Intrusion detection system in a fleet of drones

Ruohao Zhang

Université Fédérale

Toulouse Midi-Pyrénées

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut Supérieur de l'Aéronautique et de l'Espace

Présentée et soutenue par :
Ruohao ZHANG

le mardi 18 janvier 2022

Titre :

Intrusion detection system in a fleet of drones

Détection d'intrusion dans une flotte de drones

École doctorale et discipline ou spécialité :
EDSYS : Automatique et Informatique

Unité de recherche :
ENAC-LAB - Laboratoire de Recherche ENAC

Directeur(s) de Thèse :

M. Jean-Philippe CONDOMINES (directeur de thèse)
M. Nicolas LARRIEU (co-directeur de thèse)

Jury :
M. Jérôme LACAN Professeur ISAE-SUPAERO - Président
M. Julien BOURGEOIS Professeur Université Bourgogne Franche Comté - Rapporteur
M. Jean-Philippe CONDOMINES Enseignant Chercheur ENAC - Directeur de thèse
M. Yann LABIT Professeur Université Toulouse 3 - Examinateur
M. Nicolas LARRIEU Professeur ENAC - Co-directeur de thèse
M. Promethee SPATHIS Maître de conférences Sorbonne Université - Rapporteur
M. Pierre-Ugo TOURNOUX Maître de conférences Université de la Réunion - Examinateur

Acknowledgements

I would like to share my most sincere gratitude towards some of the most wonderful people in my life. The work of this Ph.D. thesis would not be possible without you all.

Firstly, I would like to thank my Ph.D. advisor Prof. Jean-Philippe Condomines and Nicolas Larrieu. It is my great honor to receive your acceptance into this project and start this wonderful journey, your kindness in sharing your profound knowledge and your patience in guiding me through the mountains of research.

I also owe special thanks to Prof. Emmanuel Lochin for your kindness in bearing the heavy responsibility in fully committing to help me resolve issues and problems in the most difficult time of my Ph.D. career. I will not be able to stand here defend my thesis if not because of you.

In addition, I am indebted to my hosting laboratory: ENAC ReSCo team and my Ph.D. following committee and everyone who have assisted me through my Ph.D. Thank you all for your help in making my Ph.D. career a pleasant journey.

To my dear friends. It is because of your love and caring, that I will never lose my drive and determination.

Most importantly, I would like to express my utmost sincere gratitude to my parents and my family. it is your cultivation and devotion in supporting me that made me who I am. I am forever indebted to you. To my grandma. It devastates me that I can not share this joy with you in person. Happy 90th birthday. Hope the joy that I am feeling right now can cross mountains and seas to make your day!

Lastly, I would like to acknowledge the selfless support and help, both technically and emotionally by the late Serge Roux. You will be forever in my heart.

Contents

Table of abbreviations and acronyms **ix**

1 Introduction **1**

1.1 Motivation 1

1.2 Relevant concepts 4

1.3 The types of intrusions considered in this thesis 11

1.4 Thesis outline 12

1.5 Contributions 13

2 Preliminaries **15**

2.1 State of the art 16

2.2 IDS in a nutshell 20

2.3 TCP queuing dynamics and robust observer 22

2.4 Wavelet Leader Multifractal (WLM) analysis 27

2.5 Curve matching and artificial intelligence classification 35

3 DoS detection: A preliminary design based on robust observer and wavelet-leader multifractal analysis **43**

3.1 Introduction 45

3.2 Methodology 46

3.3 System validation 50

3.4 Implementation 61

4 Spoofing detection: An advanced design based on WLM and enhanced by AI 69

4.1 Introduction 71

4.2 Methodology 72

4.3 Application to experimental data 75

4.4 Results 80

Conclusion 85

Bibliography 88

List of Figures

1.1 A UAS light show flying in deformation 3

1.2 General configuration of a classic UAS 5

1.3 A demonstration of how a UAS can be used and attacked 7

1.4 Use a UAS as a network relay and remote sensor carrier 8

1.5 Typical RADAR system and demonstration of a spoofing 9

2.1 Robust observer on a TCP AQM system 27

3.1 A general two-step framework of the proposed IDS system 47

3.2 An example of WLM signature of a data series at statistic moment $q = 2$ 47

3.3 Examples of WLM signature at multiple statistical moments 48

3.4 Sources / receivers connection in a fleet of UAVs 49

3.5 Test bench implementation 51

3.6 Considered topology 52

3.7 Waveform and signature comparison between normal and CFC flooded traffics 53

3.8 Waveform and signature comparison between normal and PFC flooded traffics 54

3.9 Scaling function for regular traffic 55

3.10 Scaling function for traffic with CFC anomaly 56

3.11 Similarity score over signatures of the UAV to GCS traffic 56

3.12 TCP congestion window W(t) - CFC attack 58

3.13 Queue length q(t) - CFC attack 59

3.14 Estimation with real traffic replay - CFC attack 59

3.15 TCP congestion window W(t) - PFC attack 60

3.16 Queue length q(t) - PFC attack 60

3.17 Estimation with real traffic replay - PFC attack 61

3.18 Global view of Paparazzi system 62

3.19 An Intrusion Detection System use case 64

3.20 WLM Wavelet Leader analysis result on normal traffic(left) and flooded traffic(right) 65

3.21 WLM Discrete Wavelet analysis result on normal traffic(left) and flooded traffic(right) 65

3.22 Simulated Real-time Application Scenario with Paparazzi Software 66

3.23 Real-time Signatures of the network at different states 67

4.1 General framework of the proposed IDS system 73

4.2 A simplified LSTM unit 75

4.3 Typical architecture of a Bi-LSTM 75

4.4 The process of dataset generation 79

4.5 WLM $D(h)$ Signatures of RADAR traces at different state 80

4.6 Confusion matrix of the performance verification with LSTM 82

4.7 Verification at different intensities with LSTM 82

4.8 Confusion matrix of the performance verification with SVM 83

4.9 Verification at different intensities with SVM 84

List of Tables

3.1 Equilibrium point 57

4.1 Distribution of samples in the dataset 79

Table of abbreviations and acronyms

UAS	*Unmanned Aircraft System*
UAV	*Unmanned Aircraft Vehicle*
RAPS	*Remotely Piloted Aircraft System*
GCS	*Ground Control Station*
RF	*Radio Frequency*
WANET	*Wireless Ad-hoc NETwork*
MANET	*Mobile Ad-hoc NETwork*
FANET	*Flying Ad-hoc NETwork*
UAANET	*UAv Ad-hoc NETwork*
IDS	*Intrusion Detection System*
HMI	*Human-Machine Interface*
DoS	*Denial of Service*
MITM	*Man-In-The-Middle*
IDPS	*Intrusion Detection and Prevention System*
ML	*Machine Learning*
LRD	*Long-Range Dependence*
MF	*Multifractal*
MFA	*Multifractal Analysis*
SVM	*Support Vector Machine*
ANN	*Artificial Neural Network*

CNN *Convolutional Neural Network*

RNN *Recurrent Neural Network*

LSTM *Long-Short Term Memory*

TCP *Transmission Control Protocol*

CHAPTER 1

Introduction

1.1 Motivation

In recent years, the development of Unmanned Aerial System UAS, also known as Remotely Piloted Aircraft System (RAPS), involves using swarms of Unmanned Aerial Vehicle (UAV or Drone) has experienced an unprecedented step-forward due to the simplicity in development, deployment, and management, thanks to the rapid advancements of structure, cybernetic, and network technologies. The versatile and mobile natures of the UAS have made it the go-to option for many civil and commercial applications, such as delivery, remote sensing, telemetering, surveillance, tracking, photographing, drone light show, emergency signal relaying, search and rescue, and disaster relief, etc.

Most recent examples of such applications are reported: In July 2021, in Henan Province, China, two specially designed fixed-wing Chengdu Wing-Loong 2H UAVs are deployed in the airspace above the severely flooded Mihe town to aid the search and rescue and disaster relief efforts. The two UAVs, which are designed for emergency communication response, are equipped with telecommunication pods. It allows the UAV to act as an emergency aerial base station for cellular communication and enabled emergency communication for the stranded locals for over 5 hours. The combination of network and UAS technologies is thought-provoking.

Also, in July 2021, Tokyo, the Opening Ceremony of the 2021 Olympics Games is illuminated by 1824 UAVs. The UAS behind the show, namely the "Shooting Star" system, is designed by Intel, specifically for drone light show purposes. Similar UAV light shows are becoming more and more common due to the maturation of UAS networking technology, which significantly reduced the operating cost and difficulty whilst improving safety and robustness.

In addition, enterprises such as JD, Alibaba, and Amazon are all investing heavily the unmanned delivery systems, of which the UAS for delivery plays an important role. Such complex systems are designed with mobility requirements in mind. By taking full advantage of the mobility of the UAVs, the network technologies must be adapted to allow a more flexible but also more robust connection. Consequently, an unprecedented demand for a robust communication system has been created to establish a versatile system in the sky.

Traditionally, the communication between the UAV and the Ground Control Station (GCS) is achieved by using Radio Frequency (RF) point-to-point links, where a pair of RF transmitters and receivers (or a pair of RF transceivers) is implemented onto the UAV and the GCS. Each UAV is remotely controlled by the GCS through a specific RF channel. Different techniques are implemented to allow multiple connections simultaneously but are restricted by the limited bandwidth and connectivity. The possible application scenarios are narrowed down.

Recently, the Wireless Network technology such as Wireless Ad-hoc NETwork (WANET) has quickly phased out the traditional method, demonstrating its superiority, such as it is less dependent on infrastructure, better compatibility towards changing geo-positions of each UAV, and better Quality of Service(QoS) in a mobile environment. Mobile Ad-Hoc NETwork (MANET), Flying Ad-Hoc NETwork (FANET), UAV Ad-Hoc NETwork (UAANET) are the common terminologies for WANET based wireless networks for mobile entities. Instead of using RF communication to replace wires, WANET allows to construct a network on-to-fly and change the network topology in real-time. Implementing wireless network technology inside the UAS has made it possible for a more flexible composition of UAS's to adapt for more diverse use cases.

However, despite all the advantageous features, UAANET is raising more and more concerns regarding its safety and security, especially regarding its cyber-security perspective. Superficial prosperity and demand-driven development have left many essential boxes unchecked. Especially in many situations, security problems have been overlooked to fulfill the need of the market. The network systems implemented in the current commercial UAS's are often adaptions or variants of existing network systems by adopting off-the-shelf components and communication technologies, which are not exactly well-coupled with the mobility nature of a UAS. Thus, pre-existing vulnerabilities may still exist, while new vulnerabilities that emerged from the properties of a UAS, such as mobility and inter-connectivity, are even more worrisome.

For a wireless WANET, for example, if the authentication or encryption has been compromised, the intruders will be granted the possibility to launch intrusion attacks such as a Denial of Service (DoS) or a Man In The Middle (MITM) attack. To aggravate the situation, the mobility characteristics of a UAANET made it almost impossible to ensure the physical safety of each UAV, thus leaving more possible points of entry into the network, making it easier for the malicious parties to exploit the vulnerabilities of such network.

Very recently, a number of incidents involving crash or misbehaving of a fleet of drones in commercial drone exhibitions have been reported:

[MZT18] Oct 2018, in Hong Kong; [Zhe18] May 2018, in Xi'an; [Sha20] Feb 2020, in Taichung; [Yb2] May 2020, in Yi Bing; [Tim21] Jan 2021, in Chong Qing; [Sch21] June 2021, in Shang Hai, to name a few. Many of which could be attributed to malicious intrusions.

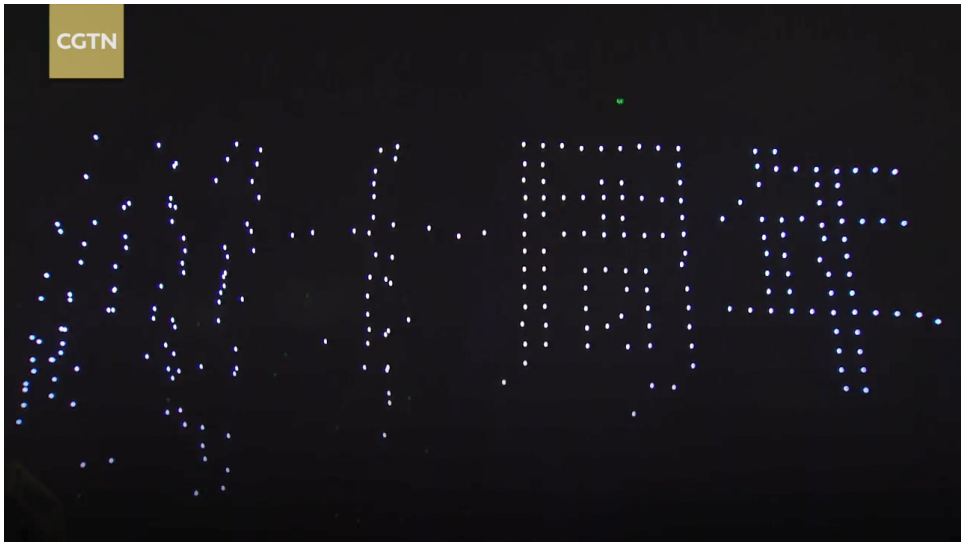


Figure 1.1: A UAS light show flying in deformation (Screenshot taken from the Video in [Zhe18])

Moreover, in [Wil+17], the authors have further investigated 152 accidents and incidents involving the RPAS from 2006 to 2015. The authors concluded that over 63% of the cases are caused by the System Component Failure/Malfunction (SCF), while the most significant contributing factor is Equipment Failure (EF) at 41%. Network intrusion could be one of the major causes of such failures.

As reported, those cases have not just caused property losses but also human injuries or even possible fatalities, especially for commercial UAS's that operate in civil airspace in the most populated areas or tourist sites. Security and safety are of utmost importance and are strictly enforced. Thus,

operations within an agglomeration, fully autonomous operations, and out-of-sight UAV operations are currently subject to precise regulations such as [EU19] for the European Union (EU) and [FAA20] the United States. In addition, with the implementation of the General Data Protection Regulation (GDPR) in the EU [EU16]. With further regulations on UAV categorization, certification, and integration into civil airspaces, such as the road maps in EU [EU21] and the relevant regulations reviewed in [St17]. We can conclude that there is a clear need for a reliable communication network for UAS's with robust measures implemented to counter network intrusions and better protect the physical system of the UAS as well as the confidentiality of the data being transmitted through the UAANET. Thus, it is of vital importance to ensure the safe and healthy development of the future UAS, well complying with the current and prospective regulations.

In order to aid the defense against malicious misuse, the Intrusion Detection System (IDS) is introduced as an additional device to the network security system. The aim of an intrusion detection system is to detect anomalies and compromises within the network. The IDS is a crucial part of network security today. As network systems expand into every corner of our lives, network attacks proliferate in number, diversity, and severity. An IDS is the primary measure of defense against malicious misuse of the network once the network security is breached.

Although there are numerous designs already proposed in the world of networks, and they have been successfully applied to many practical problems. It has become noticeable that many mature solutions are dependent on a fixed wire network with constant or predictable topology. The IDS for rapidly changing network topology alongside high mobility is rarely proposed.

In response to this lack of advancement, the present dissertation aims to contribute to designing a safer and securer UAS for the future by proposing an IDS based on cutting-edge cybernetics, statistical analytic tools, and machine learning methods.

1.2 Relevant concepts

In this section, I present the general concepts involved in this dissertation for a better understanding, including the details of the UAS, the implementation of communication network technology(such as the wireless ad-hoc network), and cases of intrusion, which are common in this type of network.

1.2.1 The classic Unmanned Aerial Systems(UAS)

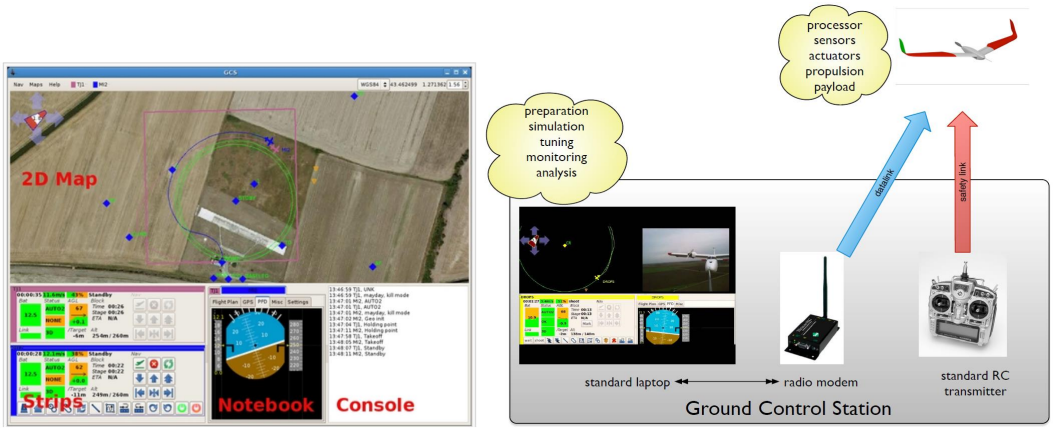


Figure 1.2: General configuration of a classic UAS

The Figure 1.2 illustrates the general configuration of a classic UAS architecture with relevant software and hardware. This architecture has a clear separation between the three segments: the ground segment, aerial segment, and communication segment:

The ground segment

This segment comprises all the hardware and software materials on the ground, including a ground control station (GCS), piloting software and means of data acquisition, etc., which allow the preparation, control, monitoring, and analysis of the flight. The GCS, in particular, acts as the central hub for all the information between the UAV and the ground to get through. In addition, a Human Machine Interface (HMI) is usually present in the GCS, which allows real-time display of the UAV or UAV fleet's telemetry data, interactive path-planning, and navigation. Due to the centralized nature, such GCS is usually well guarded both physically and in the virtual world of the network.

The aerial segment

This segment contains the essential components for wirelessly controlling the UAV from a distance. It includes the control software, control hardware, onboard computer, power management system, and sensory components. The sensors include but are not limited to airspeed sensor, compass, GPS, 6- or 9- degrees-of-freedom (DoF) Inertial Measurement Unit (IMU) and computer vision cameras, etc. The main objective of this segment is to correctly interpret and execute the commands that the UAV received from the GCS. This segment is capable of maintaining a safe and steady flight of the UAV, tracking the pre-defined flight plan, self-monitoring, and processing remote sensing data. More

advanced ones are even capable of running real-time computer vision image processing to better determine its motion parameters.

The communication segment

In a more conventional UAS, this segment consists of two RF communication modems (transceivers), antennas, necessary wired links, and the relevant, modem-specific protocols, which allow reliable communication between the aerial and the ground segment. The ground segment can be equipped with a number of such modems to communicate with several UAVs at the same time. The goal of this segment is to send and receive data between the other two segments reliably. Thus, the communication segment mainly involves defining the communication hardware (type of modem, frequency, bandwidth, range), software (protocols, codex, message content, and structure), and topology (communication structure, such as centralized or dynamic point to point), etc.

1.2.2 The general context of UAANET

Thanks to the rapid development of communication technologies, UAS's can now accomplish missions that were previously not possible. With the recent advancements in the WANET, it is now possible to construct an infrastructure-less network system while being literally on the fly. A recent example of such a network is UAV Ad-hoc NETwork (UAANET). Each UAV is equipped with network communication methods that enable it to achieve communications to its surrounding drones and network Access Points (AP). While GCS is still necessary for mission planning, system management, and data collection, it is no longer necessary to be situated in the geographical and topological center of the network. Instead, functions of the traditional GCS can be split into individual subsystems, optimistically distributed into the zone of operation, in addition to being implemented with improved fault tolerance measures such as overlaps and backups. Although it may seem futuristic, but in reality, it has been intensively studied. The use case found in the literature can be generally summarized as shown in Figure 1.3

In addition, one specific use case of such a network is illustrated in Figure 1.4. In this scenario, the project is conducted with three UAVs (DT1, DT2, DT3) and a GCS to fulfill this remote sensing mission as the actual operation site is obscured by the terrain with no network service coverage. One way to achieve this is to arrange the UAVs in a relaying formation, using DT3 as the actual sensor

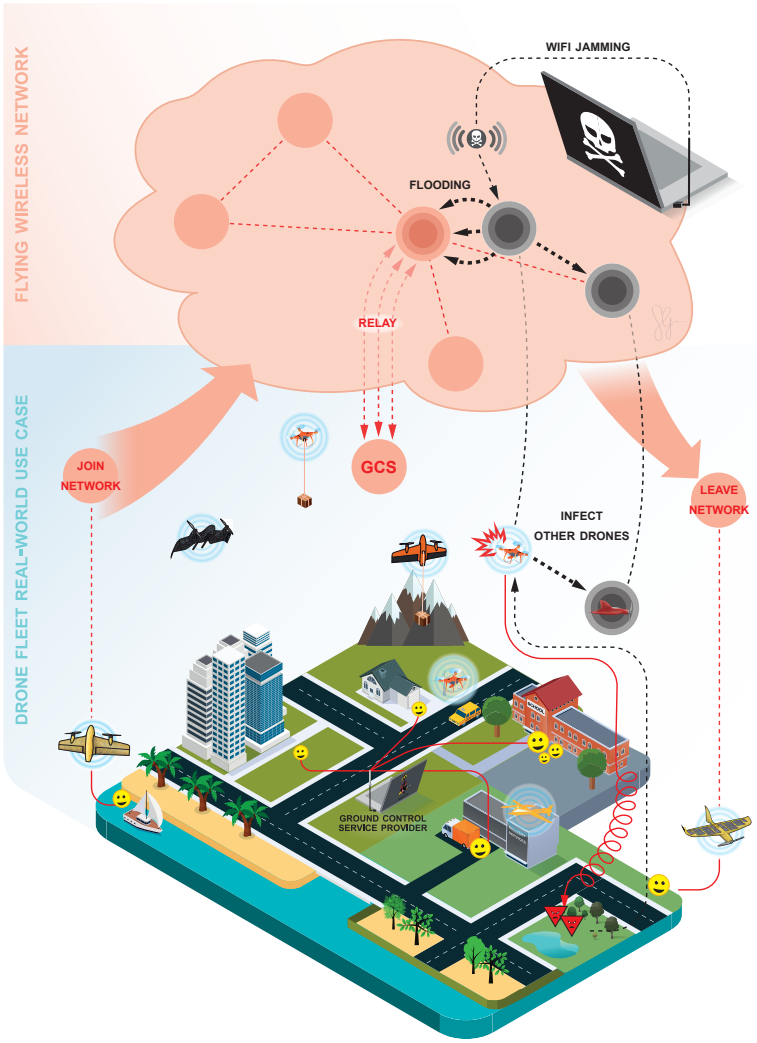


Figure 1.3: A demonstration of how a UAS can be used and attacked (illustrations and graphic design: Sarah Gluschitz)

carrier and the other 2 UAVs as the wireless network bridge to extend the network coverage. With UAANET, the configuration of each UAV is identical, and the role of the UAVs are interchangeable. The preparation of such a setup is considerably simpler than a traditional UAS, which requires pre-configuring of the communication system of each UAV by tweaking the hardware and software on the ground.

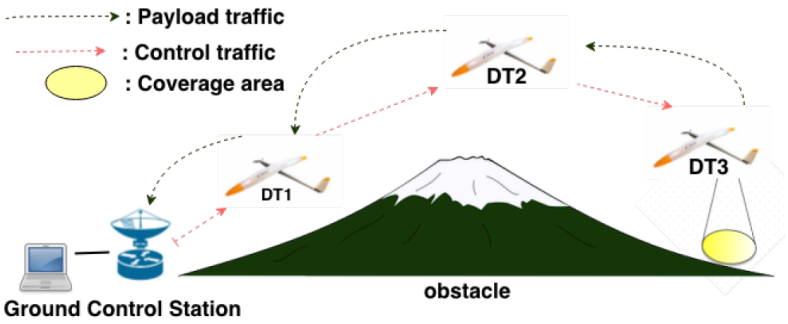


Figure 1.4: Use a UAS as a network relay and remote sensor carrier

.

1.2.3 The general context of civil aviation

It is quite obvious that there will be no clear separation between the operation of the UAS's and civil aviation in general. Instead, technical routes and government regulations have seemingly laid out the future for the full integration of the UAS's into civil aviation. It is rare to see the authorities setting up detailed rules for such a newborn system, releasing and revising the regulations in a matter of months, which suffices to see how everyone should value and respects the safety and security of civil aviation and the importance of the proper integration of the UAS's into the civil airspace. That means, the designs of UAS's need to learn from past mistakes, anticipate new problems, and do a better job in assessing the risks in advance.

In the scope of this dissertation, I consider the security problem of civil aviation to be closely related to the case of the UAS. Especially in terms of payload, security requirements, moving patterns, and characteristics. Typically, the state-of-the-art civil aviation system relies on a centralized communication topology, where each aircraft is communicating with the Air Traffic Controller (ATC) through a dedicated RF channel, and the position information of the aircraft is being transmitted and collected by a geographically distributed RADAR system. The first role of the ATC is to communicate with each AC to provide instructions to the pilots, to guarantee a proper horizontal and vertical separation between the aircraft in order to ensure the safe operation of air space. The judgments from the ATC are highly dependent on the information provided by the RADAR system. Hence it is imperative to keep an accurate monitoring of the RADAR system and a secured data transmission from RADAR stations to the ATC.

The literature[LRS18]; [Rib+20] found that the RADAR system is susceptible to spoofing attacks

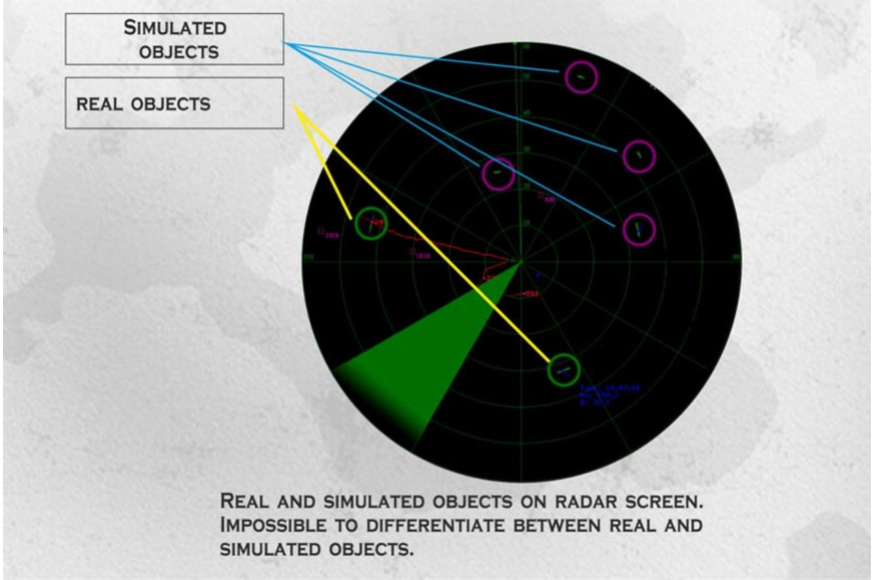


Figure 1.5: Typical RADAR system and demonstration of a spoofing

where crucial information transmitted between the RADAR systems can be captured and altered before it is sent to its final destination, the ATC, which can lead to catastrophic consequences.

