الجمهورية الجزائرية الديمقراطية الشعبية
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعليم العالي و البحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

جامعة عمّار ثليجي بالأغواط
UNIVERSITY OF AMAR TELIDJI LAGHOUAT

كلية العلوم
FACULTY OF SCIENCE
قسم الإعلام الآلي
DEPARTMENT OF COMPUTER SCIENCE

Master Thesis

Domain Mathematics and Computer Science

Field Computer Science

Option Computer Networking and Distributed Applications

By:
ISSAAD Mohammed Tahar Elakram

Topic

GPS Signal Spoofing Detection using Trust Systems

Defended Publicly in Front of the Jury Composed of

M_r.	Y. GUELLOUMA	MCA	PRESIDENT	UATL
M_r.	T. BENDOUMA	MCA	REVIEWER	UATL
M_r.	M. E. MAICHA	MCB	REVIEWER	UATL
M_r.	C. A. KERRACHE	MCA	CO-SUPERVISOR	UATL
M_r.	N. Lagraa	Professor	SUPERVISOR	UATL

Academic Year 2023/2024

Dedications

I dedicate this work to the two extraordinary people who continuously supported me and without whom this work would not have been possible.

To my dear mother and my dear father, whom no dedication can express the gratitude for their efforts, love and patience.

To my dear brothers and sister, all the members of my family, and to all my dear friends who have helped me during my studies.

And to all who have taught me throughout my academic career and to the department staff for their efforts and motivation.

Thank you all.

Mohammed Tahar .

Acknowledgements

All praise and thanks to almighty Allah, the Most Gracious, the Most Merciful, for the accomplishment of this work.

I would like to express my highest gratitude and sincere appreciation to my supervisor Professor Nasreddine Lagraa, for his invaluable counsel, patience and guidance throughout this project.

I extend my sincere and warm thanks to all my honorable teachers who have contributed in my learning career throught the years.

Lastly, I wish to convey our deep appreciation to my parents, brothers and sister and to all familly members and my dear friends whom were a source of motivation and were part in making this dissertation.

Thank you all.

Mohammed Tahar .

مُلخّص

أصبح إستعمال الطائرات بدون طيار في العصر الحديث الأكثر شيوعا، و ذلك راجع لمختلف تطبيقاتها و مرونتها في تنفيذ الأوامر عن بعد. تتنوع أنظمة هذه الطائرات من أنظمة خاصة وعامة بحيث يمكن أن تتاح للإستعمال الشخصي كما أنها في أغلب الأوقات تستعمل لإكمال المهام الخاصة. تستعمل الطائرات بدون طيار تقنيات حديثة و متطورة للتنقل في بيئات معقدة، حيث أنها كثيرا ما تعتمد على تقنية نظام تحديد المواقع العالمي لتحديد موقعها و لحساب المسار المتبقي للمهمة، كثيرا ما تتعرض أجهزة الإستقبال الخاصة بنظام تحديد المواقع العالمي إلى عدة أنواع من الهجمات إنتحال نظام تحديد المواقع مما جعلها تشكل عائق بالنسبة للطائرات بدون طيار حيث أن معظم إعتمادها يكون على أجهزة إستقبالها. لضمان إستقبال إشارات سليمة وغير زائفة نسعى في هذه الأطروحة لإقتراح طريقة لمراقبة إشارات جهاز الإستقبال عن أي نشاط غير طبيعي. وكذا محاولة الكشف عن أي هجمة عن طريق إستعمال نظام ثقة مابين الطائرات المجاورة للتقليل من نسبة الضرر من هذه الهجمات. نستعمل في نظام الثقة تبادل معلومات حول موقع الطائرة لضمها في حساب نسبة الثقة و كذا جعلها كمرجع للتأكد من أي عملية هجوم. لبناء التجارب الخاصة بالطريقة المقترحة إستعمالنا محاكي شبكات الأحداث المنفصلة وإستخراج النتائج المحققة على شكل أعمدة بيانات لتحليل مدى دقة معدل الكشف حالات الوقوع في هجمات.

الكلمات المفتاحيّة: طائرات بدون طيار، نظام تحديد المواقع العالمي، أنظمة ثقة، هجمات إنتحال نظام تحديد المواقع.

Abstract

In the modern era, the use of Unmanned Aerial Vehicles (UAVs) has become increasingly popular due to their diverse applications and flexibility in executing operations remotely. UAV systems range from specialized to general-purpose systems, can be used for personal use or used for the completion of specific missions. UAVs employ advanced technologies to navigate complex environments, often relying on Global Positioning System (GPS) technology to determine their location and calculate the remaining mission path. However, GPS receivers are vulnerable to various types of spoofing attacks, posing a significant challenge for UAVs, that heavily depend on their GPS receivers. To ensure the reception of clean and authentic signals, this thesis proposes a method to monitor GPS receiver's signals for any abnormal activity. Additionally, we aim to detect attacks using trust systems among neighboring UAVs to decrease the impact of such attacks. The trust system involves exchanging location information to calculate trust levels and serve as a reference for verifying potential attacks. To conduct experiments for the proposed method, we utilized a discrete-event network simulator and extract results in the form of data columns to analyze the accuracy of the detection rate for attack scenarios.

Keywords: Drone, UAV, GPS, Systèmes de Confiance, Usurpation GPS.

Résumé

À l'ère moderne, L'utilisation des drones est devenue de plus en plus répandue, en raison de leurs diverses applications et de leur flexibilité dans l'exécution des commandes à distance. Les systèmes de ces avions varient des systèmes privés aux systèmes publics afin qu'ils puissent être disponibles pour un usage personnel et la plupart du temps, ils sont utilisés pour accomplir des tâches spéciales. Les drones utilisent des technologies modernes et avancées pour naviguer dans des environnements complexes, car ils s'appuient souvent sur la technologie du GPS pour déterminer leur position et calculer le chemin restant de la mission à parcourir, les récepteurs des systèmes GPS sont souvent exposés à plusieurs types d'attaques par usurpation d'identité GPS, ce qui en fait un obstacle pour les drones, car la plupart de leur dépendance découle de leurs appareils de réception. Pour assurer la réception de signaux sûrs et corrects, nous cherchons dans cette thèse à proposer un moyen de surveiller les signaux de l'appareil de réception et conduire à la recherche de toute activité anormale. En plus d'essayer de détecter toute attaque en utilisant le système de confiance entre les avions voisins pour réduire le taux de dommages causés par ces attaques. Dans le système de confiance, nous utilisons l'échange d'informations sur la position de l'avion pour l'inclure dans le calcul du rapport de confiance et aussi pour en faire une référence pour s'assurer de toute attaque. Pour construire des expériences avec la méthode proposée, nous utilisons un simulateur de réseau à événements discrets pour extraire les résultats obtenus sous formede colonnes de données pour analyser la précision du taux de détection des occurrences d'attaques.

Keywords: Drone, UAV, GPS, Trust Systems, GPS Spoofing Attacks.

