Reliability approaches in networked systems : Application on Unmanned Aerial Vehicles

Rana Abdallah

SPIM
Thèse de Doctorat

école doctorale sciences pour l'ingénieur et microtechniques
UNIVERSITÉ DE TECHNOLOGIE BELFORT-MONTBÉLIARD

Reliability approaches in networked systems – Application on Unmanned Aerial Vehicles

RANA ABDALLAH

SPIM
Thèse de Doctorat

école doctorale sciences pour l'ingénieur et microtechniques
UNIVERSITÉ DE TECHNOLOGIE BELFORT-MONTBÉLIARD

THÈSE présentée par

Rana ABDALLAH

pour obtenir le

Grade de Docteur de

L'Université de Technologie de Belfort-Montbéliard

Spécialité: **Sciences pour l'Ingénieur**

Approches de fiabilité dans les systèmes communicants - Application aux drones

Unité de Recherche :
FEMTO-ST/DISC/OMNI

Soutenue publiquement le 29 mai 2019 devant le jury composé de :

Président	JALEL BEN OTHMAN	Professeur des Universités, Université Paris 13
Rapporteur	ÉRIC CHATELET	Professeur des Universités, UTT
Rapporteur	PASCAL LORENZ	Professeur des Universités, UHA
Directeur de thèse	MAXIME WACK	Professeur Émérite, UTBM
Co-directeur de thèse	RAED KOUTA	Maître de Conférences HDR, UTBM
Co-directeur de thèse	JAAFAR GABER	Maître de Conférences HDR, UTBM

THESE DE DOCTORAT DE L'ETABLISSEMENT UNIVERSITE BOURGOGNE FRANCHE-COMTE

PREPAREE A UNIVERSITE DE TECHNOLOGIE DE BELFORT–MONTBELIARD

Ecole doctorale n° 37

École doctorale SPIM (Sciences Pour l'Ingénieur et Microtechniques)

Doctorat en Sciences Pour l'Ingénieur

Par

Mlle. ABDALLAH Rana

Reliability approaches in networked systems – Application on Unmanned Aerial Vehicles

Thèse présentée et soutenue à **Belfort**, le 29 Mai 2019

Composition du Jury :

M. BEN OTHMAN Jalel	Professeur des Universités, Univ. Paris 13	Président
M. CHATELET Éric	Professeur des Universités, UTT	Rapporteur
M. LORENZ Pascal	Professeur des Universités, UHA	Rapporteur
M. WACK Maxime	Professeur Émérite, UTBM	Directeur de thèse
M. KOUTA Raed	Maître de Conférences HDR, UTBM	Codirecteur de thèse
M.GABER Jaafar	Maître de Conférences HDR, UTBM	Codirecteur de thèse

Ask and it will be given to you; seek and you will find; knock and the door will be opened to you. For everyone who asks receives; the one who seeks finds; and to the one who knocks, the door will be opened.

(Matthew 7:7-8)

Preface

The research presented in this PhD. thesis, has been prepared in University of Bourgogne - Franche-Comté, UTBM, at the FEMTO-ST Institute of research (Franche-Comté Electronics Mechanics Thermal Science and Optics – Sciences and Technologies), the department DISC (OMNI team (Optimization, Mobility, NetworkIng)) and the SPIM Doctoral School (Engineering Sciences and Microtechnologies), from February 2016 to March 2019.

Contents

Acknowledgments

First and foremost, I would like to thank God for the whole thing. A chapter of my life, with its ups and downs, is closing and a new one will be open with the publication of this report. Singular page first read but last written, this thesis would never have been without the invaluable support of many people to whom these few lines will try to thank.

My first thanks go to Mr. Charles Sarraf who should have been a member of this jury, but who unfortunately left us on February 4th. I will never forget his constant support since the day I knew him in USEK and when he was my supervisor for my Master's degree project. Charles Sarraf, who was the support, the dad, the supervisor, the friend and the person devoted to his profession, will remain an example to follow in the academic field. No words can describe how much I am thankful. Thanks to Andrew Sarraf, his son, for his support to finalize this report.

I would like to express my sincere gratitude to Prof Emirite Maxime Wack and my co-supervisors, Mr. Raed Kouta and Mr. Jaafar Gaber. I thank them for the trust they have given me by accepting to supervise this doctoral work as well as for their continued support, valuable advices and encouragement throughout these three years. This work would not be successful without their relevant ideas.

I warmly express my thanks to the jury members, Prof. Pascal Lorenz and Prof. Eric Chatelet for agreeing to judge this work as reviewers and to give me constructive remarks that will allow me to improve the manuscript. I would like to thank the examiner Mr. Jalel Ben Othman for being a member of this jury.

I also thank my colleagues in OMNI for their support, the good times spent together, and for my university UTBM that gives me a good working atmosphere to accomplish my thesis. Thanks also go to all my friends, close or distant, who have motivated and supported me during difficult times, in particular for Sara Moustafa, Sara Kassan, Amani Younes and Liliane Sleiman.

Big thanks to my parents for their unconditional encouragement and their sacrifices. It must not be forgotten to thank my only brother Wael, and my sisters, Rim and Rachel, who helped and encouraged me throughout this thesis. Without them, this work would never have been possible.

List of Publications

This thesis arises four international publications that are listed below:

International conferences *[3]*

[1] Fault tree analysis for the communication of a fleet formation flight of UAVs

R. Abdallah, R. Kouta, C. Sarraf, J. Gaber, M. Wack

(2017) 2nd International Conference on System Reliability and Safety (ICSRS) , IEEE, Milan, Italy

[2] Reliability of Data Transmission of UAVs

R. Abdallah, J. Gaber, R. Kouta, C. Sarraf, M. Wack

(2018) 2nd international conference on smart applications and data analysis for smart cities, (SADASC'18), Casablanca, Morocco

[3] Communication failure analysis for a fleet formation flight of drones based on absorbing markov chain

R. Abdallah, C. Sarraf, R. Kouta, J. Gaber, M. Wack

(2018) Proceedings of ESREL, Safety and Reliability–Safe Societies in a Changing World CRC Press, Tondheim, Norway.

International Journal *[1]*

[4] Communication reliability model for drones' networks

R. Abdallah, J. Gaber, R. Kouta, C. Sarraf, M. Wack

Submitted to (2019) IEEE transactions on Reliability (Indexed, JCR, IF= 2.729, Scimago Q1)

List of Figures

List of Tables

Abbreviations

AFIT	Air Force Institute of Technology
AMC	Absorbing Markov Chain
AMMA	Adaptive Markov Model Analysis
AWGN	Additive White Gaussian Noise
BDD	Binary Decision Diagram
BER	Bit Error Rate
BPSK	Binary Phase Shift Key
CTMC	Continuous-Time Markov Chains
DCS	Distributed Computing System
DoD	Department of Defense
DSR	Distributed System Reliability
DSSS	Direct Sequence Spread Spectrum
DTMC	Discrete-Time Markov Chains
FANET	Flying Ad-Hoc Network
FCS	Flight Computer System
FDI	Fault Detection and Isolation
FHSS	Frequency Hopping Spread Spectrum
FMEA	Failure mode and effect analysis and derivatives
FMECA	Failure mode, effects, and criticality analysis
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
GCS	Ground Control Station
GA	Genetic Algorithms
GNN	Grossberg Neural Network
GPS	Global Positioning System

HALE	High Altitude Long Endurance
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ISM	Industrial, Scientific and Medical
MA	Markov Analysis
MC	Markov Chain
MALE	Medium Altitude Long Endurance
MANET	Mobile Ad-hoc Network
MAV	Micro Unmanned Aerial Vehicles
MCS	Minimal Cut Set
MILP	Mixed Integer Linear Programming
MIMO	Multiple Input Multiple Output
MPC	Model Predictive Control
MUAV	Mini Unmanned Aerial Vehicles
NPRD	Nonelectronic Parts Reliability Data Publication
OFDM	Orthogonal Frequency Division Multiplexing
OREDA	Offshore & Onshore Reliability Data
OS	Operating System
PER	Packet Error Rate
PID	Proportional-Integral-Derivative Controller
POMDP	Partially Observable Markov Decision Processes
PSO	Particle Swarm Optimization
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Key
RBD	Reliability Block Diagram
RMS	Reliability, Maintainability and Safety

RRT	Rapidly-Exploring Random Tree
RPAS	Remotely Piloted Aircraft Systems
RUDP	Reliable User Datagram Protocol
SCTP	Stream Control Transmission Protocol
SFT	Standard Fault Tree
SOA	Service-Oriented Architecture
SNR	Signal to Noise Ratio
SUAV	Small Unmanned Aerial Vehicles
TCAS	Traffic Alert and Collision Avoidance System
TCP	Transmission Control Protocol
TIP	Timeout Interval of Packet
TIQ	Timeout Interval of Queue
TUAV	Tactical Unmanned Aerial Vehicles
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicles
UCAV	Unmanned Combat Air Vehicle
UDP	User Datagram Protocol
US	United States
WIFI	Wireless Fidelity
UUANET	Unmanned Aerial Vehicles Ad hoc Network

Abstract

Title: Reliability approaches in networked systems – Application on Unmanned Aerial Vehicles

Unmanned aerial vehicles, used and developed initially in the military field, have experienced profound changes in recent years and are increasingly used in the civilian field. Recognized as drones, they are most often used in the civil and military domains. They are used for firefighting, rescue as well as in specific applications such as surveillance and attack. The formation flight is the most used because it allows a judicious distribution of the tasks and greatly improves the efficiency of the drones (principle of the attack in pack, carnivorous animals). This will raise the issue of coordination and strategy, as well as the type of operation (master /slave, ...). The type and quality of optimal information also remain to be defined.

The increased use of these cooperative systems in hazardous environments makes their reliability essential to prevent any catastrophic event. Overall performance of the drone fleet should be ensured, despite possible degradation of components or any changes that occur to the network and the environment. It is necessary to detect the anomalous behaviors that might contribute to collisions and thus affect the mission. Taking into consideration performance and cost, the fault-tolerant system and redundant systems are not always the most efficient solution for the formation fleet flight. Different methods like the fault tree analysis (FTA), Failure Modes and Effects Analysis (FMEA) have been used in the helicopter field.

In the first part, we propose a static method based on FTA, to ensure a successful communication between the drones from one side, and between the drones and the ground station from the other side by emphasizing on the exchange of information flows. It uses various fault trees to represent the different error conditions of this complex system.

In the second part, we analyze the different fault states and their probabilities. As this process is stochastic, an absorbing Markov chain approach is developed. The proposed approach can be used to find the most risky scenarios and considerations for improving reliability.

Finally, in the third part, we put the emphasis on the message receipt problem in a drone’s communication network by proposing a protocol based on number of retransmissions. The reception of a message is provided with a certain probability of reliability depending on several attributes such as modulation and bit error rate (BER) characterizing the UAVs.

Keywords: UAV, communication, formation fleet, reliability, fault tree, Absorbing Markov chain, message receipt.

Résumé

Titre : Approches de fiabilité dans les systèmes communicants - Application aux drones

Les véhicules aériens sans pilote (UAVs), utilisés et développés pour la première fois dans le domaine militaire, ont connu de profonds changements ces dernières années et sont de plus en plus utilisés dans le domaine civil. Etant plus connus sous le nom des drones, ils sont le plus souvent utilisés dans les domaines civiles et militaires. Ils sont employés pour : la lutte contre les incendies, le sauvetage ainsi que dans des applications spécifiques comme la surveillance et l'attaque. Le vol en formation est de loin le plus utilisé car il permet une répartition judicieuse des tâches et améliore grandement l'efficacité des drones (principe de l'attaque en meute, des animaux carnassiers). Cela pose alors la problématique de la coordination et de la stratégie, ainsi que du type de fonctionnement (maitre/esclave,…).Le type et la qualité d'informations optimums restent aussi à définir.

L'utilisation accrue de ces systèmes coopératifs dans des environnements dangereux rend leur fiabilité essentielle pour prévenir tout événement catastrophique. Une performance globale de la flotte des drones doit être garantie, malgré une possible dégradation des composants ou de toute modification du réseau et de l'environnement. Il est nécessaire de détecter les comportements anormaux pouvant contribuer aux collisions et ainsi affecter la mission. Compte tenu des performances et du coût, les systèmes à tolérance de pannes et à redondance ne représentent pas toujours la solution la plus efficace pour ce type de vol de flotte en formation. Différentes méthodes telles que l'analyse par arbre de défaillance (ADD), l'analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC) ont été utilisées dans le monde des hélicoptères.

Dans une première partie, une méthode statique basée sur l'ADD est proposée, pour assurer la fiabilité de la communication entre les drones d'un côté et entre les drones et la station de base de l'autre côté en accentuant l'échange de flux d'informations. Nous utilisons des arbres de défaillance pour représenter les différentes conditions d'erreur de ce système complexe.

Dans une deuxième partie, nous analysons les différents états de défaillance des communications et leurs probabilités. Ce processus étant stochastique, une approche par chaîne de Markov absorbante est développée. L’approche proposée peut être utilisée pour trouver les scenarios les plus risqués et les éléments à prendre en compte pour améliorer la fiabilité.

Enfin, dans une troisième partie, nous étudions le problème de réception des messages d’un drone en proposant un protocole basé sur le nombre de retransmissions. La réception est assurée avec une certaine probabilité de fiabilité, en fonction de plusieurs attributs tels que la modulation, le taux d’erreur des bits (BER) caractérisant les drones.

Mots clés : Drones, communication, flottes, fiabilité, arbre de défaillance, chaine Markov absorbante, réception de message.

1

General Introduction

Contents | Chapter 1

1 Introduction

This chapter constitutes a general introduction of the thesis report by presenting an overview of the problem statement, the contributions and the thesis outline.

1.1 The research domain

General Context: Reliability of fleet formation flight of Unmanned Aerial Vehicles (UAVs).

Specific Context: Communication reliability of UAVs ensuring exchanging information with high probability among them and with the Ground Control Station (GCS).

1.2 Background

Unmanned aerial vehicles, known also as drones, are used frequently in recent years in order to accomplish a certain mission in a controlled way by a Ground Control Station (GCS) or autonomously (Howard, 2013). These types of vehicles are primarily used in the military domain for reconnaissance and surveillance. Their use has developed and they have recently entered into the civil domain for other missions such as firefighting (Qin, et al., 2016), searching (Rathinam, et al., 2007), rescuing (Wenquan, You-rong, & Shao-hua, 2011), agriculture applications (Hunt Jr & Daughtry, 2018) and delivery of parcels (Murray & Chu, 2015). Their small size is mostly due to the evolution of their use, which has led to minimizing the hardware parts (sensors, actuators, etc…) in addition to the performance of the commands boards that facilitate their control (Chao, Cao, & Chen, 2010).

The formation flying of drones has become customary due to the importance of a coordinated group in achieving a definite common task (Li & Zhang, 2007). The performance of a formation flight surpasses the high performance of a single large aircraft especially for remote sensing applications. The group of drones resolves the problem of payload limitation, enhancing on reducing the cost and increasing the reliability. It increases the probability of success of the mission (Dudek, Jenkin, Milios, & Wilkes, 1996); in particular, if one drone has a malfunction, then the others can continue the task. Proper coordination and cooperation between the drones ensure the exchange of information and the achievement of the task.

Critical system denotes usually the avionic, nuclear systems or even any other system where its failure contributes to human catastrophes. The term these days also encompasses communication satellite and other computer system failures as they can also lead to financial disasters (Knight, 2002).

The design of UAVs is subject to several constraints that affect their functions. Several scientific approaches, methods, techniques and tools were developed early in the 20th century in order to assess potential risks, predict the occurrence of failures and attempt to minimize the consequences of catastrophic situations in case they occur. All these methodological developments can define dependability. The dependability of a system consists of evaluating its availability, reliability, maintainability, safety and security. Reliability and security play an essential role in the success of a UAV's mission (Reyes, Gellerman, & Kaabouch, 2015). The flying vehicles, especially those that achieve military tasks, are required to protect their information to avoid the enemy receiving it. Moreover, the reliability of exchanging the information in-between the drones and between the drones and the GCS is important in achieving the mail goal of a mission. Drones use the wireless communication (Wi-Fi, Bluetooth, Zigbee, etc.) to transmit the commands and data in a bidirectional direction (Zeng, Zhang, & Lim, 2016). The wireless channel presents a major risk to the communication since the drones fly in external environments.

1.3 Problem Statement

As the technology of UAVs grows and their cost decreases, they become an interesting way to undertake several difficult missions, especially when the drones form a swarm. It is not practical to have a human operator that controls each UAV in a formation. Hence, the coordination of the formation flight of drones raises the interesting subject of automatic control. Although autonomous navigation still has some challenges, the improvement that has been done in this domain, makes it a practical method. The development of autonomous navigation has been focused on the control of numerous autonomous machines. The meaningful questions that could be asked are how to ensure the safety and security of drones and how they respect the geometry that they should form depending on which strategy of commands. In fact, cooperating UAVs must be supported with a high coordination with each other since they move in hostile areas collecting data in order to achieve complex tasks in a dynamic environment. The communication between the aerial vehicles is ensured by the wireless medium in a manner that they should send their data in a synchronized and decentralized way. Sharing information is an issue in multi-UAV system because the unsynchronized information may lead to incorrect decisions that affect the communication between the vehicles. A centralized control architecture, which is an unreliable architecture, could be implemented in the leader-follower structure. If the communication is based on a leader UAV following the leader-follower strategy, or on a ground base station, then the mission will be limited because the central system will represent a single point of failure. The leader UAV is predetermined according to higher-energy resources and communication capabilities. To solve the reliability problem when the swarm depends on a physical leader, a virtual leader will be selected instead of the leader in the formation (Shi, Wang, & Chu, 2006), or multiple leader solution can be proposed ensuring consensus of the UAVs and collision avoidance (Hou & Fantoni, 2015). The act of changing the leader UAV permits the readjustment of the swarm to the environmental conditions and maximizes the operation efficiency. Several researchers study the problem of the leader selection algorithm in multi-agent systems. (Lin, Fardad, & Jovanović, 2014), (Clark, Bushnell, & Poovendran, 2012). The decentralized control architecture is used to assure formation of a leader-follower structure of several UAVs. Since the interaction between the agents depend only on neighbors, this sort of architecture is scalable and reliable. As UAVs connect with other entities, the adequate cooperation between the systems imposes communication protocols and security mechanisms such as authentication, confidentiality, integrity between them that facilitate the receipt of the information flow in a secured way.

It should be noted that, several factors cause the failure of a cooperative formation flight including environmental effects, damage to at least one of the team, information flow faults, obstacles and collisions involving UAVs in addition to their anomalies details will be described in chapters 3 and 4).

. The previous works, in the literature, focused on the reliability of a single drone, on collision avoidance between drones, optimization of a trajectory of drones and the flight path control as well of applications and types of drones. Furthermore, the researchers did not take into consideration the dependability and reliability of communication between the drones.

In this work, the ultimate goal is to ensure a reliable communication between fleet formation flight of drones in a way that it guarantees the information exchanging with high probability in-between the UAVs and with the GCS.

1.4 The contributions

UAVs exchange their own positions and data captured from the environment, as well as their flight plans in order to guarantee the realization of the mission by dividing their subtasks and distributing them among the team members. This exchange reveals the unpredicted future collisions that the UAVs must desperately avoid. To fulfill these exchanges, the drones should rely on a reliable communication system characterized with limited delays and sufficient bandwidth that enable them to transfer information flows over large distances depending on the number of drones in the fleet formation, their speeds during the flight in addition to the transmitted data size. The communication system should take into consideration the exterior factors that affect the exchange of data such as the interference of the medium, the mobility of the nodes and their temporary unavailability. Communication plays an essential function in the operation of drones. This importance could be presented for example in the case of not-fully autonomous drones, remotely piloted aircraft systems known as RPAS that need to be controlled remotely.

This thesis examines issues in the reliability of communication of information in-between the drones or between the drones and the GCS. In order to control the drones, two sorts of communication channel can be used: the simplex channel and the duplex one. The simplex channel is used when there is no need of getting additional data except e.g. the visual contact. On the contrary, the duplex channel is used where the transmission of additional data is required. This additional data could refer to the telemetry, or other information about the flight. In the rest of our thesis, we consider the duplex channel since the information sent between the vehicles does not insist only on the visual concept, but telemetry, GPS information, predetermined map of the environment in addition to the exterior factors are considered before the fleet starts the mission. The data transmission in UAVs systems could be generated in two ways. On one hand, we have the data between the UAV and the GCS in order to control the movement of the drones or the sensory data streaming (photos and videos that are collected by the drones). On the other hand, we have data that is transferred between the drones for the purpose of coordination, cooperation in team and collision avoidance.

The particular objective of the thesis is to find a solution to prevent communication failure and to ensure a high data transfer rate. To accomplish this purpose, this thesis will refer to dependability methods such as fault tree analysis, Markov analysis, reliability block diagram, etc. Focus will then be shifted to how many times should a message be sent until once can be, for example 99% sure, that the message has been received depending on the characteristics of the drones.

The following contributions have been developed within the scope of the thesis:

- Increasing the reliability of the communication system in-between drones or between drones and GCS by proposing a new model based on the fault tree analysis approach (FTA).

- Identifying the different fault states and their probabilities during a communication by proposing a new model based on Absorbing Markov Analysis approach (AMC).

- Improving the robustness of a message transmission by proposing a new protocol that serves to send data a certain number of times in order to be sure with high probability that the data is accurately received.

1.5 Thesis Outline

This section presents the structure of the thesis that consists of six chapters. The first chapter represents a general introduction that describes the context of the research, the problem statement that is focused on and the contributions of the dissertation proposed to solve the problem. The rest of the thesis is organized as follows:

Chapter 2

This chapter gives some necessary background on UAV technology and aerial robotics, their types and domain of application, in addition to the fleet formation flight concept. A literature review on the numerous approaches used in dependability is discussed. Subsequently, numerous algorithms are presented to describe the flight path control, collision avoidance and cooperation of drones.

Chapter 3

Chapter 3 addresses to failure analysis of a fleet formation flight of UAVs. Numerous reliability analysis tools can be adopted in either a deductive or an inductive way. In this chapter, we refer to the use of a deductive method (the fault tree analysis) to interpret the causes of the failure of the fleet formation flight's communication. Reliable communication can be affected by damage to at least one member of the team especially when the leader is damaged, information flow faults, obstacles and collisions involving UAVs in addition to their anomalies. Using the Weibull distribution and the Nonelectronic Parts Reliability Data Publication (NPRD-2016) database, the probability of occurrence of communication failure between the UAVs is calculated. The derived results are presented at the end of the chapter.

Chapter 4

In this chapter, an Absorbing Markov chain, where there is at least one absorbing state, is proposed to model the problem and show the transition between events that affect communication, by identifying the different fault states and their probabilities during a communication. The proposed framework can be used to find the riskiest scenarios and elements that need to be addressed in order to improve reliability. The causes of risk can be distinguished between internal causes (for example software and hardware failures) and external causes that are related to human error and environment. Some events can be repaired; however, others cannot. In this case, we should choose a specific situation in order to decrease the probability of failure.

Chapter 5

This chapter proposes a new approach that improves the robustness of the protocol used for the drones. It takes into consideration the modulation and the length of the message in order to ensure all the data is sent or received from the drones depending on the mission that they are requested to do. It is based on calculating how many times a message should be resent in order to be certainly received by other drones or by the GSC with high probability.

Chapter 6

Finally, this section summarizes the contributions proposed in this thesis and also provides some recommendations for future directions and research in the future work section.

2

Dependability and UAV networks

Contents | Chapter 2

2 Dependability and UAV networks

2.1 Introduction

An unmanned aerial vehicle (UAV), well known as drone, is defined as an aircraft where the aircrew is replaced by a computer system and a radio-link. It has different level of autonomy, i.e. remote controlled, fully autonomous; and can carry military payloads depending on the type of mission (Danilov & Smirnov, 2015). The size and weight affect the capacities needed in each mission. These sorts of vehicles are characterized with sensors and payload such as a camera, a video camera, a thermal sensor, etc.; that is served to catch the information in the environment of a desired mission. In addition, they are equipped with GPS to determine the location information that indicates the path of the mission (Rabbath, 2010).

The unmanned aircraft system (UAS), which has its own rules and regulations, is composed by numerous subsystems (Austin, 2011):

- A Ground Control Station (GCS) that includes the system operators and sends commands to the aircraft.
- An aircraft, UAV, which is responsible for carrying various types of payloads.
- Communication system that transmits the commands and control inputs from the GCS to the aircraft, the payload and sensitive data from the aircraft to the GCS.
- Support equipment for the purpose of maintenance.

The UAS has grown and become widespread in the last decades, due to the advantages of this system (Clapper, Young, Cartwright, & Grimes, 2007). Accordingly, the terminology used to describe it has evolved during these years. The unmanned vehicle has been known originally as Remotely Piloted Aircraft System (RPAS) but with the appearance of the underwater and land-based vehicles, the UAV is used nowadays to denote the aircraft of the UAS. The difference between the two terms concentrates on the presence of an active autopilot on board for the term of UAV and drone, which can be distinguished from RPAS that requires an active pilot on the ground (Abid, Austin, Fox, & Hussain, 2014).

It ought be clarified that there is a fine distinction between the UAV and the notion of 'drones' (Austin, 2011). A drone aircraft is characterized with a pre-programmed mission and a return to base program. It is distinguished to flatten out sight of the operator with zero intelligence. Usually, the drone provides the results of the mission when it returns to the base station since it is unable to communicate. On the contrary, the UAV has some degree of 'automatic intelligence'. It has the ability to communicate with the controller and send the payload data, the state information, and the amount of fuel, in addition to the status of the components such as the temperature of the engines.

2.2 Unmanned Aerial Vehicles

2.2.1 Fleet formation flight

UAVs can collaborate together creating a fleet formation flight, which can be either coordinated or cooperated according to the role of the aerial robots (Park, Cho, Lee, & Kim, 2015). On one hand, in case of coordination, each UAV has certain tasks to accomplish in a manner that there is a sort of synchronization between them that respects the order of the tasks in a plan. The coordination process can be illustrated by the air traffic control, which insists on avoiding collisions between the vehicles. On the other hand, in the cooperation case, several UAVs are implemented in order to achieve a specific mission since only one UAV does not have the ability to perform the requested mission. However, it requires a strong spatial and temporal coordination between the UAVs (Yanmaz, et al., 2017). During their flight, they can form different geometries of a formation such as V geometry and diamond geometry. A typical fleet formation flight consists of a leader, who is responsible for tracking the trajectory and his followers. The main goal is to maintain a definitive distance between the neighboring UAVs whilst retaining the geometry of the formation.

Fig. 2.1 Fleet formation flight of UAVs

Flying as a fleet formation has many advantages. The workload, such as the planning of the mission, the data processing and the observation of an area, has been distributed to the whole team. This principle allows a small cost for a certain mission because small sizes of planes can be used at the same time. Furthermore, single vehicle with the performance required to execute some tasks, could be an expensive solution when comparing to several low-cost vehicles performing the same task. Redundancy is an effective solution, but it costs or cannot be applied to small UAVs. The multi-UAV approach leads to redundant solutions offering greater fault tolerance and flexibility including reconfigurability in case of failures of individual vehicles. In addition, similarly to birds, each drone has limited resources that would allow it to continue its trajectory. For this reason, it is essential to change the leader of the formation each time the leader's resources have been reduced, e.g. energy sufficiency, in order to maintain the continuity of the flight (the selection of a new leader based on leader selection algorithm).