The reason why the context of civil aviation is included in this dissertation is that the strong correlation within the mobile characteristics between civil aviation and the UAS made it an excellent candidate to examine the IDS methodology on the spoofing attacks, such as the one shown in Figure 1.5.

1.2.4 Problem description/Challenges

In the scenario introduced in 1.2.2, the use of the UAANET allows for a much easier implementation for high bandwidth communication for the remote UAV, allowing it to send back collected data in real-time, where for a more traditional RF-based UAS, the typical approach is to store the data onboard the UAV for later recovery after the UAV has landed.

Nowadays, UAANET is not only used to transmit general information, such as media feeds, telemetry data, and drones' diagnostic data, etc., but also sensitive data. With expanded functionalities of the drone swarms are becoming more dependent on the network connectivity, more and more sensitive or even critical information is being communicated through the UAANET, including

path planning, way-points, control stream, positional feedback, etc.

By adopting off-the-shelf components and pull-from-git software, the development of the UAS has been dramatically accelerated, with network security continuing to be a critical factor. At the current state, little has been considered for the cybersecurity of the UAS network approaches, leaving even the most state-of-art UAS's vulnerable to various security threats. The situation is aggravated because most of today's wireless communication solutions used in the UAS designs are not explicitly designed for a drone swarm network, nor are many IDS methodologies.

Furthermore, while the strong mobility of a UAV can help the UAANET to achieve complete coverage, a longer reach, and an overall more versatile network, it also creates problems for securing such a network. The potential problems introduced by the mobility of the WANET network have been amplified by the fact that the UAVs as network nodes have one more degree of freedom of mobility, less constrain on the area of movement, less physical protection for each node, better acceleration ability and higher velocity in metropolitan areas but much fewer power resources and network capacity, etc. Because many of the IDS methodologies depend on the assumption of fixed network topology, relatively consistent routing, centralized monitoring, and decision-making node, that have rendered some of the typical IDS strategies inadequate at best. Nevertheless, the use of a network inside of a UAS allows more points of entry into the network, creating more possibilities for the malicious intrusion to happen. Indeed, for a UAS, the risk of losing a UAV to the wrong hands remains to be possible and the A UAS that operates in a suburban area is especially vulnerable to vandalism. In such cases, hackers or malicious third parties can get access to the network regardless of the wireless encryption and launch a variety of attacks on the network from within. Such vulnerabilities are also demonstrated in Figure 1.3.

Most importantly, the UAANET is undoubtedly making its way into civil airspace. As a consequence, the safety perspective rather than the security perspective will have the uttermost importance - a secured FANET can help improve the safety of UAV fleets, but it is more important to ensure the safety of the overall system even if the network is compromised. Hence, existing network security strategies for fixed-topology are deemed ineffective. The new network security strategies must be implemented to ensure the safety of the system by also taking into account the mobility of the network, various possible attacks, and the risk of attacks from within the UAANET.

Thus attacks can happen to individual drones or systematically to the entire UAS. The UAS and drone system should be able to act effectively against the intrusion in order to be airworthy in civil airspace.

1.3 The types of intrusions considered in this thesis

Numerous research has pointed out a large number of possible vulnerabilities within UAS's of differing sizes. Such attacks include GPS spoofing, Network Denial of Service (DoS), WiFi Deauthentication, and Address Resolution Protocol cache attacks.

Through investigating the state-of-the-art literature, it is found that the remote attacks which disrupt the UAS from a distance, for example, communications stream attacks such as the MITM, are very common in recent years in the domain of the UAS, whereas the DoS attacks are even more common in the network community as a whole. Such attacks are interesting, largely due to the popularity and possible destructive results.

Denial of Service Attack

A DoS attack (also known as a flooding attack) is a type of cyber-attack within a network. After gaining access to the network, a perpetrator generates an excess amount of data within the network, floods and overloads the targets, exhausts the resource of the targets, and finally renders the system inaccessible to its intended users. This type of attack has received much attention in recent years due to its popularity among all kinds of networks. It has been demonstrated that with the limited network resource, the intruder can still effectively execute a DoS attack to disrupt the regular operation, and significantly reduce the Quality of Service (QoS) of the network. Especially when a bottleneck node is being targeted. This type of attack is particularly destructive to a UAANET because the network capacity and power capacity in a UAV are very limited, but the information transmitted could be both time-sensitive and mission-critical. The UAV cannot be equipped with a sophisticated intrusion detection and prevention system (IDPS) with near-unlimited computation power as many IDS research suggest. Instead, a specifically designed IDS, which takes into account the different characteristics of a UAV, should be studied in order to achieve an effective and efficient detection.

Main in The Middle Attack

A MITM attack is another type of attack which is gaining popularity in recent years. The attack is conducted to compromise the integrity and the confidentiality of the network by falsifying information. The intruder gains access to the network by acquiring original hardware, modifying it, and sending it back into the network. Thus, the hacked machine will rejoin the network, tricking the routing mechanism into considering it as a legitimate node at an advantageous position and sending more and more data through the hacked machine. Subsequently, the hacked machine will have the possibility of looking inside each non- or weakly-encrypted data packet, modifying the contents, and sending it to the unsuspected original destination. This type of attack is particularly destructive because the intruder may gain access to the very critical data stream, such as the control and the navigation data packet, modify the information, or simply replay the captured data packets to ruin the mission of the UAV or even cause physical damage. To a UAANET, this is particularly interesting because the UAVs typically operate in a suburban area and especially vulnerable to vandalism.

1.4 Thesis outline

This thesis is created in response to the increasing demand. In this dissertation, a new IDS methodology is proposed in searching to resolve different attacks that we are expected to observe in a UAS. The dissertation is laid out in an inverted-pyramid structure:

Chapter 1 The first chapter has given a general introduction to the topic and context of this thesis. This chapter is written in order to explain the reasoning of this dissertation as well as explaining in general the context, which is necessary to understand this thesis.

Chapter 2 The purpose of chapter 2 is to develop the basics of the main concepts involved in this dissertation, such as UAANET and IDS. Then to further develop the scientific context of the tools used in this thesis for better understanding the intuition of the choice of tools in order to achieve the goals of this thesis. Lastly, it is to provide evidence and actualities of the current research in the relevant domains by thorough reviews of the state-of-the-art literature.

Chapter 3 In this chapter, I constitute the first implementation of the newly proposed IDS methodology, which integrates robust observer theory cybernetics with spectral analysis by wavelet leader multifractal analysis (MFA), in addition to a curve matching classification. The pro-

posed proof-of-concept IDS design is tested against a DoS flooding attack, and subsequently, the methodology is realized in a real-world test environment, which returns promising results and proves the feasibility of such a methodology. Finally, the results and discussion on the performance of the first implementation are provided. Chapter 3 has been published in Ad-Hoc Networks [CZL19].

Chapter 4 In this chapter, the second implementation of the IDS methodology is introduced. This second revision of the IDS methodology involves using wavelet leader multifractal analysis with machine learning classification to improve detection accuracy further. The improved methodology is then tested against MITM attacks, which are more delicate and covert. The methodology is tested in a simulation environment, which is created based on real-world Air Traffic Management (ATM) RADAR data with simulated attacks. The results highlight the substantial advantage of this method in tackling more complex problems. The contribution of Chapter 4 has been published in MDPI Drones [ZCL22].

Chapter 5 In the last chapter, I conclude the dissertation with a discussion of the contributions. In this chapter, We summarized the contributions mentioned in the previous two chapters. The future research path which is inspired by this thesis is also discussed.

1.5 Contributions

The research of this thesis is consists of network system and IDS methodology engineering. The major contributions are:

1. to develop a new IDS methodology with the particularities of the UAS in mind, by taking advantage of the dynamic, stochastic, and multifractal properties of network statistics, which is the first of its kind in the domain of UAS networking;

2. to first establish a novel IDS scheme by analyzing the MF spectrum of the network statistics by applying the 2-D curve matching algorithm;

3. to implement a robust observer estimation scheme for a detailed intrusion reconstruction;

4. to further investigate and the performance improvement of the IDS scheme with Artificial Intelligent (AI) principles;

5. to realize the methodology in different test environments in order to explorer the strength and weaknesses of this proposed methodology;

Finally, this dissertation establishes the connection between the concept, theoretical development, and practical implementations. It is to better explain the concepts and theoretical backgrounds in the context of the UAS and civil aviation, hoping that the knowledge can be transferred into aerospace and further developed for this industry. Furthermore, tools and test environments developed for this thesis can later be used for the further integration of this methodology into an actual UAS.

CHAPTER 2

Preliminaries

Contents

2.1 State of the art 16

2.1.1 On UAANET and challenges 16

2.1.2 On general IDS 17

2.1.3 On WANET IDS 18

2.1.4 On FANET IDS 19

2.2 IDS in a nutshell 20

2.3 TCP queuing dynamics and robust observer 22

2.4 Wavelet Leader Multifractal (WLM) analysis 27

2.4.1 Power law/ scale invariance/ self-similarity/ LRD/ fractal 27

2.4.2 Fractal to multifractal 31

2.4.3 Related literature 33

2.5 Curve matching and artificial intelligence classification 35

2.5.1 Binary classification with curve matching 35

2.5.2 Improved classification with machine learning 36

2.5.3 Related literature 38

2.5.4 Discussion 40

In this chapter, I present the actuality of the research, the underlying concepts, and preliminaries that are essential for better understating the elements involved in this dissertation. The literature of each specific domain is reviewed in order to provide evidence and fundamentally support the proposed methodology.

2.1 State of the art

This section presents the literature reviewing the problems and challenges regarding the UAS, the UAANET, and network IDS. This chapter aims to provide the reader with more insights into the motivation of this research and the plenary context of the current state of research.

2.1.1 On UAANET and challenges

Today's decentralized technology promotes the distribution of missions and corresponding resources.

In [Bar+19], Baron et al. have reviewed a large number of research on the topic of using the mobility of state-of-the-art mobile entities as an advantageous data delivering method. For such a system, the performance metrics are directly proportional to the mobility and onboard data density. While the data density is physically limited by the storage technology, mobility becomes the main objective to optimize. Which, in turn, exacerbates the problems related to mobility.

In [BST13], the authors provided an in-depth review of practical implementations of FANET, including the various applications, design characteristics, and communication protocols. The authors made a clear distinction between regular ad-hoc networks, wireless ad-hoc networks, and FANET, accompanied by a detailed review of the problems raised with the different characteristics. This article provided a good reference point for the approaches of FANET. Finally, the authors discussed the open issues in the research and open issues in the field of FANET.

As demonstrated in [JS03], the nature of high mobility combined with limited resources in a MANET has made the design of an effective network security system for the MANET particularly difficult. This particular issue is further exacerbated by the more extreme nature of FANET.

In [Jav+12], the authors have provided an exhaustive breakdown of threats and risk assessment of network cyber-security of a UAS from a relatively recent point of view. According to the matrices provided by the authors, the network security risks such as DoS and spoofing surpassed other threats in terms of severity and likelihood thus resulting in the highest risk scores.

In [Rod+17], the authors made a review on the combination of the UAV and the Internet of Things technologies. One of the fundaments to achieve this is by applying an ad-hoc network in a fleet of

UAVs to form what is known as FANET. This approach allows increased redundancy in terms of critical components and improves the overall robustness of the system.

In addition, As described in [SK14]; [Tea+10], most of today's advancements in the domain of network-attached UAV fleets are focusing on the path to achieve a drone network.

In [Akr+16]; [AY17], the authors have emphasized the severity of the current state due to the lack of consideration for the cyber security of the drone network approaches leaving even the most state-of-art drone network systems vulnerable to various security threats,

In the literature, a number of contributions, such as the ones mentioned in [Kim+12]; [BcT16], have been conducted, describing in detail the possible security threats that a UAV fleet can be facing during its normal operation.

In addition, as described in [LCD04]; [HHP03], there is a multitude of threat models related to network intrusions such as overload, flash crowds, worms, port scans, and jamming attacks. Among these abnormal patterns, flash crowds have the worst impact on the fleet of UAVs because they create congestion and significantly reduce the QoS of the entire network. This is major adversity for UAV certification and integration into civil airspace. Consequently, malicious anomaly detection is an important issue nowadays.

2.1.2 On general IDS

There is already rich literature regarding IDS for regular networks. The concept of IDS can be realized by incorporating many scientific domains to achieve a common goal: detecting network anomalies and compromises.

[Bac00] has provided a great guideline and clear overview of the IDS. The authors have provided a precise classification of IDS based on the monitoring and analysis approaches. They also offered a brief introduction to the possible attacks and vulnerabilities. Finally, the authors summarized the advantages and disadvantages of different techniques.

In [Hin+20], the authors provide a clear and recent overview and a detailed taxonomy of the intrusion detection methodologies. The authors also summarized the most popular IDS research from

the past decade with relevant algorithms and datasets. A general threats taxonomy is also provided. Finally, the authors provide a statistical summary of the current trend of development in the field of IDS, showing the dominance of the machine learning algorithms in this domain.

In [CBK09], an overview is provided reviewing multiple research areas and application domains. Network anomalies and security-related problems (such as Distributed Denial of Service (DDoS) attacks) are important issues for the detection of active security threats.

The three documents have provided fundaments for the development of the intrusion detection systems, and they also laid out clear technical routes for the common problems.

2.1.3 On WANET IDS

In recent years, the development of the MANET has received more and more attention. Due to its mobility properties, the behavior of such networks is drastically different from the ones with fixed topology.

In [BK03], the authors provide a clear overview of the unique problems which could exist within the WANETs because of their variable topologies, lack of centralization, and physically hazardous nature. The author further summarized the solutions for the IDS in a WANET. The author also mentioned one way to achieve an effective IDS in a wired or wireless ad-hoc network is by applying statistical anomaly detection. The solutions proposed in this article are mostly non-ML-based, which shows that the development of the ML methods has been greatly accelerated in the last two decades.

In [MNP04], the authors target more specifically on the Wireless ad-hoc network by introducing the unique properties. They point out the vulnerabilities with respect to the power dimension, where a node inside a WANET usually have more restrictions on computation resources and power compared to a wired network, in addition to the vulnerabilities introduced in [BK03], The malicious users can exploit this simply by injecting resource-exhausting attacks such as a DoS attack and quickly compromising a UAS. The authors then discussed the requirements for the New IDS's designed specifically for a mobile ad-hoc network and then proposed several strategies, including distributed IDS, routing protocol-based IDS, and training-based anomaly detection.

In [YGA15], The authors made a clear categorization of autonomous and unmanned vehicles with

the related cyber-attacks, vulnerabilities, and potential consequences. A review of detect and defense strategies is then provided. As mentioned in this article, the DoS and MITM attacks are common threats for a WANET. The defense strategies are first being developed by the military and authorities, but now it is more and more common in civil applications especially in the mobile and aeronautical domain.

2.1.4 On FANET IDS

In [Sha+20], the authors provide a thorough review of the communication and network technologies for UAVs specifically.

In [Yan+19], beyond the excellent summary of the UAV communication channel modeling and link budget analysis, this article also serves as a great summary of the different communication methods of different use cases with a timeline of how wireless communication technology evolves.

[NAL21] is a more recent review on the issues faced by the UAV/UAS network development. The authors provide a state-of-the-art review of the network technologies, topologies, and applications for UAV communication. The authors provide a quick reference guide on the most recent discussions on network security issues faced by the UAS development community.

In [KM17], the authors provided a more detailed description of vulnerabilities within a UAS, with actual examples of various attacks towards UAS's in recent years.

In [Ran+16], the authors make specific points on the security issues in a UAS. The authors specifically address why network intrusions such as the DoS/DDoS and MITM are particularly dangerous for a UAS. The relevant tools for exploiting the vulnerabilities as well as mechanisms of defense are also reviewed. Additionally, a real-world example of hacking a well-known Parrot AR drone is provided, emphasizing the importance of network intrusion detection in a UAS network.

[HS13] is another interesting article. In which, the authors introduced the security issues laying within wireless UAV network from a more noncivil perspective, where the security of a UAS is vital. The author provided a more detailed introduction to the UAS of various structures, a matrix for better risk assessment of the complete UAS's, in addition to a comparison of commercial UAVs against specialized UAS's. The assessment method is particularly interesting due to the fact that even the

commercially operated UAS's need to have the same respect towards safety as any other aerial systems operating in civil airspace.

In [Mek+21], Y. Mekdad et al. have provided a very recent review on the security and privacy issues. The authors made an exhaustive summary on this topic. The security issues are outlined in four major categories: sensor-level, hardware-level, software-level, and communication-level. More specifically, on the communication level, the authors identified the four common UAV communication network architectures and their relevant network intrusion schemes. Furthermore, the authors summarized the most common wireless communication technologies adapted by the state-of-the-art UAS's with examples of security issues. Finally, the authors provide a comprehensive analysis of the privacy issues related to the UAS, which is becoming more and more relevant in recent years.

From the observations in the literature mentioned above, there are numerous remote attacks that can disrupt the UAS from a distance. For example, communications stream attacks such as MITM have been prevalent in recent years in the UAS's. In contrast, the DoS attacks are even more common in the network community as a whole. Such attacks are the most interesting mainly due to the popularity and possible destructive results, where countermeasures are still under development.

2.2 IDS in a nutshell

The attempts to compromise the confidentiality, integrity, availability or functionality of a computer network are defined as network intrusions. [Bac00]

An intrusion detection system is a device that has been implemented into the network system intended for monitoring the network for abnormal or malicious activities and policy violations.

Such implementation can either be centralized or distributed in the network. The information on the network activities is collected and analyzed to determine the nature of the activities. Once the anomalies or suspicious activities are found, the IDS would send a report to the security information and event management(SIEM) system for the network administrator to take appropriate actions.

Different from the network security system, which typically implies authentication and encryption, that protects the network by authorizing only the legitimate users to access the network and

limit the accessible contents. The IDS usually acts as the second line of defense, which observes the network and either passively reports (such as an IDS) or actively intervenes (such as an IPS) in the network activities.

An IDS is typically categorized within one of the following subsets:

Signature-based

In a signature-based IDS, the characteristics and patterns of the attacks are once studied and stored in the IDS, then later been used to examine the signatures from the network during the normal operation. A variety of tools for anomaly detection are principally based on data packet signature. This behavior is known to be very effective against many well-known attacks. The IDS of this category relies on the comparison of signatures to the known attacks. Thus it is imperative to guarantee a frequent update of the signature database in order to keep up with the ever-evolving network intrusions. This type of IDS is prone to vulnerabilities, such as zero-day attacks, because it relies on previous knowledge of different intrusions, and security updates containing fixes always come later than the discovery of the vulnerabilities as described in [Bac00].

Anomaly-based

In an anomaly-based IDS, the idea is to first analyze the legitimate activities and statistics of the trustworthy network during its normal operation, either by statistical tools or machine learning methods. Thus the patterns of normality are set and used to compare with new behaviors observed in the network. Instead of basing the methodology on knowledge of the intrusions, anomaly-based IDS relies on the knowledge on the normality, which is more feasible against zero-day attacks. But this type of IDS is more prone to false-positive due to the fact that most networks are not stationary but instead very random. Unexpected changes within the network and unpredictable behaviors of users may result in a false alarm from the IDS. [Bac00]

Hybrid

The hybrid IDS, namely a strategically designed IDS exploiting the advantages of signature and anomaly-based IDS, is relatively a new concept. But the idea is actually driven by the ever-evolving demands. The development of networks is inevitably heading towards better availability, higher complexity, and better robustness. But with more participants and more dynamic interactions, it is more

and more challenging to define a strict pattern for each network user as well as determine a nominal state for the network as a whole. With more varieties of interactions, it is also becoming more difficult to detect new vulnerabilities even if the attacks are already taking place, not to mention to build a proper database for training the heuristic methods. Hence, many have proposed to use combined solutions to mitigate this problem.

Statistical method

As the network grows more and more complex, it is less practical to try to keep up with the evolution of networks with the continuously intensive development of IDS. Instead, one can try to exploit the complexity to their advantage. One way to approach such a solution is to analyze the statistics of the system. In fact, statistical techniques are very commonly used for anomaly detection, especially, in the field of finance, health care, and the stock market as mentioned in [MMH17]. For example, the standard score or Z-score method is commonly used as outlier detection in statistics. It is a feasible anomaly-based intrusion detection method for systems with finite variance and constant mean [FLB12]. But such a method is too basic to take into account the internal dynamics and the evolving nature of a modern network. Hence, it is imperative to implement more advanced methods in order to explorer the patterns lays within the irregular behavior of a network.

2.3 TCP queuing dynamics and robust observer

Cybernetic theories are deeply implemented into network systems. By exploiting the capabilities of the observer or estimator, combined with existing active control methods implemented inside network systems, such as the Active Queue Management (AQM) systems, it is possible to extend the way malicious intrusion can be detected.

One part of the contribution of this dissertation involves using cybernetic theories: robust observer techniques to achieve robust anomaly detection in a Transmission Control Protocol network. The work focused on the design of a robust observer-based on Lyapunov Krasovkii functional and queuing dynamics of an AQM system in a TCP network. The queuing dynamic is a unique feature thanks to the robust transmission feature of the TCP, which requires the packet to be transmitted without any loss. The AQM system is introduced to actively remove packets in a queue to ensure a reliable

transmission, which in turn causes distinctive patterns within its own dynamics. By exploiting the dynamics of the TCP network, which contains an AQM, we are able to distinguish network traffic that contains anomalies from the normal ones. Also, the observer can be implemented as a trigger for a more intelligent AQM to deal with attacks such as the Denial of Service (DoS).

Among the non-linear methods [Tar05] described in the literature, the Super-Twisting Algorithm (STA) [RLG09]; [Rah+10]; [Rah+13] is the most widely used for chattering avoidance while detecting anomalies. Its principles rely firstly on the non-linear fluid model applied to the TCP dynamics and secondly on the sliding modes, [Ari+12] which are often used to design robust non-linear observers or control laws. Unfortunately, building upon this peculiar observer provides for a bounded input-bounded state (BIBS), finite-time stability only [RF99]. Consequently, this statement restricts the application of this observer to the class of the systems, for which the upper bound of the initial condition might be estimated in advance.

In order to tackle a wider range of applications, various implementations of TCP models have been proposed in terms of assumptions and numerical techniques [LPD02]; [Sri04]; [Tar05]. TCP network is commonly represented using a linearized fluid-flow model, [LPD02] which associates with the network topology I considered here.

Inspired by the TCP AQM control scheme that has been demonstrated in [LAG07]; [ALG08]; [Miq+17]; [Ari+09], it is possible to take a step further to implement the robust observer to measure the level of abnormal activities. In this dissertation, I first consider the topology to consist of N TCP sources, with the same propagation delay connected to a destination node through a router.

The bottleneck link is shared by N flows, and TCP applies the congestion avoidance algorithm described in [Jac88]. To implement an Intrusion Detection System (IDS) according to the network topology presented previously, it is necessary to use, if possible, additional instruments (e.g., probability of packet, the queue of the router buffer) and linear/non-linear estimation algorithms. The estimation algorithm makes use of the queue at the router buffer, which delivers a scalar q. Assuming a continuous flow, the behavior of the network can be represented mathematically as follows as

described in [LAG07]; [ALG08]; [RLG09]:

$$\mathscr{M}_s \begin{cases} \dot{W}(t) = \frac{1}{\tau(t)} - \frac{W(t)W(t-\tau(t))}{2\tau(t-\tau(t))} p(t-\tau(t)) \\ \dot{q}(t) = \frac{W(t)}{\tau(t)} N - C + d(t) \qquad (process) \\ y(t) = q(t) \qquad\qquad (measurement) \end{cases} \tag{2.1}$$

In the first differential equation, $W(t)$ represents the TCP window size, $\tau(t)$ the round trip time (RTT) which can be modeled using parameters associated with the network configuration C and T_p as $\tau = q/C + T_p$. The latter quantity C represents the transmission capacity of the router, T_p the propagation delay, and N which is the number of TCP sessions. The variable $p(t)$ is the marking/dropping probability of a packet and can be seen as known measured input. This quantity relies on the explicit congestion notification to regulate the queue size of the router buffer. In the second differential equation, $q(t)$ is the queue length of the router. The malicious anomalies are modeled by an additional signal $d(t)$ mixed with the regular traffic passing through the router and filling the buffer.