Contents

List of Figures

List of Tables

Acronyms

AoA Angle of Arrival. 19

C/N0 Carrier-to-Noise Ratio. 8, 36, 37

DoS Denial-of-Service. 29

FNR False Negative Rate. 32

FPR False Positive Rate. 32

GCS Ground Control Station. 15, 16

GLONASS Globalnaya Navigazionnaya Sputnikovaya Sistema. 23

GNSS Global Navigation Satellite System. 12, 16, 23

GPS Global Positioning System. 6, 8, 12, 23, 28, 29, 30, 31, 33, 34, 36, 38, 45, 47

IR Infrared Sensors. 16

MLP Multilayer Perceptron. 34

PRN Pseudorandom Noise. 24, 36

PSOF Particle Swarm Optimization Filter. 34

RAIM Receiver Autonomous Integrity Monitoring. 33

RSSI Received Signal Strength Indicator. 19, 34

SNR Signal-to-Noise Ratio. 34

SVM Support Vector Machine. 34

TNR True Negative Rate. 32

ToA Time of Arrival. 18

TPR True Positive Rate. 32

UAV Unmanned Aerial Vehicle. 6, 8, 12, 14, 15, 16, 17, 22, 25, 26, 27, 28, 29, 30, 31, 33, 34, 36, 37, 40, 42, 45, 47

Chapter 1

Introduction

Unmanned Aerial Vehicles UAVs are used in many domains and areas. Their flexibility in open environments made them demanded in multiple daily applications. The history of UAVs dates back when radio controlled drones were developed. They were developed for military purposes and mission sensitive actions. But not until recent decades were available to the public.
UAVs technology witnessed significant evolution throught the years due to the advancements in microchips, sensors, and communication electronic components.
UAVs tend to depend on highly accurate location detection devices such as GPS receivers, or other specific GNSS receivers. Their complex movement and mission travel flights may compromise them, and expose them to malicious entities, with wide range of risks. Since space satellites are governed by different governments there is nothing to do at the satellites ends. But their could be some alternative at the user end.
That is why researchers in different regions of the world are working on solutions and methods to either detect a GPS signal attack or prevent an attack from happening. In the first chapter, we are going to cover UAVs layers and components, As well as the UAV system. We then walk through the localization process and how different techniques are used in position determination and estimation. then we mention real world UAV applications that require accuracy.
In the second chapter, we review security requirements, type of potential attacks and the attacker model. We address some GPS defense mechanisms. We then outline some related research papers that used different approaches and technologies, alongside a summary of the obtained performance results.
In the third chapter, we cover our proposed approach for GPS spoofing attack detection. We propsed a trust system that helps in the decision of attack detection based on evaluation of nearby nodes. Once a detection is confirmed the node stops accepting information from malicious drones.

We finalize the chapter with simulation parameters and environment, as well as discuss the obtained results. We conclude this thesis with summary and some encountered limits as well as future perspective.

Chapter 2

Localization in UAVs Networks

2.1 Introduction

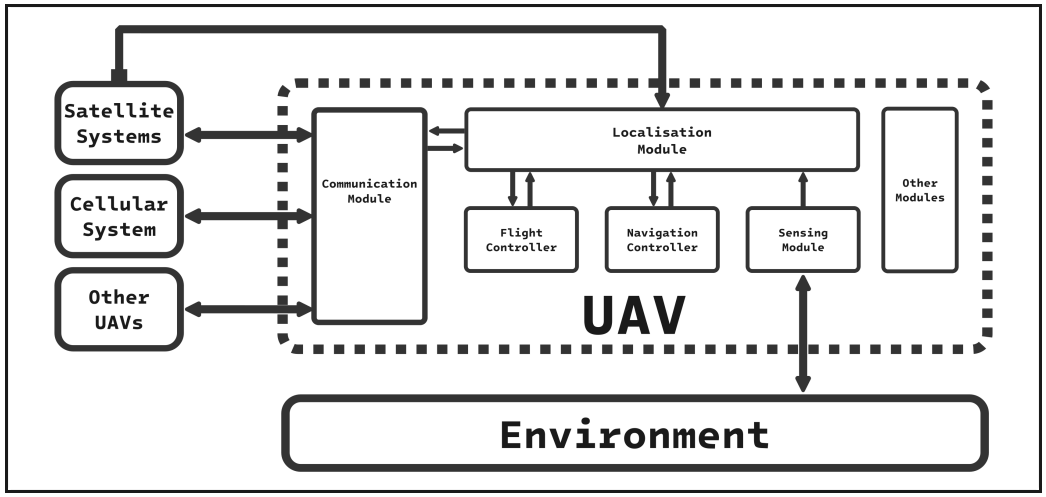
Today, drones also known as unmanned aerial vehicles UAVs are a major flying mobile devices used in multiple fields in a daily basis. It can be part of a network of such nodes (in a swarm or in groups). They can be supplied with additional extension modules to accomplish multitude of tasks, remotly. We begin our chapter by covering the building blocks of UAVs, and the UAV system. then we focus on the different localization techniques, technologies, and systems that are widely known. We finally close this chapter with a wide array of applications where localization is a major criteria.

2.2 UAV Networks

Autonomous drones are a flying vehicles that fly independently in difficult areas where humans can not intervene properly. They operate remotely by following ground base stations commands, or can be charged with specific goals and instructions to fulfill a pre-defined mission successfully.

In this section, we are going to cover the UAV communication system, as well as the other UAV modules that construct the UAV node using Figure 2.1 to demonstrate other UAV components.

Figure 2.1: UAV Layers and Components



2.2.1 Unmanned Aerial Communication System

The Unmanned Aerial System (UAS) building blocks include the UAVs, communication links, and the GCS.

UAV2X is a term used to describe communication between UAVs and other types of devices. It stands for UAV-to-Everything.
UAVs send (or receive) communication signals via UAV2Satellite links, UAV2GCS links, UAV2Cellular links and UAV2UAV links.

The communication module in each UAV is connected with these types of links to provide data exchange with the required entity.

In addition, multiple modules are embedded to provide more functionalities to the UAV.

2.2.2 Communication Modules

The drones are equipped with communication interface(s), with pre-installed protocols and software. This allows them to exchange information both in short and long range, with multiple types of entities.

UAV2Satellite Communication this type of communication is needed by the UAVs where it is difficult to reference (or assume) the current position of the node based on positioning system satellites. This communication medium are used in outdoor environments, where exist signal propogation difficulties.

UAV2GCS Communication this type of communication allows UAVs to exchange control with GCS, and to send periodic reports and/or gathered data during flights.

UAV2Cellular Communication this type of communication is used where long distance communication is needed, and where line of sight signals are of poor quality or does not exist.

UAV2UAV Communication this type of communication allows UAVs to exchange data, control, their current state and relevant information about the UAV group, and the environment.

2.2.3 Sensing Modules

Most of the time, UAVs are equipped with different types of sensors. Generally, it is favorable that each type is multiplied to increase measurement accuracy, and cover as large area as possible. The following are the most used sensors/devices in UAVs :

Image/Video Cameras are used to detect objects, and to avoid them. Data gathered are further processed and transmited for real-time monitoring and footage keeping.

Photoelectric Sensors are composed of photoelectric receivers. The emmitted lights are interrupted by the sensing object, and the reflected light is then received to determine the distance, presence, or absence of nearby objects.

Infrared Sensors (IRs) are mainly used to identify objects in proximity, and wether the surrounding objects are in motion.

Ultrasonic Sensors are based on sound spectrum, and used to measure distance between the node and other objects.

2.2.4 Localization Module

This module is formed by a set of hardware compnents that provides localization for the node. These components can be based on GNSS only, or other localization based technologies. in GNSS based localization module, a receiver is needed to acquire satellites signals and transform them into digital data. As well as filtering noise, and measuring atmospheric pressure to determine altitude.