Formation flight also has some drawbacks. Since UAVs fly in small spaces with high speed, they are exposed to hardware failures, which influence the safety of the flight. Any member who fails should be eliminated or replaced since it no longer has the ability to synchronize with the team and affects the overall communication.

2.2.2 Applications

The main goal of the UAVs is to fulfill a mission that could be military, scientific, economic, or even commercial in nature. The interest in the control and navigation of drones is due to their use in hazardous environments (Ollero & Maza, 2007). The aerial vehicles were firstly developed in the military domain for the 3D missions known as 'Dull, Dirty and Dangerous'. These missions were too long and dangerous for the presence of pilots in the aircrew. Aircraft without radio-controlled pilot firstly appeared during the First World War in order to decrease the number of pilot diseases (Jobard, 2014). However, the real appearance of military drones does not come into place until the wars of Korea and Vietnam where they were used for stealth surveillance. In the 90's, the doctrine of 'zero death' had emerged allowing for the development of army drones and for their use in every army conflict from the 2000s. The prosperity of these war machines is due to the miniaturization of the avionics vehicles' size in addition to their long distance communication. It ought to be noted that 11 states officially possess military drones: the United States, Israel, the United Kingdom, Russia, Iran, Turkey, France, Germany, Italy, India and China. It is appropriate to enumerate some military applications in which we refer to the use of the UAVs:

a) Military applications (Navy, Army and Air Force)
   - Electronic intelligence
   - Reconnaissance
   - Radar system jamming and destruction
   - Relaying radio signals
   - Shadowing enemy fleets
   - Surveillance of enemy activity
   - Target designation and monitoring
   - Elimination of unexploded bombs
   - Decoying missiles by the emission of artificial signatures

Fig. 2.2 Military Drone

In the 90's, after the emergence of UAVs in the military domain and the rapid development of this technology, they have been known for a new role in Earth monitoring and emerged to the civilian domain (Luong, 2013). Civil applications have increased nowadays and we can cite:

b) Civil applications
- Aerial topography for geographical researches
- Agriculture spraying and monitoring
- Search and rescue
- Meteorological Measurements
- Firefighting and forestry fire detection
- Surveillance for illegal imports
- Pollution Studies and land monitoring
- Pipelines and Power line inspection
- Oil and gas search
- Delivery of parcels
- Urban planning
- Detection of mobile vehicles on the ground

Fig. 2.3 Applications of UAVs

2.2.3 Classification

It is hard to achieve a unique classification for UAVs since it differs between countries. The classification depends on several parameters such as flight altitude, payloads, the weight and size of the drones, flight range, endurance, speed, wings, etc. (Cavoukian, 2012). These include Hale UAVs (High Altitude Long Endurance), MALE UAVs (Medium Altitude Long Endurance), short and medium range UAVs, Mini UAVs and Micro UAVs (MAV). They can also be distinguished according to their functions: tactical drones, strategic drones and combat drones (Unmanned Combat Air Vehicle UCAV). Moreover, the type of gear can also differentiate them: fixed-wing, rotary wings and hybrid systems (Drouot, 2013), (Arjomandi, Agostino, Mammone, Nelson, & Zhou, 2006).

The Hale UAVs fly at an attitude over 20 000 m with an endurance of several days. HALE are considered to be the heaviest UAVs, having a weight up to 12 000 kilograms. This type of UAV can fly without being in fleet formation since one Hale is sufficient for the type of missions they typically conduct such as reconnaissance. Hales play the role of strategic UAVs, and their importance could be as the refueling principle during the flight, where the Hale plays a role of a tanker. They are utilized in long-range missions, such as reconnaissance and surveillance for army

Table 2.1 Classification of UAVs

	Mini and Micro UAVs	**Tactical UAV**	**MALE UAVs**	**HALE UAVs**
Altitude	< 300 m	< 5000 m	5000-15000 m	Max 20 000 m
Weight	Micro→ <500 g Mini→ 20 kg	100-500 kg	1800 kg	12 000 kg
Application	Civil /Commercial	military	military	military
Autonomy	Micro→30 min Mini→ few hours	10 hours	24 hours	UAV Global Hawk: 35 hours

use. Nowadays, the only Hale drone available is the well-known military UAV, the American Global Hawk with 35 hours of endurance.

Concerning the MALE UAVs, they fly within an altitude range of 5 000 – 15 000 m with an endurance of 24 hours. They are similar to the HALE in their functions, but they are more concerned with short-range missions. The well-known MALE drone is the American Predator that had been used to drop missiles in Afghanistan in 2001.

Moving to the tactical drones (TUAV), which are considered to be medium range, with a range between 100 and 300 km, flying at an altitude under 5,000 m with an endurance of ten of hours. These vehicles are typically operated by land and naval forces and are used to support military applications. For example, the French army is known to be in possession of them. TUAVs of medium range serve as a communication relays. They are not used usually as part of formation fleet flight, but they can work as a team in cooperation.

Mini drones (MUAV) are characterized by an endurance of a few hours, a mass less than 20 kg and a range of up to 30 km. They can be hand-launched and used for different civilian purposes.

Micro UAV (MAV) are UAVs that have wingspan of 150 mm. They have an endurance of about thirty minutes, a weight less than 500 grams and can be contained in a sphere of 30 centimeters in diameter. These types of UAVs can only be launched by hand and must fly slowly in urban environments within buildings.

2.2.4 Fleet Control Strategies

Different fleet formation control strategies exist in the literature (Guerrero & Lozano, 2012), (Chiaramonti, Giulietti, & Mengali, 2006) and this report discusses three of them:

- ***Leader – follower*** (Hierarchical Approach): This approach is widely used for multi-agents' system in which the teammates in the fleet follow a UAV considered to be the leader (Yun B. , Chen, Lum, & Lee, 2008). It is the leader who decides the trajectory of the mission and the disciples have to follow its decision. However, the major problem occurs when the leader is lost or affected by failures, which will influence on the entirely of the mission.

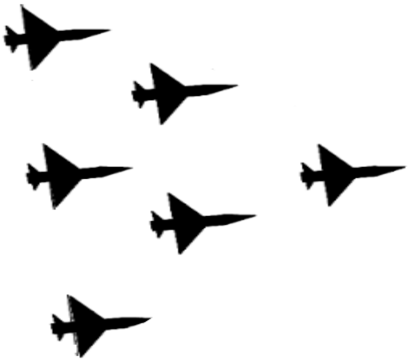


Fig. 2.4 Leader-Follower strategy

- ***Virtual Leader:*** This approach consists of replacing the leader of the formation with a virtual one. All of the fleet agents receive the mission path that is the same as the virtual leader's path. The predefined path reduces the autonomy of the fleet formation flight. Nevertheless, the risk of collision between the teammates increases (Li & Liu, 2008).

- ***Behavioral approach*** (Decentralized approach): Each agent follows specific rules in order to perform group behavior. In fact, this approach was inspired by Reynolds rules (Reynolds, 1987) in terms of collective movement of animals (Antonelli, Arrichiello, & Chiaverini, 2010). These rules are:

  - Collision avoidance with neighbors;

- Speed matching with neighbors;

- Fleet centering by trying to stay close to neighbors.

In the first rule, each agent in the fleet should guarantee a predefined security distance with its neighbors. An embedded controller on each agent in the fleet could ensure this. This controller generates pulsion forces when the distance with the neighbors became less than the security distance. In the speed-matching rule, each member has to match its speed with his nearby neighbors. The controller regulates the velocities to zero with respect to neighboring agents. In the fleet centering rule, each member attempts to stay close to his neighbors. The controller generates an attraction force toward the neighboring agents. Each agent has to maintain a global objective of the fleet that could be a rendezvous point or a reference trajectory known by all the teammates.

The behavioral approach represents an easily self-organized structure since each member should follow specific rules and knows the objective trajectory.

2.2.5 Drone’s fleet communication architectures

Different architectures could be used to ensure the communication between drones and between drones and GCS (Li, Zhou, & Lamont, 2013):

2.2.5.1 Centralized Architecture

In a centralized architecture, the GCS represents the central node of the network, to which all the UAVs in the swarm are linked. In this type of network, the drone communicates directly with the GCS (generally with a short delay), receiving and sending information relating to commands, control and sensitive data. However, the UAVs are not connected directly to each other. Hence, the network is centralized at the GCS. To ensure the inter-communication between drones, the information will be routed through a GCS that will serve as a relay in the communication. Furthermore, data between the drones will encounter a longer delay since it passes through a relay. The communication between the UAVs and the GCS requires a high transmission rate since UAVs fly for long distances to accomplish their mission. Having advanced radio transmission devices form a problem to the small or medium drones due to their limitations in the size and the capacity of payloads. Nevertheless, the centralized architecture has a lack of robustness since the GCS forms a single point of failure in a manner that when a problem occurs to the GCS, the consequence will affect the entire network and the communication will be disturbed or even disconnected.

2.2.5.2 Cellular network architecture (Semi-centralized)

Concerning the cellular communication network, it partitions the area into different zones where a base station in each zone is responsible for managing a group of nodes. The specificity of this architecture is the low power transmitters taking into consideration the range of the existing mobile operators' infrastructure (Bouachir, 2014). However, the cost of the communication is not negligible even with the installation of a new infrastructure. In addition, it is difficult to cover all areas and maintain this infrastructure especially in some cases such as after natural disasters.

2.2.5.3 Satellite communication architecture

Satellite communication is a potential solution to ensure communication between two distant nodes. There are two types of satellite communication, geostationary and orbital, for which the differences can be described as follows; the orbital satellite comprises a variable zone, whilst, the geostationary satellite is considered fixed referring to a reference (Bouachir, 2014). Moreover, the satellite communication can be realized for Drone-Drone and Drone- GCS providing that the drones are on the line covered by the satellite. Using a satellite communication has a negative effect, since it causes latency in transmission and the signal could be dropped because of obstacles such as trees or mountains.

2.2.5.4 Decentralized Architecture

Unlike the centralized architecture, the decentralized architecture permits the ability for two UAVs to communicate, directly or indirectly, with each other. The information can pass through a third UAV that plays the role of a relay, instead of the GCS extending the coverage with a multi-hop transmission. It is more robust, since it is not based on a single point of failure. Several decentralized communication architectures can be described as follows (Snooke, 2015):

a) <u>UAV Ad Hoc Network</u>

The most known multi-UAV systems is the ad hoc network, known as the UAANET (UAV Ad hoc Network) and composed with a swarm of UAVs with one or several base stations. All the drones will participate in exchanging the information between them in a manner that a leader UAV (backbone), considered as a gateway, relays the data between the GCS and the other drones. For this reason, it requires two radio transmissions. Since the group of drones fly close to each other, UAVs can have a low weight and cost transceiver. Each node can represent a relay for the transmission of the information from the source to the destination. In UAANET, the entrance or the exit of a node from the network could be at any time and the group of UAVs are homogeneous. The modification of the topology of the network remains the use of reliable protocols in order to maintain the reconstruction of the network. Furthermore, the case wherein different types of UAVs in the network can be divided in two distinct communication architectures: multi-layer UAV ad hoc network and multi-group UAV network.

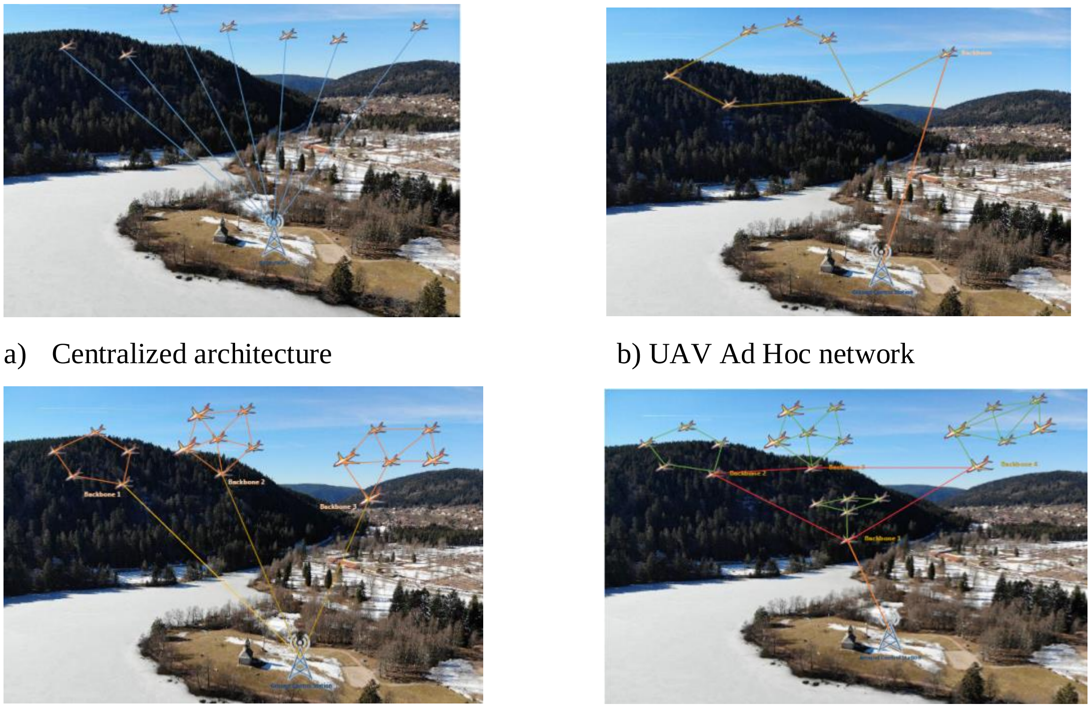
b) <u>Multi-Group UAV network</u>

The homogeneous UAVs form a group in a manner that they form their proper UAV ad hoc network with their corresponding backbone UAV connected to the GCS. Moreover, the intra-group communications follow the same principle of UAV ad hoc network. As for the inter-group communication that relates to communication between different types of UAVs, it is based on the communication between the corresponding backbones UAV of each group with the base station (Fig 2.5 c). This network architecture is favorable for the mission in which a large number of heterogeneous UAVs having different flight characteristics are required. Nonetheless, it still has a lack of robustness.

c) <u>Multi-layer UAV network</u>

The Multi-layer UAV network (Fig 2.5 d), is specified for networking several group of diversified UAVs. The lower layer includes the UAVs in a group that compose the UAV ad hoc network. The upper-layer encompasses the backbone UAVs of all the categories. Inversely to the multi-group UAV network, there is only one UAV that communicates directly with the GCS.

The following figures aims to illustrate the different architectures in drones' networks[1].



a) Centralized architecture

b) UAV Ad Hoc network

c) Multi-group network

d) Multi-layer network

Fig. 2.5 Drones fleet communication architectures: this figure describes the different architectures in drones' networks focusing on the links in-between drones and between drones and GCS.

2.3 Dependability concept

2.3.1 Definition

The first collection of statistical information of engine and aircraft accidents started in 1930. The dependability concept was reserved initially for the riskiest industries such as aviation,

[1] These photos have been taken with a DJI Mavic Air in Vosges, Belfort, France

space, petrochemical fields and nuclear. Moreover, it has progressively penetrated in other fields in which the constraints of competitivity and services are evaluated in terms of economy, reliability and quality. In 1960, aeronautical and space industries analyze the component failures and the US Department of Defense (DoD) promulgated the first true requirements of Dependability following missile accidents. Hence, the dependability concept is defined as a complete methodological corpus that must be deployed with "humility and perseverance” (Vasseur, 2006) by respecting its methods, tools and stages. According to (Laprie, et al., 1995), the procedures and methods of dependability establish a “justified” trust in the realization of the expected missions, the services integrating the performance and the incurred risk management.

2.3.2 Dependability taxonomy

Avizienis et al. define a taxonomy of dependability in a tree that consists of three concepts (Avizienis, Laprie, Randell, & Landwehr, 2004) (Fig 2.6):

- ***Attributes***: quantifiable and evaluable properties characterizing system performance.
- ***Means***: techniques to improve attributes’ values
- ***Threats***: events affecting system performance

2.3.2.1 Attributes

The attributes (Norme, 1988) can be described according to Villemeur (Villemeur, 1988) as follows:

- ***Reliability*** is defined as the ability of an entity to perform a required function under given environmental and operational conditions and for a specified period. This attribute will be the major focus in this thesis.

- ***Availability*** is defined as the ability of an entity to perform its function (s) at a particular time or over a specified period (BS4778, 1991).

- ***Maintainability*** is the capability of an entity to be maintained or re-established within a given time interval in which it can perform a required function, when maintenance is performed under specified conditions with prescribed procedures and means. It is a major key that determines the availability of the studied entity (BS4778, 1991).

- ***Safety*** designates the ability of a product to acquire an acceptable level of risk, during its life cycle, that causes degradation to the product.

- The non-occurrence of unauthorized disclosures of information leads to the ***Confidentiality***.

- The non-occurrence of inappropriate alterations of information leads to ***Integrity***.

2.3.2.2 Threats

It is important in this work to define the distinction between the three sorts of threats that will be used in the proposed fault tree analysis approach (FTA) (Chapter 3). Threats are undesirable and unexpected circumstances, generally caused or a result of unsecured malfunctions (Ciame, et al., 2009). It can be distinguished:

- ***Failure*** is the cessation of the ability of an entity to perform a required function.
- ***Fault*** is the supposed cause of an error (Villemeur, 1988)
- ***Error*** is the part of system that is likely to cause failure (Laprie, et al., 1995). When the error is active, a failure appears.

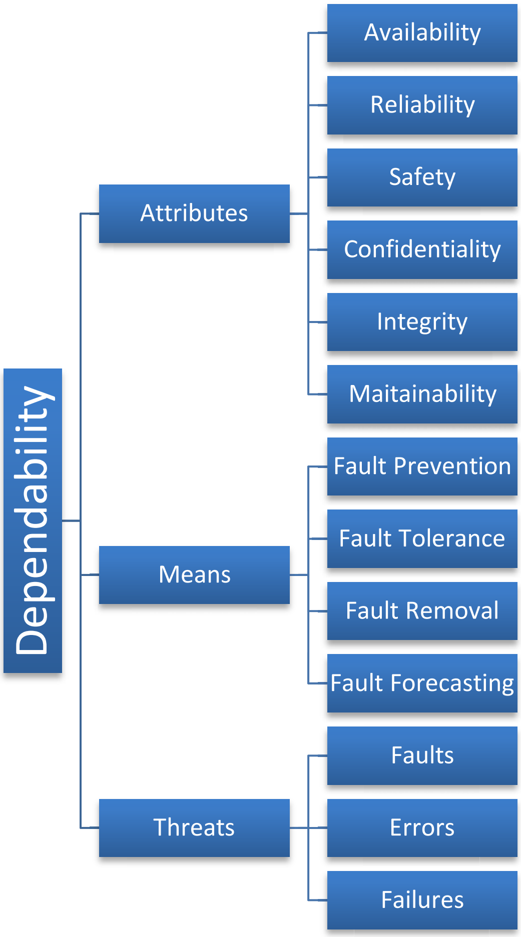


Fig. 2.6 Dependability tree: this tree illustrates the different elements of the dependability

2.3.2.3 Means

Dependability provides several means in order to limit the faults and avoid the appearance of failures:

- ***Fault Prevention*** : prevention of the occurrence or introduction of errors
- ***Fault Tolerance***: the system will deliver an acceptable service able to perform the functions despite the occurrence of faults.
- ***Fault removal***: reduce the presence, number and/or severity) of faults.
- ***Fault forecasting***: includes all methods and techniques intended to estimate the present number , the future incidence, and the likely consequences of faults

2.3.3 Safety Analysis techniques

There are numerous analysis techniques that seek to present a solution for safety assessment. They can be divided into quantitative and qualitative, inductive and deductive (Guillerm, 2011). Qualitative methods focus on the nature of risks associated for the system elements. As for quantitative methods, they measure the attributes of dependability. In what follows, we describe briefly several well-known analysis techniques.

- ***Failure mode and effect analysis and derivatives (FMEA)***: it is a qualitative inductive technique based on bottom-up analysis of a system by determining the failure modes, causes and effects of system component failures (Li & Chen, 2019).
- ***Analysis by experts:*** Another qualitative analysis, which is based on prior experiments in similar applications.
- ***Fault Tree Analysis (FTA):*** a deductive quantitative method that exposes the combinations of basic events, which lead to an undesired top-event. This analysis technique will be discussed later in Chapter 3 (Abdallah, Kouta, Sarraf, Gaber, & Wack, December 2017), (Stamatelatos, et al., 2002) .
- ***Reliability Block diagram (RBD):*** a model within the blocks indicate the system structure. It describes graphically the condition for a successful operation. It helps to calculate the reliability of a non-repairable system (Wang, Zhang, & Yoon, 2019).
- ***Markov analysis:*** a stochastic process that analyzes the safety of systems by representing different states and their transitions (Yu & Sato, 2019)(inductive and quantitative approach). Markov analysis will be described in detail in chapter 4.
- ***Petri nets:*** it identifies the system evolution in the states of operation, degradation, failure (inductive and quantitative approach) (Daniel & Descotes-Genon, 1995), (Jensen & Rozenberg, 2012).

The safety analysis techniques can be categorized into static and dynamic methods (Gandibleux, 2013) (Fig 2.7). Static approaches do not take into consideration the evolution of system over interval of time. However, dynamic approaches integrate the dynamic evolution but have limited number of states.

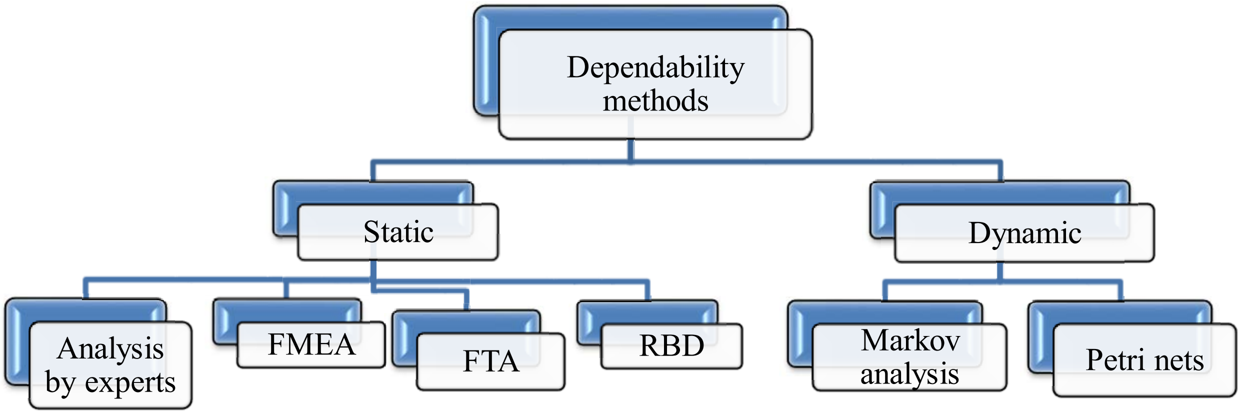


Fig. 2.7 Dependability approaches: this figure represents numerous safety analysis approaches to evaluate dependability

2.4 Related works

Several studies took the unmanned aerial vehicles as their subject. Formation flight is a subject of great attention and widely studied. Many interesting formation flight applications have been considered. Examples include forest fire monitoring, radar deception, and ground-to-air (SAM) missile jamming.

UAVs are discussed in several researchers' works in the engineering field. Various control systems have been proposed for the formation flight of drones, such as PID (proportional-integral-derivative controller), the potential method, the forces of constraint and the method based on the consensus (Zhou, Shao-Lei, Zhang, Wen-Guang, & Lei, 2012; Seo, Ahn, & Kim, 2009). Other algorithms have been developed on the problem of guidance and control in a disturbed environment. Martini's thesis presents the various control laws for a mini-UAV helicopter affected by wind gusts (Martini, 2008) while Walid Achour (Achour, 2011) takes up the same problem by trying to minimize the influence of the wind on the trajectory of drones and looking for the optimal path.

Collision avoidance is an important element to maintain the safety of the UAVs in hazardous environments and ensure the performance of a fleet formation flight of drones (Kuchar, 2005). UAVs should be able to sense, detect and avoid collision with teammates. They should be equipped with Traffic Alert and Collision Avoidance Sytem (TCAS). The authors of (Zeitlin & McLaughlin, 2006) evaluate the collision avoidance safety by using a FTA approach and analyzing its elements. In the case of a danger zone, a modified version of Grossberg Neural Network (GNN) (Wang, Yadav, & Balakrishnan, JULY 2007) is used to obtain optimal trajectories between the current position of the drone and a point outside the danger area. Among the most popular optimization-based approaches, is the MPC (Model Predictive Control) method (Zhou, Shao-Lei, Zhang, Wen-Guang, & Lei, 2012; Cheng, Necsulescu, Kim, & Sasiadek, 2008). (How, King, & Kuwata, 2004) detail coordination algorithms between drones by entering examples of "Receding Horizon Control" or appointments using time control.

Obstacle avoidance in a 2-D environment has been a recently studied topic. In (Saunders, Call, Curtis, & Beard, 2005), the Rapidly-Exploring Random Tree (RRT) concept was used to dynamically find possible paths that are free of obstacles. The disadvantage of this concept is that it takes considerable computing time. In (Kuwata & How, June 2003) , Mixed Integer Linear Programming (MILP) was used to design dynamically possible trajectories for obstacle avoidance; but this method also requires greater computing capabilities

Some authors treat the evaluation of artificial immune system approach for the Air Combat Maneuvering (Kaneshige & Krishnakumar, 2007), (Kishnakumar, 2003). Moreover, the bio inspiration approaches has also been applied for the UAVs in order to determine the path planning (Tseng, Liang, Lee, Chou, & Chao, 2014) , the flight control (Lentink, 2014). For example, Particle Swarm Optimization (PSO) (Fu, Ding, & Hu, 2013) and Genetic Algorithms (GA) (Duan, Luo, Ma, & Shi, 2013) are optimization approaches that generate high quality paths for UAVs. It is important to discuss the efficient energy of data collection with a UAV. Dac-Tu et al. (Ho & Grøtli, 2013)proposed a heuristic algorithm in order to optimize the total energy of the GCS nodes in the data collection with UAV.

An approach to addressing "rendezvous" between drones has been invoked in [22] based on a decentralized decision system that breaks down the problem into an appointment agent and a trajectory planner. The algorithm is based on a Voronoi path and ETA coordination. The authors of the article (Pastor, Lopez, & Royo, 2007) introduce a Hardware / Software architecture for the mission and control of payloads of drones by referring to the Service-Oriented Architecture (SOA) systems. In the case of a surveillance mission, the planning of the trajectories for the drones' fleet would be based on three stages (Cadi, 2010) . The modeling of the terrain with all its constraints based on Voronoi graphs, then the calculation of the shortest path in a risky environment in the presence of obstacles either by the Dijikstra algorithm or by the algorithm A* and finally the planning of a mission to monitor the fleet in a real context. The Tabou search with a double list allows us to find the routes for each UAV with the aim of minimizing the cost of the mission while respecting the risk limit and avoiding obstacles.