The non-linear state space representation corresponding to $\mathscr{M}_s$ can be described in a compact form such as: $\dot{\underline{x}} = f(\underline{x}, u, d)$ and $y = h(\underline{x}, u)$ where: $\underline{x} = [W^T, q^T]^T, u = p$ and $y = q$ are the state, input and output vectors respectively. Moreover, a linearization of $\mathscr{M}_s$ was carried out in [MGT00] to allow the use of traditional control theory approaches. The fluid-flow model of TCP now becomes :

$$\delta\mathscr{M}_s \begin{cases} \delta\dot{W}(t) & = -\frac{N}{\tau_0^2 C}(\delta W(t) + \delta W(t-\tau(t)) \\ & \quad -\frac{1}{\tau_0^2 C}(\delta q(t) - \delta q(t-\tau(t)) \\ & \quad -\frac{\tau_0 C^2}{2N^2}\delta p(t-\tau(t)) \\ \delta\dot{q}(t) & = \frac{N}{\tau_0}\delta W(t) - \frac{1}{\tau_0}\delta q(t) + d(t) \end{cases} \tag{2.2}$$

where $\delta W = W - W_0$, $\delta q = q - q_0$, $\delta p = p - p_0$ are the perturbed variables around the operating point defined by:

$$\begin{cases} d(t) = 0 \\ \dot{W}(t) = 0 \Rightarrow W_0^2 p_0 = 2 \\ \dot{q}(t) = 0 \Rightarrow \begin{cases} W_0 = \frac{\tau_0 C}{N} \\ \tau_0 = \frac{q_0}{C} + T_p \end{cases} \end{cases} \tag{2.3}$$

Inspired by the theory of time-delay systems [Ari+12], the dynamics of the queue and the congestion

window are modeled to address delay issues. Indeed, the time delay is an intrinsic phenomenon in networks whose control should improve the precision of $\delta\mathscr{M}_s$. The idea is to exploit the linearized TCP fluid-model within a time delay framework as follows where $\delta\underline{x}(t) = [\delta W(t)\ \ \delta q(t)]^T$ is the state vector and $\delta u(t) = \delta p(t)$ the input:

$$\delta\mathscr{M}_s \begin{cases} \delta\dot{\underline{x}}(t) &= \mathscr{A}\,\delta\underline{x}(t) + \mathscr{A}_d\delta\underline{x}(t-\tau(t)) + \mathscr{B}\delta u(t-\tau(t)) + \mathscr{B}_d d(t) \\ y(t) &= \begin{bmatrix} 0 & 1 \end{bmatrix}\delta\underline{x}(t) \end{cases} \tag{2.4}$$

with

$$\begin{cases} \mathscr{A} = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & -\frac{1}{\tau_0^2 C} \\ \frac{N}{\tau_0} & -\frac{1}{\tau_0} \end{bmatrix} \\ \mathscr{A}_d = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & \frac{1}{\tau_0^2 C} \\ 0 & 0 \end{bmatrix} \end{cases} \tag{2.5}$$

and

$$\begin{cases} \mathscr{B} = \begin{bmatrix} -\frac{C^2\tau_0}{2N^2} \\ 0 \end{bmatrix} \\ \mathscr{B}_d = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{cases} \tag{2.6}$$

Based on such a model, formulated in the general form of a time-delay system, it is possible to design both the AQM and estimator in order to estimate the malicious intrusion while taking into account a level of QoS (i.e., the drop probability $p(t)$), by using the Lyapunov Krasovskii method [GKC03], which is an extension of the traditional Lyapunov theory. As shown in Figure 2.1 the control law stabilizes the TCP network (queue lengths and rates) to the desired equilibrium (W_0, τ_0, q_0) in spite of the presence of some non-responsive traffics, ensuring then a certain level of Quality of Service (QoS). Various AQM mechanisms exist in the literature, such as Random Early Detection [FJ93] (RED), Random Early Marking [ALL00] (REM) and more recently using control theory (proportional and proportional integral controller [Hol+02] or state feedback controller [YYF09]). The estimator has to be designed in addition to an efficient AQM. We proposed a robust controller / observer for IDS by solving an LMI criteria (see [Miq+17], for details of proof) on the following augmented model:

$$\delta\mathscr{M}_s^+ \begin{cases} \delta\dot{\underline{\tilde{x}}}(t) &= \bar{\mathscr{A}}\delta\underline{\tilde{x}}(t) + \bar{\mathscr{A}_d}\delta\underline{\tilde{x}}(t-\tau(t)) + \bar{\mathscr{B}}\delta p(t-\tau(t)) \\ y(t) &= \bar{\mathscr{C}}\delta\underline{\tilde{x}}(t) \end{cases} \tag{2.7}$$

With

$$\begin{cases} \bar{\mathscr{A}} = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & -\frac{1}{\tau_0^2 C} & 0 \\ \frac{N}{\tau_0} & -\frac{1}{\tau_0} & 1 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathscr{A}_d} = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & \frac{1}{\tau_0^2 C} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathscr{B}} = \begin{bmatrix} -\frac{C^2\tau_0}{2N^2} \\ 0 \\ 0 \end{bmatrix} \\ \bar{\mathscr{C}} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \end{cases} \tag{2.8}$$

where the perturbed variables $\delta\underline{\tilde{x}}(t)^T = [\delta W(t)\ \ \delta q(t)\ \ d(t)]^T$ around the desired equilibrium (W_0, τ_0, q_0) represents the augmented state. Practically, the objective is to reconstruct $d(t)$ from any attack modeled by wavelet analysis from Step 1, and design an output feedback AQM. In this dissertation, the malicious intrusion $d(t)$ has been chosen constant (i.e $\dot{d}(t) = 0$) assuming a constant flash crowd attack which can be mathematically represented by a step function. Consequently, we are looking for gain controller $\mathscr{K}$ and gain observer $\mathscr{L}$ defined as (see [Miq+17], for details of proof):

$$O(L) \begin{cases} \delta u(t-\tau(t)) &= -\mathscr{K}y(t) = -\mathscr{K}\mathscr{C}\delta\underline{x}(t) \\ \delta\dot{\underline{\hat{x}}}(t) &= \bar{\mathscr{A}}\delta\underline{\hat{x}}(t) + \bar{\mathscr{A}_d}\delta\underline{\hat{x}}(t-\tau(t)) + \bar{\mathscr{B}}\delta u(t-\tau(t)) \\ &\quad + \mathscr{L}\left(y(t) - \mathscr{C}\delta\underline{\hat{x}}(t)\right) \end{cases} \tag{2.9}$$

The first equation corresponds to the dynamics of the AQM.

The second equation corresponds to the estimation of the state vector $\delta\underline{\hat{x}}$ and describes the dynamics of the observer. We recognize the typical mathematical expression of a linear state estimator with correction terms $\mathscr{L}$. The idea is to build an additive correction term based on linear gains $\mathscr{L}$ which keeps stabling the dynamics of the estimation error $e(t)$. Such an approach is systematic for more complex dynamical systems than the ones represented by a single router.

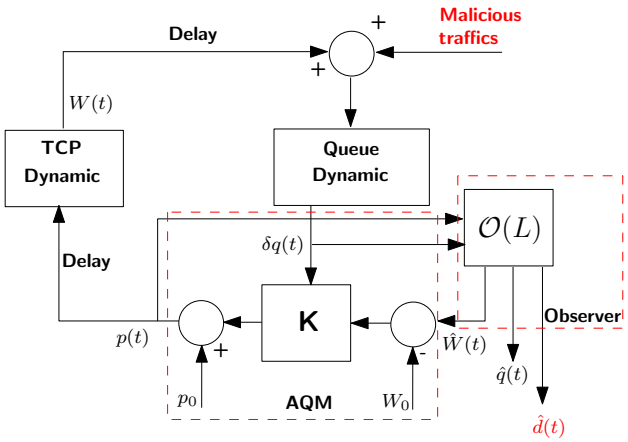


Figure 2.1: Robust observer on a TCP AQM system

2.4 Wavelet Leader Multifractal (WLM) analysis

In this section, I introduce the incentives of applying WLM to accomplish the proposed IDS methodology. In order to better understand the evolution of network-related fractal and multifractal theories, the presentation of this section is structured by first providing the underlying theoretical backgrounds, briefly introducing the fractal-related theories and MF formalism. Then it is presented the progression of research from the fractal to multifractal behaviors of the network traffic, with state-of-the-art literature to better support the choice of the particular WLM analysis tool.

2.4.1 Power law/ scale invariance/ self-similarity/ LRD/ fractal

The four notions are frequently used in literature to describe similar phenomenons as shown in [Kom04]; [Abr+03]; [Abr+02]. For a process to exhibit the power-law behavior, it usually involves taking a measurement of an object with a given size (a measurement unit), and the number of occurrences is inversely proportional to some power of the size. For example, to measure the total length of a coastline, the measured length is dependent on the scales used. A landmass shows similar features at all scales, from hundreds of kilometers to millimeters and below. Thus it is not apparent to determine the smallest or the most characteristic features when performing such measurement. Let's assume the total length of a coastline is L. To cover the coastline, some fractions of length ε are used to represent or cover the coastline. Thus the total measured length L_ε is a function of ε and the number of fractions

N utilized to cover the coastline $N\varepsilon$:

$$L_\varepsilon = N\varepsilon \tag{2.10}$$

The length L is then defined as the limit when the fraction goes to zero:

$$L = \lim_{\varepsilon \to 0} L_\varepsilon \tag{2.11}$$

Apparently, decreasing the value of ε increases the resolution of the measurement. At higher resolution, more details of the coastline will be covered by the smaller fractions. The total length L_ε will therefore increase. A British meteorologist, Lewis Richardson, analyzed this phenomenon for different countries and concluded that the number of fractions satisfied the empirical law [Kap86]:

$$N_\varepsilon = \varepsilon^{-D} K \tag{2.12}$$

Where K and D are constants depending on the coastline analyzed. We can then take the more general form:

$$y(x) = x^{-D} \tag{2.13}$$

Eq.2.13 is the expression of the general equation for power law.

This equation is particularly interesting because it exhibits the following property:

$$y(cx) = (cx)^{-D} = c^{-D} y(x) \tag{2.14}$$

This means that when zooming in or out of the function on the x-axis, what ends up is an amplified version of the same function, such that there is no characteristic scale that can be identified. Thus, such function is also described as scale invariance. The observation $y(cx)$ is a function of a constant c and an exponent D, namely the scaling exponent (also called the fractal dimension).

Two forms of the scale invariance functions can then be found: self-similarity (SS) and Long-Rang dependence (LRD).

The notion: self-similarity is frequently used to describe similar geometries observed in the physical world (either in the geometries themselves or their statistics): The whole resembles the part, which means the properties are consistent throughout the scale of observation. The most famous example

of such behavior is fractal: objects that show similar geometric features at a set of scales. It is found that in nature, many natural geometries exhibit self-similar properties: the shape of romanesco broccoli, the burn mark after lightning strikes a tree, the fern leaves, and the aforementioned geometry coastlines, etc.

The behavior of self-similarity of a continuous stochastic process $X(t)$ can be described with the following notion:

Definition 2.1

A continuous stochastic process $X(t)$ is self-similar if its distribution satisfies:

$$\{X(ct), t \in \mathscr{R}\} \overset{fdd}{=} \{c^H X(t), t \in \mathscr{R}\}, \forall c > 0, 0 < H < 1, \tag{2.15}$$

where $\overset{fdd}{=}$ means equality for all finite dimensional distributions. c is a constant, namely the dilation factor.[Abr+02]; [Loi+10]; [LB09]; Process $X(ct)$ appears to be non-distinguishable to its dilated and amplified version $c^H X(t)$, in its finite-dimension all distribution. The statistical properties of such a process are dominated by one parameter H, namely the self-similarity or Hurst parameter (Also known as Hurst Exponent).

In addition, in [Abr+03]; [Wil+03]; [Gon+05], it is introduced the Long rang dependency property of a process: A process is said to be long-range dependent if its second-order statistics (Variance) converges to a constant or its autocovariance function decays slowly.

For a discrete second-order stationary process with zero mean $Y = (Y_t : t = 1, 2, 3, ...)$, the aggregation level $m > 1$ is used to define the aggregated process $Y_t^{(m)}$ of Y_t:

$$Y_t^{(m)} = \frac{1}{m}\left(Y_{(t-1)m+1} + \cdots + Y_{tm}\right), \quad t \geq 1 \tag{2.16}$$

The aggregation partitions Y_t into non-overlapping blocks of size m and taking the block averages to obtain the new observation $Y_t^{(m)}$ where t denotes the block index. Then, for each integer $m > 1$, $Y_t^{(m)}$ defines a new second-order stationary and zero mean process. Then the following holds for a discrete self-similar process:

Definition 2.2

A discrete stochastic process Y_t is self-similar if its distribution satisfies:

$$\{Y_t, t \in \mathscr{R}\} \overset{fdd}{=} \{m^{1-H} Y_t^{(m)}, t \in \mathscr{R}\}, \forall m \geqslant 1 \tag{2.17}$$

Y_t is called asymptotically second-order self-similar (with Hurst parameter $0 < H < 1$) if the variance of $Y_t^{(m)}$ converges to a finite number:

$$\lim_{m \to \infty} \mathrm{Var}\left(m^{1-H} Y_t^{(m)}\right) = \sigma^2, 0 < \sigma < \infty \tag{2.18}$$

And the autocorrelation function $r^{(m)} = (r^{(m)}(t) : t > 0)$ of the aggregated process$Y_t^{(m)}$, follows:

$$\lim_{m \to \infty} r^{(m)}(t) = \frac{1}{2}\left((t+1)^{2H} - 2t^{2H} + (t-1)^{2H}\right) \tag{2.19}$$

Furthermore, Y_t is said to be exactly second-order self-similar if $\forall m > 1$, process $m^{1-H} Y_t^{(m)}$ and Y_t should have the same variance and autocorrelation:

$$\begin{aligned} \mathrm{Var}(Y_t) = \mathrm{Var}\left(m^{1-H} Y_t^{(m)}\right) = \sigma^2, 0 < \sigma < \infty \\ r^{(t)} = r^{(m)}(t) = \tfrac{1}{2}\left((t+1)^{2H} - 2t^{2H} + (t-1)^{2H}\right) \end{aligned}$$

Such process Y_t with autocorrelation function $r^{(t)}$is said to exhibit LRD.

To summarize, the two concepts, power-law, and scale invariance, represented by fractal dimension D and Hurst parameter H are closely related, although the two concepts are independent[Kom04]. In [GS04], the authors further discussed the relations between the two concepts with a proposed model which separated the two parameters. It is not recent for the science community to try to describe natural phenomena by studying statistical scaling laws. This mathematical tool allows us to understand the phenomenons better and more accurately model stochastic systems. Conversely, it is possible to find similarities exhibited in systems with very different physical entities and classify the systems by studying the two parameters.

However, studying the self-similar properties of practical problems can be proven to be too restrictive[Abr+02]. For a process to be strictly self-similar, it requires the Eq.2.15 to hold true $\forall c > 0$,

which, in many cases, is not practical.

To alleviate the problems faced by the self-similar modeling of complex processes, multiple models are proposed, including self-similar processes with stationary increments (H-sssi), Fractional Brownian motion (fBm), Rosenblatt Process (ROS), and α-stable motion[Rie99]; [Wer+05]; [MN68]; [Par07], readers are referred to the above literature for more detailed information.

2.4.2 Fractal to multifractal

For many natural processes, it is still not possible to describe their fractality by a single scaling exponent due to its restrictive nature. For such a signal, it is not strictly self-similar. Instead, its scaling characteristics are related to the distribution of its scaling exponents. Therefore. a function (spectrum) of scaling exponents can be used to describe the scaling behaviors of the process. Such a process is often regarded as a Multifractal process. The scaling behavior of such a process can be described by the local scaling exponents. But as it is no longer a constant, the scaling exponent can vary from one point to another and becomes everywhere discontinuous. Instead, it is more interesting to study the distribution of the scaling exponents by forming some sort of spectrum.

A spectrum of the ensemble $\mathscr{D}(h)$ formed by all the points that share the same scaling exponent versus all the scaling exponent h is called the singularity spectrum (or multifractal spectrum). Here instead of describing the global scaling behavior of the system with the notion of scaling exponent, it is more closely related to a local scaling behavior w.r.t. the local scaling exponent at small scales. Such exponent h is then named as the local Höder exponents.

MF analysis is essentially a mathematical term used for measuring or estimating the function of MF spectrum $\mathscr{D}(h)$ of a particular process. Instead of trying to describe the process by a constant scaling exponent D, the intention of the MF analysis is to provide a way to describe the distribution of the local Höder exponents h. For a random process $X(t)$, at each point t_i, its local Höder exponent can be given as $h(t_i)$. Then its iso-Höder set w.r.t. to different values of h can be expressed as:

$$I_X(h) = \{t_i | h_(t_i) = h\}. \tag{2.20}$$

Thus, the MF spectrum of such process can be defined as the Hausdorff (or fractal) dimension of the

iso-Höder set:

$$\mathscr{D}_X(h) = dim_H I_X(h). \tag{2.21}$$

In practice, the multifractal behavior of a physical process X is often not directly characterized by its singularity spectrum $\mathscr{D}_X(h)$. As shown in Eq.2.15, to obtain the complete spectrum $\mathscr{D}_X(h)$ of the process X, it requires to compute the local Höder exponents h at all time scales for the finite observation of the data, which is often impractical. Hence, instead of approaching an infinite problem, one has to resort to numerical approaches, which allow estimating the multifractal spectrum from limited observation of the data. Such formulas are called multifractal formalism (MF). [Jaf97a]; [Jaf97b]

It is found possible to describe the MF spectrum by the Hurst parameters $H(q)$ when analyzing the process at different statistical moments q. The MF spectrum $\mathscr{D}(h)$ is related to the Hurst parameter $H(q)$ through a Legendre transformation, as described in [Wen08]:

$$\mathscr{D}_f(h) = \min_{q\neq 0}(d + qh - H(q)), \tag{2.22}$$

Where d is the dimension of the signal.

This relation enables several methods to establish an accurate estimation of the MF spectrum with different multi-resolution quantities in time-, frequency, or wavelet-domain. The Wavelet leader (WL) coefficient is one of many multi-resolution quantities that can be used to estimate the MF spectrum $\mathscr{D}_f(h)$. This is achieved thanks to the multi-resolution properties of the structure-function $\zeta^L(q)$ of the WL coefficient. This allows the accurate approximation of $\mathscr{D}_f(h)$ by replacing $H(q)$ with $\zeta^L(q)$. The MF spectrum estimated by the WL structure-function provides a tight upper bound of the actual MF spectrum[Abr+02]; [Abr+03]; [Jaf04]; [Wen08]; [LB09]:

$$\mathscr{D}_f(h) \leq \mathscr{D}^L(h) = \min_{q\neq 0}(d + qh - \zeta^L(q)). \tag{2.23}$$

For simplicity, throughout the rest of the dissertation, the estimated MF spectrum $\mathscr{D}^L(h)$ is denoted as $\mathscr{D}(h)$ as the MF spectrum signature of the signal.

The WLM analysis is frequently used to quantify the variability of any time series we wish to characterize. This method was first introduced by Dr. Herwig Wendt to analyze dynamical turbulence data

(see [Fon+08]; [Wen08]; [WAJ07]; [WA07]; [Wen+09] for details) and has the advantage of capturing the complexity of traffic for different time scales and different moments of analysis. This analysis then returns a numerical signature used to find the difference between legitimate traffic and traffic that contains an attack. Comparing this to the more traditional discrete wavelet method, this method not only shares the same advantageous performance boost, because they both rely on orthogonal wavelet decomposition and benefit from fast decomposition algorithms, but it also correctly estimates the MF spectrum at negative moments.

The WLM (currently revised as the Wavelet p-Leader and Bootstrap based MultiFractal analysis (PLBMF)) MATLAB toolbox, designed by Dr. Wendt et al., provides a simple and straightforward solution for estimating the MF spectrum by calculating the scaling function with the wavelet leader coefficient at given moments and then estimating the MF spectrum. It returns multiple attributes, which show different aspects of the multifractality of the analyzed signal, such as the set of structure functions S, scaling exponent $\zeta^L(q)$, the scope of local Höder exponents, and the estimated MF spectrum $\mathscr{D}^L(h)$.

2.4.3 Related literature

When considering network traffic, we often consider the variations in the flow of network data, for example, the number of packets or bytes of data being transmitted per second within the network.

In the literature, the scaling behavior of network traffic has been mentioned and studied in numerous researches: [Lel+93] is one of the earlier contributions that associates the self-similarity property with network traffic. The authors established the theory based on data collected between 1989 and 1992 on a high-speed LAN network B-ISDN. From which, the authors concluded that the data they collected exhibits statistical self-similarity with the Hurst parameter satisfactorily describing the variability of the network traffic. Furthermore, the authors determined that self-similarity is ubiquitous and unavoidable for future network research.

In [TTW97], the authors raised the question of whether the network traffic is self-similar or actually multifractal. They finally consolidate their earlier conclusion with further evidence that statistical self-similarity is a sufficient model for the LAN and WAN data traffic they have collected. But the possibility of using a multifractal model to describe general network traffic remains open.

In [Wil+03]; [Rie+01], the authors further introduce the LRD property into the modeling of the network traffic, which invoked the need for a multifractal model of the network or even beyond. They provided rich literature of the same time period regarding the modeling of various networks with LRD or MF with diverse techniques and resulted in different levels of success. They conclude that with LRD and MF, even though it is possible to achieve very accurate modeling of the observed network traffic at the time, there exists so much more potential for the models created with the aforementioned techniques to explain the physical phenomena than simply try to find the perfect model for all networks.

In [Abr+02], the authors made a thorough summary on the relation between network traffic and MFA, in addition to the state-of-the-art wavelet-based MFA methodology. This article is by far the most comprehensive and systematic introduction to the intuition of why MFA is the most feasible tool for network traffic analysis and why wavelet-based MF is more suitable for network traffic.

In [Rie+99], the authors introduced a Multifractal Wavelet Model (MWM) designed specifically for the modeling of network traffic. This model is then used to generate high-quality synthesis network traffic data. The accuracy of the generated data is confirmed compared to real-world data in terms of statistical measures and queuing dynamics. They provide strong evidence that network traffic exhibits MF properties and can be exploited for more accurate network modeling.

In [Fon+08], the authors provided more recent empirical evidence that the internet traffic is indeed exhibiting LRD and MF properties. The longitudinal study is much more relevant because the time span of 14 years of the more recent days shows the characteristics of the modern internet. The authors conclude that the statistical study of internet traffic must taking into account the LRD properties in addition to the multifractality. The combination of the two properties allows for a more precise understanding: in which set of scales the scale-invariance property holds for the internet and how the regular traffic actually behaves in turns of multifractality.

In [Gon+13], the authors developed an anomaly detection scheme based on the piece-wise fractal behavior of network data flow. The authors paid closer attention to the efficiency benefit of such a method with time and space consumption comparison. This is a key benefit of the fractal or multifractal ADS methodology.

In [LB09], the authors made a more general review of the application of fractal and multifractal.

In this article, the authors summarized many image processing and classification applications which involved fractal and multifractal properties. The anomaly detection scheme has not only been applied in the field of networks but also in medical and other fields of image processing.

Finally, in [Fon+15], the authors demonstrate the advantageous wavelet leader multi-scale representation of the internet traffic can be used for anomaly detection by introducing an anomaly detection procedure called Sketch and MultiScale (SMS). This ADS is then tested with a public dataset, mainly against two types of attacks: DDoS and scanning. They illustrated that even though the detection accuracy of the WLM method is less performing than a dedicated ADS for specific problems, but as it is based on a different detection scheme, it is able to identify attacks that are overlooked by the other method. Thus the authors conclude that the WLM method is an excellent complement to the existing anomaly detection schemes with the additional benefit that it takes fewer resources to achieve.

To summarize, the scaling behavior of the network traffic has been extensively studied, and the LRD and MF properties' existence within the network traffics, in general, have been empirically observed as well as proven with simulations. Although it is rather difficult (if not impossible) to scientifically prove such behaviors exists in any given network traces, MFA is still considered one of the most relevant statistical analysis methods for modeling, analysis, and classification of network traffic, in order to better understand the nature and internal dynamics of a network.

2.5 Curve matching and artificial intelligence classification

To achieve automatic intrusion detection, it requires an additional step of processing, in order to compress the information about the intrusion into classes, intensities, or culprits etc. However, the most basic is to provide a binary trigger, indicating if it has caught an intrusion instance. Such detection is done through a classification scheme, whether it is analytical-based or learning-based.

2.5.1 Binary classification with curve matching

As demonstrated in the next Chapter 3, we examined the possibility of applying the analytical classification method, which incorporates a 2-D curve matching algorithm with a threshold [Gri+16].

With this methodology, it is essential to tune the WLM method's variables including moments and time scale to obtain the optimum sensitivity. One way to quantify the sensitivity is to measure how much difference there is between signatures with and without different attacks. In order to establish a comparison between collected signatures, we need to use a reliable and performant algorithm for solving equivalence problems. Among fundamental methods, the three-dimensional edge matching method introduced in [Gri+16] appears to be the most suitable signal processing methodology for classifying curves.

This method, which was designed to help solve 3D Jigsaw Puzzle problems, allows to compare two curves in a three-dimensional space and returns a value normalized between 0 and 1 called "similarity score". Let $\mathscr{C}$ and $\bar{\mathscr{C}}$ be two discrete curves. A "similarity score" is defined as $p(\mathscr{C},\bar{\mathscr{C}}) \in [0,1]$, such that if $\mathscr{C}$ and $\bar{\mathscr{C}}$ are congruent, then $p = 0$. The closer p gets to 1 the more $\mathscr{C}$ and $\bar{\mathscr{C}}$ are different.

In [Fon+15], a similar distance-based classification method is applied. We can observe from the literature that such an analytical method is becoming the performance bottleneck of the IDS with a similar design, especially in terms of detection accuracy.

There is a well-established literature on how to improve classification accuracy. In this research domain, a dominant trend of applying Machine Learning (ML) principles to improve performance in terms of higher accuracy and lower false positive/negative rate, and reduced computational cost in some instances.

2.5.2 Improved classification with machine learning

Classifying data is one of the most common tasks in machine learning. The principle of machine learning classification is to define a mapping function $\mathscr{F}$ from the input signal x to the discrete output class y with machine learning tools such as Support Vector Machine (SVM) and Artificial Neural Networks (ANN).

Support Vector Machine

SVM is a supervised ML algorithm that is mainly designed for classification and regression purposes. The idea behind this method is to expand the original signal into a much higher dimension in order to achieve an easier separation. The actual finite-dimensional space is mapped into a much

higher dimension by a so-called "Kernel Function," which is basically a dot product of two pairs of input data to ensure the computational cost doesn't explode with the drastically increasing number of dimensions. If we assume the training dataset is composed of a certain number n of points x_i of two different classes, given in the form below:

$$(x_1, y_1), ..., (x_n, y_n), \tag{2.24}$$

where the $y_n = 1$ or $y_n = -1$ indicates the exact class x_n belongs. The SVM scheme is intended to define the "maximum-margin hyperplane" that optimizes the maximum distance between the optimized hyperplane and the nearest point x_i from either class.

Neural Network

The principle of a Neural Network (NN) is to mimic the chemistry of a human brain. The NN is comprised of a certain number of layers of artificial neurons. The typical structure of an artificial neuron is essentially a non-linear function between a series of input $x_0, x_1, ..., x_m$ and output y through a weighted sum by a series of corresponding weight $w_0, w_1, ..., w_m$ with extra bias b and a non-linear activation function ϕ.

$$y = \phi(\sum_{i=1}^{m} x_i w_i + b) \tag{2.25}$$

With one or several layers of parallelly positioned artificial neurons, it is possible to construct a neural network. With a properly trained weight matrix and carefully selected activation function, such a network is capable of producing rather accurate results from linear or even non-linear processes, thus approximating almost any functions(Given that the network can grow indefinitely large). In addition, it is possible to design an architecture of NN in order to take into account extra dimensions of information. For example, by taking into consideration the time-varying nature of a time series, the NN can better understand the context of the problem, thus, produce more relevant results. The characteristics mentioned above made the NN a perfect candidate for time-series classification tasks. For classification purposes, the Convoluted Neural Network (CNN) and Recurrent neural network (RNN) are the two most commonly proposed methods as demonstrated in the following section.