2.2.5 Other Modules

There exist multiple modules embedded in the UAVs, alongside others that come as an extension and differ from UAV to UAV, and differs based on the mission, and objectives of the UAV network itself.

The most frequently used modules are :

Power Module this module manages the sources of power of the UAV, and monitors voltage, current consumption, battery capacity estimation and power saving.

Flight Controller this module is responsible for controlling the movement of the drone. this module is connected with multiple components such gyroscope, compass, accelerometer, motor controllers and others.

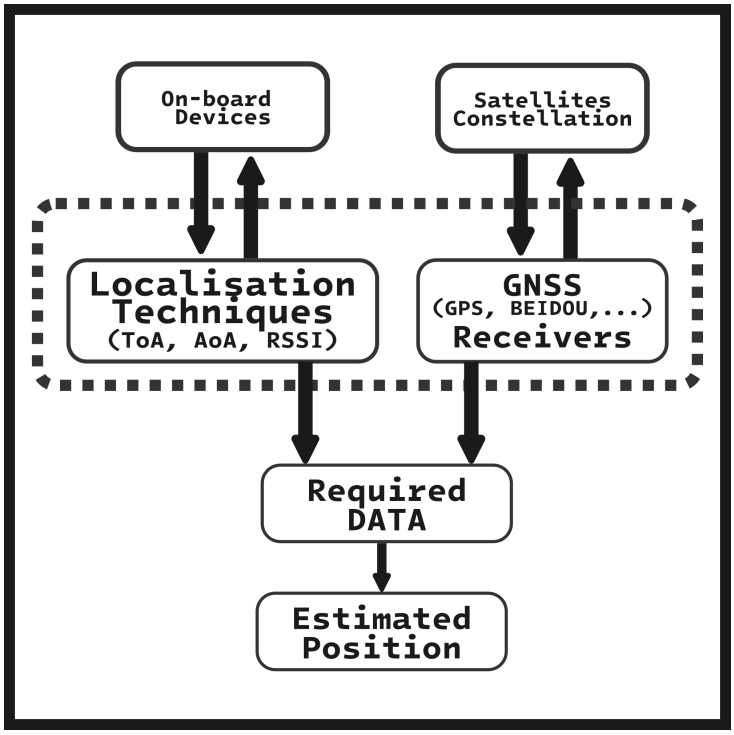
Navigation Controller this module is responsible tracing the right path of controller and desired destination. This module controls other modules for better flight management.

Autopilot Module a module that can be either a software and/or hardware that is based on a pre-programmed flight mission and/or plan.

2.3 Localization Process

As of any calculation system, a required data are needed to proceed to a final estimation phase. Localization process can be summarized in Figure 2.2.

Figure 2.2: Localization Process Layers



2.3.1 Localization Techniques

There exist multiple techniques to determine the distance and/or angle of signal reception in local environment between two nodes. These techniques are used alone or combined to further calculate the estimated (or true) node location. The most known techniques are :

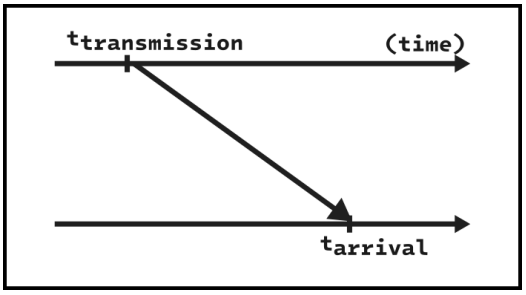
Time of Arrival (ToA)

The ToA of a signal is the true time that took the signal to transmit from a sending node to a receiving node. Figure 2.3 shows this time difference. Where it is used to calculate distance using the formula :

$$D = \Delta t * V$$

.

Figure 2.3: Time of Arrival



Angle of Arrival (AoA)

AoA can determine the position of a node based on received signal angle. This can be accomplished by determining the signal direction using multiple indepent antennas, antenna array or rotation of antenna. This technique works mostly on small range signals or very long signals. Where difference in angles matter. In addition, more antennas are preferable to increase the accuracy of calculation.

Received Signal Strength Indicator (RSSI)

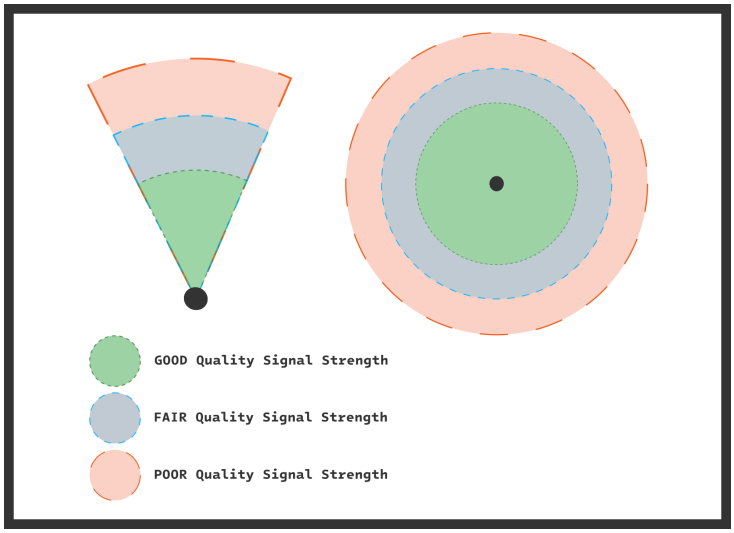
RSSI is presented in the receiver node as the strength of received power. The signal strength is demonstrated in Figure 2.4. This can be calculated using the formula :

$$P_{received} = P_{transmited} * G_r * G_t * \frac{\lambda^2}{(4\pi D)^2}$$

. Where :

- $P_{received}$ the received signal power.
- $P_{transmited}$ the transmited signal power.
- G_r The antenna gain of the receiving device.
- G_t The antenna gain of the sending device.
- D the distance between the two nodes.
- λ is the wavelength of the signal, $\{ \lambda = \frac{C}{f} \}$.
- C is the speed of light.
- f is the signal frequency.

Figure 2.4: Received Signal Strength Indicator



2.3.2 Position Estimation

When enough information gathered by a node about the distance, speed, angles, and poisitions of nearby nodes. Their own position can be calculated using estimation methods. Several estimation methods are used, most known ones are triangulation, trilateration, and other methods.

Trilateration and Multilateration

Trilateration is a used to determine the position of a point using at least three distances between the point of interest and the three known points (also called multilateration if more than three distances are involved). To calculate the position, three circles are needed. The radius of each circle is one of the known distances.

The position is calculated using the following formula :

$$(x - x_1)^2 + (y - y_1)^2 = R_1^2$$
$$(x - x_2)^2 + (y - y_2)^2 = R_2^2$$
$$(x - x_3)^2 + (y - y_3)^2 = R_3^2$$

- $\{ R_i \}$ is the radius of each circle.
- $\{ P_i(x_i, y_i) \}$ is the known position of reference point i.
- $\{ (x, y) \}$ is the position of point of interest.