The swarms of UAVs can be used as a cooperative relay for ad hoc networks. In (Palat, Annamalau, & Reed, Cooperative relaying for ad-hoc ground networks using swarm UAVs, 2005), distributed MIMO (Multiple Input Multiple Output) is applied on the fleet of UAVs in order to improve the communication between ground clusters of ad-hoc network.

In literature, reliability of the small UAV has also been discussed. Paul Freeman et al (Freeman & J. Balas, 2014) demonstrate the failure modes and effects analysis (FMEA) for the actuation system of low cost and small UAVs. Freeman identifies the critical fault modes that contribute for the loss of control and significant failures for a single UAV. Since UAVs are unreliable, the authors of (Franco & Góes, 2007) also treat this problem by focusing on FTA and FMEA for the UAV propulsion system. Moreover, the authors of (KrAwczyK, 2013) determine the level of reliability for UAVs in Poland that permit them to operate in the European sky. A framework for network management is proposed in (Thanthry & Pendse, 2009) to provide an active user interface for the flight health monitoring. In (Kladis G. P., Economou, Knowles, Tsourdos, & White, 2008) , a fault tree analysis shows the most probable cause of faults in addition to the minimum time fault-path that contributes for a specific cause. It is based on pseudo Boolean expressions with graph theory tools through a diagraph analysis. Therefore, a fuzzy fault tree analysis was used to evaluate the reliability of communication networks (Rafiee & Shabgahi, 2011). The authors (Ragi & Chong, UAV path planning in a dynamic environment via partially observable Markov decision process., 2013) propose a path-planning algorithm in order to guide UAVS for tracking multiple targets. They based in their algorithm on the theory of partially observable Markov decision processes (POMDPs). Since the safety problem has an important role for the reliability of flight control of UAVs, (Jiufu, Chen, & Zhisheng, 2011) use a weighted fuzzy Petri Nets approach in order to model the fault diagnosis of flight control system. Petri Nets approach based on fuzzy reasoning are also used to make decision for UAVs to strike a target**Source spécifiée non valide.**.

Nonetheless, the literature review does not take into consideration the reliability of communication of the formation fleet of UAVs nor how to achieve a high probability of messages being successfully delivered. Accordingly, this thesis aims to solve the problem and elaborate the problem of UAVs communication reliability.

2.5 Conclusion

This chapter involves the necessary background essential for the thesis. A literature review is introduced concerning the two topics of this thesis: Unmanned aerial Vehicles and Dependability. The different characteristics of UAVs such as classification and applications were discussed; however, this thesis focuses on the fleet formation flight of drones, their communication architectures in addition to their strategies. We aim in our work to ensure the communication reliability of drone networks. Hence, dependability that has reliability as an attribute is described. The taxonomy of dependability shows the different attributes, threats and means. A brief description of each one was presented, describing the differences between them. Subsequently, several safety analyses were introduced in order to present the different approaches used for ensuring dependability. Different authors applied their studies on UAVs. For this reason, existing related works, in the literature, that treat UAVs subject were presented focusing on the reliability of drones. The next chapter offers a method for guaranteeing the communication reliability of drones' formation flight where a fault tree analysis is proposed as the safety technique for dependability. This static approach is used in our thesis since it is the most common approach used for analyzing the dependability of UAVs in the literature, but it does not take into consideration the communication of drones' fleet formation flight. Fault trees are the easiest and most often used technique in complex systems dependability assessment.

3

Communication Reliability of drones based on Fault Tree Analysis

Contents | Chapter 3

3 Communication Reliability of drones based on Fault Tree Analysis

3.1 Introduction

Safety of the critical systems has emerged due to its importance in many fields such as automotive, energy sectors, medical and aerospace (Knight, 2002). The failure of these kinds of systems has the possibility to lead to catastrophic consequences affecting the environment as well as human life. For this, safety critical systems is essential in dependability. Moreover, dependability can be defined as the ability of averting failures considered to be more severe than acceptable. Dependability is usually achieved in the design and conception phase in order to avoid loss of life, resource or environmental damage by identifying the risks. It includes maintainability, safety, and reliability (Laprie, et al., 1995); however, this thesis will deal with the problem of reliability only.

Cooperative UAV are broadly used in both military and civilian missions in hostile and hazardous environments without risking human life. For this reason, they are recognized as the vehicles for 3D missions that are ‘dirty, dull or dangerous’ (Marshall, 2004). Cooperative drones are considered as critical systems where their communication reliability should be ensured.

Many methods are widely used in fulfilling the dependability analysis of industrial systems. One of the famous methods widely used is Failure Modes Effects and Criticality Analysis (FMECA). This inductive analysis technique, which was initially known in US Military Procedure then in the US Department of Defense, addresses the credible combinations of the effects of component failure (Jordan, 1972). It is based on a probabilistic analysis to choose the failure modes criticality. Another well-known technique used in system dependability is the fault tree analysis (FTA) that will be discussed later.

This chapter is devoted to attempting to identify a method for ensuring communication reliability of a cooperative UAV fleet. This method is based on a deductive failure analysis approach, the fault tree analysis (FTA), in which the undesired state, the communication failure, is analyzed. The analysis takes into account four different intermediate events. The rest of the chapter is organized as follows. A definition of the FTA and its characteristics is considered in section 2. In section 3, a review of related works concerning the reliability is introduced. Section 4 provides the proposed model of communication reliability based on FTA for the drones' networks including the description of each intermediate event. In section 5, a probabilistic analysis approach of the fault tree is shown taking into consideration the probabilities of related basic events, using a Weibull distribution. This section shows also simulation results that exhibit the variation of occurrence probability of the communication failure. A conclusion discussing the results is presented in section 6.

3.2 Fault tree analysis (FTA)

In this section, we define the fault tree analysis and the method to contrast it by introducing the different symbols used.

3.2.1 Definition

FTA is a well-established technique that establishes system dependability (Stamatelatos, et al., 2002). Contrary to FMECA, FTA is a deductive approach in which the analysis of system failure begins with a top event and continues towards the leaves of the tree in order to specify the basic events that are the root causes of the top event (Lee, Grosh, Tillman, & Lie, 1985). It is a graphical representation of the logical relations between the faults and their causes. It shows how combinations of different components failure and environmental circumstances can lead to system failure. Its analysis can be resumed in two levels: quantitative or qualitative level. Concerning the qualitative analysis, it is accomplished by constringing the fault trees and transform them into minimal cut sets (MCSs). These MCSs represent the sum of products depending on the smallest combination of the basic events influencing the top event (Haasl, Roberts, Vesely, & Goldberg, 1981). Moving to the quantitative analysis, the probability of occurrence of the top event can be calculated referring to the failure rate of each component of the system. It gives a hint to point out which components of the system are more influential on system reliability in a manner that analysts give more value to critical components to decrease the failure probability, i.e. using redundant components in the system.

3.2.2 Fault Tree symbols

The standard fault tree (SFT) aims to evaluate the reliability of static systems. Fault trees consist of different types of nodes: gates, events, and transfer symbols (Ericson, 1999). The following figure illustrates different sort of events:

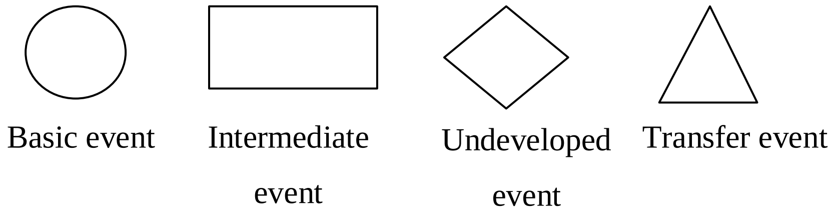


Fig. 3.1 Fault Tree events

A basic event that is graphically designed with a circle does not necessitate a further expansion. They represent the tree’s leaves and they combine using different gates in order to form the intermediate events. Therefore, an intermediate event is caused by the logical combinations of the basic events. An undeveloped event, represented by a diamond, is an event that is not considered in the analysis because there is not enough information about it or because it is unnecessary to consider it. In case the tree is too big and cannot be illustrated in one page, we can use the transfer events to extend the fault tree to other pages. The transfer gates is designed by a triangle.

Numerous symbols are used in fault trees to indicate the distinct logic gates (Fig. 3.2). The result of an AND gate is true in case all of the input events occur in a manner that there is a causal relationship between its inputs and its outputs. The OR gate in a scenario is implemented when at least one of the input events occurs. It differs from an AND gate since there is no causal relation between its inputs and outputs; inputs are like restatement of the outputs. The XOR gate is a specific case of OR gate in which its output is true when only one input is true. This thesis only refers to OR and AND gates in its proposed approach.

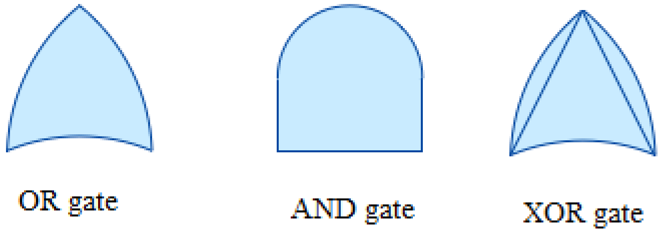


Fig. 3.2 Logic gates symbols

3.3 Related Works

Faulty behaviors of the drones or the fleet could be caused by failures, breakdown or malfunction in the components, the computers, and the platform; or in the information flow between the aerial vehicles. A single failure does not necessarily provoke the failure of the complete system (Avizienis, Laprie, Randell, & Landwehr, 2004) . Equipping each UAV with hardware redundancy would decrease the probability of failure of the vehicle. However, not all UAV could be equipped with redundancy hardware due to limited size, weight and power as well as increased costs (Freeman & J. Balas, 2014). Therefore, fault avoidance is a good solution.

Concerning the communication system, component-level faults comprise those of the sensors, actuators, control surfaces, flight computers, engine and GPS data (Tao, Chen, & Tang, 2004). Analyzing the failure of UAVs has been covered by different methods. In (Snooke, 2015), the probability of catastrophic failure has been estimated using a histogram of pre-fault control command distribution. In (Kim & Caslise, 1997), neural network is used to adapt with the effect of the inversion error. Sliding mode is adopted for a non-linear control permitting it to achieve the mission in a finite time (Patel, Patel, & Vyas, 2012). Founded on the Binary Decision Diagram (BDD), the reliability approach was also used for the mission planning of UAVs (Remenyte-Prescott, Andrews, & Chung, 2010). Their approach considers the available diagnostic data and helps to predict future capabilities of UAVs in real time. Considered as a slow process, the BDD was improved with the help of an empirical approach (Andrews, Poole, & Chen, 2013).They propose ways in which phased mission analysis is improved in order to decrease the calculation time. In their methodology, they consider the characteristics of the fault tree structures that provide the causes of phase failure for a UAV mission. To isolate the anomaly within a formation flying aerial vehicle, a data-driven approach with a sequence of input and output data pairs was used to detect the failure by spotting an abnormal change (Wang, Wang, & Wang, 2015).

They identify the model parameters for each UAV referring to input/ output data pairs achieved by a sparse optimization technique. The change in model parameters can identify the fault states in order to isolate them. The concept of the model-driven approach, developed by Beard (Beard, 1971), is widely used for fault detection and isolation (FDI). A control system adopting the leader-follower strategy with the problem of the collision avoidance is presented in (Yun B., Chen, Lum, & Lee, September 2008). In (Dermentzoudis, 2004), the authors present the different methods of reliability (FMECA, FTA, and FRACAS) used for the Small UAVs (SUAVs). The diagraph analysis reflects another approach for determining the highest cause of occurrence of failure using the graph theory with pseudo Boolean expressions and leading to the shortest path trajectory (Kladis G. P., Economou, Tsourdos, & White, September 3-5, 2008). In addition to FTA, the Markov analysis (MA) and the Dependence Diagram Analysis (DDA) constitute well-known methods for reliable analysis of aerial systems (Okafor & Eze, 2016).

3.4 The communication reliability model for drones' networks

In this section, a failure analysis of fleet formation flight of UAVs is discussed. Reliability analysis tools such as failure modes and effects analysis (FMEA) and FTA are evident for the reliability of redundancy hardware. This analysis can be adopted in two ways: inductive and deductive. In the inductive form, the component failures are designed at the lowest level and their effects on the higher level, which is contrary to the deductive form where the causes of each failure are determined.

Several factors cause the failure of a cooperative formation flight including the environmental effects, the damage of at least one of the team, the information flow faults, the obstacles and the collisions of the UAVs in addition to their anomalies. Fig. 3.3 describes the four intermediate events that influence communication within the fleet. Each event illustrated by a transfer gate, will be described later.

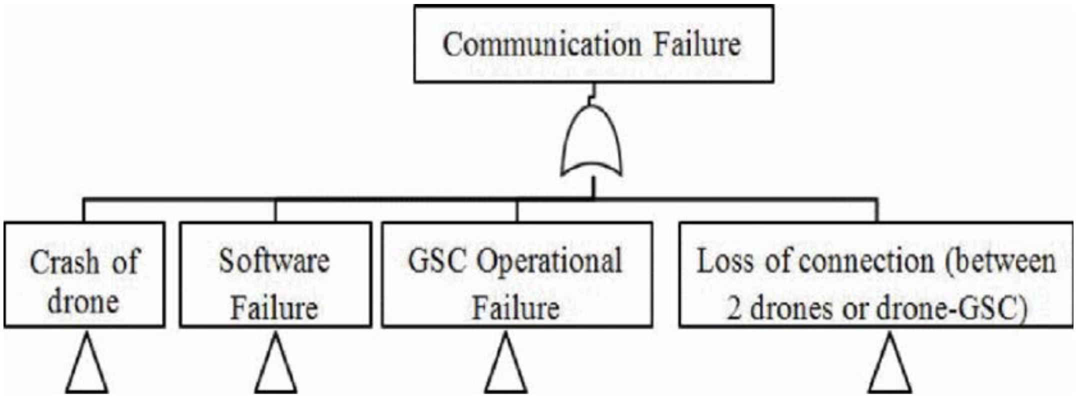


Fig. 3.3 Fault tree analysis of the communication failure of fleet of drones: this figure shows the four transfer events that are causes of the communication failure. Each event will be described in detail using another FTA

3.4.1 Crash of Drone

An environmental event can attribute to the deterioration of the UAV. It can occur to the platform itself, the components or the systems. The crash of the vehicle could be caused due to certain events such as the fleet management system failure, the attack of the drone by a sniper or an electromagnetic pulse, a collision event or even due to a mechanical failure (Fig. 3.4). Drones should know other drones' positions in order to ensure the fleet management system and avoid collisions between them. The fleet management system ensures coordination between devices. The inertial measurement unit (IMU) and the inertial navigation system (INS) are used, in addition to GPS and the altimeter, to determine the orientation, position and altitude of the drone. When an UAV submits faulty data and/or moves away from its desired trajectory, it increases the probability of collision with its neighbors and with obstacles in the environment. This failure could be presented when the proximity sensor is broken or when it gives an inaccurate decision.

Mechanical failure is one of the major causes of a crash (Fig. 3.5). Mechanical failure comprises failure of either one of the following components: the engine, more than one propeller or the power. Bad and faulty maintenance could also contribute to mechanical failure. Battery failure is attributed due to an overcurrent / undercurrent, physical damage, overheating or exhaustion. On the other hand, the engine can be interrupted due to hardware failure as the servomotor, the actuator and disruption of cables or due to the loss of onboard computers. The cooling system represents an essential factor to avert the engine from dropping out. A catastrophic problem occurs in the event of a crash of more than one propeller.

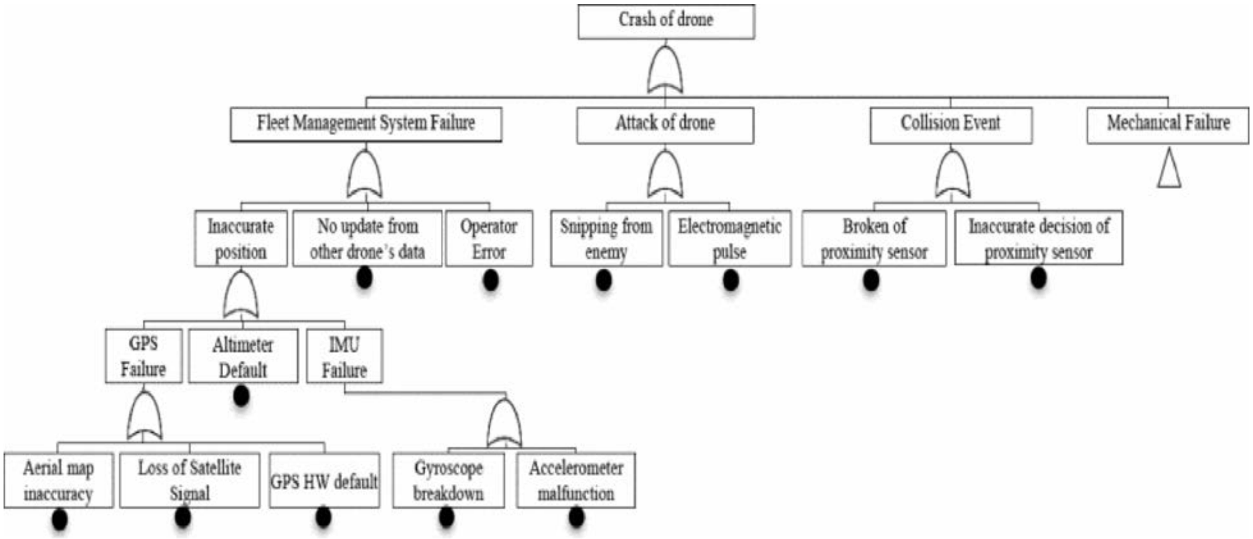


Fig. 3.4 FTA of a crash of drone: this figure defines numerous intermediate events that lead to the crash of drone.

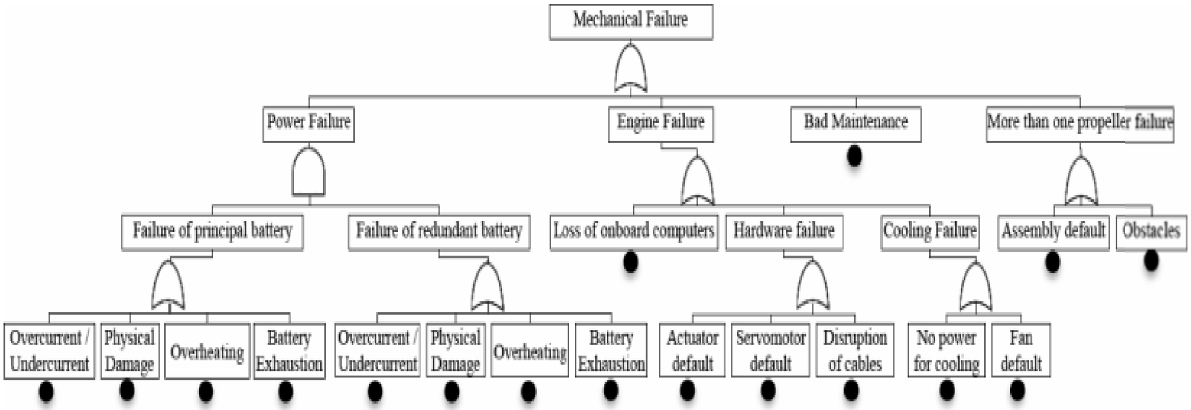


Fig. 3.5 FTA of a mechanical failure of drone: this figure specifies the causes of mechanical failure for a drone.

3.4.2 Software and Ground Station Control Operational Failure

In addition to equipment failure, a software failure can occur leading to the disruption of communication between drones. As the critical systems are highly dependent on software, software safety represents a major factor in the quality's system. The reliability of the software is ensured through good design, regular updates of both the operating system and related applications ensuring it is free of viruses/malwares. The main problem occurs when the operation system stops suddenly (Fig. 3.6). Failure of the communication Drone-GSC might be due to the transmitter/receiver faults, the operator's behavior and misjudgment of the weather (Fig. 3.7).

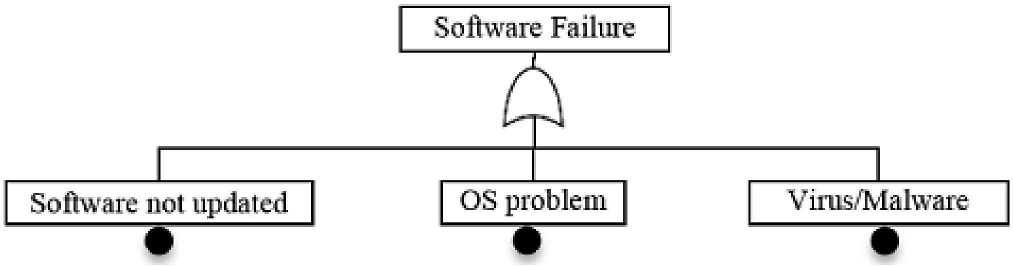


Fig. 3.6 FTA of the software failure of UAV: several causes can lead to software failure, such as a problem in the drone's operating system, the presence of virus or malware, in addition to the error when the software is not updated

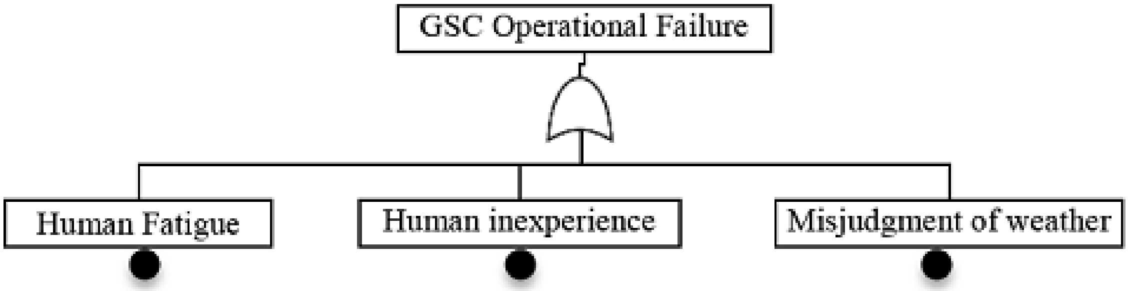


Fig. 3.7 FTA of the GSC operational failure: the GCS operational failure is one of the cause of communication failure. GCS, which is controlled by human, can have degradation in the performance due to human fatigue, inexperience or due to a misjudgment of the weather.

3.4.3 Information Flow Faults

The formation of a cooperative fleet is based on inter-vehicle communication based wireless technologies such as Bluetooth, Zigbee, or WiFi with an adhoc network. Each UAV represents a node capable of transmitting and receiving the state (position, velocity, altitude) to and from each one of its neighbors. Each one of the fleet collects the data from its sensors and transmits assigned and visited targets as well as its health status to its teammates.

If the medium of communication is exposed to jamming, echoes and noise, then that might interfere with what is transmitted, affecting the overall communication. Other factors that might influence communication are the mobility of UAVs and the presence of nearby users. Information flow is necessary to achieve the mission of the fleet. Faults or losses of information flow are pretended due to nodes loss, damage of an agent, failure of the flight system and the presence of obstacles. It might occur between two or more UAVs or between the aerial vehicle and the GCS. GCS forms a relay point for the information flow, so it can represent a major issue within the overall communication system. Antennas' faults could be due to manufacturing defects or electrical faults. Synchronization of the message is an essential mechanism in the transmission of the message. The distance between the source and the destination can influence the quality of the received information as when the distance increases, the transmitted signal can be exposed the attenuation and atmospheric noises (Fig. 3.8).

The environmental effects include each exterior factor that affects the communication of the fleet. It encloses the natural phenomenon, such as animals, human, obstacles, and weather. Weather conditions that could have a major influence include temperature, wind direction, speed, turbulence, clouds, fog, thunderstorms, atmospheric pressure and icing. Icing can increase the weight of the UAV, as it conglomerates affecting the lift and thrust forces. Air density influences the phases of takeoff and climbing. The other factors affect the visibility of the UAV.

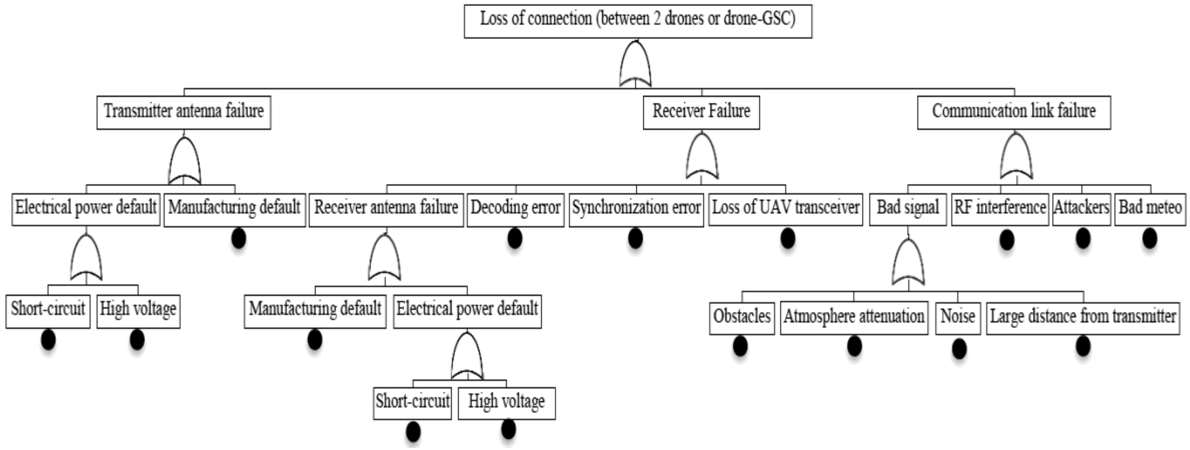


Fig. 3.8 FTA of the loss of connection between Drone - Drone or Drone – GSC: The loss of connection could be due to transmitter antenna failure, receiver failure or due to the communication link

3.5 The model analysis

This part aims to present the analysis probabilistic approach for the top event taking into consideration basic events. A FTA is used in order to estimate the probability of failure of the top event "communication failure" at a certain time. To reach the goal, some reference data can be useful. However, it is not easy to find failure rates for all basic events. In our work, the Nonelectronic Parts Reliability Data Publication (NPRD-2016) database is used to get data for basic events. In this database, it is indicated for each component, an environment and several resources that differ from one component to another. From these sources, we choose the minimum, maximum and mean failure rates with their specific number failed and hours. We proceeded this database for our simulations with real failure rate for equipment. For each one, it includes the following reliability information:

Table 3.1 Reliability information

λ_{min}	minimum failure rate
λ_{max}	maximum failure rate
λ_{mean}	mean failure rate
t_{min}	minimum operation hours
t_{max}	maximum operation hours
N_{min}	minimum number failed
N_{max}	maximum number failed

Table 3.2 extends the failure rates of these events.