2.5.3 Related literature

As mentioned in Section 2.1, there is a dominant trend of applying ML algorithms in the domain of network intrusion detection. In [Ash+20], the authors provide an informative survey of the recent research on Deep Learning (DL) based IDS. Although the scope of this article is focused on IDS for Internet of Things (IoT) systems, the authors provide an exhaustive introduction to the wireless network topology, the protocols, the relevant threats, the IDS methodologies, and the DL/ML schemes applied in this scope. In addition, the authors also provide an empirical taxonomy of several commonly used DL techniques, illustrating their pros and cons. This article grants a quick look into how IDS has been developed in recent years, which is immensely helpful for a conceptual study and preliminary design of IDS strategies.

The original algorithm of SVM has first been introduced by Vladimir N. Vapnik and Alexey Ya. Chervonenkis in the 1960s, and later published in the book *The nature of statistical learning theory* [Vap00]. The more detailed history is introduced in [Che13]. Additionally, [RDY03]; [MS03]; [CAT05]; [Fy06] are the earlier research related to the direct implementation of the SVM algorithm for network IDS purposes. The articles have shown first attempts at implementing an SVM-based IDS for several types of intrusions such as DoS and probing. The earlier research generally returns excellent results with the existing dataset due to the limitations in computational resources as well as the lack of diversity of network traffic.

More recently in [YL11], the authors proposed an updated SVM scheme based on transductive SVM and a simulated annealing algorithm. This updated IDS design is then tested against a more recent database, resulting in more realistic detection performance.

Also in [ZMZ07]; [XZY09]; [Li+12]; [Zha+19], there are some more recent advancements in the research of SVM-based network IDS. It is clear to see that this method is under continuous development with numerous proposals each year. Despite all the advancements in the domain of ML with all the newer and more powerful ML tools, SVM is still one of the most relevant tools for classification tasks.

The [DZA03] is a more relevant article that proposed to use an SVM algorithm to counter the intrusion attacks on the wireless ad-hoc routing protocol. The proposed IDS scheme has been tested

in a simulated environment against two common DoS attack types that show high detection accuracy in both cases.

The implementation of WLM with SVM is undoubtedly not a new concept. In fact, in[Leo+15], the original author of the WLM toolbox has proposed a Fetal Heart Rate (FHR) anomaly detection system by incorporating the state-of-the-art wavelet p-leader based multifractal analysis and the SVM. Indeed, due to its simplicity, robustness, and better interpretability compared to other types of ML schemes, beyond applications around network security, the SVM anomaly detection scheme is more often used in the domain of medical electrocardiogram (ECG) analysis and image processing.

In [Ven+18], the authors demonstrated the advantageous performance between SVM and ANN. In the case of ECG, the SVM scheme performs exceptionally well.

In [Sal+14], the authors proposed an anomaly detection scheme for the wireless health care sensor data that can robustly identify the sensor anomalies. The proposed scheme is then tested against real-world patient data, along with several other detection schemes. The result shows the superior performance of the SVM-based detection scheme in detecting anomalies from a sensor network data.

The wide adaptation of SVM in the field of medical applications is a strong indication of the maturity of the SVM method, and it has become the go-to option for many security and fatality concerning applications.

Similarly, the artificial neural network branch of ML also had a long history of development, with the early conceptual development dating back to the 1940s. The theory is then summarized in the book *Perceptrons: An Introduction to Computational Geometry* [Min88]. Over the years, several network models have been proposed for classification problems, including Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN), or more specifically, the Long-Short Term Memory (LSTM) and Gated Recurrent Units (GRU).

In [ADE20], the authors have provided a thorough study on the state of the art of deep learning-based IDS methodologies. From the authors' observation, it is apparent that the RNN is showing a dominating trend in the domain of classification, overshadowing the CNN and the Auto-Encoder methods. It is evident that maintaining a memory of the past plays a significant role in the performance improvement of the RNN based IDS schemes.

In addition, a number of recent research are found in the literature about the application of LSTM and GRU for wireless IDS with various degrees of success, as explored in [Che+18]; [Xu+18]; [Fen+19]; [Xia+19]; [Gwo+19]; [KS20].

[Xia+19] in particular, proposed an LSTM-RNN based IDS scheme dedicated to intrusion detection within a UAV network, which helps detect abnormal behaviors such as GPS spoofing. The LSTM based scheme not only outperforms the tested SVM and Multi-Layer Perceptrons (MLP) method in terms of detection accuracy but also require fewer computational resources, which provide more evidence on the performance advantages of RNN, compared to shallow learning methods like the SVM and the MLP w.r.t the IDS problems.

Similarly, there have been proposals to apply ML with MF analysis in network traffic identification. Shi et al. propose an interesting approach for network traffic classification in [SLW14]. The authors employ the traditional wavelet coefficients-based multifractal energy spectrum teamed with a combined neural network based on an MLP neural network. They are able to confirm an accurate classification of three networking application classes (Http, Streaming, P2P) with the proposed method. The proposed method is structurally similar to the approach introduced in Chapter 4 but with a different motivation.

2.5.4 Discussion

Although SVM and other ANNs are showing great potential in the domain of IDS, both have their own pros and cons. For SVM, due to its simplicity in nature, it is relatively less performant when facing complex random systems. Indeed, the performance of SVM depends on the position of the hyperplane. For a random system, it is very difficult to balance between a loose positioning at the cost of lower accuracy or a very strict positioning at the risk of over-fitting. In addition, the lack of consideration of the context (i.e., taking information from adjacent time frames) further limits the performance of an ordinary SVM-based IDS. For ANN, the biggest drawback lies within its lack of interpretability. Especially when the network becomes more complex and involves more layers, or the interaction between neurons becomes more complicated in the case of RNN or LSTM. In the domain of network security and civil aviation, high-reliability requirements are mandatory. An NN-based IDS, although being more relevant in the state-of-the-art literature, is still under discussion in the network

community.

The problems faced by the ML schemes mentioned above form a strong incentive to develop an IDS methodology taking advantage of both the world of stochastic random process modeling with fractal and multifractal analysis and the world of machine learning. One can expect that by combining with the WLM analysis:

- The context-insensitive issue of the SVM can be largely improved because the information of the time-dimension has already been embedded in to the MF spectrum.
- The use of SVM with a more complex kernel function to resolve stochastic problems is now alleviated. A standard SVM is fully capable of classifying MF signatures from networks at different states of traffic.
- The mysterious weighting inside a NN now becomes more reasonable because the MF spectrum provides a much more explainable representation of the network traffic. The NN is currently processing a more deterministic signature compared to an utterly stochastic process.
- In addition, the complexity of the ML scheme can be significantly reduced thanks to the massive compression ratio from the raw signal to the MF signature, resulting in a much faster training process and more accessible maintenance procedures. A much smaller NN can also contribute to the easier implementation of the IDS into a resource-limited environment, such as a UAS.

CHAPTER 3

DoS detection: A preliminary design based on robust observer and wavelet-leader multifractal analysis

Contents

3.1 Introduction 45

3.2 Methodology 46

3.2.1 Step 1: spectral analysis-based traffic signature with WLM method 46

3.2.2 Step 2: controller / observer-based robust estimation 48

3.3 System validation 50

3.3.1 UAV ad hoc network hybrid platform 50

3.3.2 Traffic characterization results for intrusion detection system calibration 51

3.3.3 WLM signature comparison results 55

3.3.4 Anomaly detection and reconstruction results 57

3.3.5 Discussion on traffic reconstruction performances 59

3.4 Implementation 61

3.4.1 Real test environment: Paparazzi software 61

3.4.2 IDS method implementation into Paparazzi 62

3.4.3 Flooding attack generation 63

3.4.4 Real traffic based flooding attack analysis 64

3.4.5 Real-time Implementation and Testings with Paparazzi UAV Emulation 65

Author's Contributions

Publications

R. Zhang, J.-P. Condomines, N. Larrieu, and R. Chemali, "Design of a novel network intrusion detection system for drone communications," in 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), 2018, pp. 1–10.

J.-P. Condomines, R. Zhang, and N. Larrieu, "Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation," Ad Hoc Networks, vol. 90, p. 101759, 2019.

Synopsis

In this chapter, I introduce the proposed IDS methodology with the application of Robust Observer and WLM analysis, with the additional validation step with the curve matching algorithm.

Here I try to address one of the networks mentioned above security issues of UAV networks by proposing a new IDS, a hybrid method based on both spectral traffic analysis and a robust controller / observer for anomaly estimation inside UAV networks. The proposed hybrid method considers, as a preliminary step, a statistical signature of the traffic exchanged in the network. By examining the resulted signatures, the differences are used to select the accurate model for accurate estimation of the abnormal traffic. The proposed IDS design has been successfully applied to some relevant practical problems such as UAANET. The effectiveness is illustrated by using real traffic traces, including Denial of Service (DoS) attacks. The first results show promising perspectives. Finally, both simulation-based validation and real-time real-world-based implementation of the proposed IDS are presented in this chapter.

3.1 Introduction

During the past years, Unmanned Aerial Vehicles (UAVs) have been attracting more and more attention. The use of UAVs has many apparent advantages over conventional manned aircraft especially in terms of operational expense, operator's safety, operability in difficult/hazardous environments, and accessibility for civil applications. Recent technical advancements have made it easier than ever to set up an Unmanned Aerial System with complex topology to achieve sophisticated missions, which were previously impossible without actual human involvement. The rapid advancements and heavy involvement of Information Technology (IT) have huge impacts on the path which drone communities take to develop future UAS's.

However, network anomalies and security-related problems (such as Distributed Denial of Service (DDoS) attacks) are important issues for the detection of active security threats. A variety of tools for anomaly detection are principally based on data packet signature. This behavior is known to be very effective for dealing with well-known DDoS attacks. However, this mechanism is inefficient when a new type of attack is performed. For this reason, It is outlined in this chapter a new type of IDS able to detect different types of DDoS.

The proposed intrusion detection model in this chapter is a two-step mechanism. First, it characterizes the traffic using a statistical signature, and then, it selects a precise estimator model to reconstruct the attack traffic. All types of attacks that do not follow the initial characteristics trigger an alarm, and, consequently, the malicious traffic can be analyzed in depth. This approach has the major advantage that it is not associated with a specific type of attack. Any attacks which do not follow the initial model can be detected, analyzed, and managed. Therefore, the security and performance of the entire network can be improved. This traffic characterization is performed thanks to a statistical signature of the traffic exchanged in the network. Note that statistical signatures based on wavelet analysis have been selected because they offer a wide spectral characterization of the entire traffic process. Each signature provides us with a unique identification of the current traffic. By looking up this signature in a bank of signatures, it is possible to characterize and make the model of the anomaly in the UAV network. Subsequently, the attack will be analyzed and correctly represented using a robust control estimation to reconstruct the attack traffic. To the author's knowledge, this is the first time that both spectral analysis and robust control estimation have been coupled and used on a UAV ad hoc network

traffic.

The main contribution of this chapter is to propose a new hybrid method that is able to detect traffic anomalies (i.e., DDoS). Tests with real network conditions have been performed to evaluate the characteristics of this method and to explore the possibilities of the future integration. The preliminary design of the new IDS process and its theoretical assessment have been faced with real traffic traces. These traces have been generated using a hybrid UAV network simulator. Subsequently, the validation of the new IDS system is improved by testing its performances faced with real DDoS attacks, actual UAV trajectories, real UAV background traffic, and real UAV fleet topology in real-time. Finally, different types of anomalies have been considered, and they are all accurately detected by the intrusion detection process proposed in this chapter.

In the sequel, Section 3.2 introduces the principles of the IDS methodology, which combines spectral analysis and traffic reconstruction. Section 3.3 gathers all the results obtained after solving the time-delay linear estimation problem in real conditions. Finally, Section 3.4 describes the details about the proposed hybrid IDS implementation in real-time real-world environments and introduces different test methods that have been examined and results obtained.

3.2 Methodology

The methodology introduced in this chapter is a two-step process (see Figure 3.1 for details). The first step is dedicated to traffic characterization. Its objective is to calculate a specific signature of the traffic we want to analyze. It is shown in Section 3.3 that it is able to obtain completely different attack signatures thanks to the Wavelet Leader Multi-fractal analysis. These different signatures are used to automatically select the different controller / observer models used in the second step of the intrusion detection process.

3.2.1 Step 1: spectral analysis-based traffic signature with WLM method

The WLM analysis is used to quantify the variability of any time series (in this chapter, I focus on network traffic). It analyzes the multifractality of a signal by computing not only the wavelet

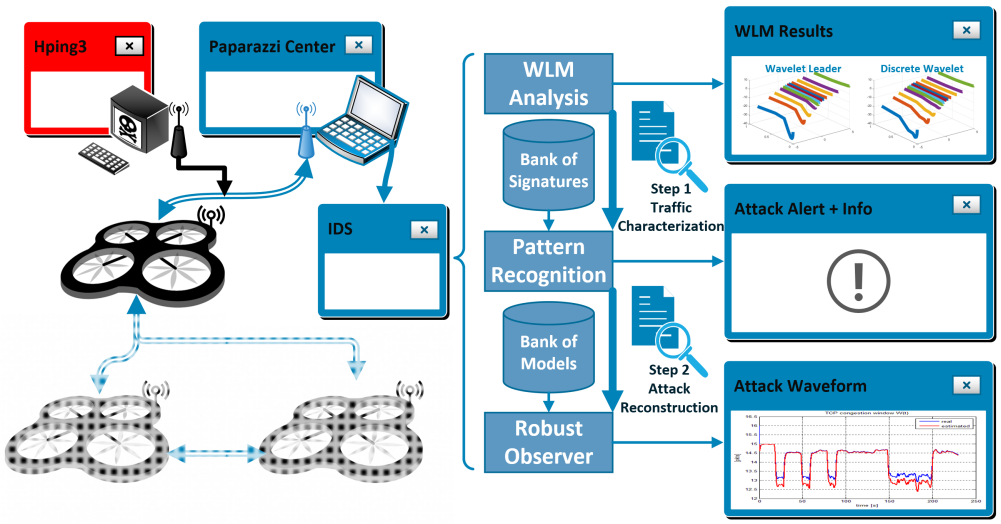


Figure 3.1: A general two-step framework of the proposed IDS system

coefficients of power-law at the 2nd order but also other arbitrary orders. This toolbox is well defined and proven by various applications[WAJ07]; [Ihl13]; [LCD04]. This process produces a graphical result (called a spectral signature), which is used to find the differences between legitimate traffic and traffic which contain an anomaly. To best capture the complexity of the traffic, the different statistic moments of analysis are also considered. The result is a set of 3-dimensional curves that represent the dynamic of the traffic at different moments and time scales.

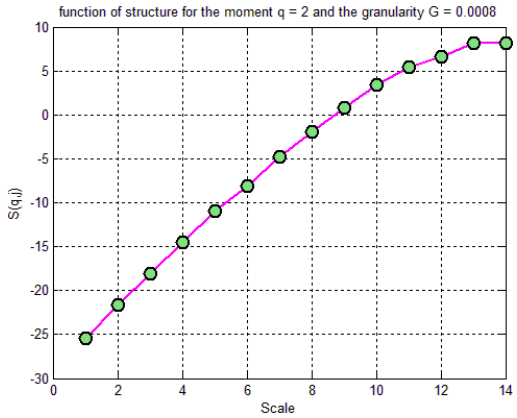


Figure 3.2: An example of WLM signature of a data series at statistic moment $q = 2$

There is an initial theoretical assumption to verify each time we use the WLM method on any specific time series. Indeed, any data series need to verify scale invariance in order to justify the self-similarity feature. This feature is also observed in the analyzed data when a power law is observed

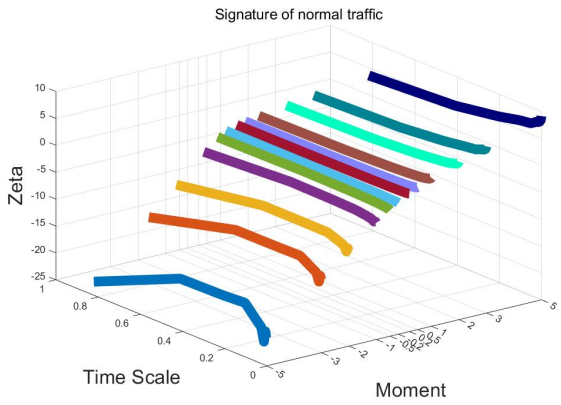


Figure 3.3: Examples of WLM signature at multiple statistical moments

when the static signature is plotted (by a log-log diagram) for specific time scales of this data. I show in Figure 3.2 an example of the power-law that can be observed for one of the network traffic series analyzed. Section 3.3 will present in detail the different attacks I have investigated and the different signatures I obtained for each one. Based on the WLM toolbox, we can quantify the variability of any time series according to two complementary parameters: the time scale and the moment of analysis. *Time scale* allows us to see any repetition in the process over time. *Moment of analysis* will enable us to analyze traffic data in different spectral representations. This second metric quantifies the variation of the traffic according to, for instance, $q = 1$ (average), $q = 2$ (variance), and so on. An example of a spectral signature for regular traffic (i.e., not containing any attacks) is shown in Figure 3.3. This figure represents the spectral characteristics of the data (i.e., the *zeta* parameter) according to the time scale of analysis and the moment of observation. I will illustrate in Section 3.3 how this signature can be different according to the types of attack that we wish to analyze and detect.

These differences are useful for traffic characterization but can also be very helpful in selecting a dedicated robust estimation model. This is the topic of the next subsection, where I will describe the observer modeling, which has been performed based on a controller / observer robust estimation.

3.2.2 Step 2: controller / observer-based robust estimation

In order to improve the future design of network IDS devices against the unknown type of attacks, we need to reconstruct the exact properties of the attack. This process is performed by using Step 1's signatures to select a model in Step 2, and tune the controller / observer. When representing

the dynamics of an observed / controlled system such as the TCP dynamics of an ad hoc network mathematically, we often use the concept of state. By definition, the state of a dynamic system is the set of parameters whose values must be known at a given moment in time, in order to predict the future evolution of the system. This idea is very natural for systems whose evolution over time can be described by differential equations. The solution of a system that is represented by differential equations of order $n \in \mathcal{N}^*$ depends on a set of n initial conditions. These initial values determine the subsequent states taken by the system over time. Thus, modeling dynamic systems by means of state representations, whether linear or non-linear, tends to be more fruitful than other types of model (such as input / output black boxes) since it gives us access to a direct formulation of the underlying physics of the process. Therefore, the role of a controller / observer is to produce an accurate estimate $\underline{\hat{x}}$ of non-measured states $\underline{x}$ (states that cannot be accessed directly by performing measurements) given knowledge of the inputs and an array of imperfect measurements. Various implementations of TCP models in terms of assumptions and numerical techniques[LPD02]; [Sri04]; [Tar05] exist. TCP network is commonly represented using a linearized fluid-flow model[LPD02] associated with this network topology. In this chapter, the topology consists of $\mathcal{N}$ TCP sources, with the same propagation delay connected to a destination node through a router (see Figure 3.4).

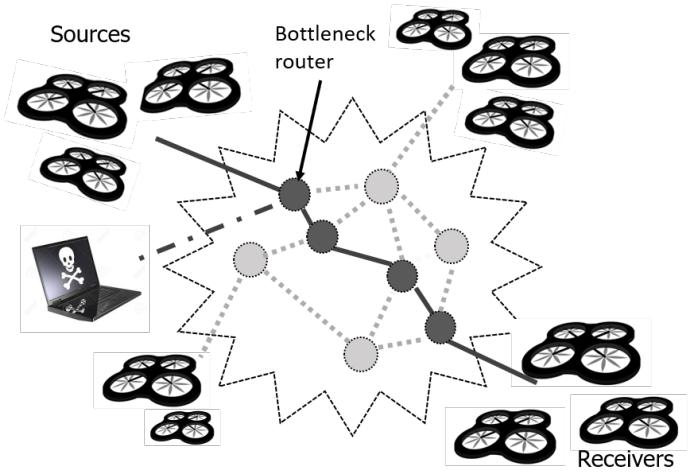


Figure 3.4: Sources / receivers connection in a fleet of UAVs

This simple topology is due to :

1. The high complexity behavior of a fleet of UAVs in which each UAV can be sender, receiver, and router;

2. The difficulty for such systems to derive a reliable and representative network modeling from scratch.

To implement an IDS according to the network topology presented previously, the estimation module inserts itself between the other modules as follows: the estimation system receives noisy measurements (e.g., probability of packet, the queue of the router buffer) as inputs from the sensors, then merges this data using the TCP model of the network to compute a solution to the estimation problem, as shown in Figure 2.1.

3.3 System validation

3.3.1 UAV ad hoc network hybrid platform

In order to validate the new traffic estimator in real traffic conditions, I use a hybrid experimental system to take advantage of the low cost of a simulation while still obtaining the accuracy of a real protocol stack. Our laboratory has been using virtual machine implementations to deal with the entire complexity of the Linux operating system. The traces used to generate UAV mobility patterns were extracted from real traces so that physically related factors could be implemented as realistically as possible. The system we have been using to evaluate protocols is divided into several parts. It includes a set of tools that can deal with several scenarios: a hypervisor to run the virtual machines, measurement tools, and a framework to allow virtual machines to communicate through a virtual wireless medium. We chose to use Virtual Box as a visualization tool because it is an easy-to-use and efficient hypervisor. The virtualized system is a 12.04 version Ubuntu, working with the 2.6.38 version of the Linux kernel. Our testbed architecture uses a Virtualmesh framework. It is a framework that interfaces a Linux-based system with an OMNeT++ simulation. OMNeT++ is a powerful network simulator that simulates several systems and normalized protocols. An illustration of this system is shown in Figure 3.5. In [MRL15], more details about this hybrid tool can be found.

The main advantage of using such a hybrid simulator is to extract any characteristics from the simulation and to inject them into the Simulink design directly. The theoretical model is then used under real traffic conditions and not only theoretical stimulus. The advantage of such an evaluation

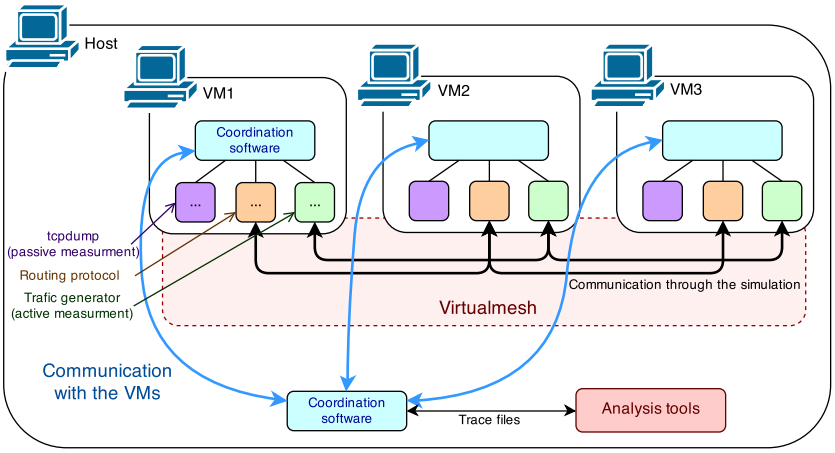


Figure 3.5: Test bench implementation

is to take into account the huge variability and complexity of real traffic. Consequently, I have been able to generate DDoS between the different virtual machines by taking into account the exact UAV environment of the drone mission that has been considered in this research. First, I captured the network traffic generated (both regular and DDoS traffic) and then injected this traffic into the Simulink design.

3.3.2 Traffic characterization results for intrusion detection system calibration

The objective of this analysis is to create a bank of signatures, in order to extract a specific pattern for each type of intrusion and to analyze the differences between normal traffic without anomaly, and traffic with the anomaly. In order to obtain traffic signature in three dimensions (3D), it is measured the scaling function (Zeta) with respect to the statistic moments (q), which can take positive or negative values, and also with respect to the time scale of the traffic. I now illustrate the results obtained by the wavelet multifractal analysis (WLM) method on the basis of the hybrid UAV network simulator. The normal TCP traffic is generated by 5 TCP sources generating long-life TCP flows to a receiver through a router with a link capacity $C = 1,250$ packets/s (equivalent to 3 Mbit/s), and $T_p = 30ms$ the propagation delay.

The traffic is analyzed against different DDoS (Distributed Denial of Service) attacks. Two types of DDoS attacks are considered: a Constant Flash-Crowd (CFC) and a Progressive Flash-Crowd (PFC)

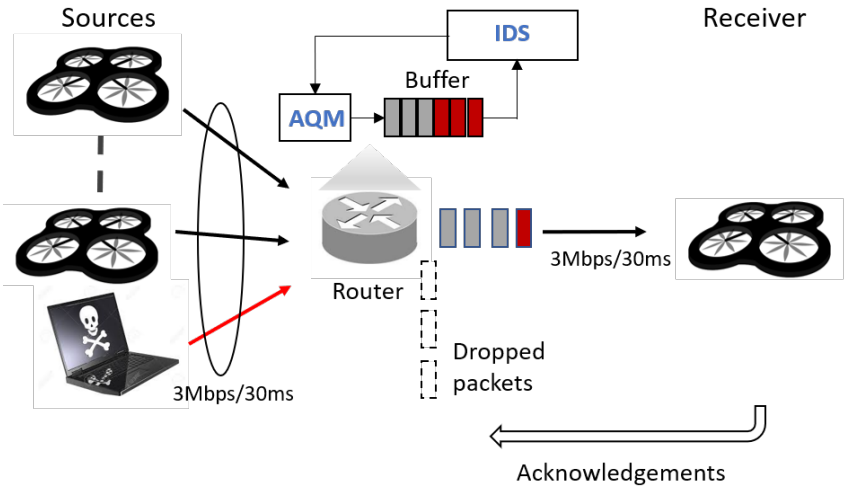


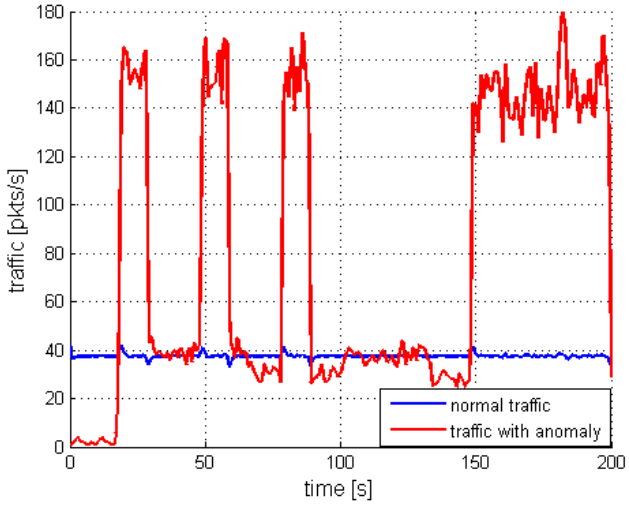
Figure 3.6: Considered topology

attack. These anomalies have been generated using the HPing3[1] tool. This software runs on the hacker node (see Figure 3.6 for details about the network topology) and can run different types of attacks but mainly flooding attacks. Indeed, in this scenario, HPing3 exchanges thousands of small TCP flows in order to generate a synchronized flooding attack on the receiver node. The resulting malicious traffic is much more significant than the regular traffic. Figure 3.7a shows the features of the traffic which has been generated through the hybrid network simulation tool. This traffic includes four different CFCs of the same magnitude but with different duration and, consequently, different impacts for the UAV network.