Triangulation

As trilateration uses distance, triangulation instead uses angles made by the point of interest and other referenced points, where their positions are known. The point of interest and the known two points form a triangle. Let $((x, y))$ be coordinates of the point of interest, and both $((x_1, y_1))$ and $((x_2, y_2))$ be the coordinates for the known points A and B respectively. Let :

$$\theta_1 = \angle ABC$$

$$\theta_2 = 360 - \angle ACB$$

We can write the formula of the slope lines as follows :

$$tan(\theta_1) = \frac{y - y_1}{x - x_1}$$

$$tan(\theta_2) = \frac{y - y_2}{x - x_2}$$

Solving the equations (1) and (2) for x and y, we get :

$$x = \frac{(y_1 - y_2) + x_2 * tan(\theta_2) - x_1 * tan(\theta_1)}{tan(\theta_2) - tan(\theta_1)}$$

$$y = \frac{(y_1 * tan(\theta_2)) - (y_2 * tan(\theta_1)) + (x_2 - x_1) * tan(\theta_2) * tan(\theta_1)}{tan(\theta_2) - tan(\theta_1)}$$

2.4 Localization Technologies in UAV Networks

Every year, new technology evolve and help in motion detection and position estimation. These technologies varies depending on the environment, ranges and accuracy. UAV Networks may deploy multiple types of technologies, and that depends on the equipments of UAVs, and depends on the general purpose (or goal) targted by the mission.

2.4.1 Indoor Localization Technologies

Sometimes, UAVs are deployed in a small area, where distance measurement, and signal propagation are short. That is why low frequency bands are used to locate objects in indoor environments. The following technologies are the generally used.

Radio Spectrum

The radio spectrum, also known as radio frequency, is an electromagnetic wave that travel at the speed of light. This type of spectrum cover the planet and can travel through the atmospheric layers. Beyond the well known purposes for computer networking, audio communications, and video calls. The radio spectrum are also used in various types of applications, including radar for detecting objects, emitting a signal to measure distance and to calculate angles. Their flexibility allows it to move accross objects, breakthrough obstacles and walls.
It spreads between the range of $3kHz$ and $300GHz$.

Optical Lights

The optical technology is now widely used in numerous applications. It is mostly known for the impact added to the Internet, as of optical fiber cables are installed in almost every home, office, and station. this technology involves transmission, detection, and processing light pulses for data communication, sensing, medical imaging, and other tasks, such as motion detection, object detection, and more.

Ultrasonic and Sound Spectrum

Sound is generated with rapid small scale pressure fluctuations, which the human ear can sense most. But different ranges varies in sensitivity than others. Sound can travel faster in more dense mediums, with a velocity of

around 343 m/sec in a standard pressure. As of other technologies, sound is widely used in embedded systems, and widely known for the ultrasonic applications, from ultrasonic cleaning, scanning, ultrasonography, echocardiography and measuring distances and diameters.

2.4.2 Outdoor Localization Technologies

Outdoor environments tend to be wide along with many obstacles, noises, and signal distortion. That is why in these situations wide range and long frequency bands are used. The following technologies are the mostly used.

Cellular Networks

With the increase of mobile device fame and daily uses, more cellular services are being developed. This type of network is widely known, that helps in long range wireless communications, with high speed, high capacity voice and video communication. Its primary uses were for phone calls, user localization, emergency reports.

Global Navigation Satellite Systems

Global Navigation Satellite System, or GNSS, is a term that describes a formation of satellites set up to provide services such as time synchronisation, location determination, and navigation guidance. All these services must be precise, with high accuracy and error toleration. There exist multiple GNSSs. The most globally known is the GPS [14] system governed and deployed by the U.S government. BeiDou Navigation Satellite System [2], or BDS, is a system operated and owned by the People's Republic of China. Galileo [4] owned and operated by the European Union. GLONASS [13] owned and operated by the Russian Federation. and other global navigation systems owned by other regions and nations.

The essential elements that makes the navigation system works are :

Satellites (or Space Vehicles) : Medium-Earth orbit satellites are needed in navigation systems supplied with highly accurate atomic clocks.

Mobile Users : The end user that receives the satellite signals. Usually supplied with low cost internal clock.

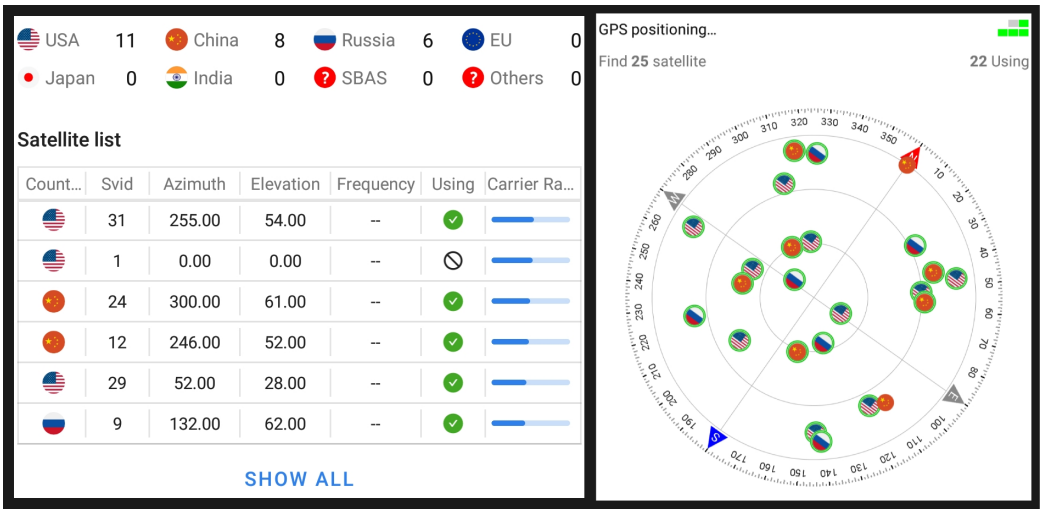
Navigation Messages : These messages transport required information about the satellites, includingg current position in orbit (called ephemeris), time of transmission of the message and information about other available satellites.

Navigation Signals : messages are commonly sent over three channels called the *Lbands*, with a bandwidth of $1575.42Mhz$, $1227.60Mhz$ and $1176.45Mhz$ for L1, L2, and L5 respectively.

PRN Codes : These are well crafted codes that gets inserted as a noise in each satellite signal. These codes helps differentiate between different satellites.

Figure 2.5 is a screenshot taken from [8] that provide mobile users some insights about the nearby detected satellites signals from different satellite constellation.

Figure 2.5: Signal Detector Mobile Application



2.5 UAV Applications based on Localization

The major goal of a UAVs is to be deployed in complex environments, urgent situations, and where accurate actions are necessary. Here we examine the different types of applications that requires three different levels of accuracy.

2.5.1 Low Precision Applications

This type of applications can work fine with low accuracy in localization. Because localisztion is not a high priority for the task run by the drone(s). these applications can be one of the following :

Cinematography : in cinematography drones must be equipped with cameras in order to capture high quality footage. Localization is not critical because the drones does need to state their exact location, but rather move in the environment based on a map or based on referenced objects.

Surveillance Apps : surveillance and monitoring applications can report details on scenes and locations with the help of sensors and cameras. In order for the drones to position in the area by only sensing nearby objects and environment.

2.5.2 Medium Precision Applications

This type of applications does not require high precision localization. drone(s) may frequently check their current position in order to correct errors, and diversions in long routes and paths. these applications can broadly be one of the following :

Land Mapping : is a task where multiple drone(s) can work together to analyze and take pictures of the required area in order to plan the area in 3D or 2D maps. Land mapping can require somehow a medium accuracy in order to create a map that is almost real.