Table 3.2 Failure Rate of Basic Events from NPRD-2016 database[2]

Basic Events	**Minimum Failure Rate (λ_{min}) (x10^{-6})**	**Maximum Failure Rate (λ_{max}) (x10^{-6})**	**Mean Failure Rate (λ_{min}) (x10^{-6})**
Operator Error	1.771E+01	6.733E+01	3.191E+01
Broken of proximity sensor	4.290E+00	3.717E+01	4.418E+00
Inaccurate decision of proximity sensor	3.783E-02	4.087E-01	2.981E-01
Altimeter default	2.725E+00	2.067E+01	1.183E+01
Loss of onboard computers	2.786E+00	2.783E+01	2.891E+00
Assembly default	8.992E+01	6.296E+02	2.07E+02
Aerial map inaccuracy	1.007E+00	2.891E+00	1.567E+00
Loss of satellite signal	3.483E-01	4.087E+00	2.891E+00
GPS hardware fault	6.306E-01	6.385E+00	1.452E+00

[2] https://www.quanterion.com/product/publications/reliability-online-automated-databook-system-roads-all-databooks-nprd-eprd-fmd-subscription/

Gyroscope breakdown	6.484E+00	1.794E+01	1.243E+01
Accelerometer malfunction	9.997E-01	7.883E+01	3.504E+00
Overcurrent/ Undercurrent	1.669E+01	7.809E+01	3.711E+01
Battery physical damage	3.483E-01	4.087E+00	3.134E+00
Overheating of the battery	1.262E+01	7.782E+02	4.442E+01
Battery exhaustion	3.483E-01	4.087E+00	2.891E+00
Actuator default	1.218E-01	8.569E-01	3.444E-01
Servomotor default	3.575E-01	3.952E+00	2.961E+00
Disruption of cables	4.000E-05	4.087E+00	4.800E-05
No power for cooling	3.483E-01	4.087E+00	2.891E+00
Fan Default	3.483E-01	4.087E+00	2.891E+00
Manufacturing default	3.662E+00	2.047E+01	1.189E+01
Synchronization error	1.317E+00	4.613E+00	2.487E+00
Loss of UAV transceiver	7.285E-01	3.740E+00	9.635E-01
RF interference	4.905E+01	2.491E+02	1.526E+02
Short-circuit	2.352E+00	9.104E+00	4.813E+00
High voltage	1.445E+00	2.044E+00	1.545E+00
Noise	1.741E-01	1.995E+00	1.445E+00

For the other basic events that are not included in the database, such as bad meteo, obstacles, etc. a minimum, maximum and mean probability based on estimated values, is considered as shown in Table 3.3.

- P_{min} = minimum probability of failure
- P_{max} = maximum probability of failure
- P_{mean} = mean probability of failure

Table 3.3 Probabilities of basic events

Basic Events	P_{min}	P_{max}	P_{mean}
No update from other drone’s data	5.5E-02	3.7E-01	1.4E-01
Snipping from enemy	6.0E-03	1.8E-02	8.0E-03
Electromagnetic pulse	4.6E-03	2.6E-02	1.8E-02
Bad maintenance	4.0E-03	2.2E-02	1.2E-02
Software not updated	4.0E-03	2.0E-02	6.0E-03
OS problem	2.0E-03	8.0E-03	3.0E-03
Virus / Malware	6.0E-03	1.4E-02	1.0E-02
Human Fatigue	1.0E-02	4.0E-02	2.0E-02
Human Inexperience	1.6E-02	6.0E-02	2.4E-02
Misjudgment of weather	1.1E-02	3.6E-02	2.2E-02
Obstacles	1.5E-01	4.0E-01	3.5E-01
Decoding Error	1.2E-03	6.8E-03	4.6E-03
Attackers	2.4E-02	8.0E02	3.0E-02
Bad weather	1.4E-02	6.8E-02	4.7E-02
Atmospheric attenuation	8.0E-03	2.6E-02	1.2E-02
Large distance from transmitter	2.9E-03	1.1E-01	4.3E-03

3.5.1 Weibull distribution

A Weibull distribution on a total duration of 100,000 hours is considered since it represents the most probabilistic approach used to describe a random distribution of a component lifetime (Hallinan, 1993). Our aim is to ensure a successful communication between the UAVs on one side and between the drones and GCC on the other side considering the real conditions of environment, such as large obstacles, bad weather, sniping from an enemy, etc. Since the failure rate λ is considered as a random variable, which is defined between two limits $[\lambda_{min}, \lambda_{max}]$, the failure rate can be modelled using a Beta 1 distribution (Pearson theory on the distributions of probability (Johnson, Kotz, & Balakrishnan, 1995)) in order to obtain the probability that the event occurs before a time t. 1000 simulations were considered in our work. The coefficient of dispersion is considered between 0.05 and 0.1 ($0.05 < v_\lambda < 0.1$) for the events of the NPRD database that depend on a certain timescale. However, all other events are independent as they represent the possibilities of them occurring during the mission. The probability distribution considers two parameters following these formulas:

$$p = -m_y + \left(\frac{1-m_y}{v_y^2}\right) \tag{3.1}$$

$$q = \left(\frac{1-m_y}{m_y}\right) . p \tag{3.2}$$

Where m_y and v_y represent respectively the mean and the standard deviation of a random variable Y.

$$m_y = \frac{\lambda_{mean} - \lambda_{min}}{\lambda_{max} - \lambda_{min}} \tag{3.3}$$

$$v_y = \frac{v_\lambda}{\lambda_{mean} - \lambda_{min}} \lambda_{mean} \tag{3.4}$$

Degradation modelling is proposed using Weibull distribution. The probability takes a shape factor β that should be between 1.5 and 4 whose dispersion is realistic (β=3 in our case). (Hall & Strutt, 2003). The following equation represents the Weibull distribution:

$$P(Y < y) = 1 - \; e^{-\left(\frac{y}{\eta}\right)^{\beta}} \tag{3.5}$$

The scale factor η can be defined regarding λ and β.

$$\eta = \frac{1}{\lambda}\left(\frac{1}{\Gamma\left(1+\frac{1}{\beta}\right)}\right) \tag{3.6}$$

Where $\Gamma(t) = \int_0^{+\infty} e^{-u} u^{t-1} du.$

3.5.2 Communication Failure Probability and Simulations Results

Using the Weibull distribution, the probability of having communication failure between the UAVs is calculated. Two cases are considered: (1) communication failure that is dependent on the four intermediate events of Fig. 1 and (2), being the case that excludes the crash of drone event.

In case 1 (Fig. 3.9), it can be seen that the communication failure depends on time and takes the shape of the crash of drone as most of the events are those of the components failure. The communication is successful with some minor defaults until it reaches 40 000 hours. The probability of occurrence of the failure increases until it attains it maximum at 63 000 hours. From this time, the exchange of information between the drones or between the drone and the ground station will be stopped.

In case 2; we avoided mechanical failures, the collision, the fleet management system failure and the attack. The communication is influenced by the loss of connection where the events are independent on time (Fig. 3.10). The probability of occurrence of the communication failure has a maximum of 0.2 (Fig. 3.11).

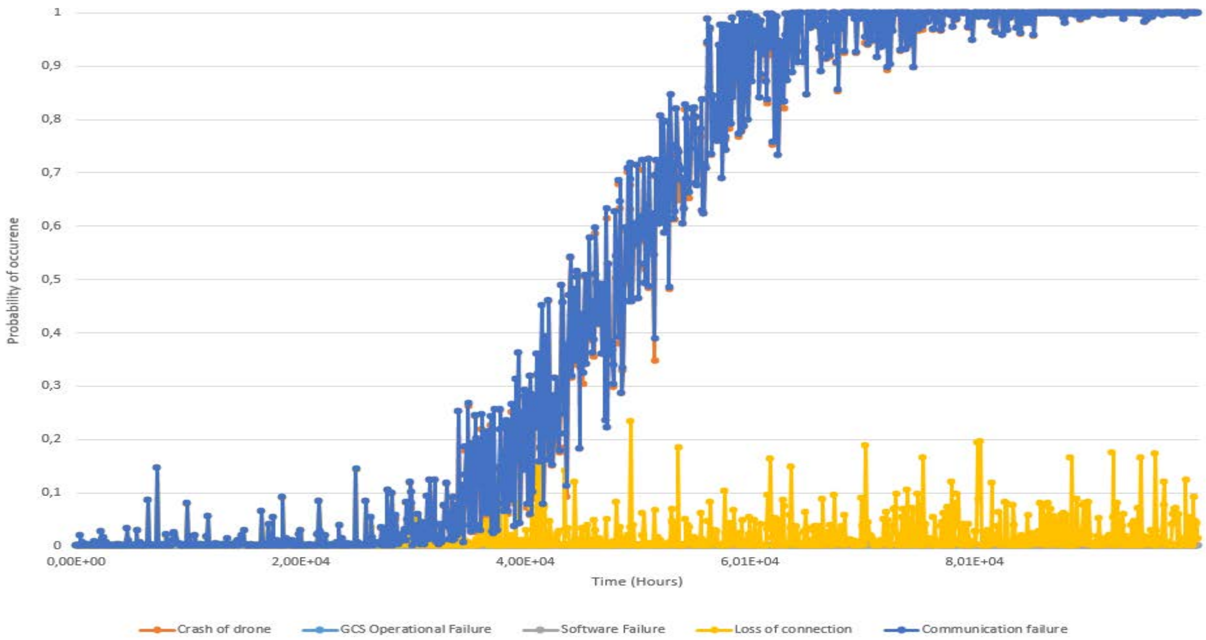


Fig. 3.9 Probability of communication failure between UAVs depending on crash of drone: this figure shows the variation of probability of communication failure (dark blue) in function of time in hours. It takes into consideration the four intermediate events: crash of drone (orange), GCS operational failure (light blue), loss of connection (yellow) and software failure (gray). It appears that the other events have not an important influence on communication failure.

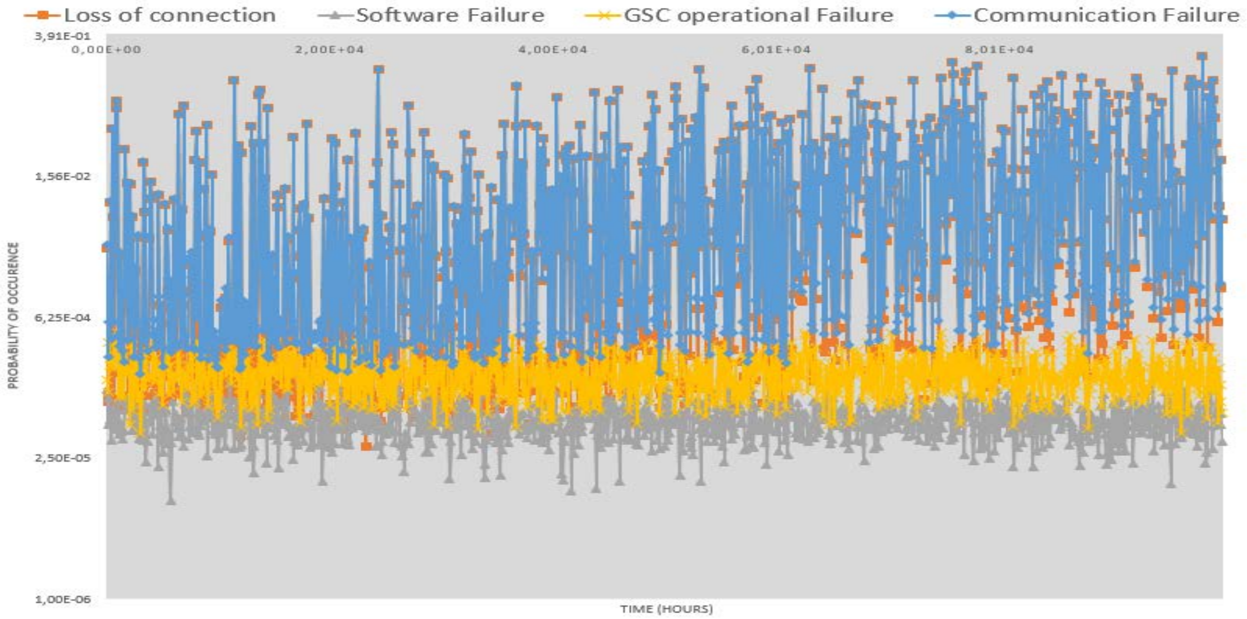


Fig. 3.10 Probability of communication failure between drones without having a crash: it illustrates the same intermediate events without taking a consideration the crash of drone. In this figure, we have the events: loss of connection (orange), software failure (gray), GCS operational failure (yellow).

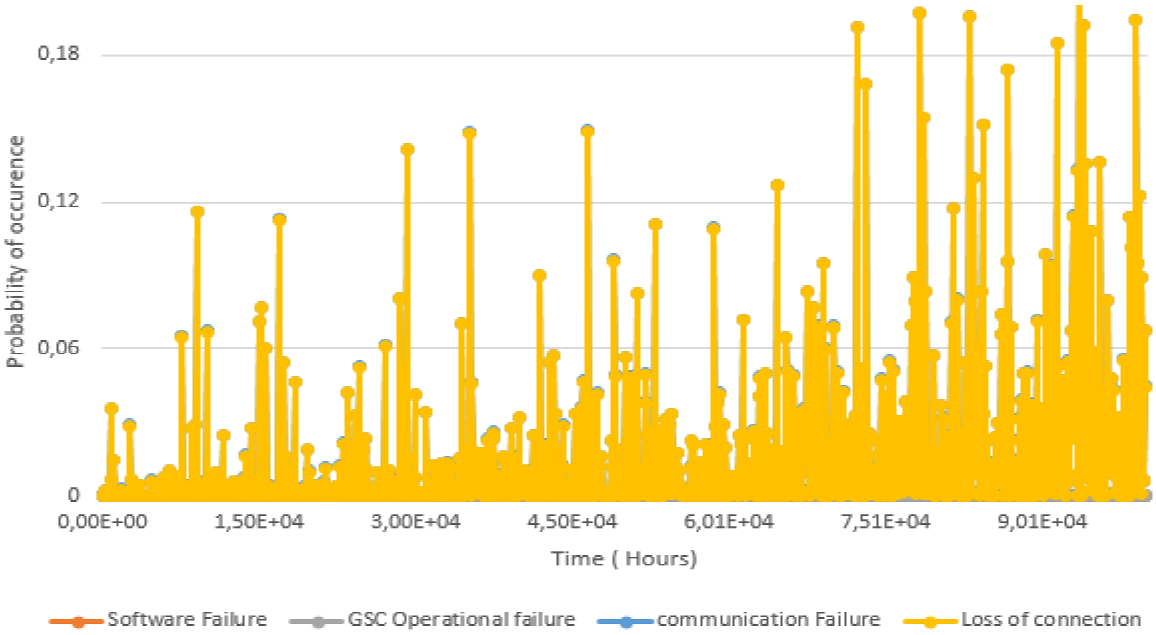


Fig. 3.11 Probability of occurrence of a communication failure: this figure shows the probability of occurrence of communication failure in function of time. Events are represented as follows: software failure (orange), GCS operational failure (gray), loss of connection (yellow) and communication failure (dark blue). The curve of communication failure has the same shape of the curve of loss of connection.

3.6 Conclusion

Several fault tree analysis are considered in this chapter showing the causes of communication failures. These fault trees describe the causes of drone's crash including the details of mechanical failure, the software failures, GSC operational failure and the information flow faults. The degradation modelling is proposed using Weibull distribution. The crash of a drone is the major cause of communication failure. Moreover, loss of communication can also occur due to the loss of connection between the transmitter and the receiver with a probability of occurrence of 0.2. Further studies should be conducted to find suitable solutions that should decrease this probability and ensure more reliable communication. A solution to this issue will be described in chapter 5.

Other methods can be used to evaluate the communication reliability of the drones' network such as the Markov chain that will be discussed in the next chapter. It shows the different riskiest scenarios and their transitions.

4

Communication reliability of drones based on Absorbing Markov Chain

Contents | Chapter 4

4 Communication reliability of drones based on Absorbing Markov Chain

4.1 Introduction

Since a single UAV has a limited energy and payload, the focus is shifted toward the cooperative UAV fleet formation due to their mission in a large hazardous environment. The multi UAV system needs to ensure several properties such as robustness, cooperativeness and scalability (Richards, et al., 2005). These proprieties can be attained by assuring the navigation of each UAV, the control of the whole fleet as well as constant and reliable communication in-between the drones on one side and between the drones and the ground station control (GSC) on the other side. Their different size and payloads, their flight times, the distance between two UAVs and the communication ranges are the causes that affect the overall performance of the fleet formation flight (Wang, et al., 2016). The essential role of these cooperative systems reflects the importance of enhancing reliability in order to avoid the failure of communication between the aerial vehicles. Coordination between them should always be guaranteed despite the uncertainties of the environment, the network and simple failure in the hardware of a vehicle. Therefore, the detection of the anomalous aircraft prevents collisions between the aerial vehicles and the degradation of the team performance. The information flow between UAVs can be collected by an entity on GSC, which controls the mission and makes decisions for the aircrafts; or alternatively, they share the information between them and make collective decisions.

Considering the importance of the reliability of the communication system, this chapter focuses on the development of a different method than the one used in chapter 3, to evaluate reliability. The proposed framework, based on the Markov model, takes in consideration the internal elements, both hardware and software, of the system as well as the surrounding environment. This chapter is organized as follows. Section 2 presents a description of the Markov chain in general and introduces the absorbing Markov chain used in our approach. Section 3 provides the related work, in the literature review, on the reliability of the aerial vehicles focusing on the Markov chain. Section 4 describes the proposed model of state diagram for the communication failure between UAVs. The conclusion is attributed in Section 5.

4.2 Markov Chain (MC)

4.2.1 Definition

A Markov Chain is a stochastic process showing several subsequent states evolving in time. It is considered a memoryless process since the future states rely on the current state, marginalizing the previous states and how the current state is attained (Ross, et al., 1996). Moreover, the Markov Chain aims to analyze complex systems having sequence-dependent failures, redundancy, maintenance strategies, and interdependency. Two sorts of analysis of the Markov Chain can be used with a finite number of states: discrete-time Markov chains (DTMC) and continuous-time Markov chains (CTMC) (Li & Hunter, 2001).

Markov process, which is characterized for dynamic systems, has been applied in many areas such as health services, economics, and engineering. It gives information about the system performance such as the mean time for the first failure, availability, expected number of failures. At each step, the interest may remain in the same state or change from its current state depending on a certain probability distribution. These changes of states are known as transitions and probabilities of these changes are called transition probabilities (Ross, et al., 1996). Furthermore, it is easier for non-specialists in dependability domain to understand a transition state diagram having important information. The transition state diagram describes all the possible transitions between the discrete states

The disadvantage of the Markov Chain analysis is that it is difficult and complicated to contrast in the case of large systems, as it is a time-consuming method (Cox, 2017). Markov models should be limited to small systems having a restricted number of states and strong dependencies. Concerning the continuous-time analysis, it is limited for constant transition rates. In addition, when the size of the diagram increases, it becomes difficult to evaluate by hand the time-dependent unavailability. For this, computerized methods are a solution for large Markov systems.

4.2.2 Absorbing Markov Chain (AMC)

An absorbing Markov chain (AMC) is a Markov chain within any state that can reach an absorbing state. An absorbing state *i* is a state that once it is entered, it cannot be left, and in this case the probability of transition p (i, i) =1 (Ruegg, 1989). As we have seen for the Markov chain, AMC can also be continuous-time with an infinite state space. The chain is known as an absorbing chain in case it fulfills one of the two conditions: it has at least one absorbing state or the transition from each of non-absorbing state to absorbing state is available, even if not in one-step. In other words, it is called absorbing if each state *i* has a path of successors.

Absorbing Markov Chain is characterized with four elements: canonical form of transition matrix, fundamental matrix, time to absorption in addition to absorption probabilities.

i) Canonical form of transition matrix

The state that is not absorbing is called transient state. Considering *r* absorbing states and *t* transient states, and by permuting the states of an absorbing chain so that the transient states come first, the transition matrix follows a canonical form:

$$P= \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix} \tag{4.1}$$

Where *Q* is a *t*-by-*t* matrix

R is a non-zero *t*-by-*r* matrix

0 is a zero *r*-by-*t* matrix

I is an identity *r*-by-*r* matrix

ii) Fundamental matrix

The inverse of the matrix $I - Q$ is denoted *N* where N=I + Q + Q^2 + …

Hence, the matrix $N = (I - Q)^{-1}$ is called the fundamental matrix of an absorbing Markov chain *P*. *N* has n_{ij} as entries, which are the expected number of times where the process that has started in the transient s_i , is in the transient state s_j

iii) Time to absorption

t_i is considered as the number of steps before reaching the absorbing state , knowing that the chain begins in state s_i and t is the column vector whose *i*th entry is t_i . In hence,

$$t = Nc \tag{4.2}$$

Where c is a column vector wherein all of its entries are 1.

iv) Absorption probabilities

b_{ij} is the probability that the absorbing chain which begins in the transient state s_i is absorbed in the absorbing state s_j . b_{ij} are the entries of a t-by-r matrix *B* which can be written:

$$B = NR \tag{4.3}$$

Where *R* is as in the canonical form and *N* is the fundamental matrix.

4.3 Related work

Since the UAV's accidents and failure rates are higher than the manned aircraft, the reliability analysis of these systems presents an important focus for the researchers. The fault-tolerant system and the redundancy hardware do not always represent the efficient solution for this formation fleet flight due to incurred costs and weight. Different methods like the Fault Tree Analysis (FTA) (Abdallah, Kouta, Sarraf, Gaber, & Wack, December 2017), Failure Modes and Effects Analysis (FMEA) has been used to improve the reliability of the helicopters. In some cases, various FTA are needed to represent the different failure conditions of a complex system. The evaluation of reliability of a system considers the state-space models, such as Markov Chain (Frattini, Bovenzi, Alonso, & Trivedi, 2010), that handle the failure/repair of its components and surrounding elements that might affect the reliability model. The Markov chain defines the derogation states of operation, where the functions are not all performed or where the state functions are absolutely stopped. In (Kitchin, 1988), distinct techniques used for establishing Markov models for the reliability of systems are provided emphasizing on the exponential model. It is devised to detect the failure and the method to recover it. The reliability of the flight computer system (FCS) components including the flight computer and the navigation system is discussed in (Pashchuk, Salnyk, & Volochiy, 2017). It enquires a fault tolerant model considering two cases: the case where no additional standby microprocessors are implemented and the case of inherent standby microprocessor. A mathematical model based on Markov chain is applied to improve the reliability for the FCS components. An explanation of the Markov chain and Markov process is given in (Fuqua, 2003). It clarifies the powerful relation between the Markov chain and the reliability, maintainability and safety engineering (RMS) insisting of the International Standards that deal with this approach such as IEC 61165 and IEC 61508 that estimate the probability of failure of a critical system. The issue of packet dropout for the drones' communications via wireless is investigated in (Zhou, Li, Lamont, & Rabbath, 2012). The authors proposed a two state Markov model in order to model the wireless channels taking into consideration the impacts of the Ricean fading. Their computer simulations are better than those of the most known models for wireless channels, the Gilbert-Elliott model (Gilbert, 1960), (Elliott, 1963), since their approach simulate the non-stationary errors. A distributed computing system (DCS) is multiple processors that are interconnected via a network. In DCSs, the information is spread out among the nodes that consist of the data files, the processing elements, the shared resources and programs. In order to ensure the exchange of the information and the control of the data, the reliability of this system is important to be studied. It focuses on the analysis of the distributed program reliability (DPR) and the distributed system reliability (DSR). (Wang J.-L. , 2004) suggested two reliability stochastic measures for these distributed systems: Markov-chain distributed program reliability (MDPR) and Markov-chain distributed system reliability (MDSR). The article describes the employment of one absorbing state for this problem and the probability of transition between the states. An Adaptive Markov Model Analysis (AMMA) is proposed in order to isolate the faults in the critical components. This proposed approach serves to make better the robustness and the availability of the UAV autopilot by incorporating the Fault Detection Isolation (FDI) approach (Krishnaprasad, Nanda, & Jayanthi, 2016). In (Kumar & Jackson, 2009), the paper discusses the reliability models based on the stochastic approach of Markov analysis, merged with the probabilistic approach of Weibull distribution in order to approximate the failure attributes of wear out components. This method is used since the components with wear out failure are characterized with variable failure rates depending on the operation time of the components. For this issue, a state transition diagram for six components optical telescope calibration system (OTCS) is shown. The partially observable Markov decision processes (POMDPs) is used in (Ragi & Chong, UAV path planning in a dynamic environment via partially observable Markov decision process, 2013) in order to determine a path planning for the UAVs to track different targets. The failure analysis of the flight control system of Air Force Institute of Technology (AFIT) UAV based on Markov analysis is elaborated in (Okafor & Eze, 2016). It shows the failure states and the probability of being in these states.

4.4 Communication reliability model for drones' networks

An Absorbing Markov Chain (AMC), where there is at least one absorbing state, is considered. Each state in the transition diagram can be taken as an absorbing state. The transition between states can have multiple steps in order to attain the absorbing state. Two important variables should be calculated: the mean time t_{mean} in addition to the length of the path until the state is absorbed. We aim to evaluate the probability of being in each transient state leading to the absorbing state. Transitions between states are based on the probabilities that are function of the failure rates, of internal components as well as the occurrences of related events within the surrounding environments. The main focus is to maintain a communication between the drones although all the uncertainties that can occur. We propose an Absorbing Markov Chain to model the problem and show the transition between the events that affect the communication. First, the exchange of information and the communication is considered in a normal state. However, several causes can affect this state. The causes can be divided in internal causes at the level of the software and hardware failures and the external causes that are related to the human and the environment.

4.4.1 Hardware failure

The hardware failure can attack the engine, the power, the propellers and the antenna of transmission and reception. The issue is that during a flight, a hardware failure cannot be repairable and lead to an absorbing state of communication failure. Fig. 4.1 shows the causes of the hardware failure of a drone in addition to the transition between the transient states. The antenna failure can directly lead to a communication failure. The drones cannot send and receive anymore the information between them or to/from their ground station control. Moving to the power failure, it can be caused from the ventilation default and the disruption of the cables that induce an overheating of the drone and consequently a power failure. It is also attributed to an overcurrent/undercurrent, physical damage, overheating or exhaustion of the battery. The loss of the UAV transceiver affects the servomotor which its failure involves the actuator default and in hence the engine failure. So on, the engine failure, the power failure and the default assembly of the propellers can lead to the damage of a drone. The crash of the leader of the fleet formation flight is the most risky case since the leader controls the exchange of information between the fleet. Since the crash of a drone cannot be repairable, it leads to an absorbing communication failure between the drones. The failure rates of these events are known from the Nonelectronic Parts Reliability Data Publication (NPRD-2016) database.

