency", DoubleValue
(collFrequency));
  experiment->SetAttribute ("ImagePacketSize", UintegerValue
(imagePacketSize*1024*1024));
  experiment->SetAttribute ("ImagePacketFrequency", DoubleValue
(imageFrequency));
  experiment->SetAttribute ("PHYmode", StringValue (phyMode));

  averages = std::to_string (numDrones);

//Start test

  datasets = experiment->Run (Rx, true, onStateChange);

  Graphgnu("Throughput_RX" , "Seconds" , "Throughput" , datasets[1]);

//End test

  throughput.AddDataset (datasets[1]);

return 0;
}
```