Package Delivery : to deliver packages, routes must be known as well as the speed, and position of the drone in order to report delay, traffic and collisions. Approximate positioning can accomplish the delivery service, but high accuracy and periodic localization are preferable constraints.

2.5.3 High Precision Applications

For public safety cases, disaster, and emergency situations precision is a must. These urgent applications needs to be handled rapidely with low rate of errors and accidents. Drones are deployed in order to analyze, and forecast the source of threat (in case of fire), and send accurate exchange accurate information with the concerned authorities. the number of these applications is tremendous, but the most sensitive ones are :

Medical and Emergency: because UAVs are so flexible in complex environments, this versatility makes them valuable for delivering critical supplies and saving lives. They can offer exciting help services such as rapid delivery of aids, search, rescue, communication restoration, and more. All these services requires high precision of navigation and positioning information.

Military Defense: in the military field, military drones are extensively used for gathering intelligence on enemy positions, troop movements, and potential threats. In addition, they are used to provide precision for targeted strikes against enemy combatants, bomb disposal, mine detection and border patrol. Therefore, errors in localization may cause serious damage.

2.6 Conclusion

The capabilities of UAVs are rapidly evolving, driven by advancements in microchips, hardware technologies, software solutions as well as newly created protocols. Given their critical role in various systems, they must be designed with high precision to minimize errors and maximize reliability. considering factors such as safety, reliability, and security. Ongoing research and development will be crucial for addressing challenges and ensuring the continued growth and innovation of UAV technology.

Chapter 3

Security Threats and State of Art

3.1 Introduction

Driven by growing security concerns, UAV networks have emerged as a prominent area of research, particularly regarding security applications and threats. Vulnerabilities in localization and navigation systems are a key area of investigation. In this chapter, we delve into the evolving security requirements, potential attacks, and defense mechanisms specifically designed for localization in a UAV network. Then we cover previous works, latest and related research papers and compare the different mechanisms used in each paper.

3.2 Localization Security in UAV Networks

UAVs are vulnerable to many types of attacks. Our main concern in this section are the security risks driven by malicious attacks and errors in navigation and localization of nodes.

3.2.1 Security Requirements

To ensure low number of risks and minimal security concerns, our network needs to satisfy multiple requirements. These requirements depend on a variety of factors, such as the type of data being exchanged, industry regulations, organization's risk tolerance and the sensitivity of the planned mission.

Confidentiality: is about protecting sensitive data from access, modification,

destruction and compromise by unauthorized users (or nodes). The confidentiality of a network system can be compromised by inside threats coming from nearby nodes, or can be due to malicious attacks targeting GPS signals or exchanged messages.

Integrity: is about ensuring the accuracy of data and its reliability. Information integrity is a must for decision making and maintaining trust especially for autonomous systems. In order for UAVs to take actions, and perform at full capacity, satellite navigation signals must be accurate and trustworthy.

Availability: is needed so that authorized nodes (or users) can access data and messages completly whenever they need it. This helps the sustainability of the system, fully operational and functioning properly when required. The GPS signal must be available at any required moment, with ease of access.

Non-Repudiation: is used to prevent nodes from denying their actions, behavior, the release and reception of certain information. This strengthens accountability of each node for their actions within the system, reducing security incidents that may occur.

3.2.2 Types of Attacks

Before we dive into the details of the attacker mechanisms and tools that thargets UAVs. We should discuss the number of threats a drone or a UAV swarm might encounter. UAVs are exposed to multiple attacks. The most common threats are :

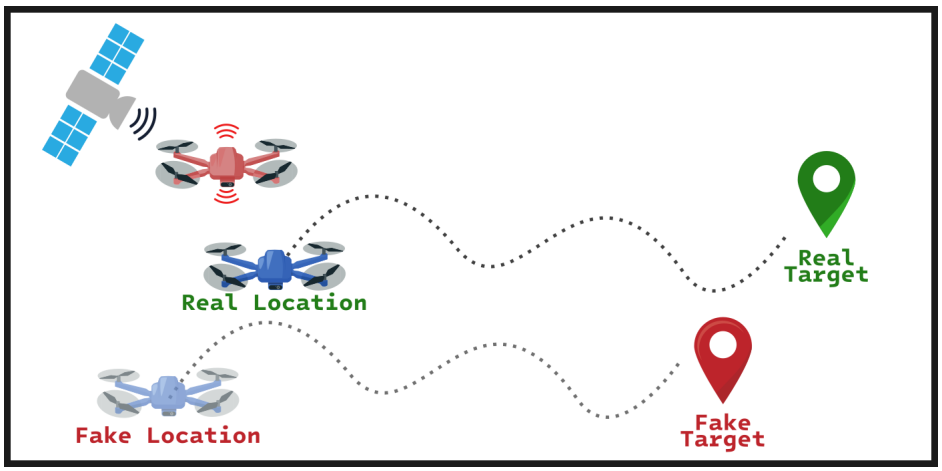
Physical Attacks: these tactics often involve specialized equipment or exploiting the drone's physical limitations and showcase a more direct approach to disrupting or destroying them.

Data-Interception Attacks: a major threat is data interception. These attack includes eavesdropping and key logging, Which is the exploit of the reliance of wireless communication channels beetween UAVxGCS and/or UAVxUAV to gather and steal private information and reports exchanged during flights and missions. This stolen data could be anything from high-resolution video footage used for surveillance, to sensitive information like infrastructure layouts, security protocols, flight control data, command and control signals and can be sensitive reports.

Data-Manipulation Attacks: such as GPS spoofing attacks, message injection, deletion and modification. The main purpose of this type of attacks is to hijack and take control of the UAVs in the system, the deception of targets, locations, flights and alter the overall system integrity. an example is shown in Figure 3.1.

Disruption and Denial-of-Service (DoS) Attacks: these attacks neutralize a drone's ability to function or transmit data, affecting its mission or creating safety hazards. they exploit vulnerabilities in the communication channels. These attacks can be radio frequency jamming, GPS signal jamming/spoofing and disrupting the network communication. These attacks can lead to loss of control, crashing, collisions, communcation weakness and multiple denial of services.

Figure 3.1: GPS Spoofing Attack

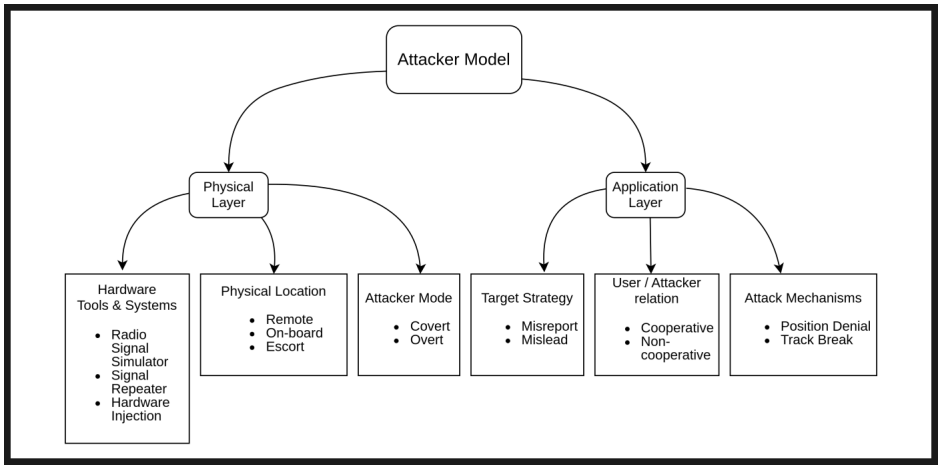


3.2.3 Attacker Model

From the attacker perspective, he can launch attacks with specific objectives, modes, strategies using a multiple choice of hardware and software tools that are freely available or available at reasonably low cost budget.