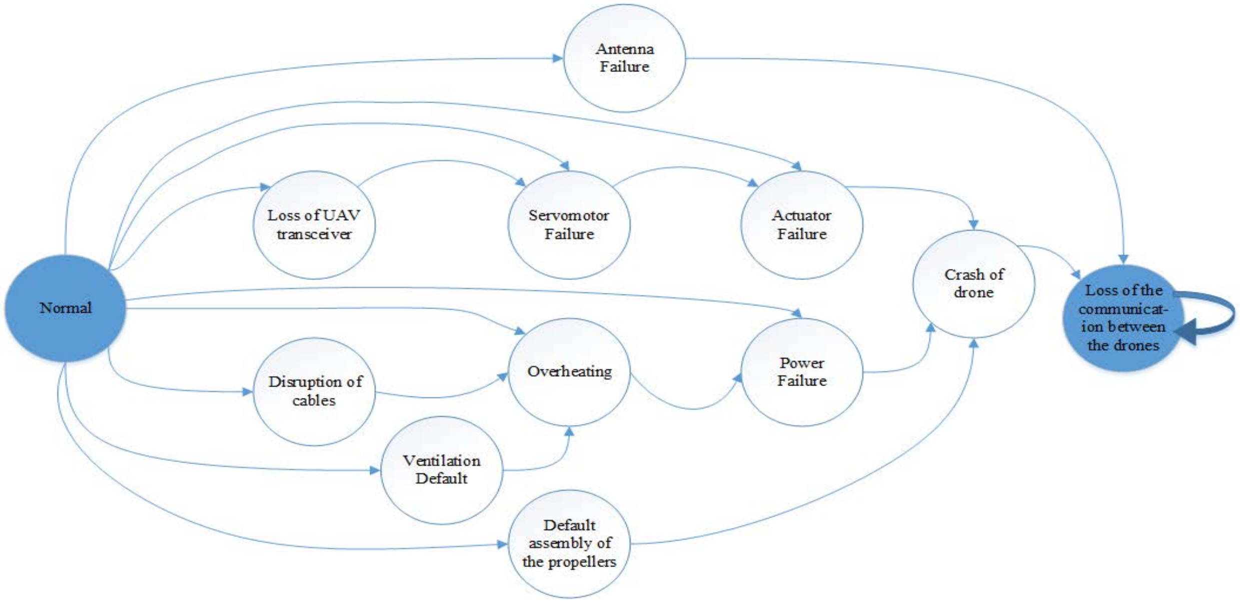


Fig. 4.1 Hardware Failure: This figure describes all the transient states that occur in case of hardware failure and lead to the absorbing Markov state of loss of communication between two drones

Table 4.1 Brief description of hardware failure states

State index	State	Description
ns	Normal State	This is the normal situation where the communication system, between drones and with GSC, is functioning normally.
af	Antenna failure	Hardware fault affecting the transmitter and/or receiver antennas of one or more drones of GSC
lt	Loss of UAV transceiver	Loss of an electronic device that transmits and receives the signal
sf	Servomotor failure	Hardware failure of the motor that permits the control of the position, the acceleration and velocity.
af	Actuator failure	Hardware failure of an electronic speed controllers that is linked to the engine, servomotors and propellers UAV actuators
dc	Disruption of cables	Internal incident that cut the cables
vd	Ventilation default	The cooling system is in failure
oh	Overheating	The temperature of the drone is high due to a disruption of cables or due to a default in the cooling system
pf	Power failure	Due to short-circuit, overcurrent/undercurrent, battery damage, overheating
da	Default assembly of propellers	Loss of more than two propellers
l1d	Loss of one drone	Loss of one drone due to collision with obstacles, snipped by enemies, and/or due to internal operation failure
lmd	Loss of 2 or more drones	Loss of 2 or more drones due to collision between them

Table 4.2 exhibits the failure rates of these hardware events considering the previous state as normal state ns. The annotation of the failure rates is λ from the previous status of transition to the next status of transition. The database gives only the failure rates from the normal states. The other transition failure rates are not known.

Table 4.2 Failure rates of the hardware events from NPRD database[3]

Events	**Minimum Failure Rate (λ_{min}) ($\times 10^{-6}$)**	**Maximum Failure Rate (λ_{max})($\times 10^{-6}$)**	**Mean Failure Rate (λ_{mean})($\times 10^{-6}$)**
Loss of UAV transceiver ($\lambda_{ns\text{-}lt}$)	7.285E-01	3.740E+00	9.635E-01
Servomotor default ($\lambda_{ns\text{-}sd}$)	3.575E-01	3.952E+00	2.961E+00
Actuator default ($\lambda_{ns\text{-}ad}$)	1.218E-01	8.569E-01	3.444E-01
Disruption of cables ($\lambda_{ns\text{-}dc}$)	4.000E-05	4.087E+00	4.800E-05
Ventilation Default ($\lambda_{ns\text{-}vd}$)	3.483E-01	4.087E+00	2.891E+00
Overheating ($\lambda_{ns\text{-}oh}$)	12.617E+00	778.2E+00	44.421E+00
Power Failure ($\lambda_{ns\text{-}pf}$)	2.352E+00	9.104E+00	4.813E+00
Default assembly of propellers ($\lambda_{ns\text{-}da}$)	8.992E+01	6.296E+02	2.07E+02
Antenna failure ($\lambda_{ns\text{-}af}$)	3.662E+00	20.467E+00	11.886E+00

4.4.2 Software failure and collision events

The normal situation can be affected by a software failure bringing a disruption to the communication between the drones (Fig. 4.2). An infected virus or malware represents an important reason for a mal-functioning of the UAV. It disturbs the operating system OS of the drone in a manner that the two causes engender a software fault. The virus/malware and the OS fault can also

[3] https://www.quanterion.com/product/publications/reliability-online-automated-databook-system-roads-all-databooks-nprd-eprd-fmd-subscription

attack the ground station control (GSC). The reliability of the software is ensured by regular updates of the operating system in addition to a good antivirus. The software faults affect the GPS data leading to a communication error between the drones or between one drone and the base station in a manner that the communication is not lost but there is an error in exchanging the information. The GPS data inaccuracy permits a confusion of the position of other's drones that influences the coordination of the fleet formation flight. The wrong positions' data received from other drone might lead to collision between two or more UAVs or even to collision of the drones with an obstacle such as a building, trees, birds, etc. From the one hand, the collision between two drones leads to an absorbing state that cannot be avoided and repairable, the loss of communication between two or more drones *lcma*. On the other hand, the collision with obstacles in addition to the snipping of a drone from an enemy cause the loss of communication with only one drone *lca*, since it will not be presented in the fleet. This event is also an absorbing state.

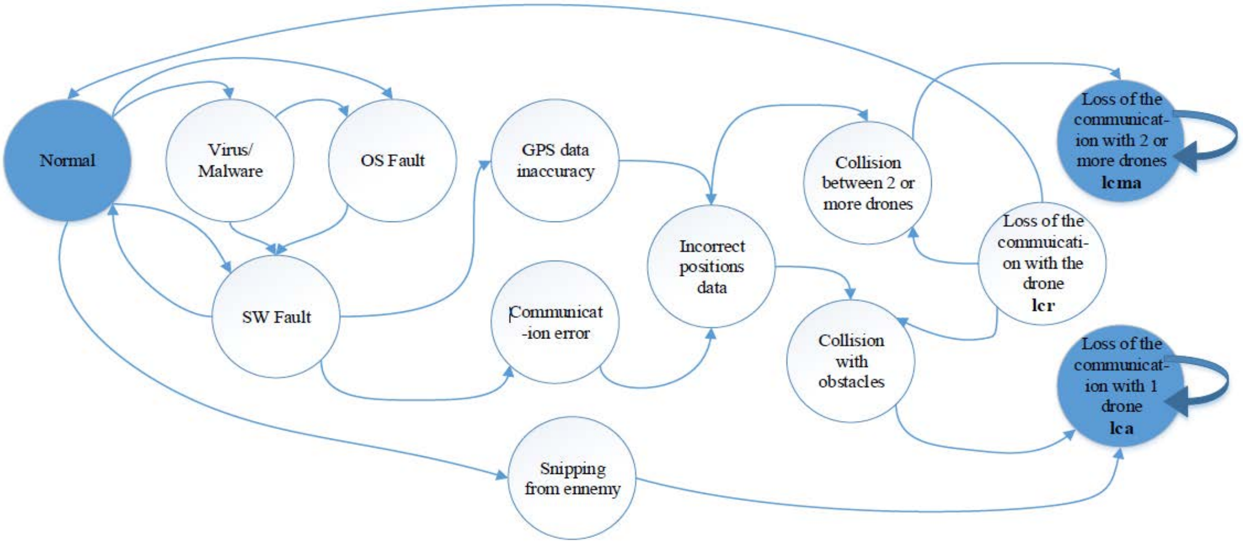

Normal
Virus/ Malware
OS Fault
GPS data inaccuracy
SW Fault
Communicat -ion error
Incorrect positions data
Collision between 2 or more drones
Loss of the communicat- ion with 2 or more drones lcma
Loss of the commuicati- on with the drone lcr
Collision with obstacles
Loss of the communicat- ion with 1 drone lca
Snipping from ennemy

Fig. 4.2 Software failure and collision events: this figure shows the transient states in case of software failure and collision events that lead to two distinct absorbing Markov states

Table 4.3 Brief description of software failure and collision events states

State Index	State	Description
ns	Normal State	This is the normal situation where the communication system, between drones and with GSC, is functioning normally.
vm	Virus or malware	The system has been infected by a virus or malware leading to mal-functioning and abnormal behavior
OSf	Operating System fault	The operating system of a drone or GSC is not properly functioning due to being infected by virus or malware or due to some internal fault or error
swf	Software fault	A fault in the software that handles GPS data or the communication system within the drone or the communication system within the GSC
gpsf	GPS data inaccuracy	GPS data of one or more drones are inaccurate
wpd	Incorrect positioning data	Wrong positions of one or more drones have been communicated to other drones and/or GSC
cf	Communication error	No communication between 2 or more drones and/or between 1 or more drones and GSC
cd	Collision between drones	Collision between 2 or more drones have occurred
co	Collision with obstacle(s)	A drone has collided with obstacle(s)
se	Snipping from enemy	A drone or more have been shut down by enemies or third parties
lcr	Loss of communication with a drone	Loss of communication with a drone due to environmental conditions or software faults.

		This state is repairable and the system could go back to its normal state (ns)
lca	Loss of communication with a drone due to the loss of the drone	Loss of communication with a drone due to the loss of the drone itself caused by collision, snipping with enemies, environmental conditions and/or some internal faults. This state is not repairable and therefore it is an absorbing state.
lcma	Loss of communication with multiple drones	Loss of communication with multiple drones due to collision between them. This state is not repairable and therefore it is an absorbing state.

4.4.3 Exterior factors

Different exterior factors influence the communication of the fleet formation flight. It englobes the animals, the weather, the obstacles and the human. The bad weather is an important state to prevent it. It includes temperature, wind, clouds, rain, ice, thunderstorms and fog. The transmitted signals might be subjected to an atmospheric attenuation due to a bad weather or other environmental conditions. An attenuation involves an interference and a noise that contributes to a bad signal transmitted between the aerial vehicles. If the medium of communication is exposed to jamming, echoes and noise, then that might interfere with what is transmitted, affecting the overall communication. Synchronization and the decoding of the message is an essential mechanism in the transmission of the message that can be affected by the interference phenomenon. The human plays an important role in the communication especially with the GSC.

The exhaustion of the GSC operator and his lack of experience and qualification in flying a certain type of drones contribute to the human error. The distance between the source and the destination can influence the quality of the received information as when the distance increases, the transmitted signal can be exposed the attenuation and atmospheric noises. In order to avoid these events, the operator should chose the typical environment for the fleet. He might take in consideration the weather, the season and the time of flight. However, although all these events lead to the loss of communication with the drone, but this state is not absorbing. It is repairable since we can change the environment, chose the right persons to flight the fleet, the interference could affect the signal for a certain time then the fleet continues its mission. Figure 4.3 resumes the external factors. On the contrary of hardware failure, the loss of communication with the drone lcr is a repairable state. It could be caused by software faults or environmental effects. A software fault in the communication could be repaired through alternative channels or by the ground station. The environment effects can be controlled by making the drones flying in close distances or alternatively planning the mission in some other time with better weather conditions. Once the *lcr* occurs, it might attribute to the collisions between the drones or with an obstacle.

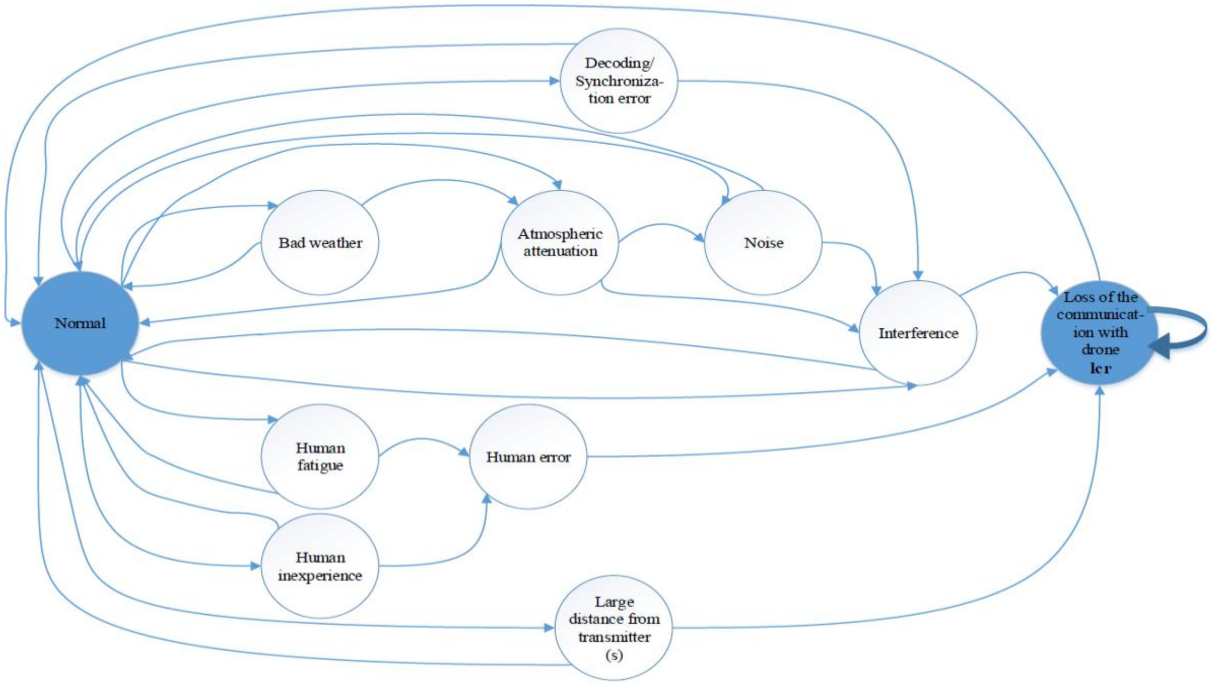

Decoding/ Synchronization error
Bad weather
Atmospheric attenuation
Noise
Normal
Interference
Loss of the communication with drone lcr
Human fatigue
Human error
Human inexperience
Large distance from transmitter (s)

Fig. 4.3 Exterior factor events: this figure represents the transient states showing the exterior events that affect the communication of drones.

Table 4.4 Brief description of exterior factor states

State Index	State	Description
ns	Normal state	This is the normal situation where the communication system, between drones and with GSC, is functioning normally.
bw	Bad weather	A bad weather that might have impacts on the communications between drones and/or between the drones and GSC
aa	Atmospheric attenuation	Transmitted signals might be subjected to attenuation due to bad weather or other environmental conditions
no	Noise	Transmitted signals might be subjected to noise
in	Interference	Transmitted signals might be subjected to interference
de	Decoding/synchronization errors	Transmitted data might be subjected to decoding and/or synchronization errors
ld	Large distance	One or more drones have flown away from transmitters of other drones and GSC
hf	Human fatigue	GSC operator is experiencing exhausted and tired
Lcr	Loss of communication with a drone	Loss of communication with a drone due to environmental conditions or software faults. This state is repairable, and the system could go back to its normal state (ns)

4.5 Comparison between Absorbing Markov chain and Fault Tree Analysis

Reliability analysis of critical applications is complicated to estimate due to the characteristics of fault tolerant systems for these applications. Systems should attain high levels of reliability by using several methods such as employing high level of redundancy, error recovery techniques in addition to dynamic system reconfiguration (Dugan, Bavuso, & Boyd, 1993). The two well-known techniques used to evaluate reliability of a system are Markov models and Fault Trees.

Using fault tree as reliability analysis has some drawbacks. Fault tree analysis with many basic events is expensive in terms of developing of a model or in solving it. It does not take into consideration in the standard method the dynamic behavior, such as intermittent errors, transient recover and sequence dependency. Markov models are modeling technique for dynamic system. It is simple to construct a Markov model; however, it could be error prone.

Fault trees represent the faults in a current state of system and can identify its failure modes in a briefly and comprehensible way. In order to overcome the problem of sequence dependent failures, fault tree representation could be transformed into a Markov chain that could be augmented with recovery models (Bouissou & Bon, 2003).

In this work, from the fault tree analysis, the sequence dependencies that lead to an absorbing state of communication failure are represented in order to prevent them. The model represents the repairable states that could decrease the communication failure.

4.6 Conclusion

Different states diagrams are presented in this paper showing the causes of loss of communication between the drones or between the drones and the ground station control. It includes the hardware failure, the software failure in addition to the external factors that affect transmitted signals. The software failure is a repairable state in addition to the external factors that we can prevent them by choosing the suitable environment, season and time. On the contrary, as they are not recoverable, hardware failures will lead to an absorbing state for the loss of communication.

We aim to consider in our future works the failure rates of the external and software events, the failure rates of transitions in addition to the repairable rates taking into consideration the different strategies of fleet formation flight.

After modelling two different methods (FTA, AMC) on the risks that can influence on the communication between the UAVs or between UAVs and GSC, we will focus, in the following chapter, on the reliability of reception of all the messages sent by the sender (drone or GSC) in order to be surely from their receipt. The objective is to calculate the well-suited number of retransmissions of data considering several parameters.

5

Message transmission reliability for drones’ networks

Contents | Chapter 5

5 Reliability of message transmission for drones' networks

5.1 Introduction

Communication systems are defined as the concept of transferring the data between two systems having common procedures in order to establish an integrated system and accomplish a certain purpose. In our work, a specific communication system is considered: the Unmanned Aerial Vehicles (UAVs).

Initially, drones were used in the military domain in order to prevent the risk of pilot's life in the risky missions such as the surveillance of a target. Recently, they have been then proliferated and used by civilians and businesses by implementing them for mapping, taking photos and videos, for monitoring and also in the agriculture domain (Hayat, Yanmaz, & Muzaffar, 2016), (Noor-A-Rahim, et al., 2019). Moreover, they are characterized with payload such as a camera, a video camera, a thermal sensor, audio etc.; that is designed to capture information in the difficult environment of a mission (Austin, 2011). In order to improve the mission, they should be disposed as UAV swarms in a manner that they can divide tasks between them and share information (Peng, 2018).

A multi-UAV system allows for the coverage of spacious zones in a way that enable UAVs to observe the area from different points of view. It increases the reliability of the data, but it requires a high degree of coordination between the aerial vehicles, and between them and the ground station. Reliable communication between UAVs or between UAVs and the GCS as most UAVs send information that needs high throughput, such as images and videos with high resolution.

In this chapter, we aim to guarantee a reliable communication despite all factors that could influence on the transmission of data flow and the medium channel. In the rest of this paper, Section 2 presents the existing data transmission protocols in the literature, and their reliability.

Section 3 describes the related work of existing routing protocols for UAVs. Section 4 gives a brief description of drones' network in terms of data types and communication channels. In Section 5, a model is proposed for the reliability of message exchanges in UAV networks based on well-defined parameters. This model serves to determine the number of retransmissions that assure reliable data reception by teammates. Finally, a conclusion is presented in Section 6.

5.2 Communication reliability

An important problem that should be taken into consideration is the reliability of the transmission of data especially during real-time missions. Three distinct data transmission protocols are familiar and used in the telecommunications: User Datagram Protocol (UDP) (Postel, User datagram protocol), Transmission Control Protocol (TCP) (Postel, Transmission Control Protocol, 1981), and Stream Control Transmission Protocol (SCTP) (Stewart, 2007). In the connectionless-oriented transport layer, UDP, the source does not receive an acknowledgment that data has been received by the receiver, conversely to the TCP and SCTP that are reliable protocols. Though the reliability of these two protocols, they cannot be used in the multicast delivery and they are characterized with the complexity of the control mechanism. Hence, it is necessary to deal with the reliability and efficacy of the data flows' transmission of these contradictory protocols. For this reason, researchers focus on a method to develop a more reliable UPD protocol, called Reliable User Datagram Protocol (Yong-qiang & Hong-bin, 2010). The authors (Guo & Chengtong, 2012) implement a queue to keep temporarily in reserve the data in order to let the sender send and then send them next packet without receiving an acknowledgement from the receiver. The lack of need to await an acknowledgement guarantees more time and enhances the efficiency of the data transmission.

In (Hei, Chen, Lu, & Meng, 2017), several factors are considered in improving the reliability of UDP such as the security, congestion control and the error control. This improvement is assigned in the multi agent communication, such as the UAVs network. RUDP, which is not used for big data transmission because of its long waiting delay, has taken some TCP characteristics such as the retransmission of the undelivered packets, the error control and order of the packets, the recognition technology, the data security and packing/unpacking of information.

However, TCP protocol is not advised to be use for real-time missions. For this reason, researchers prefer to use the RUDP to increase the response.

Concerning the data transmission protocols, the authors of (Hei, Chen, Lu, & Meng, 2017) show the existing protocols then establish the Deque - ERUDP (Deque Efficient and Reliable Protocol Based on UDP) layer between the transport and application layer of the TCP/IP layers architecture for data efficiency and reliability. It consists of recognition, data packet subcontracting and retransmission of the data. It combines with the UDP in a manner that it uses, identically to the TCP, three-way of handshake, before transmitting the data, between the sender and receiver. The sender sends the message to the data buffer queue which exists with the sender and the receiver. In this manner, it averts the congestion of the channel by controlling the Timeout Interval of Queue (TIQ) and the Timeout Interval of Packet (TIP).

The different applications for UAVs in the military and civilian missions such as delivery of parcels, firefighting, rescuing, and illegal hunting detection, increase their importance in the last decades. For this, attackers try to get access to the communication link to get the data sent. Authors focus on the problem of the lack of encryption of the communication channel between the UAV and the GCS. In (Pleban, Band, & Creutzburg, 2014), it is described the security of the Parrot AR Drone 2.0 quadcopter. However, the FTP (port 21) and Telnet (port 23) are open access, without any sort of encryption by passwords, which lead the unauthorized users to send malicious data especially as the remote access is available. However, improving the security is a pricey solution. In (Asadpour, Giustiniano, & Hummel, 2013), two nodes are only considered for the communication, i.e. Drone-Drone or Drone-GCS, using the IEEE 802.11n. Various papers focus on sending wrong GPS signals, known as GPS spoofing, to cause the UAV to lose its path (Kerns, Shepard, & Bhatti, 2014).

The reliability evaluation of the communication considers several factors such as the antenna characteristics, the frequency, the bandwidth and the propagation of the signal. Despite the importance of this phenomenon, this topic is not well examined. The authors of (Vergouw, Nagel, Bondt, & Custers, 2016)discuss the legal spectrum and the distinct types of payloads in UAV networks. Moreover, in (Chandhar, Danev, & Larsson, 2016), the Massive MIMO (Multiple Input Multiple Output) is suggested to guarantee the performance of a swarm of UAVs that require for communication a high throughput, low latency of transmission and low power consumption. This approach is proposed since the Bluetooth, Wireless Fidelity (WiFi) and Zigbee that allows the short-range communication and characterized with a limited throughput, cannot ensure simultaneous communication between the fleet and GCS.

5.3 Related works

The characteristics of a fleet formation of UAV networks are close enough to a MANET (Mobile Ad-hoc Network) network. FANET (Flying Ad-Hoc Network) is a special MANET, in which the UAVs that represent the nodes, provide an Ad hoc network (Priya, Jakhar, & Syan). Some papers discuss the safety assessment for a UAV (Gonçalves, Sobral, & Ferreira, 2017) and optimization of the mission using Petri nets (Levitin & Finkelstein, 2018). Many works focus on communication protocols facilitating the cooperation between UAVs. The papers (Jiang & Han, 2018) and (Maxa, Ben Mahmoud, & Larrieu, 2017) enumerate and compare the different routing protocols used for UAVs, dividing them into five classifications reactive routing, single-hop routing, hybrid routing, proactive routing, and position-based routing. In (Lee, et al., 2018), a ground control system (GCS) routing protocol is elaborated to ensure a reliable multi-UAV control system based on the GCS utilization and to enhance the network performance. Therefore, in (Khan, Khan, Safi, & Quershi, 2018), authors present the important topology-based routing protocols in FANETs enhancement and improvement of throughput, the network load and the end-to-end delay.

The Micro Air Vehicle Communication Protocol (MAVlink protocol) is a point-to-point protocol that allows agents to communicate over wireless channel and ensures data transmission (Marty, 2013). This protocol permits the exchange of information flow between the flying robot and the GSC having three types of vulnerabilities: availability, confidentiality and integrity. The GCS transmits control commands to the UAVs while the drone transmits telemetry and status data (Veena, Vaitheeswaran, & Lokesha, 2014). Messages are transmitted as data packets and a checksum is available for the error correction. When the checksum gives different results, the message will be deleted. 255 aircraft can be controlled by one GCS when we use the MAVLink. It is characterized with 8 bytes as minimum packet length and 263 as maximum packet length

(Atoev, Kwon, Lee, & Moon, 2017). Moreover, it is important to enhance the security of this protocol precluding the intervention of eavesdroppers by adding encryption (Butcher, Stewart, & Biaz, 2013).

The MAVLink protocol is a criterion for the bidirectional communication between the fleet of UAVs and the GCS. The authors of (Domin, Marin, & Symeonidis, 2016) handle the vulnerabilities of MAVLink by adding the principle of fuzzy logic. Lately, we refer to the wireless nodes used as virtual antennas to enhance the reliability of point-to-point links. Researchers focus on the necessity of the reliability of sensor data. The sensor faults and measurement errors caused by faulty sensor readings lead to a lack of reliability. For this, Wei-min Qi et al. (Qi, Hu, Xiao, & Zhang, 2013) propose a new algorithm for data verification based on data refinement, measurement error elimination and adaptive fault checking. In (Palat, Annamalau, & Reed, Cooperative relaying for ad-hoc ground networks using swarm UAV, 2005), they describe the influence of the Doppler effect and the position error on distributed transmit beamforming due to various speed of wind. Tao et al. address the problem of reliability and robustness of the wireless video transmission of UAV by proposing a pixel-row-interleaved error concealment algorithm (Wang, Zheng, Lin, Shihong, & Xie, 2018) .

5.4 Drone Networks

5.4.1 Data types

We can distinguish three types of data in a multi UAV system: sensing, coordination and control. For real-time missions that are time-critical like rescue and search, a distributed architecture will be applied, and reliable networking and sensing data are necessary to guarantee the success of the mission. Conversely, for missions that are not time crucial, such as monitoring of the environment, a centralized architecture can be applied, the trajectory of the UAVs can be known before the mission starts and hence, the sensed data could be sent after the mission has been finished. Concerning the delivery of parcels, the UAVs can be implemented based on a centralized or decentralized architecture, but the communication and sensed data should be reliable in order to avoid collisions and obstacles and ensure a safe delivery.