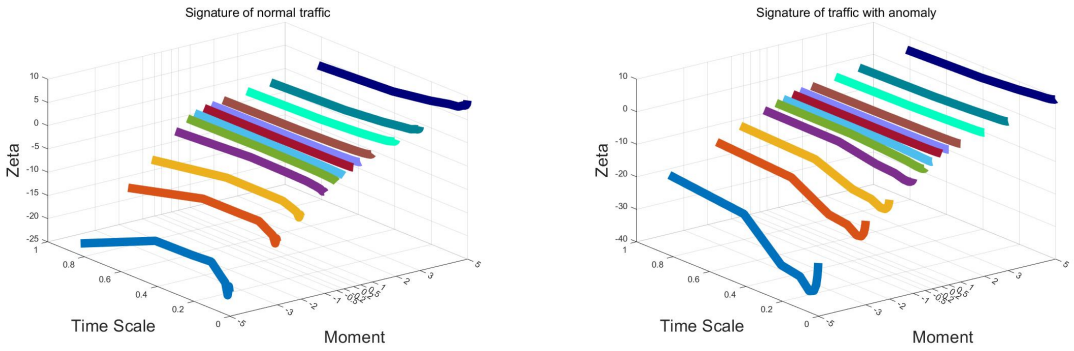
3.3.2.1 Attack signature for traffic with Constant Flash-Crowd CFC

In this time, the network is exposed to CFC attacks (see Figure 3.7a for details). The objective is to obtain a dedicated spectral analysis for this specific type of DDoS attack. In Figures 3.7b and 3.7c, a comparison of the signatures of the regular traffic and traffic including CFC attacks is presented. The obtained results show a sizable difference in the scaling function $\zeta(q)$ (zeta), especially in the case of negative moments, for traffic including attacks. It is observed that the scaling function (for the negative moment $q = -5$) reaches values $\zeta(q) \leq -33$ for traffic including DDoS attacks while it does not exceed the value of $\zeta(q) \leq -23$ for normal traffic.

[1] http://www.hping.org/hping3.html



(a)

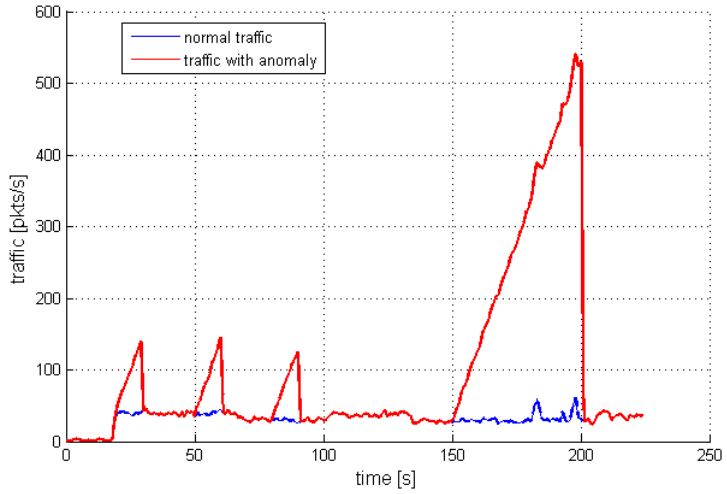


(b) (c)

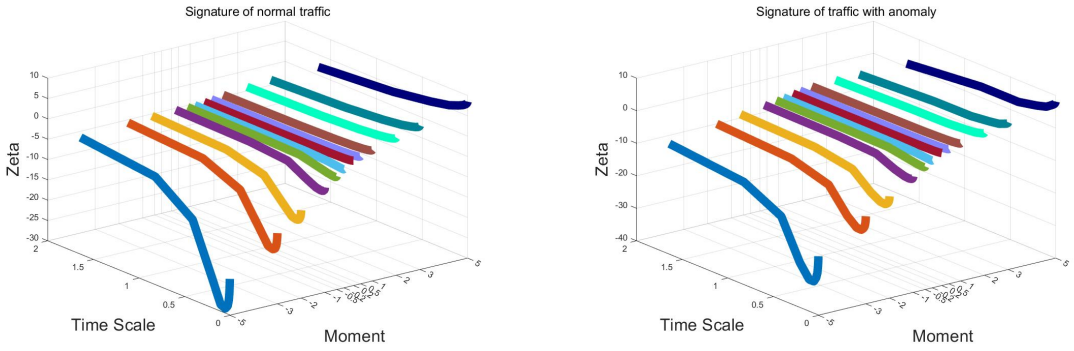
Figure 3.7: Waveform(a) and signature comparison(b,c) between normal and CFC flooded traffics

3.3.2.2 Attack signature for traffic with Progressive Flash-Crowd PFC

In a second time, the network is exposed to PFC attacks (see Figure 3.8a for details). The comparison between traffic with and without attack shows that the variation of the scaling function $\zeta(q)$ is always noteworthy in negative statistic moments (here $q = -5$). Indeed, as shown in Figure 3.8b the values of the scale function are ranged between $-30 \leq \zeta(q) \leq 0$ for regular traffic. On the contrary, in the case of traffic including PFC attack, the values $\zeta(q)$ are ranged between$-31 \leq \zeta(q) \leq -5$ (see Figure 3.8c for details).



(a)



(b) (c)

Figure 3.8: (a) Waveform and (b,c) signature comparison between normal and PFC flooded traffics

3.3.2.3 Discussion on traffic signature characterization

These characterization results show that it is possible to extract unique signatures for traffic with and without anomalies. Moreover, the spectral analysis provides different signatures for each type of DDoS. As it has been observed, the scaling functions are not the same for CFC and PFC. Consequently, one can build a classifier and a selector according to each specific spectral signature which will be able to select automatically a specific controller / observer for the IDS tool. In the rest of this chapter, I am going to present additional results related to the second step of this process: anomaly reconstruction and detection using robust controller / observer.

3.3.3 WLM signature comparison results

In this case, by having multiple signature curves at different moments of analysis, I simply connect the curves end-to-end and consider them as one three-dimensional curve and perform the similarity score calculation. This method has been tested and validated with signatures acquired from our UAV ad hoc network hybrid platform generating communications from one drone to one host PC acting as GCS. This experimental scenario was a two-step process. In the first step, I generated only regular drone-to-GCS traffic, and in the second step, I generated regular drone-to-GCS traffic plus CFC flooding attack to GCS.

Some samples of the resulted signatures are taken from Subsection 3.3.2 during the test and plot them all together as shown in Figure 3.9 and 3.10. As noticed previously, it can be observed that the signatures are visually very different when the GCS is attacked by CFC flooding attacks. With this specific CFC flooding attack only the GCS, the shape of the signature is also modified compared to the original CFC flooding attack (see Figure 3.8c for details). As shown in Figure 3.11, the curve similarity score has clearly distinguished the differences in the signatures when each of the six attacks happened during the test.

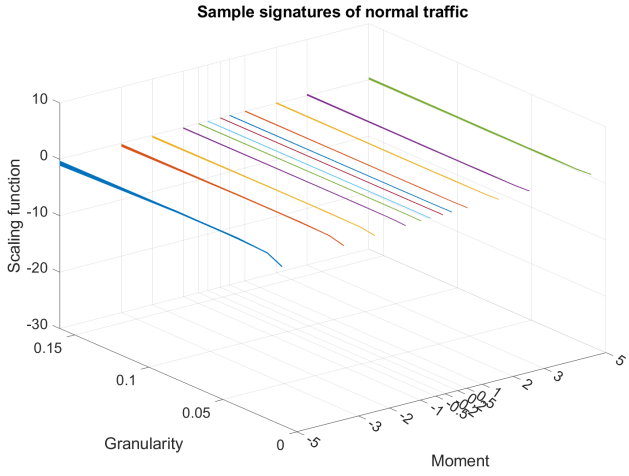


Figure 3.9: Scaling function for regular traffic

Although it can be observed in Figure 3.11, that during the 3rd, 4th, and 5th attacks, the similarity score experienced two peaks and form a valley shape waveform during the attack as if there are two attacks. This is caused by prolonged attacks, which saturated the reception buffer of this experimental

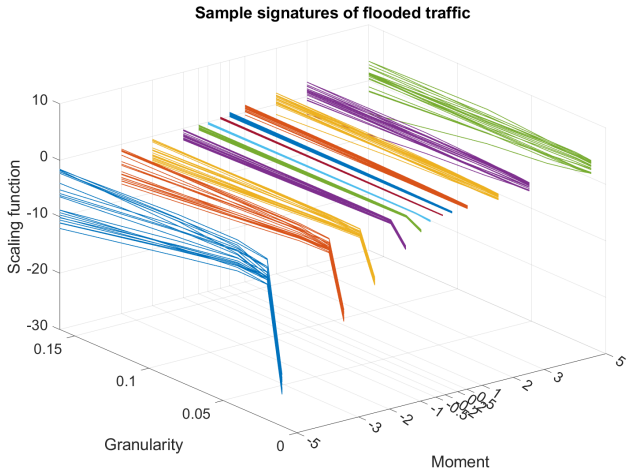


Figure 3.10: Scaling function for traffic with CFC anomaly

IDS design. In this case, because the buffer is saturated, the IDS does not see any difference in the incoming traffic and therefore results in a signature that resembles normal traffic with only small variations that are not significant in terms of similarity score analysis. The performance is shown by the curve matching algorithm also helps the optimization of the WLM parameters. Indeed, the scale-invariance properties of the network traffic are not shown on the infinite spectrum of scales. Instead, at certain scales, it is much easier to observe the changes in multifractal properties induced by network anomalies, and the curve matching algorithm here helps the search of the optimum parameters.

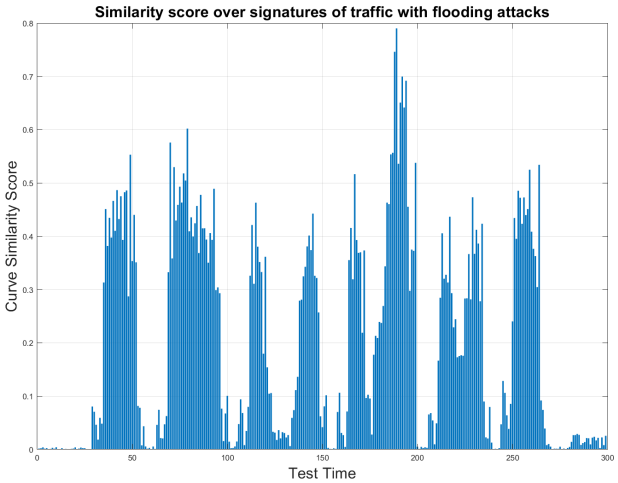


Figure 3.11: Similarity score over signatures of the UAV to GCS traffic with 6 CFC attacks (attack No.3 4 5 saturate the reception buffer)

Therefore it has successfully demonstrated that how the first step of the newly purposed IDS can distinguish network traffic with and without CFC flooding, and how the variation of some parameters such as the test duration, which translates into the size of reception buffer, will influence the performance of this implementation. With an addition of an analytical method such as the curve similarity score method mentioned in this section, it is possible to achieve an automatic detection of anomalies. But the curve similarity score method has worked exceptionally well in the test case, which has led us to think it is actually possible to implement a similar mechanism in the IDS. Because an actual pattern recognition algorithm is expensive in terms of computation power, it is less efficient to perform such calculations on all signatures that are obtained in a drone network. Consequently, a simple and algorithmic efficient curve matching method can be implemented on individual nodes in a distributed drone network, and it can act as an alarm and a trigger to the command center/ground station to notify the operators about the anomalies. Then, the decisions can be made to investigate further the anomalies with more powerful tools such as pattern recognition and anomaly reconstruction.

In the next section, I am going to present additional results related to the second step of this process: anomaly reconstruction and detection using robust controller / observer.

3.3.4 Anomaly detection and reconstruction results

I now illustrate the performances reached by the developed controller / observer on the basis of our hybrid UAV network simulator. To conduct such a task, I define in Table 3.1 the values of the congestion window size and the router queue length at the equilibrium point of the system: W_0 and q_0. They have been selected by considering the mean value for N sessions around which $W(t)$, and $q(t)$ oscillate respectively. The proposed observer has been tested with the state feedback AQM in [Ari+12], and observer gains are $L = [1.2338538, 5.2445906, 2.24 * e + 3, 1.94 * e + 2]$. This observer is synthesized to construct the state of CFC and PFC attacks.

W_0	15 packets
q_0	37.5 packets/s
p_0	0.0089
R_0	0.06 s

Table 3.1: Equilibrium point

3.3.4.1 Attack reconstruction for traffic with constant flash-crowd (CFC)

Figures 3.12, 3.13, and 3.14 illustrate a typical realization of traffic estimation including CFC attack which can be detected by the time-delay linear observer. This CFC attack generated by our hybrid UAV network simulator has been injected into Simulink to compare the IDS model to the real traffic traces. This is depicted in Figure 3.14 where regular traffic is around 30 pkt/s. Where, for the malicious traffic, the throughput is increased to 150 pkt/s. Moreover, the real traffic (blue) and estimated intrusion (red) are plotted on the same figure for comparison purposes. Figure 3.13 shows the time response of the estimated queue $q(t)$ calculated by the time-delay linear observer method. As expected, the queue is stabilized above the desired level and the intrusion does not affect the different steady states of the system. Figure 3.12 shows the time response of the TCP congestion windows $W(t)$. As expected, the TCP congestion window evolution is reconstructed with great accuracy.

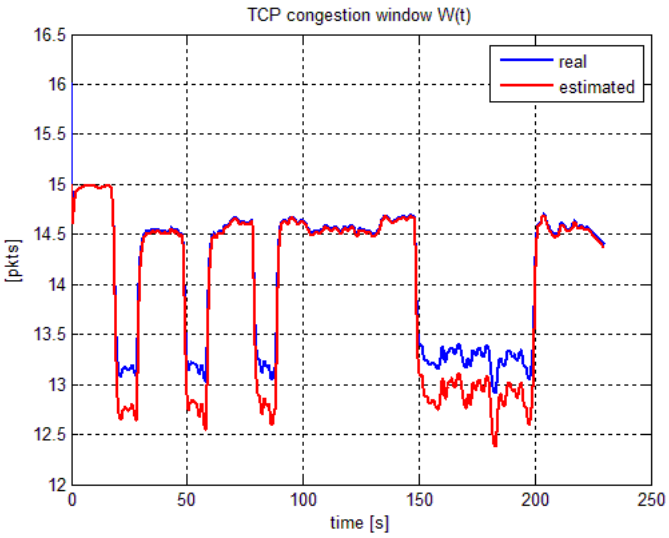


Figure 3.12: TCP congestion window W(t) - CFC attack

3.3.4.2 Attack reconstruction for traffic with progressive flash-crowd (PFC)

In this section, the PFC attack generated by our hybrid UAV network simulator is considered. As previously mentioned, these attacks have been injected into Simulink to compare the IDS model with the real traffic traces. This is depicted in Figure 3.17 where regular traffic is around 40 pkt/s; but for the malicious traffic, the throughput is increased slowly to reach values close to 140 pkt/s. It can be observed that the estimator is able to reproduce the shape of the anomaly quickly and make an

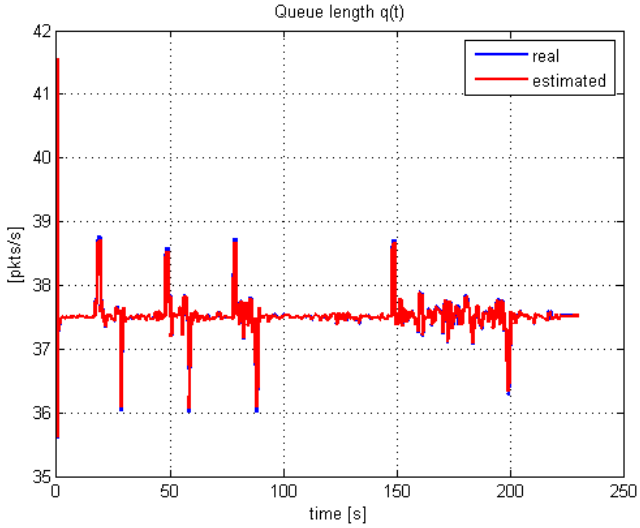


Figure 3.13: Queue length q(t) - CFC attack

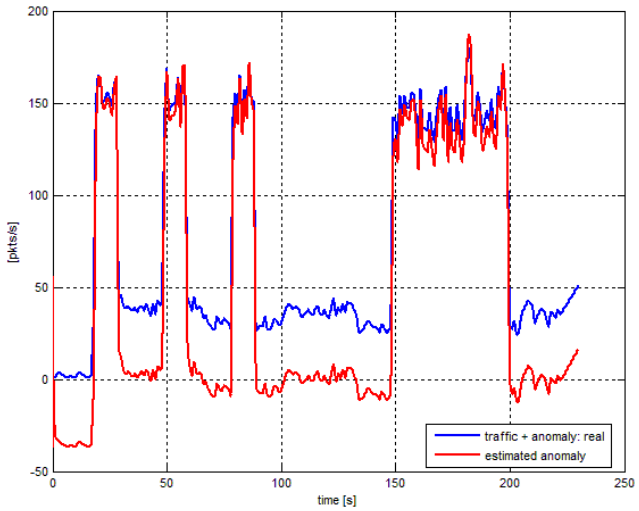


Figure 3.14: Estimation with real traffic replay - CFC attack

accurate distinction between the normal traffic and the intrusion traffic (see Figure 3.17). In addition to this, the controller / observer is able to estimate the states of the system $W(t)$ and $q(t)$ with accuracy (see Figures 3.15 and 3.16 for details).

3.3.5 Discussion on traffic reconstruction performances

These results look promising given that the estimator simulated with Matlab Simulink is able to detect the different intrusions rapidly and with an accurate threshold. The delay in the detection is negligible,

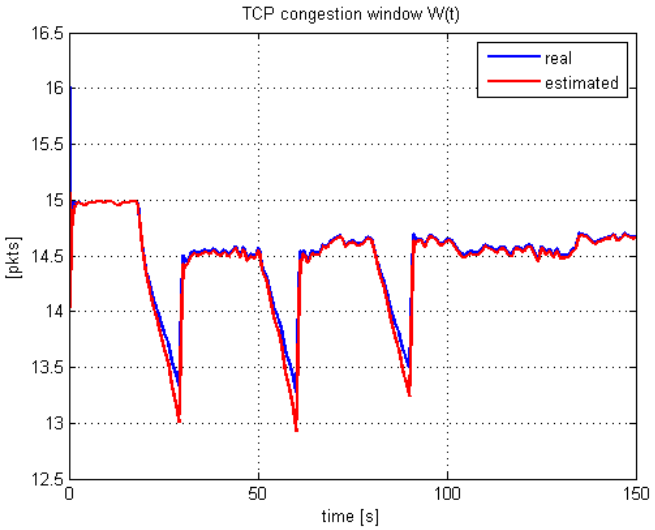


Figure 3.15: TCP congestion window W(t) - PFC attack

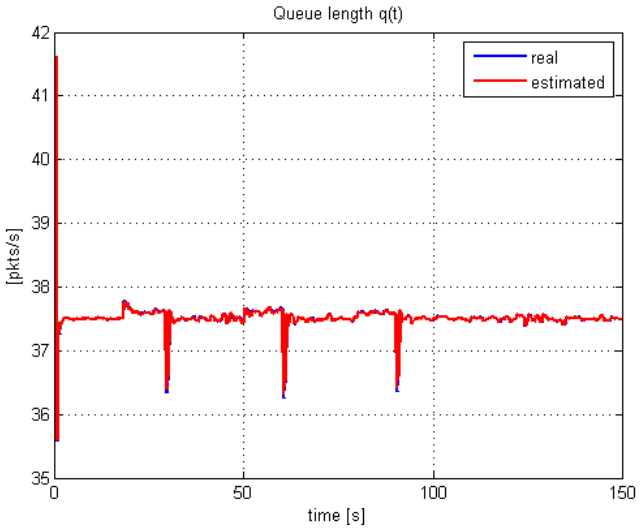


Figure 3.16: Queue length q(t) - PFC attack

and the estimator can make an accurate distinction between legitimate traffic and traffic with intrusions. Consequently, this is the first promising result for intrusion detection system design applied to the UAS network. In the next section, I will consider a more complex environment. Indeed, I will deploy the IDS in a real drone system and analyze if the first promising results I got with both the hybrid simulation / emulation platform and the Matlab Simulink estimator are confirmed.

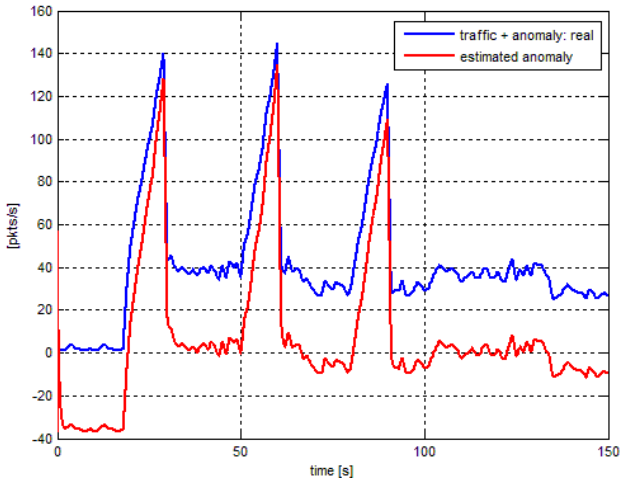


Figure 3.17: Estimation with real traffic replay - PFC attack

3.4 Implementation

In this section, it is described how to implement the proposed IDS methodology in a real environment. This real environment is built on real communications between a drone (Parrot ARDrone) and a dedicated GCS. The GCS is performed with Paparazzi software. Malicious data will be generated to stress the communications between the GCS and the drone, and it will be able to perform a real validation of the IDS methodology.

3.4.1 Real test environment: Paparazzi software

The overall Paparazzi UAS can be decomposed into three segments (Figure 3.18):

Autopilot and ground control station (a part of the ground segment) are closely bonded and usually developed and proposed by the same provider. The autopilot uses an onboard GPS receiver for navigation and returns this information to the ground station. In an autonomous flight phase, the pilot can monitor the device in real-time and intervene if a deviation from the preset mission is detected. Thus, the ground control station is dedicated to visualizations for flight preparation, monitoring, control, and engineering tasks (flight tuning, logs post-processing). The onboard and ground systems cannot be mixed. Consequently, there are two types of control systems. Moreover, the first available systems were proprietary and closed source. Today they are challenged by the open-source community that proposed opened hardware and source code solutions (cf. Paparazzi project at:

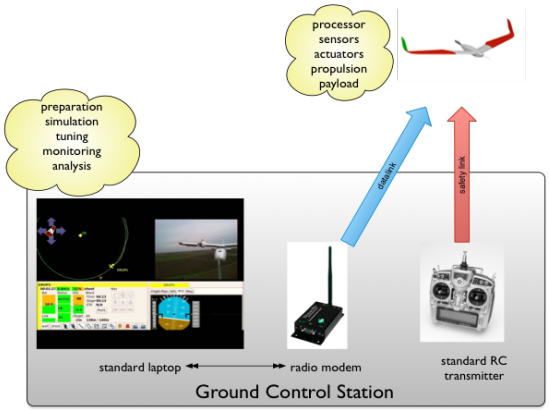


Figure 3.18: Global view of Paparazzi system

`https://wiki.paparazziuav.org/`). Open source autopilots are mainly used by universities, laboratories for research and development activities such as the IDS system proposed by ENAC. These systems are constantly improved by the community members.

3.4.2 IDS method implementation into Paparazzi

Paparazzi software is developed in a modular fashion, such that it allows easy development of individual function blocks. To be specific, the communication between GCS and test UAV node is done by a Linker module.

The IDS software is designed to first intercept / sniff packets between the Linker module and the UAV, then apply WLM analysis, in real-time, on collected packets and compare the resulted signature with a bank of signatures to determine the nature of the traffic. Then, according to the attack information, the corresponding model is chosen from a bank of models to perform a signature characterization of the attack.

The aforementioned WLM analysis Matlab toolbox has been then implemented in a C++ environment for the best performance and easiest implementation into different platforms. This first implementation of the WLM analysis tool is an independent program running in Windows/Linux environment, and it is to demonstrate the functionality and performance of this algorithm. Besides the calculation of signatures, the program also visualizes the results by calling open-source libraries:

MathGL[2] and FLTK[3] and plotting the result in a new window. This allows us to have a global perspective of how the results will differ when malicious traffic is injected into the communication before the actual acquisition of the bank of signatures.

Once we verified the steady performance of the WLM analysis module, the bank of signatures can be acquired by feeding the tool with collected packets from known normal or malicious traffics and recording the resulted signatures. To have a more general understanding of different traffics, I consider an extra degree of freedom: acquisition period, in addition to moments of analysis and time scales (sampling frequencies). This is because the duration of an attack is actually an important parameter to distinguish the type and intensity of the attack.

In the end, the IDS software module will provide us, in real-time, an animated window updating the signatures of current traffic, an alert when the signatures of current traffic are matched in the bank of signatures; some detailed information on the nature of the attack; the model to represent the attack; and the figure of the simulated attack from the observer.

3.4.3 Flooding attack generation

The main objective of the flooding attack scenario is to stress the communication network (between the GCS and the drone for instance) with malicious packets in order to saturate either the GCS or the drone and to generate a DoS into the communication. This malicious traffic will be generated thanks to Hping3 tool with the same experimental process is then described in Section 3.3. This tool helps us to forge and generate as many TCP or UDP packets as we want in the network and for whatever network destination (e.g., IP address). Moreover, an additional tool has been used to monitor the network and to analyze the traffic in real-time. This is the Wireshark sniffer packet analyser[4]. This tool helps us to observe, count, and separate packets for both malicious and normal traffic.