The diagram in Figure 3.2 demonstrates the attacker model layers and modes.

Figure 3.2: Attacker Model Diagram



Hardware System: different systems are used to generate fake signals, such as repeaters to capture legitimate signal and alter it, simulators to simulate GPS signals or hardware injection systems to fraud and misreport.

Attacker Location: the attack may be initiated in three different locations. Either "on-board" with other UAVs, in which we call the attacker as a malicious UAV, "escort", in which the attacker is nearby, following the target or remotly at a distance covering a well known area. These locations are shown in Figure 3.2.

Attacker Modes: the attacker can initiate the attack with caution of being detected or launching a sever attack with triggering different detection mechanisms.

User/Attacker Relation: in case of an attack with on-board malicious UAVs. The attacker may be cooperative – exchange messages with other nodes, or non-cooperative – without exchanging data with other nodes not even fake data.

Attack Mechanisms: these mechanisms are chosen in order depends on the objective and target strategy.

Target Strategy: which is the final objective of the attack is either to mislead the UAV or misreport to other UAVs and to the whole system.

3.2.4 GPS Defense Mechanisms

In order to prevent being attacked, or to identify situation before or in case of an attack. Several mechanisms and technologies are employed. These latter can be combined together in order to enhance the system and avoid malicious activities. The following are the major categories used for GPS defense mechanisms :

- Using Onboard Devices.
- Game Theory Methods.
- Machine/Deep Learning Based Methods.
- Received Signal Processing.

3.3 State of the Art

A quite number of research studies have explored the potential consequences of GPS signal manipulation on UAV missions and on UAV behavior. Additionally, these studies have conducted experiments using diverse detection techniques and technologies for the sake of proposing a solution that identifies malicious attempts and distinguish them from unintentional errors. In this part, we cover multiple performance metrics that are crucial for evaluationg these systems. As well as a short comparison of the performance of some related works.

3.3.1 System Metrics

This section details the performance metrics and indicators that are used to evaluate the effectiveness of a proposed system.

System Parameters

The following are some of parameters and constraints that could be monitored by a detection system :

- Received power of GPS signal.
- GPS signal noise.
- False Data exchanged by cooperative UAVs.

- SatelliteToUAV and UAVToUAV Distances.
- Transmission range.
- Number of detected drones by onboard devices/sensors.

Performance Metrics

The following are the performance metrics used in final results for analysis and comparison :

True Positive represents the number of attacks correctly identified by the system.

True Positive Rate (TPR) is the ratio of the true positive value to the total number of attacks made against the system.

False Positive represents the number of non-attacks incorrectly identified as attack cases by the system.

False Positive Rate (FPR) is the ratio of the false positive value to the total number of non attack cases.

False Negative represents the number of attacks not identified by the system.

False Negative Rate (FNR) is the ratio of the false negative value to the total number of attacks made against the system.

True Negative represents the number of non-attacks not considered by the system.

True Negative Rate (TNR) is the ratio of the false negative value to the total number of non-attack cases.

System Accuracy represents the overall correctness of the system, which is the ratio of correct predicitions to the total number of cases, $Accuracy = (Tp + Tn)/(Tp + Fp + Tn + Fn)$.

Detection Latency represents the time difference from when the attack was initiated to the time when the attack was succesfully detected

3.3.2 Comparison Of Realted Work and Results

In this section, we provide a brief review of some related works and their results. These studies have chosen a specific technology and/or mechanisms to enhance the detection process, through monitoring and analysing different parameters throughtout the experiments.

[9] proposed an approach for true position estimation of an UAV in case of a GPS signal spoofing attack. Their solution is based on hypothesis method and real trajectory is estimated during spoofed situations. The method used Particle Swarm Optimization Filter (PSOF), the experiences of each particle is compared with those of neighbors for trajectory estimation. The system reached 97% of accuracy in positioning.

[7] proposed a method to GPS spoofing attack detection and mitigation at the level of UAV receiver using Receiver Autonomous Integrity Monitoring (RAIM) schemes. The fake satellite signal is compared with other satellite signals in three groups for fraud satellite detection and isolation. The simulation was conducted using OMNet++ and using a GPS model called UAVSim.

[10] proposed a method using artificial intelligence that employs a machine learning classification model that classifies GPS signals based on Signal-to-Noise ratio, Doppler Shift and pseudo-range. The authors used real life GPS signals and created a repeated fake signals. The model training were based on the gathered GPS data. The method exceeded 98.2% of accuracy and 99.4% of detection rate.

[1] proposed a detection solution for UAV networks modeled as Bayesian Networks, while monitoring and analysing different GPS signal characteristics including (Signal-to-Noise ratio, Doppler Shift and pseudo-range, etc.). and comparing with the estimation of the conditional probability in the Bayesian Networks. The results reached 96.2% of detection rate.

[12] proposed a detection method based on Support Vector Machine Model, which is one of the famous classification algorithm used in anomaly detection. The model is trained with normal cases experiments, so that it decision boundary for future deviation detection in abnormal cases. The method achived a latency of $30s$ of detection latency.

[3] proposed a method based on statistical analysis and artificial neural network, the Multilayer Perceptron model that is trained with multiple path

loss parameters (probability distribution difference, quartile and moment). The MLP defines specific threshold value for the path loss between base station and UAV. The actual path loss is compared with a theoretical path loss, if the difference exceeds the threshold an attack is detected. The proposed method achieved a detection rate of 93%.

The following table 3.1 is a summary of the preformance obtained in the previously discussed works.

Table 3.1: Performance Comparison Table of Related Works

Article	Goal	Technology	Techniques/Parameters	Used Tools	Results
[9]	Detection and Mitigation	Onboard Sensors and Devices	Particle Swarm Optimization Filter (PSOF)	Matlab	97% Accuracy
[7]	Detection and Mitigation	Radio and GPS Signal Processing	RSSI and Triangulation	OMNet++ using UAVSim	Latency ($90s$)
[10]	Detection	Machine Learning	SNR Classification	RTKLIB	99.4% Detection Rate
[1]	Detection	GPS Signal Processing	Signal-to-Noise Ratio, Doppler Shift monitoring	MATLAB	96.2% Accuracy
[12]	Detection	Machine Learning	Support Vector Machine (SVM) Model	MATLAB	Latency ($30s$)
[3]	Detection	Machine Learning	Multilayer Perceptron (MLP) Model	Python and TensorFlow	Detection Rate 93%

3.4 Conclusion

The availability of GPS signals makes them vulnerable to spoofing attacks. That is why it has become a research trend in the past couple years. This chapter has provided an overview of existing research on GPS spoofing detection for UAVs, covered attacker models, detection techniques and summarized

some potential solutions.