5.4.1.1 Sensing

This type of data includes the transmission data of onboard sensors to the station since onboard analysis of data is unachievable. Distinct sensors are installed onboard the aerial vehicles depending on the type of mission that they are required to undertake, e.g. passive sensors like cameras for aerial monitoring, pictures transmission or live video streaming, and active sensors like wireless transmitter-receiver, laser-scanners, ultrasonic for observation. These sensors have to be low weight; nonetheless, they have to provide an accurate and reliable data with sufficient quality to meet the purpose of the mission. With a high resolution of images, an image or a video stream has a downlink throughput up to several megabits per second. For this reason, transmission reliability is a necessity especially for video streaming since a dropped packet can influence the result of the mission in addition to decoding due to high compression/decompressing rate. For medium reliability, increasing the throughput in parallel with decreasing the compression rate is able to ensure the goal.

5.4.1.2 Coordination

This information flow is disseminated among the UAVs ensuring the communication between them for local decision. It guarantees the cooperation, collision avoidance and self-organization of the network without a direct intervention from the base station. The unmanned vehicles coordinate their positions to accomplish an end-to-end transport of data. It could be also a sort of relaying of the information. Therefore, a certain level of autonomy is essential to increase the reliability of the network. In case two flying robots are close exceeding a certain distance, they should stop preventing crashes and delay in data transmission. In this type of data, the UAVs should ensure the task allocation.

5.4.1.3 Control

Control reflects the information between the GCS and the vehicles in sort of mission commands that control the behavior of the UAVs, e.g. telemetry data. The vehicles should relay their positions to the GCS to enable decision-making to be made. Communication should be robust against the factors in the environment and the modification in the topology of the network.

5.4.2 Data transmissions Links

In telecommunications, the information flow such as voice, images and videos are sent through a data link that is specified to connect a device to another. Data links comprises physical devices that are responsible for sending and receiving data in addition to the protocols that determine the method of sending/receiving. A UAV relies on an operator at ground level to ensure its control, and on protocols for the communication. Moreover, each physical device is specified by a frequency, message format, data rate, link protection, transmission range in addition to the weight and power of the transceiver. In a fleet formation flight of drones' system, there are different links that can be distinguished:

- Air-to-Air links
- Ground-to-Air links
- Air-to-Ground links

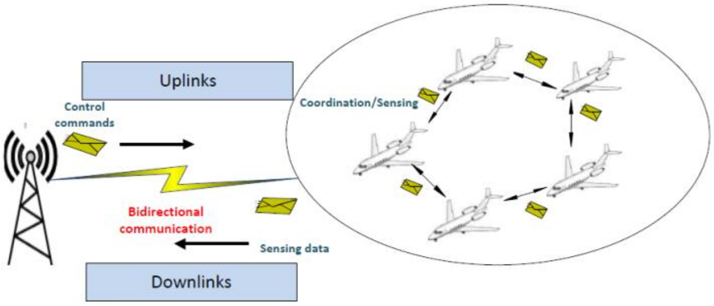


Fig. 5.1 Communication links in UAS system

From one hand, the Ground-to-Air and Air-to-Ground links are dedicated for the information related to the mission such as the commands that are sent to control the mission from the ground control station (GCS) and the telemetry information to the GCS in order to update the mission status. Air-to-Air links are served for the delivery of sensor and map data within the fleet. Despite the different properties of the links such as their throughput, reliability and delay constraints, data should be reliably delivered.

The microwave spectrum is used for the transmission between the UAVs instead of an optical one that is not effective for all the applications. Several wireless technologies have been used for UAV networks such as 3G/LTE, IEEE 802.111 (Wi-Fi), IEEE802.15.4 and infrared. The authors of (Andre, et al., 2014) elaborate the different technologies used for commercial micro aerial vehicles (MAVs) by listing the distinct projects with the functions of each technology. Since the communication between the drones from one side and between the drone and the GSC from the other side is based on wireless communication, we elaborate the drawbacks of this interconnection. A wireless channel suffers from an insufficiency of information confidentiality in addition to high latency. This sort of channel is exposed to noise, interference and jamming in a manner that affects the channel reliability and lead to erroneous data and fault decisions.

Remote attacks are available when it comes to a wireless communication. Eavesdroppers are able to spy the channel in order to have access and know the data sent from a source to a destination. Attackers can also send malicious commands to the UAV or make changes in the operating system leading to several faults, especially in the military applications. Our principal goal is to warrant the receipt of all the data sent from the flying robots taking in consideration the task that they should fulfill. Due to their attributes like adaptive altitude, mobility, modification in their network's topology and flexibility, the signal propagation will be affected. In addition, the characteristics of the antennas, in terms of polarization and radiation pattern, affect the transmission of information flows. Hence, we strive to evolve the robustness of the sending/receiving protocol by calculating the number of times the message should be sent until it will be definitely received by the GCS or by the other aerial vehicles.

We concentrate in our work on the reliability of the communication link of UAVs since the environment that is applied for drones' missions is more and more complex. For this, the channel medium, which connects the UAVs among them and between them and the GCS, should provide a security and an effective data link. The UAV system has major requirements in order to emphasize the success of the mission:

- Low latency
- Reliability
- Efficient link
- Bidirectional transmission
- Long flight time
- Long range operation

Since the communication channel is responsible of the transmission for the control, sensed and coordination data and influences the performance of the data link, the UAV data link should ensure a high data rate transfer in addition to high reliability in data transmission. To provide an effective data link, the wireless communication for a civil UAV refers to the ISM bands (Industrial, Scientific and Medical bands) occupying different frequencies, e.g. 2.4GHZ, 433 MHz, 815 MHz and 5.8 GHz. In this band, receivers should have immunity against the interference problems.

Nowadays, the requirements of long flight time and long-range operation lead us to adopt the best potential modulation technique that assures the efficacy and reliability of the data link.

As we previously describe, there are two types of communication link between the drone and the GCS:

- **Uplink** (from GCS to UAV) is dedicated to transmitting the control information. These links require stability and robustness to overcome the noise and interference. For this reason, the 2.4 GHz frequency is mostly used for control with a combination of two spread spectrum that are the direct sequence spread spectrum (DSSS) and the frequency hopping spread spectrum (FHSS).

- **Downlink** (from UAV to GCS) is used to transfer the sensed data from the onboard sensors and cameras, e.g. real-time images and videos. In order to ensure reliable transmission, they should provide high throughput. For this, they often use 5 GHz frequency for videos with orthogonal frequency-division multiplexing technology (OFDM).

5.5 The message transmission model

This section presents the reliability model to ensure the transmission protocol and guarantee the message reception by a receiver. We will proceed in three steps to describe the model. The following subsections represent the parameters used for retransmission’s number calculation. Subsection V.1 presents distinct modulations used for UAVs. Moving to subsection V.2, it describes the Bit Error Rate (BER) parameter that depends on the modulations type. In subsection V.3, Packet Error Rate (Pe) and Packet received during an attempt (Preceived) are calculated. In the last subsection, the retransmissions number of messages, depending on a successful probability of the protocol is estimated. presents distinct modulations used for UAVs. Moving to subsection V.2, it describes the Bit Error Rate (BER) parameter that depends on the modulations type. In subsection V.3, Packet Error Rate (Pe) and Packet received during an attempt (Preceived) are calculated. In the last subsection, the retransmissions number of messages, depending on a successful probability of the protocol is estimated.

5.5.1 Modulation techniques for drones

Let us describe the three types of modulation techniques used for drones [33] in our approach:

5.5.1.1 DSSS

The direct sequence spread spectrum (DSSS) represents a sort of spread spectrum modulation. It is limited firstly to military applications before it is intervened in the civilian domain. This modulation transmits the digital signal through a large bandwidth in a manner that it occupies simultaneously the whole bandwidth when the signal is passing within the bandwidth across several frequencies. It operates at high data rates with low signal to noise ratio (SNR), conversely to FHSS. It is able to communicate with low probability of interference and jamming.

5.5.1.2 FHSS

The other technique of spread spectrum, known also as anti-jamming technique, is the frequency hopping spread spectrum. As for DSSS, a predetermined information about the signal is recognized for the success of the link. In this technique, the signal should rapidly change frequencies at high energy and narrower bandwidth than DSS based on the frequency hopping principle. The hop time is defined as how many times it takes to change frequencies.

5.5.1.3 OFDM

The Orthogonal Frequency Division Multiplexing (OFDM) is a familiar multicarrier technique used for communication systems. The communication technique that is realized for variable data rates is well used for its advantages such as it is resistant to multipath fading without referring to complex equalizers. It is supposed to transfer the data using distinct modulation techniques, e.g. Quadrature Phase Shift Key (QPSK), Binary Phase Shift Key (BPSK) in addition to Quadrature Amplitude Modulation (QAM). In OFDM, each channel has multiple sub-channels characterized with different frequencies that are used in parallel transmission.

5.5.2 Bit error rate (BER)

Another factor that is considered to examine the performance of the wireless communication channel of a UAV network is the bit error rate (BER). It defines the number of errors that are present in the received data and can be estimated by subtracting the transmitted signal from the received one. The BER comprises the number of bit errors per transmission (P_b) divided by the total number of sent bits per transmission (P_S) as shown in this equation:

$$BER = \frac{P_b}{P_S} \tag{5.1}$$

As mentioned in our previous work based on fault tree analysis (Abdallah, Kouta, Sarraf, Gaber, & Wack, December 2017) or on Absorbing Markov Chain (Abdallah, Sarraf, Kouta, Gaber, & Wack, 2018), the exterior conditions and the modification of the propagation of the signal play an important role in the degradation of the channel and in increasing the number of errors in the received message. Mostly, the multipath fading and the Additive White Gaussian Noise (AWGN) are the main reasons for the performance's degradation in wireless channels. The AWGN covers the unwanted signals, e.g. electronic devices, switches, sunrays, atmospheric particles, etc. When the noise is added to the data sent, it becomes difficult to extract the original information by the receiver. As for the multipath fading, it arises when the receiver receives distinct signals. It is preferable that the signal has a line-of-sight (LOS) path without any obstacles. However, many reasons such as reflection, shadowing, scattering, diffraction, due to mountains, buildings, trees and obstacles, affect the propagation of the signal.

It is considered that an acceptable BER for sending the control commands on the uplink could be in a range between 10^{-6} –10^{-9}, while the acceptable BER to transmit the sensed data, known as the payload, on the downlink is estimated to 10^{-3} – 10^{-4}. To decrease the effects of an error, it is necessary to recover the original data and evolve the overall BER based on a high level of error correction. The goal in the UAS network is to highlight a bidirectional communication between two nodes with a high signal-to-noise ratio (SNR) in a manner that the BER will be trivial and will not have an influential effect overall network.

The BER formula for diverse modulations in presence of AWGN can be expressed in the following table:

Table 5.1 BER over AWGN for different modulations

Modulation technique	Bit error rate (BER) formula
BPSK	$BER = \frac{1}{2}\, erfc\sqrt{\frac{E_b}{N_0}}$
QPSK	$BER = \frac{1}{2}\, erfc\sqrt{\frac{E_b}{N_0}}$
M-PSK	$BER = \frac{1}{m}\, erfc\sqrt{\frac{mE_b}{N_0}}\, sin\left(\frac{\pi}{M}\right)$
M-QAM	$BER = \frac{2}{m}\left(1 - \frac{1}{\sqrt{M}}\right) erfc\sqrt{\frac{3mE_b}{2(M-1)N_0}}$

M defines the constellation size of the modulation and m=log2 (M).

$E_b\,/N_0$ is the ratio of the Energy per Bit divided by the noise power density.

The theoretical BER formula for DSSS over AWGN is expressed as:

$$BER = \frac{1}{2}\, erfc\left(\frac{\sqrt{E_b}}{\sqrt{J\,T_C}}\right) \tag{5.2}$$

Where T_C : Chip duration and J: Jamming power.

However, the theoretical BER formula for FHSS over AWGN follows this formula:

$$BER = 0.333\ exp\big((-SNR * R_C) \div 2\big) \tag{5.3}$$

Where R_C is the chip rate.

We consider in our work some modulation techniques, e.g. BPSK, QPSK, M-PSK and M-QAM, with different values of M, to compare their BER over AWGN. Referring to a MATLAB code to simulate the performance of BER, we notice that it is affected by the modulation technique and the number of M chosen. The lower of order of modulation M contributes to a better BER. Simulations gives the following results (Fig. 5.2, 5.3, 5.4)

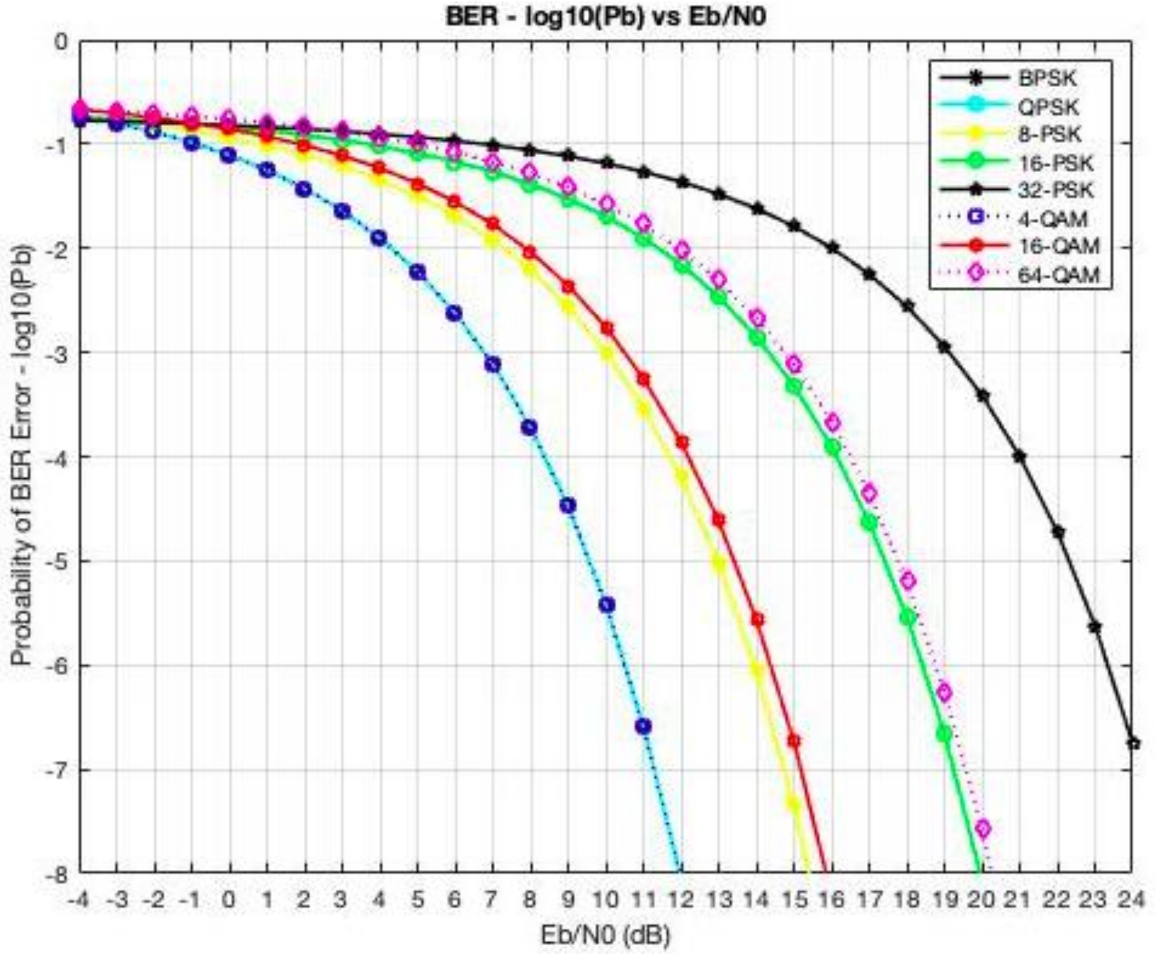


Fig. 5.2 Variation of BER in function of E_b/N_o over AWGN for OFDM modulation: this figure shows the probability of bit error rate in function of E_b/N_0 taking into consideration different values of M for PSK and QAM OFDM modulation.

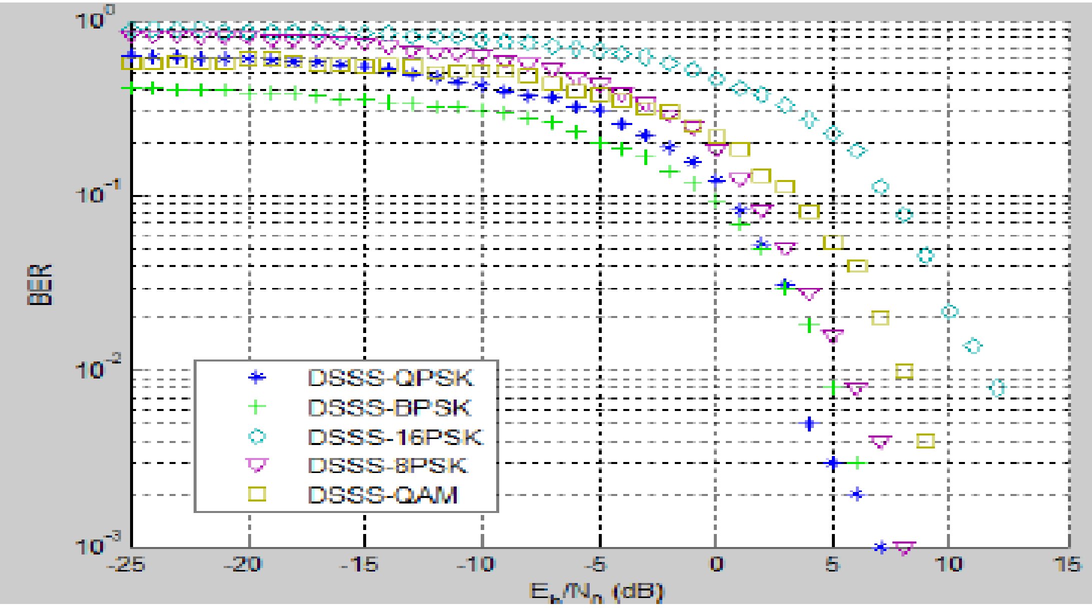


Fig. 5.3 Variation of BER in function of E_b/N_o over AWGN for DSSS modulation: this figure represents the probability of bit error rate in function of E_b/N_0 taking into consideration different values of M for PSK and QAM DSSS modulation.

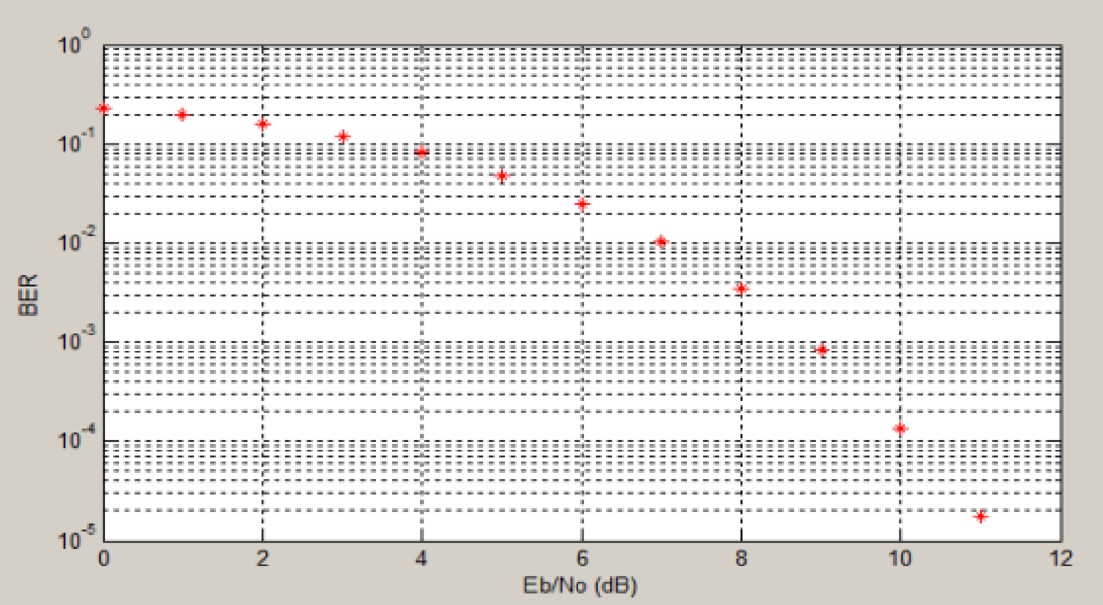


Fig. 5.4 Variation of BER in function of E_b/N_o over AWGN for FHSS modulation: this figure represents the probability of bit error rate in function of E_b/N_0 taking into consideration BPSK FHSS modulation.

It is important to point out that each kind of modulation has a proper value of BER. This act refers to the fact that each modulation technique executes differently in the presence of noise.

The probability of bit error (*P_b*) indicates the probability that an error emerges in the received message. We notice that when $E_b\ /N_0$ increases, the BER takes a decrease function in the three types of modulation techniques.

5.5.3 Packet Error Rate and Packet received measures

Let us suppose that *P_e* is the probability of a dropped message (Packet error rate), *g* is the number of data sent, *L* is the number of lost packets and *n* is the number of times the message should be sent. The drop rate of the sending/receiving protocol takes a binomial distribution:

$$P_e(L = n) \sim B(n, P_e) \tag{5.4}$$

$$P_e\ (L = n) = \binom{n}{g}\ {P_e}^n(1 - P_e)^{n-g} \tag{5.5}$$

We should clarify that P_e could be calculated for UAVs using the following formula:

$$P_e\ = 1 - (1 - BER)^{m_L} \tag{5.6}$$

Where m_L is identified as the length of the message.

The results of Fig 5.5 show that when the BER increases, the P_e increases depending on the length of the sent message. From the previous part, we can consider $BER_1= 10^{-6}$ for the control commands and $BER_2=10^{-3}$ for sensing data. For example, assuming that they send information depending on a MAVLink protocol, i.e. *$(m_L)_{min}$* = 8 bytes (64 bits) and *$(m_L)_{max}$* = 263 bytes (2104 bits), we obtain the four respective packet error rate values:

$BER_1= 10^{-6}$ and *$(m_L)_{min}$* = 8 bytes → $P_{e,1} = 6.4\ \times 10^{-5}$ (5.7)

$BER_2=10^{-3}$ and *$(m_L)_{min}$* = 8 bytes → $P_{e,2}$ = 0.062 (5.8)

$BER_1= 10^{-6}$ and *$(m_L)_{max}$* = 263 bytes → $P_{e,3} = 2.1 \times 10^{-3}$ (5.9)

$$BER_2 = 10^{-3} \text{ and } (m_L)_{max} = 263 \text{ bytes} \rightarrow P_{e,4} = 0.878 \qquad (5.10)$$

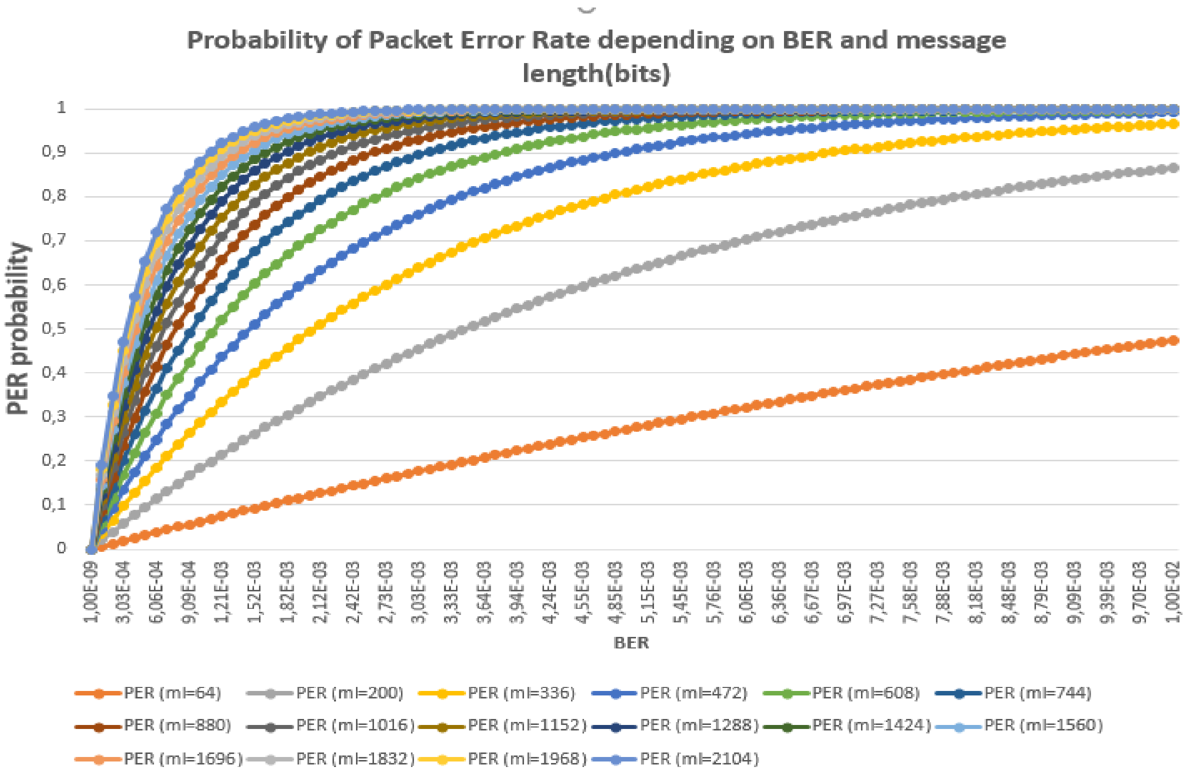


Fig. 5.5. Probability of Packet Error Rate depending on BER and the m_L: different values of message length m_L have been taken in our simulations. These values, represented with different colors, correspond to MAVLink protocol messages with a length range from 8 bytes to 263 bytes. This figure shows the variation of PER in function of BER taking into consideration values of m_L.