[2]http://mathgl.sourceforge.net
[3]http://www.fltk.org
[4]https://www.wireshark.org

3.4.4 Real traffic based flooding attack analysis

One of the communication use cases I envision conducting during the flooding attack is detailed in Figure 3.19. This research application scenario involves three agents (one UAV named ARDRONE, a GCS, and a monitor) in order to have the network topology considered in Figure 3.6. In the beginning, GCS continuously sends telemetry (attitude, flight plans, and in-door positioning) to the UAV. It is then assumed that based on HPing3, thousands of small TCP flows are exchanged, generating a flood attack on the UAV. With such a flooding process, it is possible to generate a CFC in the network. With this type of real application use case, it is possible to test and validate the software communication architecture proposed in this chapter within a real environment.

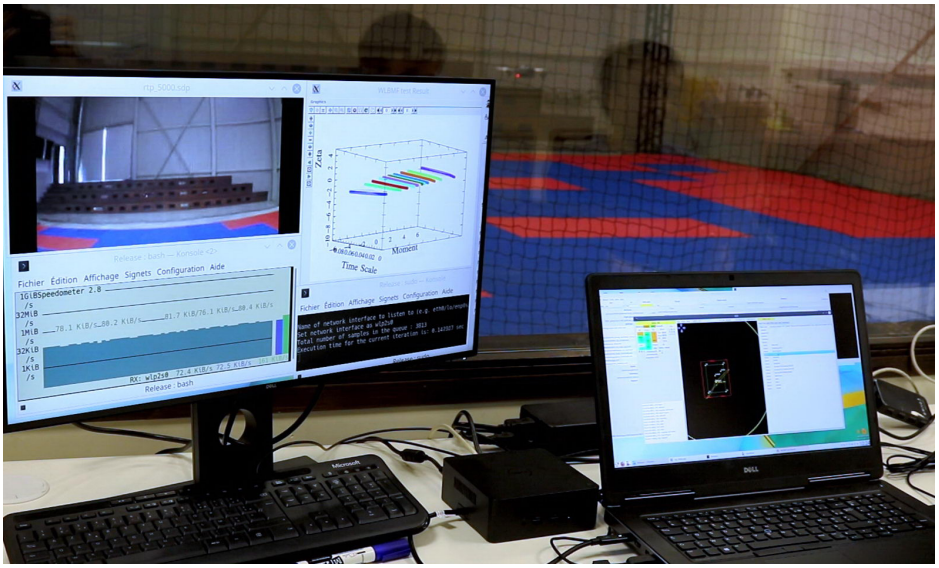


Figure 3.19: An Intrusion Detection System use case

The real-world performance testings of the WLM analysis tool have been performed on traffic collected on the aforementioned test scenario. The packet rate is extracted from Wireshark recordings split into segments, each containing 12,500 samples. Then the segmented samples are fed continuously into the WLM toolbox to simulate a real-time application scenario. The resulting signatures of the whole test period are plotted in the same figure to better demonstrate the characteristics of this analysis method.

It is shown in Figure 3.20 and 3.21, that for normal traffic the signatures are more uniform and stay in a relatively small range of zeta. Meanwhile, when the traffic is under CFC attack, the signatures

are clearly disturbed and lowered significantly especially at the negative moments.

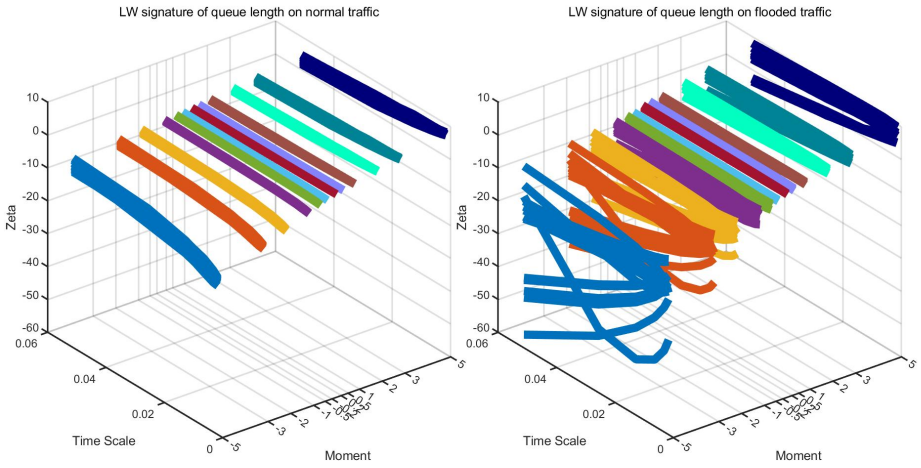


Figure 3.20: WLM Wavelet Leader analysis result on normal traffic(left) and flooded traffic(right)

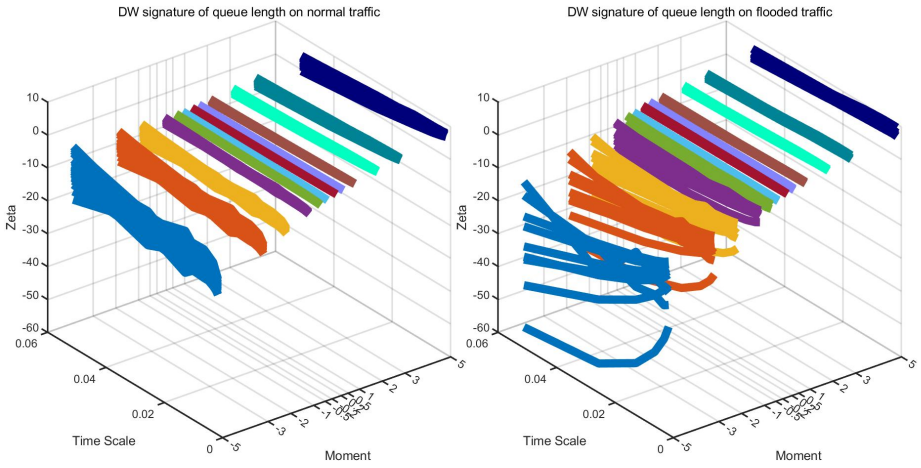


Figure 3.21: WLM Discrete Wavelet analysis result on normal traffic(left) and flooded traffic(right)

3.4.5 Real-time Implementation and Testings with Paparazzi UAV Emulation

Paparazzi software included a very convenient yet very realistic emulation setup. It allows us to test the methodology without the use of a real UAV and gives us better control over its network traffics. This specific Paparazzi module has been convenient to perform some tests in real-time of the IDS methodology. No need to generate a significant flooding attack between a real drone and the Paparazzi GCS. Consequently, the emulation only takes into account the UDP traffic between the GCS and the UAV, which contains periodic updates of the UAV's vital information. The network part of the emulation is realistic, and it is done through sockets on the localhost. The IDS demonstration program

takes advantage of this setup, and by altering the reception port of the simulated Linker module, it can achieve the interception of packets transmitted between the GCS and the simulated UAV. The sums of packets' length during a given sample period are then collected in a ring buffer and fed into the WLM toolbox in batch. This implementation performs packet forwarding upon the reception of each packet to keep the emulation in the right order.

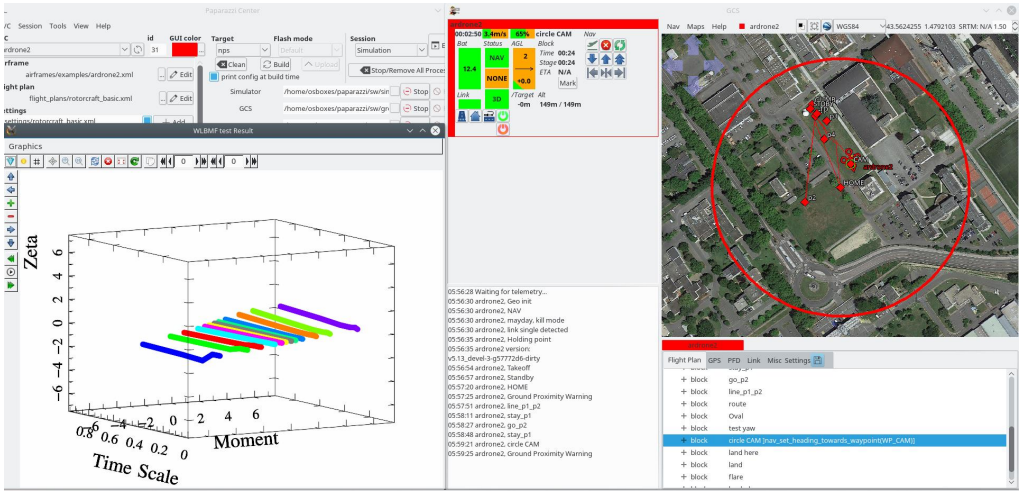


Figure 3.22: Simulated Real-time Application Scenario with Paparazzi Software

In the particular setup shown above in Figure 3.22, a sliding-window technique is applied: for a sampling window of 10 thousand samples, I extract 10 thousand previous samples upon the reception of each 1 thousand samples and perform the calculation of the signatures. Thus, for the duration of the sampling windows, there will be 10 frames of signatures. This allows us to avoid the possibility of losing resolution when the attack happens at the exact switching moment of two sampling windows. Also, this allows us to have a more continuously animated figure of the signatures and enables us to test the computation limit by increasing the window-sliding frequency.

It can be seen in Figures 3.23a, 3.23b and 3.23c, that the signatures of flooded traffic have significantly lower zeta values than the ones of normal traffic, especially at negative moments. It is also noted that the signatures vary depending on the packet data size. By default, HPing3 floods the target socket with empty packets. This will result in the most significant changes in the signatures (shown in Figure 3.23b), because this current implementation only takes into account the message size of the packets received on the socket. The malicious empty packets will not impact the calculation directly but they hinder the normal packet transmission, hence resulting in a set of very different signatures. When the socket is subject to an attack which is filled with data, the signatures (shown in Figure 3.23c)

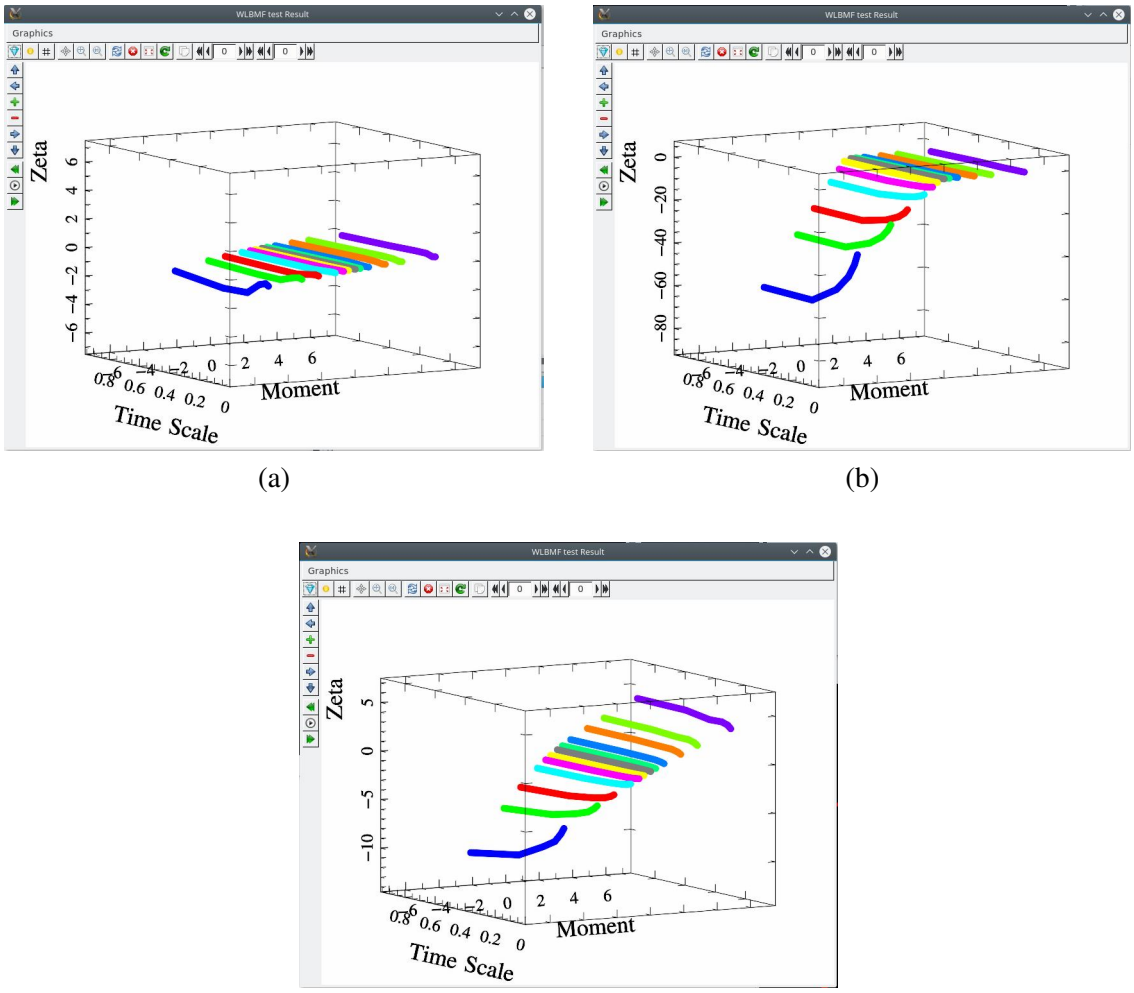


Figure 3.23: Real-time Signatures of the network at different states:
(a) Normal Traffic
(b) Traffic flooded with default packet payload data size=0
(c) Traffic flooded with packet payload data size=100

show a more inclined pattern w.r.t. moment axis compare to the signatures of a normal traffic.

The real-time testings have provided us an intuitive knowledge of how WLM analysis can help us to distinguish different types of attacks. But how to tune the tool remains to be an open question. Especially, to best preserve the Long-Range Dependence (LRD) characteristic of WLM analysis, a more extensive sampling window must be chosen. But that will cost the real-time performance of the IDS system.

CHAPTER 4

Spoofing detection: An advanced design based on WLM and enhanced by AI

Contents

4.1 Introduction 71

4.2 Methodology 72

4.2.1 IDS framework 72

4.2.2 WLM Analysis 72

4.2.3 Machine learning signature classification 73

4.3 Application to experimental data 75

4.3.1 UAS mobility simulation 75

4.3.2 Pre-treatment Euclidean distance 76

4.3.3 Test environment 77

4.3.4 Datasets 78

4.4 Results 80

4.4.1 WLM signatures 80

4.4.2 Machine learning classification 81

Author's Contributions

Patent

J.-P. Condomines, R. Zhang, N. Larrieu, and C. Moy, "Système de détection et de prévention d'intrusions pour des agents communicants," submitted 2021.

Publications

R. Zhang, J.-P. Condomines, and E. Lochin, "Multifractal Analysis and Machine Learning based Intrusion Detection System with Application in a UAS/RADAR system," MDPI Drones, accepted.

Synopsis

The rapid development of the Internet of Things, together with mobile network technology, has created a never-before-seen world of interconnection, evoking research on how to make it vaster, faster, and safer. To support the ongoing fight against the malicious misuse of networks, in this chapter I propose a novel algorithm called AMDES (unmanned Aerial system Multifractal analysis intrusion DEtection System) for spoofing attack detection. This novel algorithm is based on both Wavelet p-Leader Multifractal analysis and Machine Learning principles. In this chapter, I pay special attention to another type of network intrusions commonly observed in the UAS networks, which is the Man In The Middle attack (MITM). In this work, this promising methodology introduced in Chapter 3 has been accommodated to detect a spoofing attack within a UAS. This methodology highlights a robust approach in terms of false-positive performance in detecting intrusions in a UAS location reporting system.

4.1 Introduction

The 'information age' has provided infinite possibilities of interconnecting various devices. Nowadays, networks have extended to every corner of our lives, thanks to its accessibility and versatility. Network technologies that used to be mission-specific and platform-restricted are now becoming more open and free of charge for general, day-to-day applications. However, the rapid growth of networks also creates bubbles, especially from the Internet of Everything (IoE) perspective.

In recent years, the number and diversity of applications involving the UAS have grown rapidly. Swarms of UAVs are gaining popularity in commercial applications, such as drone light shows. Despite its magnificent and striking appearance, the related security issues are concerning. In critical situations where a cyber-attack is introduced into a wireless drone network, the physical UAS can be threatened, which can cause the whole swarm to crash. Such concern has led to an increased interest from the network community to design Anomaly Detection Systems (ADS) or IDS for this specific situation. Beyond that, with UAV certification and integration into civil airspace found in EU regulation [EU19], there is a clear need for reliable communication networks of UAV, particularly against network intrusions with potentially destructive consequences. Therefore, improved methods for accurate IDS are imperative in developing a robust and powerful Intrusion Prevention System (IPS).

As a preliminary result of this chapter, the newly designed algorithm has been successfully applied to some relevant practical problems, such as a low intensity MITM attack in RADAR traces. Results are provided to illustrate the performance and potentials of this algorithm.

To the best of the author's knowledge, the proposed method is unique in solving a MITM problem in a wireless network that exhibits mobile proprieties. The contribution differentiates itself from the methods proposed in [KS20]; [Xu+18]; [Zha+20] and others reviewed in [Ash+20]; [CBK09]; [ADE20]. This method eliminates the use of a deep neural network, which is advantageous in terms of scalability and computation overheads.

The rest of the chapter is structured as follows. The presentation in Section 4.2 of the methodology explains the general framework of the proposed IDS system. In addition, the theoretical backgrounds involved are clarified. Section 4.3 examines the application and simulation of the proposed methodology. Detailing the specific simulation environment, data treatment, and dataset generation from

realistic RADAR traces obtained from a real Air Traffic Management (ATM) RADAR network system. Section 4.4 presents the results and discuss the performance of this methodology based on the results.

4.2 Methodology

4.2.1 IDS framework

To take into account a new type of intrusion which is more covert, such as a MITM attack within a location report and control packets, the research effort is shifted from the network statistics to the payload of network packets (e.g., the geo-position packets). The IDS methodology is also based on a two-step process (as shown in Figure 4.1). In general, the IDS framework works starting by collecting information from the network by means of network sensors that are running capturing devices (either distributed or centralized sensors depending on the topology of the network). The collected data is then properly treated within the pre-treatment step to better expose the features of interest. This stage of processing is unique and differentiates from one problem to another. In the demonstration shown in Section 4.3, the particular pre-treatment step is achieved by a moving sample window and an algorithm to calculate the moving euclidean distance of each aircraft. Then the first stage of IDS (Step 1) is dedicated to traffic characterization. Its objective is to obtain a specific signature of the signal we seek to analyze. The next stage (Step 2) is to achieve the automatic classification of the signatures by a neural network model, the objective being to provide a binary trigger to either alert the administrator or start countering mechanisms, such as an IPS.

4.2.2 WLM Analysis

As demonstrated in the last chapter, I present the advantageous capability of the WLM analysis at capturing different density levels of singularities of the signal at different time scales and statistical moments of analysis. I show that this method can be efficient against flooding attacks within the UAS wireless network. Network signals of the same system, during different times of day and time scales should share similar MF characteristics.

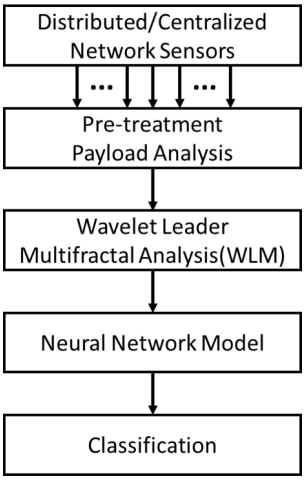


Figure 4.1: General framework of the proposed IDS system

The theory and application of the WLM analysis are detailed in Chapter 2 and 3. It is not illustrated here to avoid repetition.

Although, it is noted that when defining a fractal or self-similar system, it is necessary to verify the existence of the most significant scale which dominates the random process. For a measured network statistics, such behaviors have been demonstrated and verified numerous times in the literature as mentioned in Chapter 2. Instead, for other types of random systems which only exhibit fractal behaviors in some individual ranges scales, the multifractal spectrum is a powerful tool for analyzing and characterizing such a process.

In this case, it is important to verify the similarity and patterns that emerge from the collected test samples of normal and abnormal data. as later shown in Figure 4.5. It is quite apparent that even though it is not strictly proven that the moving traces acquired in this chapter is multifractal, the MF signature is still capable to distinguish the differences.

4.2.3 Machine learning signature classification

The next step after the signature acquisition is to compare the signatures of the normal traffic to that of the traffic containing malicious intrusion, then to observe the patterns that emerge from the different intensities of attack.

When considering the applicable methods, the first research is to investigate the possibility of ap-

plying analytical methods, such as the curve matching algorithm as mentioned in Chapter 3. However, this is found to be inefficient. Such a method can be effectively applied in detecting a DoS attack due to the fact that this attack can significantly deviate the signature of the signal from that of the normal ones, thus making it apparent to the similarity score. In addition, in the literature reviewed in Chapter 2 it is found that the possibility of applying a simple machine learning classification out-performs the results from the analytical method.

For the purpose of this research, which is to demonstrate the possibility of achieving an automatic alert when an intrusion is detected within the system, I first consider the supervised learning, such that a binary trigger can be obtained from the classification. The Long Short Term Memory (LSTM) network is then selected as the classification method, as it is simple and relatively easy to implement with good results for time series classification. Nevertheless, it is also possible to apply other classification methods, such as the Support Vector Machine (SVM).

LSTM is a modified Recurrent Neural Network (RNN), frequently used for time series, voice, and text classification. In comparison to the more conventional feed-forward neural network structures, such as CNN, RNN allows the modification of its internal states based on the output of the previous state, therefore forming a feedback structure. Classic RNN structures suffer from a gradient vanishing problem. To solve this, recent research has widely suggested to use LSTM cells, as they can retain the memory of arbitrary duration and potentially solve this problem.

As shown in Figure 4.2, a typical LSTM neural unit consists of a cell, an input gate, an output gate and a forget gate. This structure allows the network to preserve information from the previous state (past) with a weight. The cell state (c) is constantly updated by the gates according to the input state (X) and the hidden state (h), where first the forget gate (F) decides to what extend the information in the cell state will be preserved. Next, the input gate (I) decides which individual values in the cell state are to be updated, as well as the level of modification. In the end, the output gate (O) makes a filtered copy of the cell state to pass to the next state.

The particular LSTM network I have applied is a bidirectional LSTM (BiLSTM) network structure, typically used for sequence and time series classification. A BiLSTM basically duplicates and stacks an additional LSTM layer alongside the original LSTM layer and makes it run in the opposite, backward direction which allows the network to preserve information from the next state, as shown in

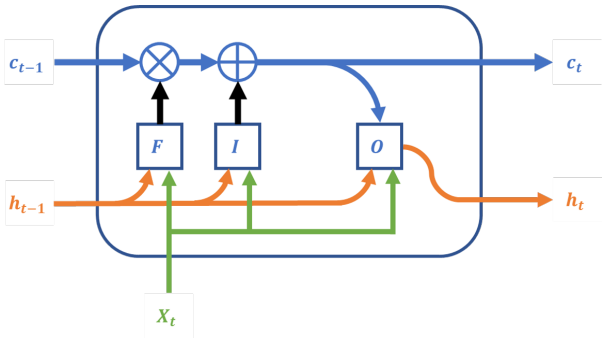


Figure 4.2: A simplified LSTM unit

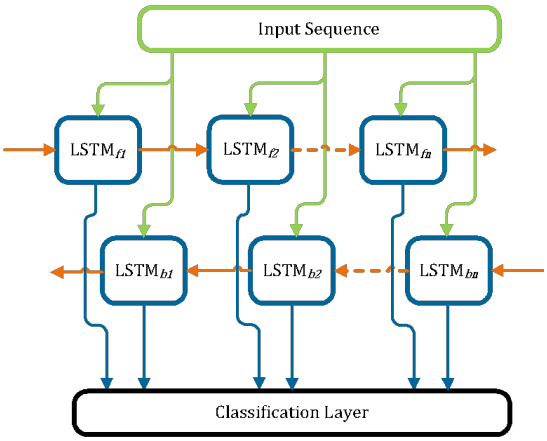


Figure 4.3: Typical architecture of a Bi-LSTM

Figure 4.3. This method of implementation increases the network's ability to understand the context of the signal. A BiLSTM will generally outperform the regular unidirectional LSTM of similar complexity in tasks such as classification and forecasting, as illustrated in [STN19]; [GFS05]; [GS05]. The proposed model consists of a 1D sequence input layer, a BiLSTM layer of 500 hidden units, a fully connected layer, and a softmax layer.

4.3 Application to experimental data

4.3.1 UAS mobility simulation

To demonstrate the feasibility of such a methodology, in the absence of a physically operating UAS, It is designed as a test bench based on pre-recorded RADAR network recordings. Instead of applying random walk mobility models that have been employed in other research, I consider the mission

profiles and mobility patterns of modern aircraft to be more suitable representations of a complex UAS. Thus, I consider that the RADAR recordings are viable representations of what a UAS Ground Control Station would observe in a UAS network for the following reasons:

•**Payload** Each UAV would report its geographical position at a certain time period either for displaying or back-feeding purposes to allow its backend control and path planning;

•**Mobility** The individual UAVs can join and leave the network at random times. The RADAR traces capture this behavior approximately by observing aircraft entering and exiting the scope of the RADAR;

•**Infrastructure** A UAS, like any other modern complex system, relies heavily on modern infrastructures, such as ports, stations, and checkpoints, which closely resembles what is available in an existing civil aviation system;

•**Mobile patterns** The moving patterns of planes are considerably similar to those of a drone system in an operational condition.