Chapter 4

Our Contribution

4.1 Introduction

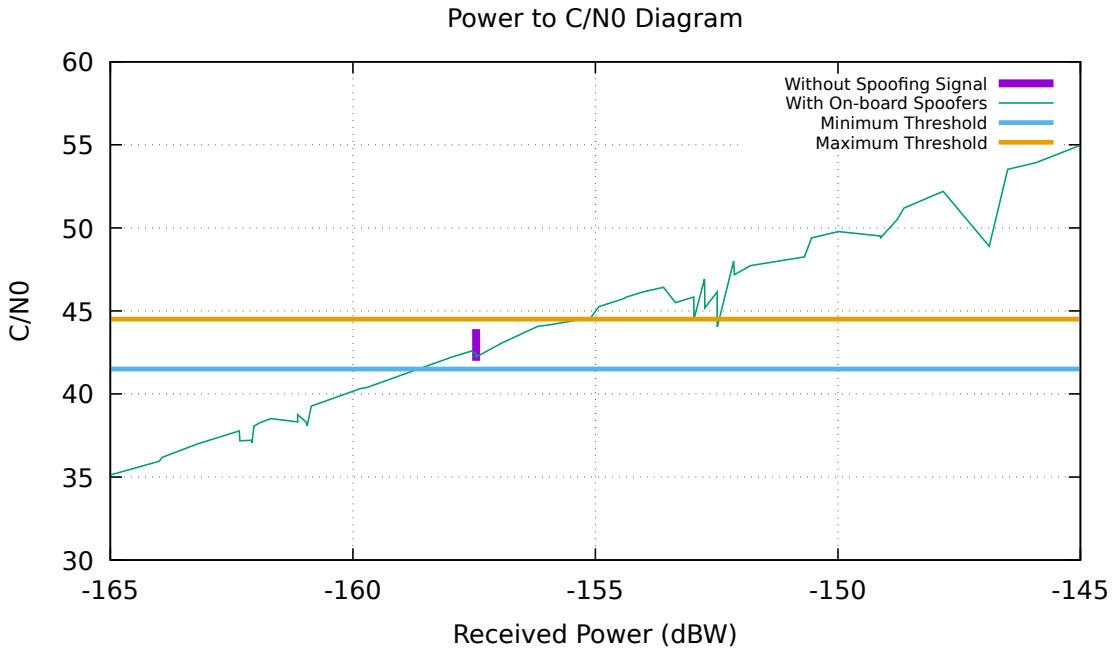
In addition to traditional satellite-based data, incorporating UAV-specific features and advanced data analysis techniques can significantly enhance GPS attack detection. These features enable UAVs to contribute to data collection and mission accomplishment but also grant them the ability to defend against GPS attacks and potentially identify the attacker's location and/or model. In this chapter we are going to propose an approach that benefits from satellite received data, as well as data gathered by nearby UAVs.

4.2 Proposed Solution

Our solution monitors GPS signal power and C/N0 for each PRN code. A minimum and maximum thresholds need to be assigned for Carrier-to-Noise ratio and for GPS signal strength to differentiate beetween signal error and possible attack case as shown in Figure 4.1. When abnormal activity or fluctuations are detected, we initiate a trust system based on nearby nodes that exchange information and position to enhance detection rate and confirm attacks.

Carrier-to-Noise Ratio is a measure of signal quality in wireless communication systems. It is the ratio of the power of the desired signal to the power of the noise interfering with it.

Figure 4.1: Power to C/N0 Diagram



4.2.1 Attacker Perspective

The attacker model taken into consideration is an attacker that has an on-board UAVs that fly alongside the victims. The data exchanged with malicious drones – needed parameters for the trust system, might be inaccurate data and probably corrupted data. That is why each received parameter is normalized and checked carefully for the sustainability of the trust system. The attacker may alter the exchanged distance, or the transmission power, as well as faking their own position. That is why in this proposed method we tried to incorporate all these constraints and carefully choose the paramters that should be exchanged.

4.2.2 Trust Model

The proposed model is a Reputation-Based Trust Model that assigns to different nodes in the system a specific "worthiness" (value/level) based on past/present behavior. the nodes in our trust model are nearby UAVs that cooperate and interact throught the mission and the evaluation process. The parameters taken into account are : received signal strength, received position and an approximated distance acquired when the sending node transmits

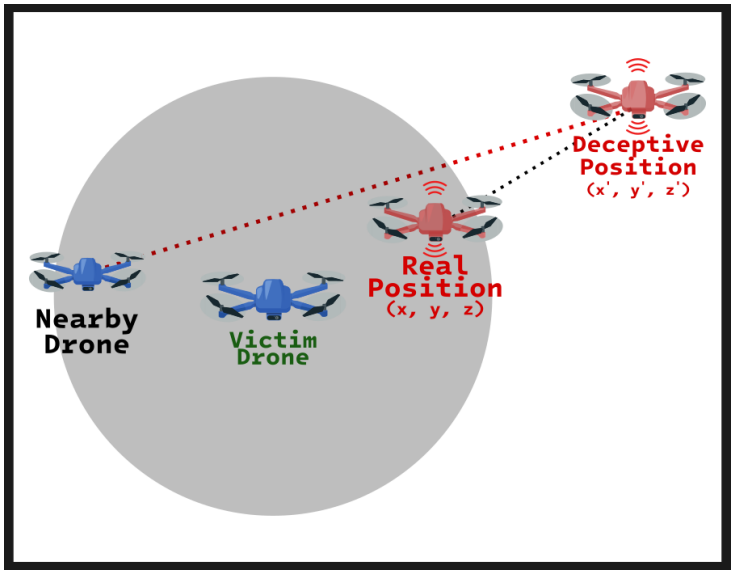
an estimated distance, while the receiving node calculates the equivalent distance based on the received signal strength. The weighted average formula can calculate the average values of different input parameters.

We then can assign a threshold, a lower bound of the trust level. That will be used for final decision of the authenticity of the node.

The evaluation starts after the reception of data from nearby nodes. Once we receive the data, we start the normalization process of the parameters. We compare them with the maximum possible value.

We use the *ApplyPositionCheck* method that checks for the integrity of the position provided by sending node. This latest checks abnormal fluctuations in previous stored positions, as well as the distance between the position provided and positions of neighboring nodes. If we find that the distance is greater than two times the maximum node range, that means one of the positions provided might be a deception. Figure 4.2 illustrates this scenario.

Figure 4.2: Check Position Integrity



After the normalization process is succefully executed, we move to the evaluation process of each node and calculate the trust level.

A full version of the simulation code can be found in [6]. The evaluation process keeps executing repeatdly between nodes, until a malicious node is detected and the GPS spoofing attack is detected. If their is no attack the system keeps accepting information only from nodes that exceeds the lower threshold of the trust system.

4.3 Execution Environment

This section specifies the environment in which our simulation was conducted. We present simulation software, the environment parameters and the hardware gear.

4.3.1 Execution Hardware

We used for our simulation a desktop computer for the ease of simulation and rapid execution time. Table 4.1 summarizes the technical specifications of the machine.

Table 4.1: Hardware Machine Specifications

Machine Type	Desktop
CPU	AMD Ryzen 5 5600G
RAM	16 GigaBytes
Operating System	Ubuntu 22.04.4 LTS
Operating System Type	64 Bits

4.3.2 Simulation Software and Tools

For the experiments and performance statistics we used different software solutions that are available either offline and online. The following are the major softwares and tools used :

NS3 Simulator [11] is a discrete event simulator widely used in the academic and industrial communities to model and analyze complex network systems. It's particularly valued for its flexibility and ability to simulate a broad range of protocols and network topologies. NS3 is free, open-source software, licensed under the GNU GPLv2 license, and maintained by a worldwide community.