As a first step, we aim to calculate the probability of receiving all the packets without any loss ($L = 0$):

$$P_e(L = 0) = (1 - P_e)^g \qquad (5.11)$$

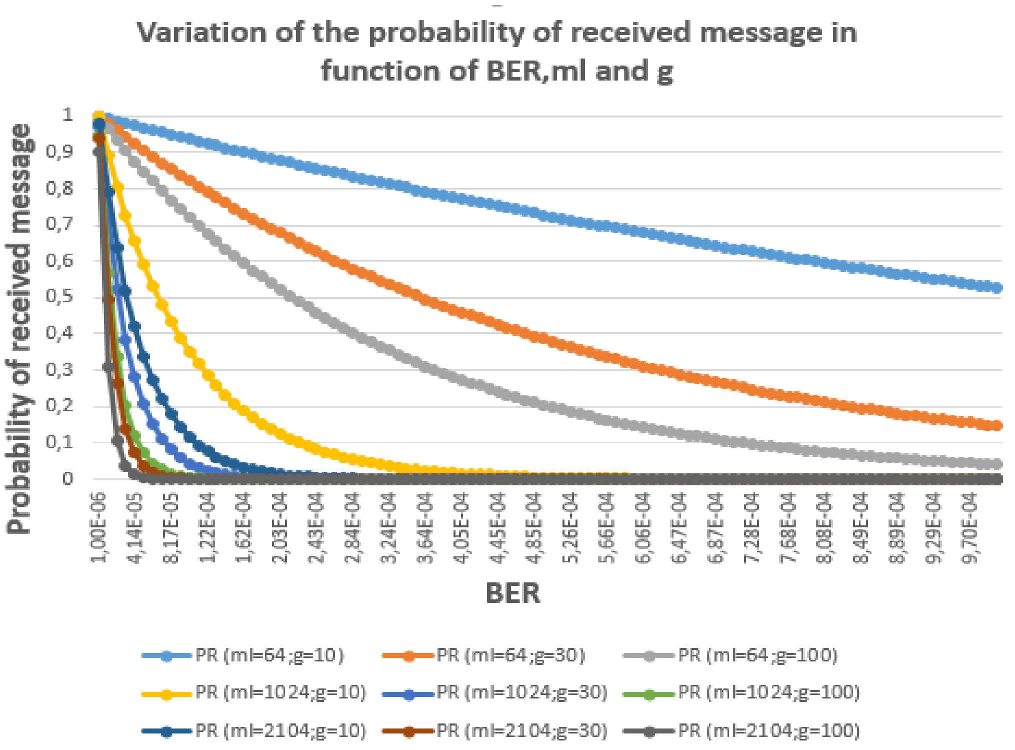


Fig. 5.6 Probability of receiving the message depending on BER, m_L and g: two different values of m_L with three values of g are considered in our simulations. Packet received decreases in function of BER for these different values of m_L and g. When $\mathrm{m_L}$ and g increase, the probability of received message decreased faster for low values of BER.

We notice that when the number of error increase in a packet, the probability of receiving the message will decrease depending on the message length chosen and the amount of data that should be transmitted. However, in some cases the protocol has an issue; such as in case when we consider that P_e = 0.01 and there are 1000 messages to be sent. For this, a certain number of attempts should be considered in order to launch the protocol.

The fleet of drones system requires a high level of reliability with low delay in order to send the information flow especially in real-time missions. We propose Preceived, the probability of receiving the message during an attempt. Hence, for P_e = 0.001 with g = 1000, Preceived is equal to 0.368. For the calculated values of P_e in equations (5.7), (5.8), (5.9) and (5.10) and g=1000, the Preceived will be respectively:

$\mathrm{P_{received,1}} = 0.9994$; $\mathrm{P_{received,2}} = 0.527$; $\mathrm{P_{received,3}} = 0.979$; $\mathrm{P_{received,4}} = 7.3 \times 10^{-10}$

5.5.4 The model validation

We seek to guarantee that the protocol will correctly perform its purpose with a minimum probability p in a way that the probability of failure ok N retransmissions is less than 1- p. Thus, for N attempts of retransmission, the failure of the protocol is: $(1 - P_{\text{received}})^{N}$.

Accordingly,

$$(1- P_{received}\,)^{N} \leq (\,1-p) \tag{5.12}$$

$$e^{\,(1-P_{received})^{N}} \;\leq\; e^{(1-p)} \tag{5.13}$$

From this equation, we can estimate the number of retransmissions that we should take in consideration to send the message so as to be sure of its reception:

$$N > \frac{\ln\,(1-p)}{\ln\,(1-P_{received}\,)} \tag{5.14}$$

Where p and $P_{received}$ are in a range between zero and one.

In the case where we consider that $P_{received}$ =0.368 and the protocol has been 99% successful of sending/receiving the message, we get that the message should be transmitted N = 11 retransmissions in order to have a certainty of 99% that the packets are well received. For the calculated $P_{received}$, and a certainty of 99% for a successful protocol, the number of retransmissions will be:

$N_1 = 1$; $N_2 = 7$; $N_3 = 2$; $N_4 = 6.3 \times 10^{9}$

We conclude that for a same number of data sent, the number of retransmissions is lower when the BER is lower. To increase the probability for a value of 99% successful transmission, the message should be with small length and low BER. The length of the message depends from the routing protocol used and the type of the message (video, image, control commands). For a maximum length of message and a high BER, the message should be sent infinitely to ensure a probability of 99% of a successful protocol.

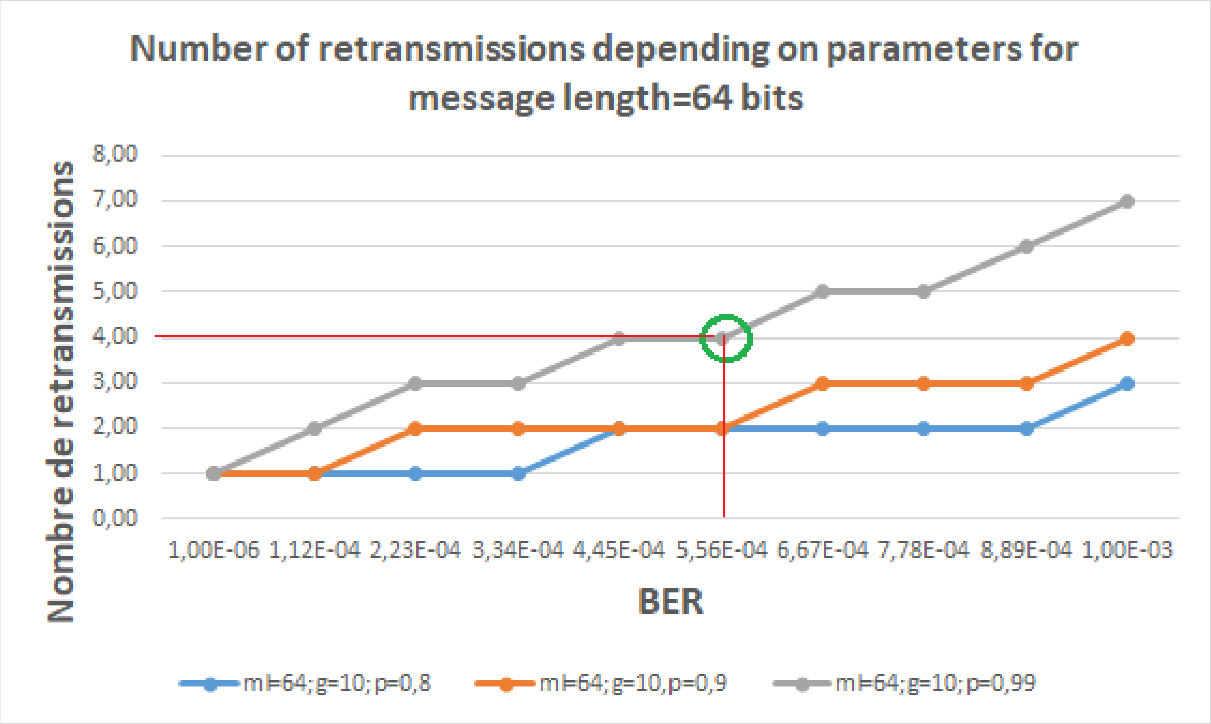


Fig. 5.7 Number of retransmissions depending on BER for g=10 and ml=64 bits: an evaluation for the number of retransmissions is considered in function of BER with three different values of reliability probability p=0.8 (blue), p=0.9(orange) and p=0.99 (gray).

In figure 5.7, we can notice that for the same amount of data transmitted and for a same length of packets (64 bits), the number of retransmissions increases proportionally with the increase of BER depending on the probability of successful of the protocol (p). For BER= 5.56 x10^{-4}, m_L=64 bits and g=10, the message should be retransmitted four attempts in order to ensure a high probability of reception (99%). This number attains 7 when the BER increase to 1x10^{-3}. We conclude that for the same amount of data sent, the number of retransmissions is lower when the BER is lower. To increase the probability for a value of 99% successful transmission, the message should be with small length and low BER. The length of the message depends from the routing protocol used (e.g. MAVLink protocol) and the type of the message (video, image, control commands). For a maximum length of message and a high BER, the message should be sent infinitely to ensure a probability of 99% of a successful protocol. For this, it is important, in our future works, to decrease the retransmissions number in case the message length and BER are high.

Moreover, several simulations have been implemented for 10^{-6}<BER<10^{-3} in order to evaluate the number of message retransmissions. For a fixed message length (m_L=64 bits) and three different values of p (p=0.8; p=0.9; p=0.99), we consider two different series within a randomly value of g following a beta distribution have been picked up:

Series g1: g varies between a minimum of g_{min} =5 and maximum of g_{max} =50 with a mean of g_{mean} =10 and low coefficient of variation v =0.1

Series g2: g varies between a minimum of g_{min} = 50 and maximum of g_{max} =500 with a mean of g_{mean} =100 and high coefficient of variation v =0.8

The beta distribution has to parameters whose formulas are as follows:

$$p_g = -m_g + \left(\frac{1-m_g}{v_g^2}\right) \tag{5.15}$$

$$q_g = \left(\frac{1-m_g}{m_g}\right) . p_g \tag{5.16}$$

Where v_g and m_g are respectively the coefficient of variation and the mean of a random variable g ,

$$m_g = \frac{g_{mean} - g_{min}}{g_{max} - g_{min}} \tag{5.17}$$

$$v_g = \frac{v}{1 - \frac{g_{min}}{g_{mean}}} \tag{5.18}$$

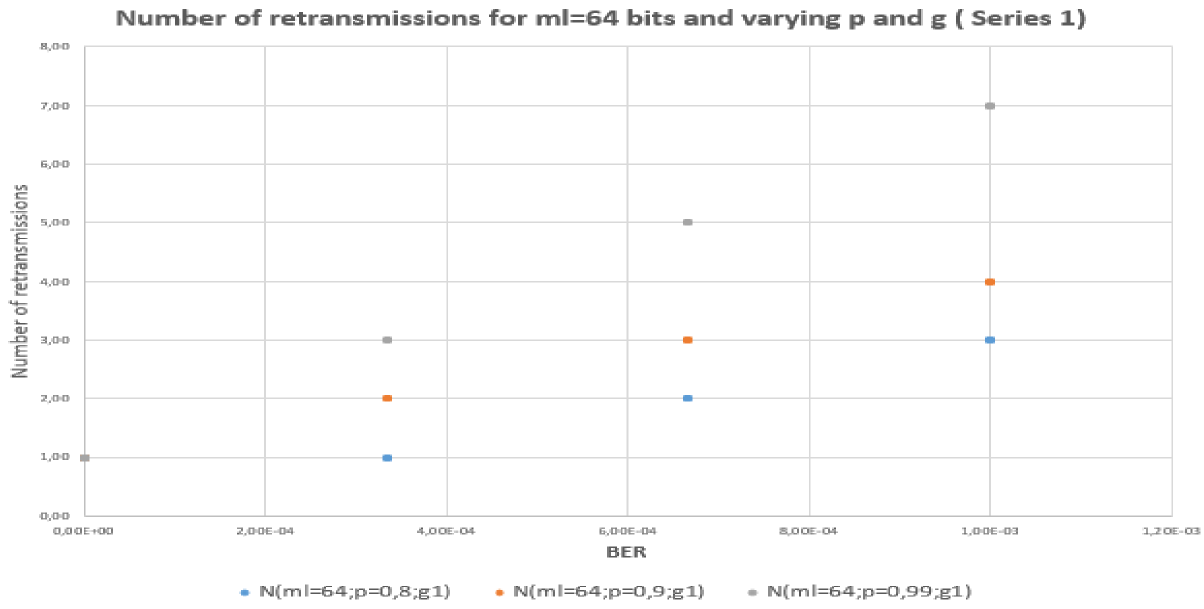


Fig. 5.8 Evaluation of number of retransmissions for m_L=64 bits depending on *g1*: For a specific m_L=64 bits, a random variable g has been considered with g_{min} =5 and g_{max} =50 and g_{mean} = 10 and with low coefficient of variation v =0.1. We evaluate the number of retransmissions in function of BER depending on these values, and three different probabilities (*p*=0.8, *p*=0.9, *p*=0.99).

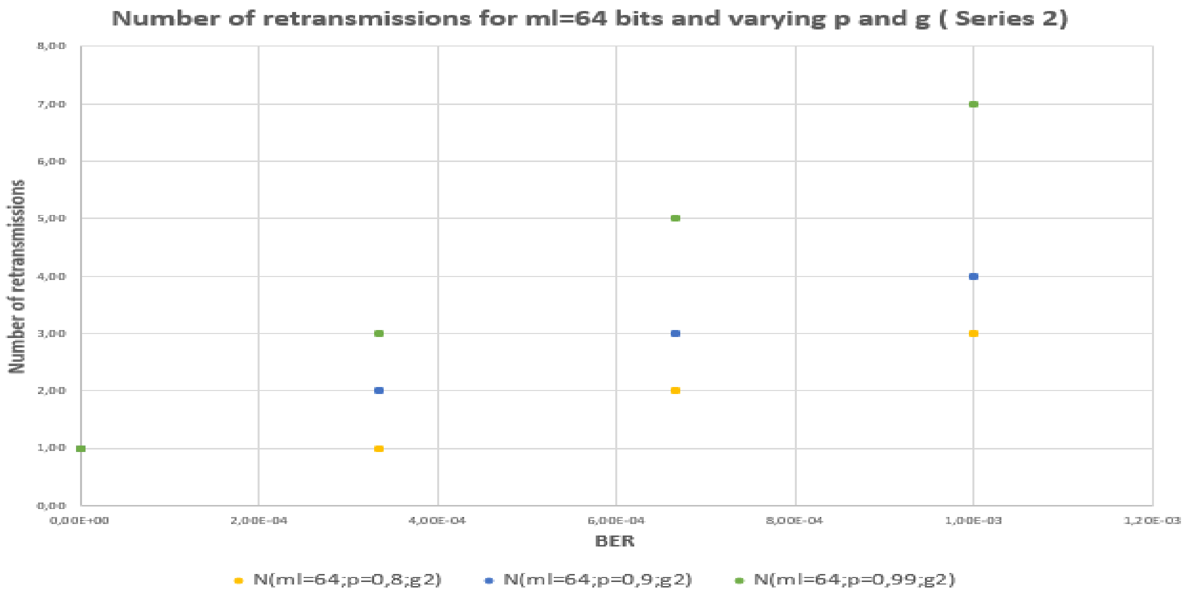


Fig. 5.9 Evaluation of number of retransmissions for m_L=64 bits depending on *g2*: For a specific m_L=64 bits, a random variable g has been considered with g_{min} =50 and g_{max} =500 and g_{mean} = 100 and with high coefficient of variation v =0.8. We evaluate the number of retransmissions in function of BER depending on these values, and three different probabilities (*p*=0.8, *p*=0.9, *p*=0.99).

We noticed that for the same length of message m_L=64 bits, the number of retransmissions has not significant changes (Fig 5.8 and Fig 5.9) despite the variation of g and its high coefficient of variation in series 2. However, the retransmission number increases when we try to attain a high reliability of the protocol and increase p.

However, for m_L=1024 bits, two different series have been considered:

Series g1: g varies between a minimum of g_{min} =5 and maximum of g_{max} =50 with a mean of g_{mean} =10 and low coefficient of variation $v = 0.1$

Series g2: g varies between a minimum of g_{min} = 10 and maximum of g_{max} =100 with a mean of g_{mean} =30 and high coefficient of variation $v = 0.8$

We noticed that the high value of dispersion of g affects significantly the number of retransmissions especially for $BER > 6.67\ x\ 10 - 4$. We obtain huge number of retransmissions in function of the increase of BER when the message and g are large (Fig. 5.10).

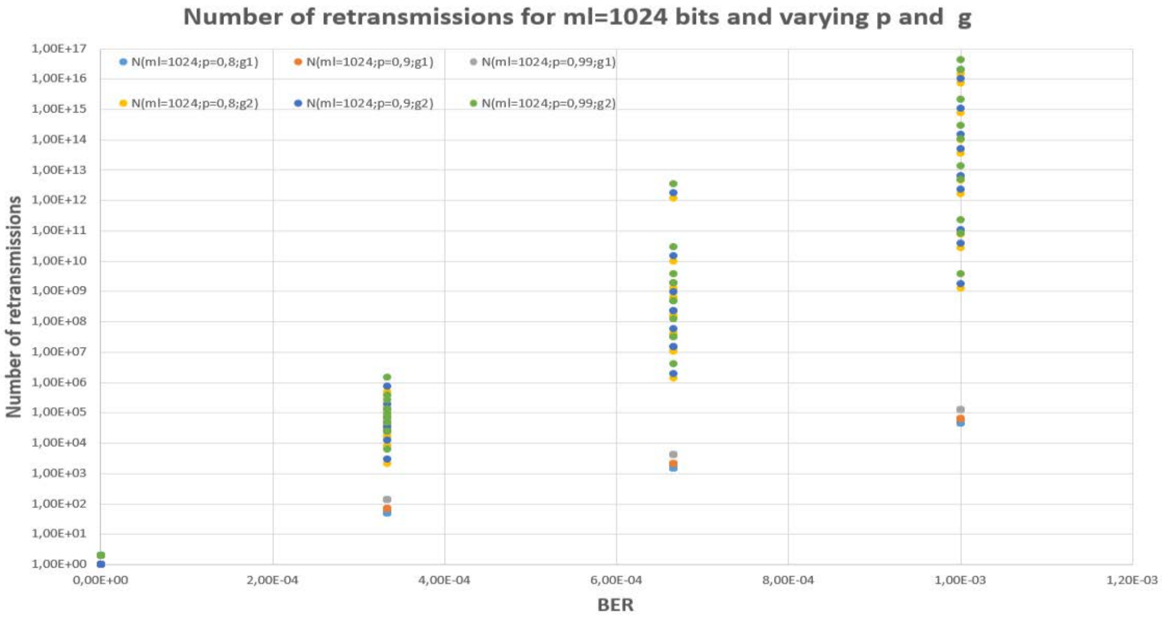


Fig. 5.10 Evaluation of number of retransmissions for m_L=1024 bits depending on g1 and g2: For a specific m_L=1024 bits, a random variable g has been considered within the two previous series. We evaluate the number of retransmissions in function of BER depending on these values, and three different probabilities (p=0.8, p=0.9, p=0.99).

5.6 Conclusion

The communication of the fleet formation flight of drones is affected by many risks caused by the environment of the various missions. In this chapter, we described a strategy for the robustness of transmission protocol that ensures the receipt of the message from the GCS or from other drones. The transmission takes into consideration several factors such as the BER, which is impacted by the bandwidth and the Gaussian noise, the modulation of the channel, the routing protocol used, the length of the message that depends on whether its control commands, image or even a video. We can estimate the packet error from the BER and hence calculate the number of attempts that the message should be sent in order to ensure a certain probability of the receipt of the message. The problem of number of retransmissions of the data occurs when their mission is required in real-time. For a robustness reliability, the message should be with a low BER and minimum length and low message length with a low coefficient of variation for number of message sent.

6

General Conclusion and Future Works

Contents | Chapter 6

6 General Conclusion and Future Works

6.1 Conclusion

In this thesis, we focused the topic of fleet of drones flying in formation, in a hostile environment. This thesis has implemented several dependability approaches in order to ensure the communication reliability for UAVs fleet formation flight in addition to the communication between the drones and their ground control station. Firstly, a description of UAVs was given showing their strategies and communication architectures for drones' fleet. The dependability concept was also introduced in order to define the importance of the reliability term, in addition to safety analysis approaches. From this description, we studied, based on FTA approach, the different causes that affect this communication such as crash of drone, information flow faults, the drones' software, and the status of the GCS as well as the environmental factors that play an important role in connection loss. This method was evaluated by simulations representing several cases.

Furthermore, a second probabilistic approach was proposed based on a stochastic process, Absorbing Markov Chain, to ensure the communication reliability. The objective is to improve the efficiency of the fleet performance in their environment by avoiding the reasons of presence of threats and failures. We show the transition states in addition to the absorbing states that should be prevent. Despite the hardware failures, software failure is considered as a repairable state. Environmental factors could be prevented in non-emergency cases since we can choose the suitable place for the mission, the season and the appropriate time.

After exposing the different risks that influence the communication in drones' networks, we aim to guarantee the message transmission by the receiver that could be another drone or the GCS. Numerous parameters play role in wireless medium transmission such as the number of bits error in a single message, the length of the message depending on data's type, the throughput of the signal, the modulation in addition the number of data that should be transmitted. Noise and interference are the major factors that affect the wireless medium. For this, the proposed protocol focus on the attempt of retransmissions in order to be ensured with a high probability of reliability, the message receipt. Different scenarios have been considered within we vary the parameters values.

6.2 Future Works

In this thesis, we put emphasis on the problem of communication failure in drones' networks. Several potential directions can extend our future research in this domain. The aspects that could be taken into consideration in the future are listed in what follows.

Further experiments could be implemented in order to evaluate the failure rates of the external and software events, the transitions 'failure rates in addition to the repairable rates that are not indicated in reliability databases such as OREDA and NPRD. These experiments should consider the different strategies of fleet flying in formation since the failure of the leader in leader-follower strategy bring to catastrophic consequences. Failures due to the lack of energy could also be considered in the future experiments.

The performance efficiency in hazardous environment is ensured with the drones' fleet since they rapidly accomplish their missions by dividing their tasks. The importance of these vehicles is the data flows that should be sent to the GCS. Hence, studying the reception of all the messages exchanged, on time, in real-time missions is a necessary to ensure the reliability of the communication and the successful of the mission. The data that could be videos with large length or even large images should be received without any faults. We could modify our protocol depending on the attempts of retransmissions to take other factors in consideration in a manner that the message should be received once it has been sent in real-time.

Security of information flows in drone' networks is also another problem that should be solved since drones are used in military domain and there is a risk in losing information.

UAV operations and ensuring their safety operations can be realized by designing and developing innovative wireless communication technologies and cooperative networks schemes. High-capacity mission-related data transmissions for rate-demanding applications could be ensured with the integration of UAV fleets into 5G communications.

Bibliography

Abdallah, R., Kouta, R., Sarraf, C., Gaber, J., & Wack, M. (December 2017). Fault Tree Analysis for the Communication of a Fleet Formation Flight of UAVs. *2017 2nd International Conference on System Reliability and Safety.* Milano: IEEE.

Abdallah, R., Sarraf, C., Kouta, R., Gaber, J., & Wack, M. (2018, Jun 17-21). Communication failure analysis for a fleet formation flight of drones based on absorbing markov chain. In *Proceedings of ESREL* (pp. 2595–601). Trondheim, Norway: Safety and Reliability–Safe Societies in a Changing World. CRC Press, 2018.

Abid, M. E., Austin, T., Fox, D., & Hussain, S. S. (2014). *Drones, UAVs, and RPAs: An Analysis of a Modern Technology.* Worcester Polytechnic Institute, Worcester, Massachusetts.

Achour, W. (2011). France: Thèse de Doctorat de Supelec.

Andre, T., Anna Hummel, K., Schoellig, A. P., Yanmaz, E., Asadpour, M., Bettstetter, C., . . . Zhang, S. (2014). Application-driven design of aerial communication networks. *IEEE Communications Magazine, 52*(5), 129-137.

Andrews, J. D., Poole, J., & Chen, W.-H. (2013). Fast mission reliability prediction for Unmanned Aerial Vehicles. *Reliability Engineering & System Safety, 120*, 3-9.

Antonelli, G., Arrichiello, F., & Chiaverini, S. (2010). Flocking for multi-robot systems via the null-space-based behavioral control. *Swarm Intelligence, 4*(1), 37.

Arjomandi, M., Agostino, S., Mammone, M., Nelson, M., & Zhou, T. (2006). *Classification of unmanned aerial vehicles.* Adelaide, Australia: University of Adelaide.

Asadpour, M., Giustiniano, D., & Hummel, K. A. (2013). From ground to aerial communication: dissecting WLAN 802.11 n for the drones. In ACM (Ed.), *Proceedings of the 8th ACM international workshop on Wireless network testbeds, experimental evaluation & characterization*, (pp. 25-32).

Atoev, S., Kwon, K.-R., Lee, S.-H., & Moon, K.-S. (2017). Data analysis of the MAVLink communication protocol. *2017 International Conference on Information Science and Communications Technologies (ICISCT)* (pp. 1-3). IEEE.

Austin, R. (2011). *Unmanned aircraft systems: UAVS design, development and deployment* (Vol. 54). John Wiley & Sons.

Avizienis, A., Laprie, J., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11-33.

Beard, R. V. (1971). *Failure accomodation in linear systems through self-reorganization.* Massachusetts Institute of Technology.

Bouachir, O. (2014). *Conception et mise en oeuvre d'une architecture de communication pour mini-drones civils.* Université Toulouse 3 Paul Sabatier.

Bouissou, M., & Bon, J.-L. (2003). A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering & System Safety, 82*(2), 149-163.

BS4778, B. S. (1991). *Quality vocabulary: Availability, reliability and maintainability terms.* Glossary of international terms: British Standards Institute.

Butcher, N., Stewart, A., & Biaz, S. (2013). *Securing the mavlink communication protocol for unmanned aircraft system.* Appalachian State University, Auburn University, USA.

Cadi, A. A. (2010). *Planification de trajectoires pour une flotte d'UAVs.* Canada: Thèse de Doctorat de l'Ecole Polythechnique de Montréal.

Cavoukian, A. (2012). *Privacy and drones: Unmanned aerial vehicles.* Ontario: Ontario : Information and Privacy Commissioner of Ontario.

Chandhar, P., Danev, D., & Larsson, E. G. (2016). Massive MIMO as enabler for communications with drone swarms. In IEEE (Ed.), *2016 International Conference Unmanned Aircraft Systems (ICUAS),* (pp. 347-354).

Chao, H., Cao, Y., & Chen, Y. (2010). Autopilots for small unmanned aerial vehicles: a survey. *International Journal of Control, Automation and Systems, 8*(1), 36-44.

Cheng, Z., Necsulescu, D., Kim, B., & Sasiadek, J. (2008). Nonlinear control for UAV formation flying . *Proceedings of the 17th World Congress, The International Federation of Automatic Control.* Seoul, Korea.

Chiaramonti, M., Giulietti, F., & Mengali, G. (2006). Formation control laws for autonomous flight vehicles. *2006 14th Mediterranean Conference on Control and Automation* (pp. 1-5). IEEE.

Ciame, G., Augé-Blum, I., Bayart, M., Wahl, M., Benoit, G., B. E., & Conrard, B. (2009). *Réseaux de terrain-critères de sûreté de fonctionnement.*

Clapper, J., Young, J., Cartwright, J., & Grimes, J. (2007). Unmanned systems roadmap 2007-2032. *188*.

Clark, A., Bushnell, L., & Poovendran, R. (2012). On leader selection for performance and controllability in multi-agent systems. *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)* (pp. 86-93). IEEE.

Cox, D. R. (2017). *The theory of stochastic processes.* Routledge.

Daniel, O., & Descotes-Genon, B. (1995). *Les réseaux de Pétri stochastiques pour l'évaluation des attributs de la sûreté de fonctionnement des systèmes manufacturiers.* Thèse de doctorat, Grenoble INPG.