4.3.2 Pre-treatment Euclidean distance

Before the actual test, the individual recordings are processed to calculate the Euclidean distance: The output array consists of the moving distance that each UAV has traveled between each consecutive recording. Within the original recordings, each UAV position is defined using polar coordinates, such as:

$[\theta_{i,t}, \rho_{i,t}]$ where

$$\begin{pmatrix} i \in \mathbb{R}^+ \triangleq \text{ “The aircrafts' identification number TN”} \\ t \in \mathbb{R}^+ \triangleq \text{ “Time of Day index ToD”}. \end{pmatrix} \tag{4.1}$$

It is then defined a function $F_{eucd} : \mathbb{R} \to \mathbb{R}^+$ is detailed thereafter:

$$F_{eucd}([\theta_{i,t}, \rho_{i,t}], [\theta_{i,t+t_{INT}}, \rho_{i,t+t_{INT}}]) = \sqrt{\rho_{i,t}^2 + \rho_{i,t+t_{INT}}^2 - 2\rho_{i,t}\rho_{i,t+t_{INT}} \cos(\theta_{i,t} - \theta_{i,t+t_{INT}})} \tag{4.2}$$

where $t_{INT} \in \mathbb{R}^+$ is the reporting interval of each individual UAV.

The pseudo-code of Euclidean distance array calculation from UAV positions is detailed in Algorithm 1.

Algorithm 1 Euclidean distance from UAV position

Require: Recording loaded as a table TBL
Output: New table containing an array of Euclidean distance

```
TNuniq = Find unique values in field TBL.TN
Create an empty table TBLnew
for ii = 1,..., Length of TNuniq do
    rows of TBL to TBLtemp
    where TBL.TN = LBuniq(ii)
    for i3 = 1,..., Length of TBLtemp - 1 do
        Create an empty table TBLeu
        TBLeu.Eucl = run F_eucd at index i3
        TBLeu.Tod = TBLtemp.Tod(i3)
    end for
    Parsing table TBLeu with t_INT ⩽ 10seconds
    Append TBLnew with TBLeu
end for
Sort TBLnew with property TBLnew.Tod
```

As shown in Algorithm 1, each recording file is loaded as a table (TBL) with fields, such as Position in θ and ρ, Packet destination (DST), Flight number (TN), and Time of Day (ToD). The purpose of Algorithm 1 is to obtain a new table to record the calculated travel distance of each UAV. It achieves this by calculating the Euclidean distance of each UAV between two consecutive records and saving this information in a field $Eucl$ of a new table $TBLnew$. The ToD of the latter record is used as the time stamp.

Then iterate F_{eucd} according to Algorithm 1 to each recording file, this obtaining the Δ_t: the list of random aircrafts' travel distance recorded at time t. This process better compresses the data and better exposes the abnormal moving patterns induced by the intruders.

4.3.3 Test environment

Instead of focusing on variations in the network traffic, in this chapter, I only partially take into account the payload of the network, such as the coordinates and time. I exclude the physical effects

of the network, such as propagation delay, network congestion, and packet loss, as considered in the last chapter.

In this test, it is considered that the link between the drone and the GCS is compromised and the malicious user is initiating a MITM attack by intercepting packets from UAVs, changing the coordinates and transmitting the forged packets to their original destination. Such an attack is particularly interesting because it is silent and trivial. Network traffic will not be significantly modified, and the normal operation for the network itself remains mostly unaltered. Here, it is necessary to exploit the internal pattern within the payload of each packet instead of the statistics of the network. The received packets on the receiver side are all stored and processed into a .csv file, with each row containing one polar coordinate record of a UAV's position, time of scan, flight number, and frame number.

In this bench test, I consider $t_{INT} \in \mathbb{R}^+$ to be a random time variable close to the physical period of the RADAR which indicates the time interval of the radar scanning through the same aircraft twice.

Note that only $t_{INT} \leqslant 10 seconds$ is taken into account as one trajectory. It is possible for the network to lose packets or for the aircraft to leave and re-join the network at a different time of day and at a different point of exit and re-entry. There are also cases where after an aircraft has left the network for a long period of time, the flight number is reassigned to a new aircraft entering the scope. Hence it is important to filter the recordings with a properly defined filter.

4.3.4 Datasets

The simulation environment is constructed based on the RADAR records. In total, 31 RADAR records are processed, which corresponded to one month of data. Each original recording contains around 800,000 samples. Each original recording is then used to generate 36 versions of traces with different levels of attack. The simulated attacks are conducted by randomly selecting a number of aircraft with the specific TN, then altering the recorded trajectories by a random percentage between 0-10%. Each original or modified recording is then scanned by a moving window with a length of 100,000 samples and the moving step is 10,000 samples. The process of dataset generation is illustrated in Figure 4.4.

The windowed samples, which contain TNs that belong to the selected attack list, are set to label 1, indicating that they are attacked records, and those that do not contain such TNs are labeled as 0,

accordingly, indicating that they are not attacked.

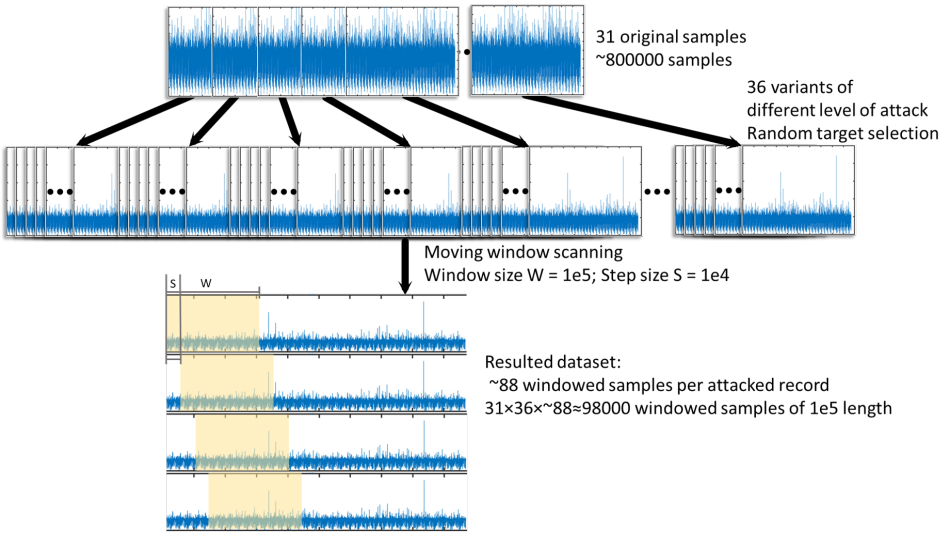


Figure 4.4: The process of dataset generation

To avoid significantly out-weighting the normal set by the attacked set, a number of traces with a miniature attack (1 A/C, 1-10%) are also generated into the training set and considered as a normal record. Due to the limited number of recordings available, the number of samples of a normal recording is around 25,000. To finally balance the dataset, the normal samples are padded by duplicating the normal dataset by a factor of 3, thus creating a normal set of around 75,000 samples. The exact distribution of the datasets is given in Table 4.1.

For verification purposes, the dataset generation process is replicated to generate a performance verification set, excluding the consideration of the balancing.

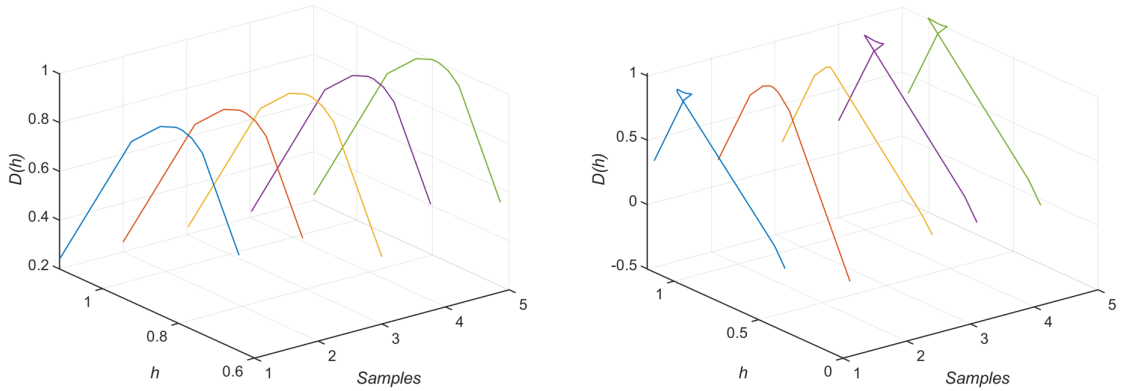
Table 4.1: Distribution of samples in the dataset

	Training set	Verification set
Normal	76263	25420
Abnormal	88195	88196

4.4 Results

4.4.1 WLM signatures

As shown in Figure 4.5, there are two sets of sample MF spectrum signatures $D(h)$ obtained from the WLM toolbox. During the test, it is found that the signatures of the Euclidean distance records Δ_t of attacked traffic deviate from the normal ones. With the normal signal, the level of multifractality is relatively consistent as shown by the span of h, which mostly ranged between 0.6 to 1 as shown on the left-hand side of Figure 4.5a. The span of h is much wider, however, ranging between 0.3 to 1 in the sampled abnormal signal, as shown on the right-hand side of Figure 4.5b. The MF spectrum $D(h)$ also shows different trends as the curves appear to be mirrored. Some twisting patterns are also shown. Such twists are observed in the extreme cases where a high-intensity attack with large modifications is present in the signal. This kind of attack will disrupt the originally monotonic descending behavior of the Hurst dimension $H(q)$ to become non-monotonic, thus creating the twist in the estimated MF spectrum.



(a) (b)

Figure 4.5: WLM $D(h)$signatures of: (a) Normal traces, (b) Abnormal traces

The signatures, though containing visually distinguishable features, are extremely difficult to identify by applying the curve matching algorithm mentioned in [CZL19]; [Gri+16], because it is almost impossible to set a correct detection threshold without significantly sacrificing the accuracy or the false positive rate, particularly in cases where the attack level is low enough. In addition, the twisting behavior exhibited in the abnormal signatures is not correctly taken into account by the curve match-

ing algorithm, hence, the motivation for applying more advanced classification methods, such as the LSTM.

4.4.2 Machine learning classification

To apply a machine learning classifier to the problem, I first have to train with the training dataset. Since the training set is relatively balanced, it would not provide a significantly biased classification result.

The performance of the methodology is firstly measured by the following evaluation matrices:

- **True positive (TP):** attacked record that has returned 1 from the IDS;
- **True Negative (TN):** non-attacked record that has returned 0 from the IDS;
- **False positive (FP):** non-attacked record that has returned 1 from the IDS;
- **False Negative (FN):** attacked record that has returned 0 from the IDS;

The matrices are typically compiled as one matrix, called a confusion matrix. From this the detection accuracy (ACC) is defined:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4.3}$$

The verification performance is shown in Figure 4.6: The IDS performance is also measured against attacks with different intensities (dictated by the number of A/C attacked). This is represented by an accuracy vs inaccuracy matrix in percentage, as shown in Figure 4.7.

As for Figure 4.6, the main confusion matrix is plotted in red vs green boxes, where the number of samples and overall probability of samples falling into particular categories are shown. The additional derived performance indexes:

- True positive rate (TPR) Positive predictive value (PPV);
- False negative rate (FNR) False discovery rate (FDR);
- True negative rate (TNR) Negative predictive value (NPV);

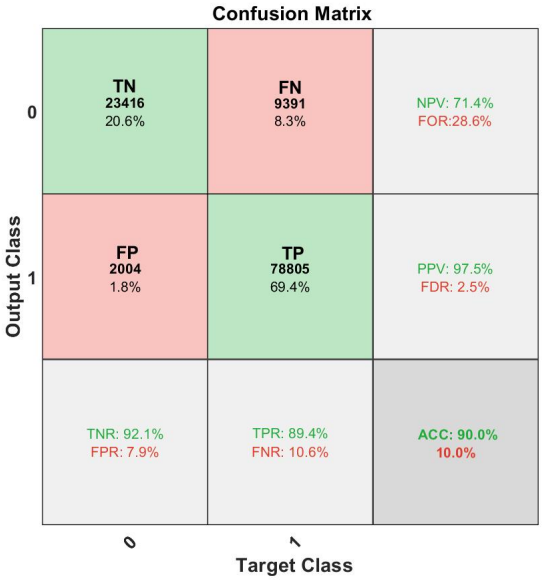


Figure 4.6: Confusion matrix of the performance verification with LSTM

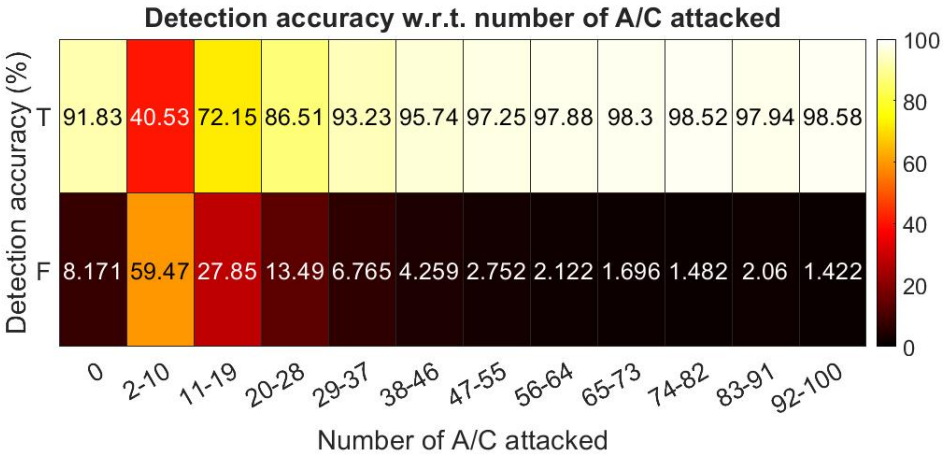


Figure 4.7: Verification at different intensities with LSTM

• False positive rate (FPR) False omission rate (FOR);

are provided in the corresponding grey boxes. The overall accuracy is around 90.0%, whereas the relative FP and FN rates are 7.9% and 8.3%, respectively. Due to the way in which the modification levels are generated, 600 aircraft of different TN numbers are presented on average. The attack intensity is mostly dependent on the number of A/Cs attacked. It is apparent in Figure 4.7 that with a higher intensity of the attack, it is extremely easy to distinguish the malicious recordings from the normal

ones. In the scenarios where only a small number of A/Cs are spoofed, the proposed methodology struggles to provide a valid classification. When there is zero A/C attacked, as shown on the very left of Figure 4.7 (which means the input samples contain no TN which appears on the attack list), the method is able to return a good accuracy of true negative.

Aside from the LSTM classification mentioned above, to better establish a performance baseline and demonstrate the advantages of LSTM, the experiment is replicated with another commonly used ML classification algorithm: SVM. The IDS performance is also measured against attacks with

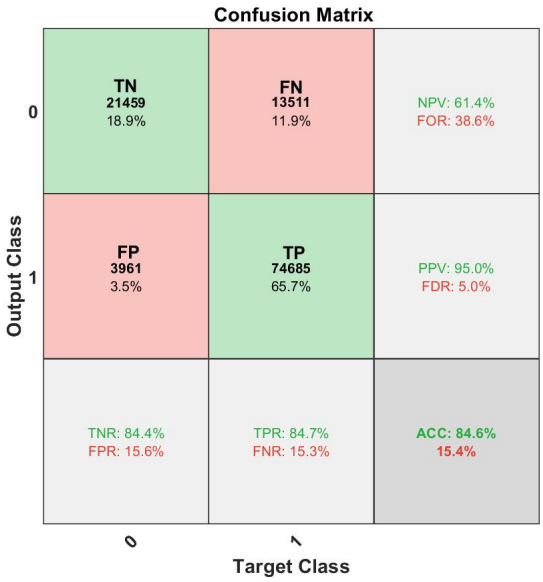


Figure 4.8: Confusion matrix of the performance verification with SVM

different intensities (dictated by the number of A/C attacked). This is represented by an accuracy vs inaccuracy matrix in percentage, as shown in Figure 4.8.

As shown in Figure 4.8 and 4.9, the performance demonstrated here with SVM shows slightly worse performance compared to the ones obtained with LSTM. Although it should be noted that the performance matrices are dependent on the design and optimization of the ML schemes. With proper design, the performance of the two classification tools can both be improved. Thus, the purpose of bringing up the SVM classification into the context is to provide a better empirical perspective into the possible performance with an IDS of a similar methodology.

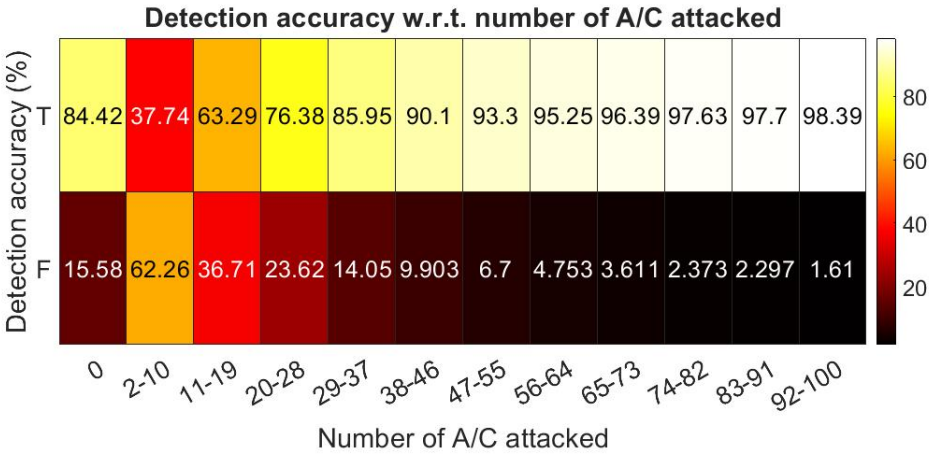


Figure 4.9: Verification at different intensities with SVM

Conclusion and perspectives

The work presented demonstrated a powerful intrusion detection methodology with great potentials to be implemented in a UAS network environment. The work reviews the context of network IDS in searching for a performant strategy in this specific domain with dedicated designs for UAS. This work incorporates several scientific domains and tools to establish an IDS methodology and evaluate it in relevant scenarios. The study is a valuable contribution towards the future research of UAS technology and is envisioned to be adaptable to other types of networks with similar characteristics.

The progress of this thesis mainly involves the advancements in the following three domains: The first part involves using cybernetic theories with statistical analysis to achieve accurate detection of flooding attacks within a UAS network. The second part involves using multifractal theory to identify traffics with an anomaly. The third part of the thesis involves using Artificial Intelligent(AI) to improve detection performance.

In this dissertation, I have demonstrated that a robust observer of cybernetic theories can improve intrusion detection systems in the specific context of a UAS network. A part of the work is focused on designing a robust observer based on Lyapunov Krasovkii functional and queuing dynamics of an AQM system in a TCP network. By exploiting the TCP network dynamics, which contains an AQM, it is possible to distinguish network traffics that contains anomalies from the normal ones. This method of benefits allows for a rapid reconstruction of the intrusion representation, allowing a nearly real-time intrusion detection and information display with its advantageously low delay. As demonstrated in Chapter 3, the performance of this method is notable against a DoS attack. The observer can also be implemented as an information source for a more intelligent AQM or the network administrator to deal with attacks. However, the drawbacks of this method are evident. This method is highly model-dependent, and many of today's network protocols do not impose a guaranteed transmission like the TCP dose. Such networks have also neglected the use of an AQM. Consequently, the another-equally performant feature needs to be modeled and implemented in place of the AQM modeling to achieve similar performance.

Next in order, I have demonstrated that the multifractal properties of the UAS network are an advantageous tool to examine the statistical properties of a UAS network. The work is first focused

on designing a working prototype of a WLM analysis-based IDS to identify the anomalies such as network congestion invoked by a DoS attack. It has been observed that the network traffic, in general, exhibits long-range dependence and multifractal behaviors. Statistics of network traffic is often considered one of the artificial signals that are scale-invariant (or self-similar). To better expose and take advantage of this property, the multifractal analysis is introduced. Combining with the robust observer, this proposed IDS is tested against the DoS attack. It is observed that the WLM signatures of the simulated UAS network can present drastic differences between normal traffic and traffic affected by a DoS attack. By applying a simple analytical comparison algorithm, such as the 3D curve matching algorithm, between the different signatures, it is possible to reach a satisfying level of detection accuracy with this proposed IDS. Later, this combined method is realized in an actual UAS and tested in a real environment, which returns promising results.

Later in this dissertation, it is proposed an innovative approach to achieve network spoofing attack detection with improvements to the previously designed IDS. Such improvement is achieved by incorporating a machine learning classification process. The benefits of incorporating the ML for the classification are not just the improvement in accuracy thanks to more sophisticated computation, but also the ability to take into account the context of the to-be-classified signal. The successful implementation of WLM against DoS attack has provided us enough confidence in extending the application of WLM-based IDS into the domain of detecting other types of network intrusions. Thus, a test bench is designed and demonstrates the preliminary performance results. It is shown that this combined method based on both the WLM analysis and the ML is effective against the MITM attack. This new design permits achieving a high detection accuracy while keeping a satisfied false positive rate when tested against a MITM attack. The resulting overall good performance opens many more possibilities to further investigate the methodology and its implementation possibilities.

As a future perspective, for a good continuation of this study, I identify several points that the current research have not yet addressed:

The current research successfully addressed the DoS and MITM attacks in the scope of the UAS network. For future development, it is important to address some other network security issues reviewed in the literature.

The current research on the implementation of AI into the WLM based IDS has only been tested in

a simulated environment. The next step is to address the performance in a more realistic environment, with emulation of UAV swarms, or preferably an actual UAS.

The current research has successfully implemented the theoretical WLM analysis into a working IDS. However, the tuning of the WLM toolbox has been done manually with experience. Future development on the actual dataset collected from the UAS simulator / actual UAS can help optimize this process.

The current research was conducted based on an empirical dataset, which highlights the importance of a valid dataset. Future research can be focused on the performance comparison of other different IDS methodologies in a scientific manner, and based on a valid dataset.

At last, it has been proposed to optimize the WLM (PLBMF) toolbox for the mobile communication network environment with even less computational overhead.

Bibliography

[Abr+02] Patrice Abry et al. “Multiscale nature of network traffic.” In: *IEEE Signal Processing Magazine* 19.3 (Apr. 2002), pp. 28–46 (cit. on pp. 27, 29, 30, 32, 34).

[Abr+03] Patrice Abry et al. “Self-similarity and long-range dependence through the wavelet lens.” In: *Theory and applications of long-range dependence* 1 (2003), pp. 527–556 (cit. on pp. 27, 29, 32).

[ADE20] Arwa Aldweesh, Abdelouahid Derhab, and Ahmed Z. Emam. “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues.” In: *Knowledge-Based Systems* 189 (2020), p. 105124 (cit. on pp. 39, 71).

[Akr+16] Raja Naeem Akram et al. “Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements.” In: *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, Aug. 2016 (cit. on p. 17).

[ALG08] Yassine Ariba, Yann Labit, and Frédéric Gouaisbaut. “Design and Performance Evaluation of a State-Space Based AQM.” In: *2008 International Conference on Communication Theory, Reliability, and Quality of Service*. IEEE, June 2008 (cit. on pp. 23, 24).

[ALL00] S. Athuraliya, D. Lapsley, and S. Low. “An enhanced random early marking algorithm for Internet flow control.” In: *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064)*. Vol. 3. 2000, 1425–1434 vol.3 (cit. on p. 25).

[Ari+09] Yassine Ariba et al. “Robust control tools for traffic monitoring in TCP/AQM networks.” In: *3rd IEEE Multi-Conference on Systems and Control (MSC 2009)*. St Petersbourg, Russia, July 2009 (cit. on p. 23).

[Ari+12] Y. Ariba et al. “Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer.” In: *IET Control Theory & Applications* 6.4 (2012), p. 506 (cit. on pp. 23, 24, 57).

[Ash+20] Javed Asharf et al. “A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions.” In: *Electronics* 9.7 (2020) (cit. on pp. 38, 71).

[AY17] Riham Altawy and Amr M. Youssef. “Security, Privacy, and Safety Aspects of Civilian Drones.” In: *ACM Transactions on Cyber-Physical Systems* 1.2 (Feb. 2017), pp. 1–25 (cit. on p. 17).

[Bac00] Rebecca Gurley Bace. *Intrusion detection*. Sams Publishing, 2000 (cit. on pp. 17, 20, 21).

[Bar+19] Benjamin Baron et al. “Mobility as an Alternative Communication Channel: A Survey.” In: *IEEE Communications Surveys & Tutorials* 21.1 (2019), pp. 289–314 (cit. on p. 16).

[BcT16] İlker Bekmezci, Eren Şentürk, and Tolgahan Türker. “SECURITY ISSUES IN FLYING AD-HOC NETWORKS (FANETs).” In: *Journal of Aeronautics and Space Technologies* 9.2 (July 2016), pp. 13–21 (cit. on p. 17).

[BK03] P. Brutch and C. Ko. “Challenges in intrusion detection for wireless ad-hoc networks.” In: *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.* 2003, pp. 368–373 (cit. on p. 18).

[BST13] İlker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. “Flying Ad-Hoc Networks (FANETs): A survey.” In: *Ad Hoc Networks* 11.3 (2013), pp. 1254–1270 (cit. on p. 16).

[CAT05] Srilatha Chebrolu, Ajith Abraham, and Johnson P. Thomas. “Feature deduction and ensemble design of intrusion detection systems.” In: *Computers & Security* 24.4 (June 2005), pp. 295–307 (cit. on p. 38).

[CBK09] Varun Chandola, Arindam Banerjee, and Vipin Kumar. “Anomaly detection.” In: *ACM Computing Surveys* 41.3 (July 2009), pp. 1–58 (cit. on pp. 18, 71).

[Che13] Alexey Ya. Chervonenkis. “Early History of Support Vector Machines.” In: *Empirical Inference*. Springer Berlin Heidelberg, 2013, pp. 13–20 (cit. on p. 38).

[Che+18] Z. Chen et al. “Recurrent Neural Networks for Automatic Replay Spoofing Attack Detection.” In: *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2018, pp. 2052–2056 (cit. on p. 40).

[CZL19] Jean-Philippe Condomines, Ruohao Zhang, and Nicolas Larrieu. “Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation.” In: *Ad Hoc Networks* 90 (2019). Recent advances on security and privacy in Intelligent Transportation Systems, p. 101759 (cit. on pp. 13, 80).

[DZA03] Hongmei Deng, Qing-An Zeng, and D.P. Agrawal. “SVM-based intrusion detection system for wireless ad hoc networks.” In: *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484)*. IEEE, 2003 (cit. on p. 38).

[EU16] EU. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. 2016 (cit. on p. 4).

[EU19] EU. *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance) C/2019/3824*. 2019 (cit. on pp. 4, 71).

[EU21] EU. *Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (Text with EEA relevance) C/2021/2671*. 2021 (cit. on p. 4).

[FAA20] FAA. *Small unmanned aircraft Systems (UAS) REGULATIONS (Part 107)*. Oct. 2020 (cit. on p. 4).