Danilov, A. S., & Smirnov, U. D. (2015). The system of the ecological monitoring of environment which is based on the usage of UAV. *Russian journal of ecology, 46*(1), 14-19.

de Goeij, G., van Dijken, E. H., & Brouwer, F. (2016). *Research into the Radio Interference Risks of Drone.* Vianen, NL.

Dermentzoudis, M. (2004). *Establishment of models and data tracking for small UAV reliability.* Monterey ,California: Naval Postgraduate school.

Domin, K., Marin, E., & Symeonidis, I. (2016). Security Analysis of the Drone Communication Protocol: Fuzzing the MAVLink protocol. In W. v.-e. Communicatietheorie (Ed.), *Proceedings of the 37th Symposium on Information Theory in the Benelux.*

Drouot, A. (2013). *Stratégies de commande pour la navigation autonome d'un drone projectile miniature.* Thèse de doctorat. Université de Lorraine.

Duan, H., Luo, Q., Ma, G., & Shi, Y. (2013). Hybrid particle swarm optimization and genetic algorithm for multi-uav formation reconfiguration. *IEEE Computational intelligence magazine, 8*(3), 16-27.

Dudek, G., Jenkin, M. R., Milios, E., & Wilkes, D. (1996). A taxonomy for multi-agent robotics. *Autonomous Robots,, 3*(4), 375-397.

Dugan, J. B., Bavuso, J. B., & Boyd, M. A. (1993). Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. *Reliability Engineering & System Safety, 39*(3), 291-307.

Elliott, E. O. (1963). Estimates of error rate for codes of burst-noise channels. *The Bell System Technical Journal, 42*(5), 1977-1997.

Ericson, C. A. (1999). Fault tree analysis. *System Safety Conference,Orlando, Florida*, *1.*

Franco, B. J., & Góes, L. C. (2007). Failure Analysis Methods In Unmanned Aerial Vehicle (UAV) Applications. *Proceedings of COBEM 2007 19th International Congress of Mechanical Engineering*.

Frattini, F., Bovenzi, A., Alonso, J., & Trivedi, K. (2010). Reliability indices. *Wiley Encyclopedia of Operations Research and Management Science*.

Freeman, P., & J. Balas, G. (2014). Actuation Failure Modes and Effects Analysis for a Small UAV. *2014 American Control Conference* . Portland, OR .

Fu, Y., Ding, M. Z., & Hu, H. (2013). Route planning for unmanned aerial vehicle (UAV) on the sea using hybrid differential evolution and quantum-behaved particle swarm optimization. *EEE Transactions on Systems, Man, and Cybernetics: Systems, 43*(6), 1451-1465.

Fuqua, N. B. (2003). The applicability of markov analysis methods to reliability, maintainability, and safety. *Selected Topic in Assurance Related Technologies (START), 2*(10), 1-8.

Gandibleux, J. (2013). *Contribution à l'évaluation de sûreté de fonctionnement des architectures de surveillance/diagnostic embarquées. Application au transport ferroviaire.* Thèse de doctorat. Université de Valenciennes et du Hainaut-Cambresis.

Gilbert, E. N. (1960). Capacity of a Burst-Noise Channel. *Bell Labs Technical Journal, 39*(5), 1253-1265.

Gonçalves, P., Sobral, J., & Ferreira, L. A. (2017). Unmanned aerial vehicle safety assessment modelling through petri Nets. *Reliability Engineering and System Safety, 167*, 383-393.

Guerrero, J., & Lozano, R. (2012). *Flight formation control.* John Wiley & Sons.

Guillerm, R. (2011). *Intégration de la Sûreté de Fonctionnement dans les Processus d'Ingénierie Système.* Thèse de doctorat. Université de Toulouse.

Guo, L., & Chengtong, L. (2012). Research and Achievement of a Way to Improve the Data Transmission Reliability of UDP. *2012 International Conference on Computer Science and Service System* (pp. 627-630). IEEE.

Haasl, D. F., Roberts, N. H., Vesely, W. E., & Goldberg, F. F. (1981). *Fault tree handbook.* Nuclear Regulatory Commission.

Hall, P. L., & Strutt, J. E. (2003). Probabilistic physics-of-failure models for component reliabilities using Monte Carlo simulation and Weibull analysis: a parametric. *Reliability Engineering & System Safety, 80*(3), 233-242.

Hallinan, A. J. (1993). A review of the Weibull distribution. *Journal of Quality Technology, 25*(2), 85-93.

Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *EEE Communications Surveys & Tutorials, 18*(4), 2624-2661.

Hei, X., Chen, J., Lu, H., & Meng, H. (2017). A UDP-based way to improve data transmission reliability. *2017 29th Chinese Control And Decision Conference (CCDC)* (pp. 2612-2617). IEEE.

Ho, D.-T., & Grøtli, E. I. (2013). euristic algorithm and cooperative relay for energy efficient data collection with a UAV and WSN. *2013 International Conference on Computing, Management and Telecommunications (ComManTel).*, pp. 346-351.

Hou, Z., & Fantoni, I. (2015). Distributed leader-follower formation control for multiple quadrotors with weighted topology. *2015 10th System of Systems Engineering Conference (SoSE)* (pp. 256-261). IEEE.

How, J., King, E., & Kuwata, Y. (2004). Flight Demonstrations of Cooperative Control for UAV Teams. *AIAA 3rd "Unmanned Unlimited"Technical Conference.* Chicago, illinois.

Howard, C. (2013). *UAV command, control & communications.* Military & Aerospace Electronics, militaryaerospace. com.

Hunt Jr, E. R., & Daughtry, C. S. (2018). What good are unmanned aircraft systems for agricultural remote sensing and precision agriculture? *International journal of remote sensing, 39*(15-16), 5345-5376.

Jensen, K., & Rozenberg, G. (2012). High-level Petri nets: theory and application. *pringer Science & Business Media*.

Jiang, J., & Han, G. (2018). Routing protocols for unmanned aerial vehicles. *IEEE Communications Magazine, 56*(1), 58-63.

Jiufu, L. I., Chen, K., & Zhisheng, W. A. (2011, March). Fault analysis for flight control system using weighted fuzzy Petri Nets. *Journal of Convergence Information Technology, 6*(3).

Jobard, R. (2014). *Les drones: La nouvelle révolution.* Editions Eyrolles.

Johnson, N. L., Kotz, S., & Balakrishnan, N. (1995). *Continuous univariate distributions-1.* Wiley.

Jordan, W. E. (1972). *Failure modes, effects and criticality analyses.*

Kaneshige, J., & Krishnakumar, K. (2007). Artificial immune system approach for air combat maneuvering. *Intelligent Computing: Theory and Applications V. International Society for Optics and Photonics*, 656009.

Kerns, A. J., Shepard, D. P., & Bhatti, J. A. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 617- 636.

Khan, M., Khan, I., Safi, A., & Quershi, I. (2018). Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols. *Drones, 2*(3), 27.

Kim, B. S., & Caslise, A. J. (1997). Nonlinear flight control using neural networks. *Journal of Guidance, Control, and Dynamics, 20*(1), 26-33.

Kishnakumar, K. (2003). Artificial immune system approaches for aerospace applications. *41st Aerospace Sciences Meeting and Exhibit*, 457.

Kitchin, J. F. (1988). Practical Markov modeling for reliability analysis. *Reliability and Maintainability Symposium Proceedings* (pp. 290-296). IEEE.

Kladis, G. P., Economou, J. T., Knowles, K., Tsourdos, A., & White, B. A. (2008). Digraph matrix reliability analysis for fault assessment for a UAV platform application. A fault-tree analysis approach. *In 2008 IEEE Vehicle Power and Propulsion Conference* (pp. 1-6). IEEE.

Kladis, G. P., Economou, J. T., Tsourdos, A., & White, B. A. (September 3-5,2008). Digraph Matrix Reliability Analysis For Fault Assessment For A UAV Platform Application. A Fault-Tree Analysis Approach. *IEEE Vehicle Power and Propulsion Conference (VPPC).* Harbin,China.

Knight, J. C. (2002). Safety critical systems: challenges and directions. *Proceedings of the 24th international conference on software engineering*, pp. 547-550).

KrAwczyK, M. (2013). Conditions for unmanned aircraft reliability determination. *Eksploatacja i Niezawodność, 15*, pp. 31-36.

Krishnaprasad, R., Nanda, M., & Jayanthi, J. (2016). Adaptive Markov Model Analysis for Improving the Design of Unmanned Aerial Vehicles Autopilot. *Intelligent Systems Technologies and Applications*, 259-271.

Kuchar, J. K. (2005). Safety analysis methodology for unmanned aerial vehicle (UAV) collision avoidance systems. *USA/Europe Air Traffic Management R&D Seminars, 12*.

Kumar, R., & Jackson, A. (2009). Accurate reliability modeling using Markov Analysis with non-constant hazard rates. *Aerospace conference* (pp. 1-7). IEEE.

Kuwata, Y., & How, J. (June 2003). *Real-time Trajectory Design for Unmanned Aerial Vehicles using Receding Horizon Control.* MIT S.M. thesis.

Laprie, J.-C., Arlat, J., Blanquart, J.-P., Costes, A., Crouzet, Y., Deswarte, Y., . . . Thévenod, P. (1995). *Guide de la sûreté de fonctionnement.* Toulouse: Editions Cépaduès.

Lee, W. S., Grosh, D. L., Tillman, F. A., & Lie, C. H. (1985). Fault Tree Analysis, Methods, and Applications ძ A Review. *IEEE transactions on reliability, 34*(3), 194-203.

Lee, W., Lee, J., Lee, J., Kim, K., Yoo, S., Park, S., & Kim, H. (2018). Ground Control System Based Routing for Reliable and Efficient Multi-Drone Control System. *Applied Sciences, 8*(11), 2027.

Lentink, D. (2014). Bioinspired flight control. *Bioinspir. Biomim, 9*(020.301).

Levitin, G., & Finkelstein, M. (2018). Optimal mission abort policy for systems in a random environment with variable shock rate. *Reliability Engineering & System Safety, 169*, 11-17.

Li, C., & Hunter, D. K. (2001). *Stochastic processes.*

Li, J., Zhou, Y., & Lamont, L. (2013). Communication architectures and protocols for networking unmanned aerial vehicles. *2013 IEEE Globecom Workshops (GC Wkshps)* (pp. 1415-1420). IEEE.

Li, N. H., & Liu, H. H. (2008). Formation UAV flight control using virtual structure and motion synchronization. *2008 American Control Conference* (pp. 1782-1787). IEEE.

Li, W.-H., & Zhang, H. (2007). Reviews on Unmanned Aerial Vehicle Formation-Flight. *FLIGHT DYNAMICS-XIAN-, 25*(1), 9.

Li, Z., & Chen, L. (2019). A novel evidential FMEA method by integrating fuzzy belief structure and grey relational projection method. *Engineering Applications of Artificial Intelligence, 77*, 136-147.

Lin, F., Fardad, M., & Jovanović, M. R. (2014). Algorithms for leader selection in stochastically forced consensus networks. *IEEE Transactions on Automatic Control, 59*(7), 1789-1802.

Luong, P. (2013). *Securing embedded systems for autonomous aerial vehicles.* Worcester Polytechnic Institute.

Marshall, D. M. (2004). Dull, Dirty, and Dangerous: The FAA's Regulatory Authority over Unmanned Aircraft Operations. *Issues Aviation L. & Pol'y*, 10085.

Martini, A. (2008). *Modélisation et commande de vol d'un hélicoptère soumis à une rafale de vent.* France: These de Doctorat Paul Verlaine.

Marty, J. A. (2013). *Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft.* AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

Maxa, J.-A., Ben Mahmoud, M.-S., & Larrieu, N. (2017). Survey on uaanet routing protocols and network security challenges. *Ad Hoc & Sensor Wireless Networks*.

Murray, C. C., & Chu, A. G. (2015). The flying sidekick traveling salesman problem: Optimization of drone-assisted parcel delivery. *Transportation Research Part C: Emerging Technologies, 54*, 86-109.

Noor-A-Rahim, M., Khyam, M., Ali, G. G., Liu, Z., Pesch, D., & Chong, P. H. (2019). Reliable State Estimation of an Unmanned Aerial Vehicle Over a Distributed Wireless IoT Network. *IEEE Transactions on Reliability*.

Norme, N. F.-5. (1988). *Terminologie relative à la fiabilité-Maintenabilité-Disponibilité.*

Okafor, E. G., & Eze, I. H. (2016). Failure analysis of a UAV flight control system using Markov analysis . *Nigerian Journal of Technology, 35*(1), 167 – 173.

Ollero, A., & Maza, I. (2007). *Multiple heterogeneous unmanned aerial vehicles.* Springer.

Palat, R. C., Annamalau, A., & Reed, J. R. (2005). Cooperative relaying for ad-hoc ground networks using swarm UAV. *Military Communications Conference, 2005. MILCOM 2005* (pp. 1588-1594). IEEE.

Palat, R. C., Annamalau, A., & Reed, J. R. (2005). Cooperative relaying for ad-hoc ground networks using swarm UAVs. *MILCOM 2005-2005 IEEE Military Communications Conference*, pp. 1588-1594.

Park, C., Cho, N., Lee, K., & Kim, Y. (2015). Formation flight of multiple uavs via onboard sensor information sharing. *Sensors, 15*(7), 17397-17419.

Pashchuk, Y., Salnyk, Y., & Volochiy, S. (2017). Reliability Synthesis for UAV Flight Control System. *ICTERI*, 569-582.

Pastor, E., Lopez, J., & Royo, P. (2007). UAV Payload and Mission Control Hardware/Software Architecture. *IEEE Aerospace and Electronic Systems Magazine, 22*(6), 3 - 8.

Patel, A. R., Patel, M. A., & Vyas, D. R. (2012). Modeling and Analysis of Quadrotor using Sliding Mode Control. *Proceedings of the 2012 44th Southeastern Symposium on System Theory (SSST).* Jacksonville, FL.

Peng, R. (2018). Joint routing and aborting optimization of cooperative unmanned aerial vehicles. *Reliability Engineering & System Safety, 177*, 131-137.

Pleban, J.-S., Band, R., & Creutzburg, R. (2014). Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy. *Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014. 9030*, p. 90300L. International Society for Optics and Photonics.

Postel, J. (1981, September). Transmission Control Protocol. *RFC793* .

Postel, J. (n.d.). User datagram protocol. *RFC768*, p. 1980.

Priya, A., Jakhar, I., & Syan, H. (n.d.). FANET Communication and Routing Protocol. *IJCSN, 6*, 430-432.

Qi, W.-m., Hu, W.-j., Xiao, J., & Zhang, X. (2013). Research on high reliability of data verification in wireless sensor networks. *2013 32nd Chinese Control Conference (CCC)* (pp. 7389-7393). IEEE.

Qin, H., CuiI, J. Q., Li,Jiaxin, Bi, Y., Lan, M., Shan, M., . . . Chen, B. M. (2016, June 1-3). Design and implementation of an unmanned aerial vehicle for autonomous firefighting missions. *2016 12th IEEE International Conference on Control and Automation (ICCA)*, pp. 62-67.

Rabbath, C. A. (2010). *Safety and reliability in cooperating unmanned aerial systems.* World Scientific.

Rafiee, P., & Shabgahi, G. L. (2011). Evaluating the reliability of communication networks (WAN) using their fuzzy fault tree analysis–a case study. *The Journal of Mathematics and Computer Science, 2*(2), 262-270.

Ragi, S., & Chong, E. K. (2013). UAV path planning in a dynamic environment via partially observable Markov decision process. *IEEE Transactions on Aerospace and Electronic Systems, 9*(4), 2397-2412.

Ragi, S., & Chong, E. K. (2013, October). UAV path planning in a dynamic environment via partially observable Markov decision process. *IEEE Transactions on Aerospace and Electronic Systems, 49*(4), 2397-2412.

Rathinam, S., Almeida, P., Kim, Z., Jackson, S., Tinka, A., Grossman, W., & Sengupta, R. (2007). Autonomous searching and tracking of a river using an UAV. *2007 American control conference*, pp. 359-364.

Remenyte-Prescott, R., Andrews, J. D., & Chung, P. W. (2010). An efficient phased mission reliability analysis for autonomous vehicles. *Reliability Engineering & System Safety, 95*(3), 226-235.

Reyes, H., Gellerman, N., & Kaabouch, N. (2015). A cognitive radio system for improving the reliability and security of UAS/UAV networks. *2015 IEEE Aerospace Conference*.

Reynolds, C. W. (1987). Flocks, herds and schools: A distributed behavioral model. *ACM SIGGRAPH computer graphics, 21*(4), 25-34.

Richards, M. D., Whitley, D., Beveridge, J. R., Mytkowicz, T., Nguyen, D., & Rome, D. (2005). Evolving cooperative strategies for UAV teams. *Proceedings of the 7th annual conference on Genetic and evolutionary computation* (pp. 1721-1728). ACM.

Ross, S. M., Kelly, J. J., Sullivan, R. J., Perry, W. J., Mercer, D., Davis, R. M., & Bristow, V. L. (1996). *Stochastic processes* (Vol. 2). New York: Wiley.

Ruegg, A. (1989). *Processus stochastiques: avec applications aux phénomènes d'attente et de fiabilité* (Vol. 4). PPUR presses polytechniques.

Saunders, J. B., Call, B., Curtis, A., & Beard, R. W. (2005). Static and Dynamic Obstacle Avoidance in Miniature Air Vehicles. *AIAA Infotech@Aerospace Conference.* Arlington, Virginia.

Seo, J., Ahn, C., & Kim, Y. (2009). Controller Design for UAV Formation Flight Using Consensus based Decentralized Approach. *AIAA Infotech Aerospace Conference.* Seattle, Washington.

Shi, H., Wang, L., & Chu, T. (2006). Virtual leader approach to coordinated control of multiple mobile agents with asymmetric interactions. *Physica D: Nonlinear Phenomena, 213*(1), 51-65.

Snooke, N. (2015). Automated Failure Effect Analysis for PHM of UAV. In *Handbook of Unmanned Aerial Vehicles* (pp. 1027-1051). Springer Netherlands.

Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J., & Railsback, J. (2002). *Fault tree handbook with aerospace applications.*

Stewart, R. (2007). Stream control transmission protocol . *RFC 4960, Internet Engineering Task Force*.

Suescun, C. A., & Cardei, M. (2016). Unmanned Aerial Vehicle Networking Protocols. *The Fourteen LACCEI International Multi-Conference for Engineering, Education, and Technology: "Engineering Innovations for Global Sustainability.* San José, Costa Rica.

Tao, G., Chen, S., & Tang, X. S. (2004). *Adaptive Control of Systems with Actuator Failures.* London: Springer London.

Thanthry, N., & Pendse, R. (2009). Aircraft health management network: A user interface. *IEEE Aerospace and Electronic Systems Magazine, 24*(7), pp. 4-9.

Tseng, F.-H., Liang, T.-T., Lee, C.-H., Chou, L.-D., & Chao, H.-C. (2014). A Star Search Algorithm for Civil UAV Path Planning with 3G Communication. *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 942-945). IEEE.

Vasseur, D. (2006). *Risques industriels: complexité, incertitude et décision: une approche interdisciplinaire.* Tec & Doc: Lavoisier.

Veena, S., Vaitheeswaran, S., & Lokesha, H. (2014). Towards the Development of secure MAVs. *CRAMAV-2014 (3rd International Conference).* JNTU.

Vergouw, B., Nagel, H., Bondt, G., & Custers, B. (2016). Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments. *TMC Asser Press*, pp. 21-45.

Villemeur, A. (1988). *Sureté de fonctionnement des systèmes industriels: fiabilité-facteurs humains, informatisation.* Eyrolles.

Wang, J., Jiang, C., Han, Z., Ren, Y., Maunder, R. G., & Hanzo, L. (2016). Cooperative distributed unmanned aerial vehicular networks: Small and mini drones. *IEEE Vehicular Technology Magazine*, 1-18.

Wang, J., Zhang, Q., & Yoon, S. (2019). Reliability and availability analysis of a hybrid cooling system with water-side economizer in data center. *Building and Environment, 148*, 405-416.

Wang, J.-L. (2004). Markov-chain based reliability analysis for distributed systems. *Computers & Electrical Engineering, 30*(3), 183-205.

Wang, T., Zheng, Z., Lin, Y., Shihong, Y., & Xie, X. (2018). Reliable and Robust Unmanned Aerial Vehicle Wireless Video Transmission. *IEEE TRANSACTIONS ON RELIABILITY*(99), 1-11.

Wang, X., Yadav, V., & Balakrishnan, S. (JULY 2007). Cooperative UAV Formation Flying with Obstacle/Collision Avoidance. *IEEE Transactions On Control Systems Technology , 15*, 672 - 679.

Wang, Y., Wang, D., & Wang, J. (2015). A data driven approach for detection and isolation of anomalies in a group of UAVs. *Chinese Journal of Aeronautics, 28*(1), 206 - 213.

Wenquan, H. A., You-rong, R. E., & Shao-hua, Z. H. (2011). Primary Usages of UAV Remote Sensing in Geological Disaster Monitoring and Rescuing [J]. *Geospatial Information, 5*.

Yanmaz, E., Quaritsch, M., Yahyanejad, S., Rinner, B., Hellwagner, H., & Bettstetter, C. (2017). Communication and coordination for drone networks. *Ad Hoc Networks*, 79-91.

Yong-qiang, Z., & Hong-bin, G. (2010). Design and implementation of RUDP protocol for multiple mobile agent communication. *In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). 8*, pp. V8-614. IEEE.

Yu, K., & Sato, T. (2019). Modelling and Analysis of Error Process in 5G Wireless Communication Using Two-state Markov Chain. *IEEE Access*.

Yun, B., Chen, B. M., Lum, K. Y., & Lee, T. H. (September 2008). A Leader-Follower Formation Flight Control Scheme for UAV Helicopters.

Yun, B., Chen, B. M., Lum, K.-Y., & Lee, T. H. (2008). A leader-follower formation flight control scheme for UAV helicopters. *2008 IEEE International Conference on Automation and Logistics* (pp. 39-44). IEEE.

Zeitlin, A., & McLaughlin, M. (2006). Modeling for UAS collision avoidance. *UVSI Unmanned Systems North America, Orlando,* .

Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Communications Magazine, 54*(5), 36-42.

Zhou, C., Shao-Lei, Zhang, Wen-Guang, & Lei, M. (2012). UAV Formation Flight Based on Nonlinear Model Predictive Control. *Hindawi Publishing Corporation*, 15.

Zhou, Y., Li, J., Lamont, L., & Rabbath, C.-A. (2012). Modeling of packet dropout for UAV wireless communications. *International Conference on Computing, Networking and Communications Invited Position Paper Track* (pp. 677-682). IEEE.

Résumé :

Les véhicules aériens sans pilote (UAVs), utilisés et développés pour la première fois dans le domaine militaire, ont connu de profonds changements ces dernières années et sont de plus en plus utilisés dans le domaine civil. Etant plus connus sous le nom des drones, ils sont le plus souvent utilisés dans les domaines civiles et militaires. Ils sont employés pour : la lutte contre les incendies, le sauvetage ainsi que dans des applications spécifiques comme la surveillance et l'attaque. Le vol en formation est de loin le plus utilisé car il permet une répartition judicieuse des tâches et améliore grandement l'efficacité des drones (principe de l'attaque en meute, des animaux carnassiers). Cela pose alors la problématique de la coordination et de la stratégie, ainsi que du type de fonctionnement (maitre/esclave,…).Le type et la qualité d'informations optimums restent aussi à définir.

L'utilisation accrue de ces systèmes coopératifs dans des environnements dangereux rend leur fiabilité essentielle pour prévenir tout événement catastrophique. Une performance globale de la flotte des drones doit être garantie, malgré une possible dégradation des composants ou de toute modification du réseau et de l'environnement. Il est nécessaire de détecter les comportements anormaux pouvant contribuer aux collisions et ainsi affecter la mission. Compte tenu des performances et du coût, les systèmes à tolérance de pannes et à redondance ne représentent pas toujours la solution la plus efficace pour ce type de vol de flotte en formation. Différentes méthodes telles que l'analyse par arbre de défaillance (ADD), l'analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC) ont été utilisées dans le monde des hélicoptères.

Pour notre part, nous proposons dans une première partie, une méthode statique basée sur l'ADD est proposée, pour assurer la fiabilité de la communication entre les drones d'un côté et entre les drones et la station de base de l'autre côté en accentuant l'échange de flux d'informations. Nous utilisons des arbres de défaillance pour représenter les différentes conditions d'erreur de ce système complexe.

Dans une deuxième partie, nous analysons les différents états de défaillance des communications et leurs probabilités. Ce processus étant stochastique, une approche par chaîne de Markov absorbante est développée. L'approche proposée peut être utilisée pour trouver les scenarios les plus risqués et les éléments à prendre en compte pour améliorer la fiabilité.

Enfin, dans une troisième partie, nous étudions le problème de réception des messages d'un drone en proposant un protocole basé sur le nombre de retransmissions. La réception est assurée avec une certaine probabilité de fiabilité, en fonction de plusieurs attributs tels que la modulation, le taux d'erreur des bits (BER) caractérisant les UAVs.

Mots-clés : Drones, communication, flottes, fiabilité, arbre de défaillance, chaine Markov absorbante, réception de message

Abstract:

Unmanned aerial vehicles, used and developed initially in the military field, have experienced profound changes in recent years and are increasingly used in the civilian field. Recognized as drones, they are most often used in the civil and military domains. They are used for firefighting, rescue as well as in specific applications such as surveillance and attack. The formation flight is the most used because it allows a judicious distribution of the tasks and greatly improves the efficiency of the drones (principle of the attack in pack, carnivorous animals). This will raise the issue of coordination and strategy, as well as the type of operation (master /slave, ...). The type and quality of optimal information also remain to be defined.

The increased use of these cooperative systems in hazardous environments makes their reliability essential to prevent any catastrophic event. Overall performance of the drone fleet should be ensured, despite possible degradation of components or any changes that occur to the network and the environment. It is necessary to detect the anomalous behaviors that might contribute to collisions and thus affect the mission. Taking into consideration performance and cost, the fault-tolerant system and redundant systems are not always the most efficient solution for the formation fleet flight. Different methods like the fault tree analysis (FTA), Failure Modes and Effects Analysis (FMEA) have been used in the helicopter field.

In the first part, we propose a static method based on FTA, to ensure a successful communication between the drones from one side, and between the drones and the ground station from the other side by emphasizing on the exchange of information flows. It uses various fault trees to represent the different error conditions of this complex system.

In the second part, we analyze the different fault states and their probabilities. As this process is stochastic, an absorbing Markov chain approach is developed. The proposed approach can be used to find the most risky scenarios and considerations for improving reliability.

Finally, in the third part, we put emphasis on the message receipt problem in a drone's communication network by proposing a protocol based on number of retransmissions. The reception of a message is provided with a certain probability of reliability depending on several attributes such as modulation and bit error rate (BER) characterizing the UAVs.

Keywords: UAV, communication, formation fleet, reliability, fault tree, Absorbing Markov chain, message receipt

■ École doctorale SPIM - Université de Technologie Belfort-Montbéliard
F - 90010 Belfort Cedex ■ tél. +33 (0)3 84 58 31 39
■ ed-spim@univ-fcomte.fr ■ www.ed-spim.univ-fcomte.fr