[Fen+19] Fang Feng et al. “Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device.” In: *Ad Hoc Networks* 84 (2019), pp. 82–89 (cit. on p. 40).

[FJ93] S. Floyd and V. Jacobson. “Random early detection gateways for congestion avoidance.” In: *IEEE/ACM Transactions on Networking* 1.4 (1993), pp. 397–413 (cit. on p. 25).

[FLB12] Erik M. Ferragut, Jason Laska, and Robert A. Bridges. “A New, Principled Approach to Anomaly Detection.” In: *2012 11th International Conference on Machine Learning and Applications*. IEEE, Dec. 2012 (cit. on p. 22).

[Fon+08] R. Fontugne et al. “Scaling in Internet Traffic: A 14 Year and 3 Day Longitudinal Study, With Multiscale Analyses and Random Projections.” In: *IEEE/ACM Transactions on Networking* 25.4 (8), pp. 2152–2165 (cit. on pp. 33, 34).

[Fon+15] R. Fontugne et al. “Random projection and multiscale wavelet leader based anomaly detection and address identification in internet traffic.” In: *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, Apr. 2015 (cit. on pp. 35, 36).

[Fy06] Liu Feng-yu. “Application of Support Vector Machines on Network Abnormal Intrusion Detection.” In: *Application Research of Computers* (2006) (cit. on p. 38).

[GFS05] Alex Graves, Santiago Fernández, and Jürgen Schmidhuber. “Bidirectional LSTM Networks for Improved Phoneme Classification and Recognition.” In: *Artificial Neural Networks: Formal Models and Their Applications – ICANN 2005*. Ed. by Włodzisław Duch et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 799–804 (cit. on p. 75).

[GKC03] Keqin Gu, Vladimir L. Kharitonov, and Jie Chen. *Stability of Time-Delay Systems*. Birkhäuser Boston, 2003 (cit. on p. 25).

[Gon+05] Wei-Bo Gong et al. “Self-similarity and long range dependence on the internet: a second look at the evidence, origins and implications.” In: *Computer Networks* 48.3 (June 2005), pp. 377–399 (cit. on p. 29).

[Gon+13] Xueqing Gong et al. “Fractal Based Anomaly Detection over Data Streams.” In: *Web Technologies and Applications*. Springer Berlin Heidelberg, 2013, pp. 550–562 (cit. on p. 34).

[Gri+16] Anna Grim et al. “Automatic Reassembly of Three-Dimensional Jigsaw Puzzles.” In: *International Journal of Image and Graphics* 16.02 (2016), p. 1650009. eprint: `https://doi.org/10.1142/S0219467816500091` (cit. on pp. 35, 36, 80).

[GS04] Tilmann Gneiting and Martin Schlather. “Stochastic Models That Separate Fractal Dimension and the Hurst Effect.” In: *SIAM Review* 46.2 (Jan. 2004), pp. 269–282 (cit. on p. 30).

[GS05] A. Graves and J. Schmidhuber. “Framewise phoneme classification with bidirectional LSTM networks.” In: *Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.* Vol. 4. 2005, 2047–2052 vol. 4 (cit. on p. 75).

[Gwo+19] Hyeokmin Gwon et al. *Network Intrusion Detection based on LSTM and Feature Embedding*. 2019. arXiv: `1911.11552 [cs.LG]` (cit. on p. 40).

[HHP03] Alefiya Hussain, John Heidemann, and Christos Papadopoulos. “A framework for classifying denial of service attacks.” In: *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications - SIGCOMM '03*. ACM Press, 2003 (cit. on p. 17).

[Hin+20] Hanan Hindy et al. “A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems.” In: *IEEE Access* 8 (2020), pp. 104650–104675 (cit. on p. 17).

[Hol+02] C.V. Hollot et al. “Analysis and design of controllers for AQM routers supporting TCP flows.” In: *IEEE Transactions on Automatic Control* 47.6 (June 2002), pp. 945–959 (cit. on p. 25).

[HS13] Kim Hartmann and Christoph Steup. “The vulnerability of UAVs to cyber attacks - An approach to the risk assessment.” In: *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. 2013, pp. 1–23 (cit. on p. 19).

[Ihl13] Espen A. F. Ihlen. “Multifractal analyses of response time series: A comparative study.” In: *Behavior Research Methods* 45.4 (Dec. 2013), pp. 928–945 (cit. on p. 47).

[Jac88] V. Jacobson. “Congestion avoidance and control.” In: *ACM SIGCOMM Computer Communication Review* 18.4 (Aug. 1988), pp. 314–329 (cit. on p. 23).

[Jaf04] Stephane Jaffard. *Wavelet techniques in multifractal analysis*. Tech. rep. PARIS UNIV (FRANCE), 2004 (cit. on p. 32).

[Jaf97a] S. Jaffard. “Multifractal Formalism for Functions Part I: Results Valid For All Functions.” In: *SIAM Journal on Mathematical Analysis* 28.4 (July 1997), pp. 944–970 (cit. on p. 32).

[Jaf97b] S. Jaffard. “Multifractal Formalism for Functions Part II: Self-Similar Functions.” In: *SIAM Journal on Mathematical Analysis* 28.4 (July 1997), pp. 971–998 (cit. on p. 32).

[Jav+12] Ahmad Y. Javaid et al. “Cyber security threat analysis and modeling of an unmanned aerial vehicle system.” In: *2012 IEEE Conference on Technologies for Homeland Security (HST)*. 2012, pp. 585–590 (cit. on p. 16).

[JS03] Audun Jøsang and Gunnar Sanderud. “Security in mobile communications: Challenges and opportunities.” In: *Proceedings of the Australasian Information Security Workshop*

Conference on ACSW Frontiers 2003 - Volume 21. Australian Computer Society, Inc., 2003, pp. 43–48 (cit. on p. 16).

[Kap86] Jay Kappraff. “The geometry of coastlines: a study in fractals.” In: *Computers & Mathematics with Applications* 12.3, Part 2 (1986), pp. 655–671 (cit. on p. 28).

[Kim+12] Alan Kim et al. “Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles.” In: *InfotechAerospace 2012*. American Institute of Aeronautics and Astronautics, June 2012 (cit. on p. 17).

[KM17] C. G. Leela Krishna and Robin R. Murphy. “A review on cybersecurity vulnerabilities for unmanned aerial vehicles.” In: *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. 2017, pp. 194–199 (cit. on p. 19).

[Kom04] Tiina Komulainen. *Self-similarity and power laws*. Tech. rep. Helsinki University of Technology, 2004 (cit. on pp. 27, 30).

[KS20] Sydney Mambwe Kasongo and Yanxia Sun. “A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System.” In: *ICT Express* 6.2 (2020), pp. 98–103 (cit. on pp. 40, 71).

[LAG07] Yann Labit, Yassine Ariba, and Frederic Gouaisbaut. “On designing Lyapunov-Krasovskii based AQM for routers supporting TCP flows.” In: *2007 46th IEEE Conference on Decision and Control*. IEEE, 2007 (cit. on pp. 23, 24).

[LB09] R. Lopes and N. Betrouni. “Fractal and multifractal analysis: A review.” In: *Medical Image Analysis* 13.4 (2009), pp. 634–649 (cit. on pp. 29, 32, 34).

[LCD04] Anukool Lakhina, Mark Crovella, and Christophe Diot. “Diagnosing Network-wide Traffic Anomalies.” In: *SIGCOMM Comput. Commun. Rev.* 34.4 (Aug. 2004), pp. 219–230 (cit. on pp. 17, 47).

[Lel+93] Will E. Leland et al. “On the self-similar nature of Ethernet traffic.” In: *ACM SIGCOMM Computer Communication Review* 23.4 (Oct. 1993), pp. 183–193 (cit. on p. 33).

[Leo+15] R. Leonarduzzi et al. “P-leader multifractal analysis and sparse SVM for intrapartum fetal acidosis detection.” In: *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, Aug. 2015 (cit. on p. 39).

[Li+12] Yinhui Li et al. “An efficient intrusion detection system based on support vector machines and gradually feature removal method.” In: *Expert Systems with Applications* 39.1 (Jan. 2012), pp. 424–430 (cit. on p. 38).

[Loi+10] P Loiseau et al. “Investigating Self-Similarity and Heavy-Tailed Distributions on a Large-Scale Experimental Facility.” In: *IEEE/ACM Transactions on Networking* 18.4 (Aug. 2010), pp. 1261–1274 (cit. on p. 29).

[LPD02] S.H. Low, F. Paganini, and J.C. Doyle. “Internet congestion control.” In: *IEEE Control Systems Magazine* 22.1 (2002), pp. 28–43 (cit. on pp. 23, 49).

[LRS18] Nicolas Larrieu, Theobald de Riberolles, and Guthemberg Silvestre. “Design, Development and Implementation of a Network Intrusion Detection Tool for Air Traffic Management Systems.” In: *DSN 2018, 48th IEEE/IFIP International Conference on Dependable Systems and Networks*. Luxembourg, Luxembourg, June 2018 (cit. on p. 8).

[Mek+21] Yassine Mekdad et al. *A Survey on Security and Privacy Issues of UAVs*. 2021. arXiv: 2109.14442 [cs.CR] (cit. on p. 20).

[MGT00] Vishal Misra, Wei-Bo Gong, and Don Towsley. “Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to RED.” In: *Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication - SIGCOMM ’00*. ACM Press, 2000 (cit. on p. 24).

[Min88] Marvin Minsky. *Perceptrons : an introduction to computational geometry*. Cambridge, Mass: MIT Press, 1988 (cit. on p. 39).

[Miq+17] Thierry Miquel et al. “Design of a robust controller/observer for TCP/AQM network: First application to intrusion detection systems for drone fleet.” In: *2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, Sept. 2017 (cit. on pp. 23, 25, 26).

[MMH17] Kishan G. Mehrotra, Chilukuri K. Mohan, and HuaMing Huang. *Anomaly Detection Principles and Algorithms*. Springer International Publishing, 2017 (cit. on p. 22).

[MN68] Benoit B. Mandelbrot and John W. Van Ness. “Fractional Brownian Motions, Fractional Noises and Applications.” In: *SIAM Review* 10.4 (1968), pp. 422–437 (cit. on p. 31).

[MNP04] A. Mishra, K. Nadkarni, and A. Patcha. “Intrusion detection in wireless ad hoc networks.” In: *IEEE Wireless Communications* 11.1 (2004), pp. 48–60 (cit. on p. 18).

[MRL15] Jean-Aimé Maxa, Gilles Roudiere, and Nicolas Larrieu. “Emulation-Based Performance Evaluation of Routing Protocols for Uaanets.” In: *Lecture Notes in Computer Science*. Springer International Publishing, 2015, pp. 227–240 (cit. on p. 50).

[MS03] Srinivas Mukkamala and Andrew H. Sung. “Feature Selection for Intrusion Detection with Neural Networks and Support Vector Machines.” In: *Transportation Research Record: Journal of the Transportation Research Board* 1822.1 (Jan. 2003), pp. 33–39 (cit. on p. 38).

[MZT18] Simone McCarthy, William Zhang, and Denise Tsang. *HK$1 million HKD in damage caused by GPS jamming during drone light show*. Oct. 2018 (cit. on p. 3).

[NAL21] Haque Nawaz, Husnain Mansoor Ali, and Asif Ali Laghari. “UAV Communication Networks Issues: A Review.” In: *Archives of Computational Methods in Engineering* 28.3 (May 2021), pp. 1349–1369 (cit. on p. 19).

[Par07] JC Pardo. “A brief introduction to self-similar processes.” In: *Department of Mathematical Sciences, University of Bath, United Kingdom* 9 (2007), pp. 305–316 (cit. on p. 31).

[Rah+10] Sandy Rahme et al. “Second order sliding mode observer for anomaly detection in TCP networks: From theory to practice.” In: *49th IEEE Conference on Decision and Control (CDC)*. IEEE, Dec. 2010 (cit. on p. 23).

[Rah+13] Sandy Rahme et al. “Sliding Modes for Anomaly Observation in TCP Networks: From Theory to Practice.” In: *IEEE Transactions on Control Systems Technology* 21.3 (May 2013), pp. 1031–1038 (cit. on p. 23).

[Ran+16] Chaitanya Rani et al. “Security of unmanned aerial vehicle systems against cyber-physical attacks.” In: *The Journal of Defense Modeling and Simulation* 13.3 (2016), pp. 331–342. eprint: `https://doi.org/10.1177/1548512915617252` (cit. on p. 19).

[RDY03] Xian Rao, Chun-Xi Dong, and Shao-Quan Yang. “An intrusion detection system based on support vector machine.” In: *Journal of Software* 14.4 (2003), pp. 798–803 (cit. on p. 38).

[RF99] K. Ramakrishnan and S. Floyd. *A Proposal to add Explicit Congestion Notification (ECN) to IP*. Tech. rep. Jan. 1999 (cit. on p. 23).

[Rib+20] Theobald de Riberolles et al. "Characterizing Radar Network Traffic: a first step towards spoofing attack detection." In: *AeroConf 2020, IEEE Aerospace Conference*. 2020 IEEE Aerospace Conference. Big Sky, United States: IEEE, Mar. 2020, ISBN:978–1–7281–2734–7 (cit. on p. 8).

[Rie+01] Rudolf H. Riedi et al. "Network Traffic Modeling Using a Multifractal Wavelet Model." In: *European Congress of Mathematics*. Birkhäuser Basel, 2001, pp. 609–618 (cit. on p. 34).

[Rie+99] R.H. Riedi et al. "A multifractal wavelet model with application to network traffic." In: *IEEE Transactions on Information Theory* 45.3 (Apr. 1999), pp. 992–1018 (cit. on p. 34).

[Rie99] Rudolf H Riedi. *Multifractal processes*. Tech. rep. Rice Univ Houston Tx Dept Of Electrical And Computer Engineering, 1999 (cit. on p. 31).

[RLG09] Sandy Rahme, Yann Labit, and Frédéric Gouaisbaut. "Sliding Mode Observer for Anomaly Detection in TCP/AQM Networks." In: *2009 Second International Conference on Communication Theory, Reliability, and Quality of Service*. 2009, pp. 113–118 (cit. on pp. 23, 24).

[Rod+17] Mariana Rodrigues et al. "UAV integration Into IoIT: opportunities and challenges." In: *International Conference on Autonomic and Autonomous Systems - ICAS*. IARIA, 2017 (cit. on p. 16).

[Sal+14] Osman Salem et al. "Anomaly Detection in Medical Wireless Sensor Networks using SVM and Linear Regression Models." In: *International Journal of E-Health and Medical Communications* 5.1 (Jan. 2014), pp. 20–45 (cit. on p. 39).

[Sch21] Jaron Schneider. *Error causes mass of light show drones to tumble out of the sky*. June 2021 (cit. on p. 3).

[Sha20] Shelley Shan. *Drones crash during light display at lantern festival*. Feb. 2020 (cit. on p. 3).

[Sha+20] Abhishek Sharma et al. “Communication and networking technologies for UAVs: A survey.” In: *Journal of Network and Computer Applications* 168 (2020), p. 102739 (cit. on p. 19).

[SK14] Vishal Sharma and Rajesh Kumar. “A Cooperative Network Framework for Multi-UAV Guided Ground Ad Hoc Networks.” In: *Journal of Intelligent & Robotic Systems* 77.3-4 (Aug. 2014), pp. 629–652 (cit. on p. 17).

[SLW14] Hongtao Shi, Gang Liang, and Hai Wang. “A novel traffic identification approach based on multifractal analysis and combined neural network.” In: *annals of telecommunications - annales des télécommunications* 69.3 (Apr. 2014), pp. 155–169 (cit. on p. 40).

[Sri04] R. Srikant. *The Mathematics of Internet Congestion Control*. Birkhäuser Boston, 2004 (cit. on pp. 23, 49).

[St17] Claudia Stöcker et al. “Review of the Current State of UAV Regulations.” In: *Remote Sensing* 9.5 (2017) (cit. on p. 4).

[STN19] S. Siami-Namini, N. Tavakoli, and A. S. Namin. “The Performance of LSTM and BiLSTM in Forecasting Time Series.” In: *2019 IEEE International Conference on Big Data (Big Data)*. 2019, pp. 3285–3292 (cit. on p. 75).

[Tar05] Sophie Tarbouriech. *Advances in communication control networks*. Berlin: Springer, 2005 (cit. on pp. 23, 49).

[Tea+10] W. T. Luke Teacy et al. “Maintaining connectivity in UAV swarm sensing.” In: *2010 IEEE Globecom Workshops*. IEEE, Dec. 2010 (cit. on p. 17).

[Tim21] Global Times. *Mainframe malfunction causes dozens of drones to crash into building in SW China*. Jan. 2021 (cit. on p. 3).

[TTW97] Murad S. Taqqu, Vadim Teverovsky, and Walter Willinger. “Is Network Traffic Self-Similar or Multifractal?” In: *Fractals* 05.01 (Mar. 1997), pp. 63–73 (cit. on p. 33).

[Vap00] Vladimir N. Vapnik. *The Nature of Statistical Learning Theory*. Springer New York, 2000 (cit. on p. 38).

[Ven+18] C. Venkatesan et al. “ECG Signal Preprocessing and SVM Classifier-Based Abnormality Detection in Remote Healthcare Applications.” In: *IEEE Access* 6 (2018), pp. 9767–9773 (cit. on p. 39).

[WA07] Herwig Wendt and Patrice Abry. “Multifractality Tests Using Bootstrapped Wavelet Leaders.” In: *IEEE Transactions on Signal Processing* 55.10 (Oct. 2007), pp. 4811–4820 (cit. on p. 33).

[WAJ07] Herwig Wendt, Patrice Abry, and Stephine Jaffard. “Bootstrap for Empirical Multifractal Analysis.” In: *IEEE Signal Processing Magazine* 24.4 (July 2007), pp. 38–48 (cit. on pp. 33, 47).

[Wen08] Herwig Wendt. “Contributions of Wavelet Leaders and Bootstrap to Multifractal Analysis: Images, Estimation Performance, Dependence Structure and Vanishing Moments. Confidence Intervals and Hypothesis Tests.” Theses. Ecole normale supérieure de lyon - ENS LYON, Sept. 2008 (cit. on pp. 32, 33).

[Wen+09] Herwig Wendt et al. “Wavelet leaders and bootstrap for multifractal analysis of images.” In: *Signal Processing* 89.6 (June 2009), pp. 1100–1114 (cit. on p. 33).

[Wer+05] Aleksander Weron et al. “Complete description of all self-similar models driven by Lévy stable noise.” In: *Physical Review E* 71.1 (Jan. 2005) (cit. on p. 31).

[Wil+03] Walter Willinger et al. *Long-range dependence and data network traffic*. 2003 (cit. on pp. 29, 34).

[Wil+17] Graham Wild et al. “A Post-Accident Analysis of Civil Remotely-Piloted Aircraft System Accidents and Incidents.” In: *Journal of Aerospace Technology and Management* 9.2 (Apr. 2017), pp. 157–168 (cit. on p. 3).

[Xia+19] Ke Xiao et al. “Abnormal Behavior Detection Scheme of UAV Using Recurrent Neural Networks.” In: *IEEE Access* 7 (2019), pp. 110293–110305 (cit. on p. 40).

[Xu+18] C. Xu et al. “An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units.” In: *IEEE Access* 6 (2018), pp. 48697–48707 (cit. on pp. 40, 71).

[XZY09] Lixia Xie, Dan Zhu, and Hongyu Yang. “Research on SVM Based Network Intrusion Detection Classification.” In: *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery*. IEEE, 2009 (cit. on p. 38).

[Yan+19] Chaoxing Yan et al. “A Comprehensive Survey on UAV Communication Channel Modeling.” In: *IEEE Access* 7 (2019), pp. 107769–107792 (cit. on p. 19).

[Yb2] *Seventeen drones crashed during an air show*. May 2020 (cit. on p. 3).

[YGA15] Eray Yağdereli, Cemal Gemci, and A Ziya Aktaş. “A study on cyber-security of autonomous and unmanned vehicles.” In: *The Journal of Defense Modeling and Simulation* 12.4 (2015), pp. 369–381. eprint: https://doi.org/10.1177/1548512915575803 (cit. on p. 18).

[YL11] Manfu Yan and Zhifang Liu. “A New Method of Transductive SVM-Based Network Intrusion Detection.” In: *Computer and Computing Technologies in Agriculture IV*. Springer Berlin Heidelberg, 2011, pp. 87–95 (cit. on p. 38).

[YYF09] Ariba Yassine, Labit Yann, and Gouaisbaut Frédéric. “Congestion control of a single router with an active queue management.” In: *International Journal on Advances in Internet Technology* 2.1 (2009) (cit. on p. 25).

[ZCL22] Ruohao Zhang, Jean-Philippe Condomines, and Emmanuel Lochin. “A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System.” In: *Drones* 6.1 (2022) (cit. on p. 13).

[Zha+19] Yuan Zhang et al. “Anomaly-Based Network Intrusion Detection Using SVM.” In: *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, Oct. 2019 (cit. on p. 38).

[Zha+20] Jianming Zhang et al. “Lightweight deep network for traffic sign classification.” In: *Annals of Telecommunications* 75.7 (Aug. 2020), pp. 369–379 (cit. on p. 71).

[Zhe18] Gong Zhe. *Why Ehang’s Record-breaking 1,374-DRONE show became a disaster?* May 2018 (cit. on p. 3).

[ZMZ07] Hua Zhou, Xiangru Meng, and Li Zhang. “Application of Support Vector Machine and Genetic Algorithm to Network Intrusion Detection.” In: *2007 International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, Sept. 2007 (cit. on p. 38).

Résumé — Ces dernières années, le développement du système aérien sans pilote (UAS) impliquant des essaims de véhicules aériens sans pilote (UAV) a connu des progrès sans précédent. Cependant, les systèmes de réseau mis en œuvre dans les UAS commerciaux actuels sont souvent des variantes des systèmes de réseau existants. Ainsi, des vulnérabilités préexistantes peuvent persister, tandis que de nouvelles vulnérabilités émergeant des nouvelles propriétés des UAS, telles que la mobilité et l'interconnectivité, sont encore plus préoccupantes. Étant donné que les UAS opèrent dans l'espace aérien civil, la sûreté et la sécurité sont essentielles. Cette thèse a été créée en réponse à une demande croissante. Dans ce rapport de thèse, trois stratégies sont explorées pour chercher à résoudre différentes attaques que l'on peut s'attendre à observer dans un UAS. La première partie de la thèse implique l'utilisation de théories cybernétiques : des techniques d'observation robustes pour réaliser une détection robuste d'anomalies dans un réseau TCP (Transmission Control Protocol). Les travaux se sont concentrés sur la conception d'un observateur robuste basé la méthode des fonctionnelles de Lyapunov-Krasovkii et d'un système de gestion de file d'attente active (AQM) dans un réseau TCP. En exploitant la dynamique du réseau TCP, nous pouvons détecter un trafic réseau anormal. La deuxième partie de la thèse utilise la théorie multifractale pour identifier les trafics présentant une anomalie. Les travaux se sont concentrés sur la conception d'un prototype d'IDS fonctionnel basé sur l'analyse Wavelet Leader Multifractal (WLM) pour identifier des anomalies telles que la congestion du réseau générée par une attaque DoS. Dans l'expérience, nous observons que la signature WLM d'un réseau UAS simulé peut être radicalement différente entre un trafic normal et un trafic affecté par une attaque DoS. Par une simple comparaison analytique entre les différentes signatures, nous pouvons identifier le trafic avec ou sans attaque. La troisième partie de la thèse consiste à utiliser l'intelligence artificielle (IA) pour améliorer les performances de détection. Nous avons introduit un réseau de classification Long Short-Term memory (LSTM) (et d'autres réseaux de neurones) pour augmenter la qualité de détection. Ici, au lieu de cibler une attaque évidente, telle que l'attaque DoS, nous avons tourné notre attention vers une attaque plus délicate, telle que l'attaque Man in the Middle (MITM). En adaptant l'analyse WLM et les principes d'apprentissage automatique, nous avons constaté qu'il est possible d'atteindre un niveau de détection prometteur pour une attaque de falsification des coordonnées géographiques des drones dans un réseau UAS simulé.

Mots clés : Drone, UAV, UAS, Réseau Ad-hoc, Détection d'intrusion, Observateur Robuste, Analyse Multifractale, Machine Learning, Déni-de-service, Man-In-The-Middle.

Abstract — In recent years, the development of the Unmanned Aerial System (UAS) involving swarms of unmanned aerial vehicles (UAVs) has experienced unprecedented progress. However, network systems implemented in current commercial UASs are often variations of existing network systems. Thus, pre-existing vulnerabilities may still exist, while new vulnerabilities emerging from the new properties of a UAS, such as mobility and inter-connectivity, are of even greater concern. As UASs operate in civilian airspace, safety and security are essential.

This thesis was created in response to growing demand. In this thesis report, three strategies are explored to seek to resolve different attacks that we would expect to observe in a UAS.

The first part of the thesis involves the use of cybernetic theories: robust observation techniques to achieve robust detection of anomalies in a TCP (Transmission Control Protocol) network. Work focused on the design of a robust observer based on the Lyapunov-Krasovkii functional and queuing dynamics of an Active Queue Management system in a TCP network. By exploiting the dynamics of the TCP network, which contains AQM, we can distinguish anomalous network traffic.

The second part of the thesis consists in using the multifractal theory to identify the traffics presenting an anomaly. Work focused on designing a working prototype of an IDS based on Wavelet Leader Multifractal (WLM) analysis to identify anomalies such as network congestion generated by a DoS attack. In the experiment, we observe that the WLM signature of a simulated UAS network can be radically different between normal traffic and traffic affected by a DoS attack. By applying a simple analytical comparison between the different signatures, we can identify traffic with or without attack.

The third part of the thesis consists in using artificial intelligence (AI) to improve detection performance. We introduced a long short-term memory (LSTM) classification network (and other neural networks) to increase detection accuracy. Here, instead of targeting an obvious attack, such as the DoS attack, we turned our attention to a more delicate attack, such as the Man in the Middle (MITM)

attack. By adapting WLM analysis and Machine Learning principles, we have found that it is possible to achieve a promising level of detection for an spoofing attack on the geographic coordinates of individual UAVs in a simulated UAS network.

Keywords: Drone, UAV, UAS, Ad-hoc Network, Intrusion Detection, Robust Observer, Multifractal Analysis, Machine Learning, Denial-of-Service, Man-In-The-Middle.

RESCO,SINA,Ecole Nationale de l'Aviation Civile, 7 Avenue Edouard Belin, 31055 Toulouse