GNUPlot [5] is a portable command-line driven graphing utility for Linux, OS/2, MS Windows, OSX, VMS, and many other platforms. It was originally created to allow scientists and students to visualize mathematical functions and data interactively, but has grown to support many non-interactive uses such as web scripting. It is also used as a plotting engine by third-party applications like Octave. Gnuplot has been supported and under active development since 1986.

4.3.3 Simulation Parameters

The initial paramaters used in the NS3 environment are listed in Table 4.2.

Table 4.2: NS3 Environment

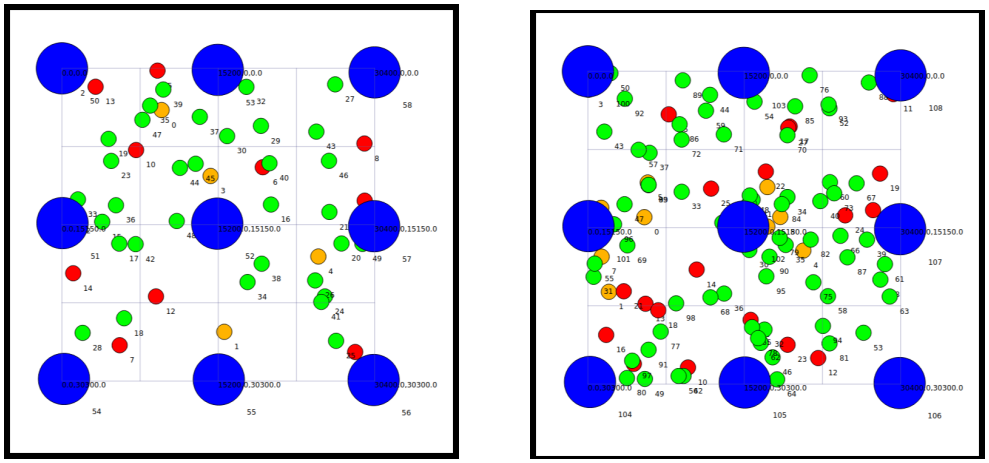
Parameter	Value
Simulation Area L x W x H	(30 x 30 x 2) KM
Number of Satellites	9 Satellites
Satellite Power Max Threshold	-156dBW
Carrier-to-noise Ratio Threshold	[42, 44]
Number of UAVs	50 / 100 nodes
Node Transmission Range	1000 / 3000 meters
Transmission Power	2dBm
Propagation Model	Line of Sight
Delay Model	Constant Speed Propagation Delay Model
Node Mobility	Random2DWalk Mobility Model
Speed	[0 to 20] m/s
Number of Malicious UAVs	20%
Number of Victim UAVs	10%

The parameters of the trust model is specified in Table 4.3

Table 4.3: Trust System Parameters

Parameter	Value
Parameter 1	Difference in Distance between Received Distance and Calculated Distance
Weight 1	20%
Parameter 2	Received Position
Weight 2	20%
Parameter 3	Received Distance
Weight 3	20%
Parameter 4	Received Signal Power
Weight 4	40%
Parameter 5	Calculated Evaluation
Weight 5	10%
Parameter 6	Previous Trust Level
Weight 7	90%
Minimum Threshold	25%

The nodes distribution in the system for both 50 nodes and 100 nodes, respectively, are shown in Figure 4.3. The satellites are represented with the blue color, malicious nodes with the red color, victim nodes with the orange color and normal nodes with the green color.



(a) 50 Nodes (b) 100 Nodes

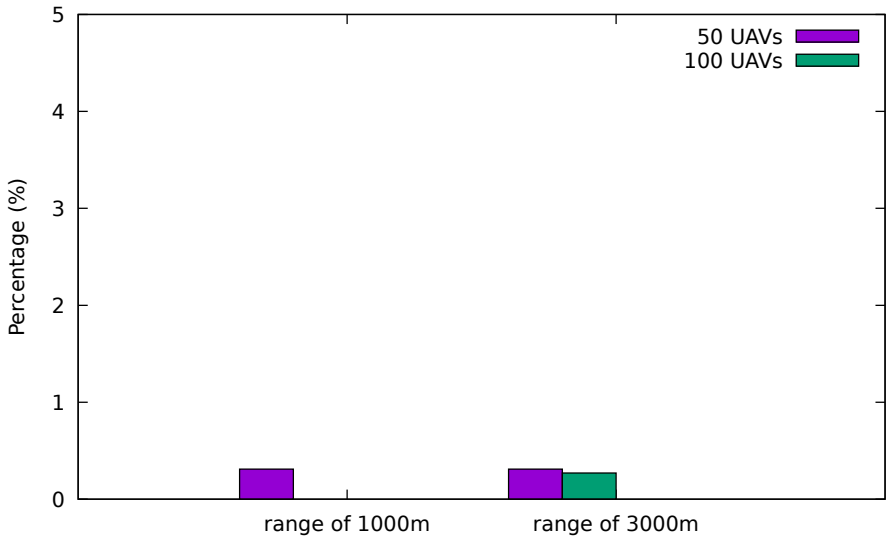
Figure 4.3: Node Distribution in Netanim

4.4 Performance Results

For detailed system analysis of obtained results, we have exported the False Negative rate, False Positive rate, True Positive rate and True Negative rate, as well as the total calculated accuracy of the overall nodes in the system presented by two specific node ranges (1000 meters and 3000 meters).

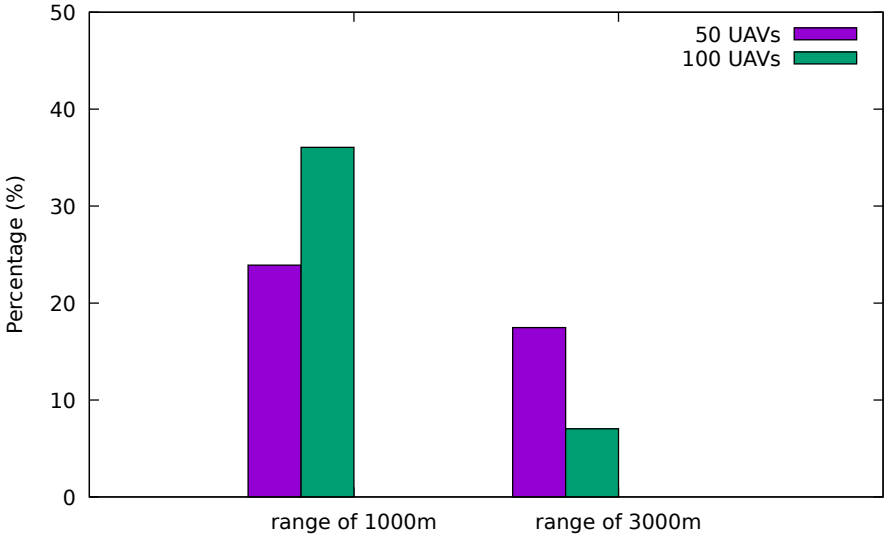
As shown in Figure 4.4. The numbers of attacks not detected against the system in both specified node ranges, did not exceed 0.5% of the overall cases. This result shows us that the system effectively filters out attacks, preventing them from influencing position calculations, which at most can lead to a slight deviation in node routes and can be corrected over time.

Figure 4.4: False Negative Percentage



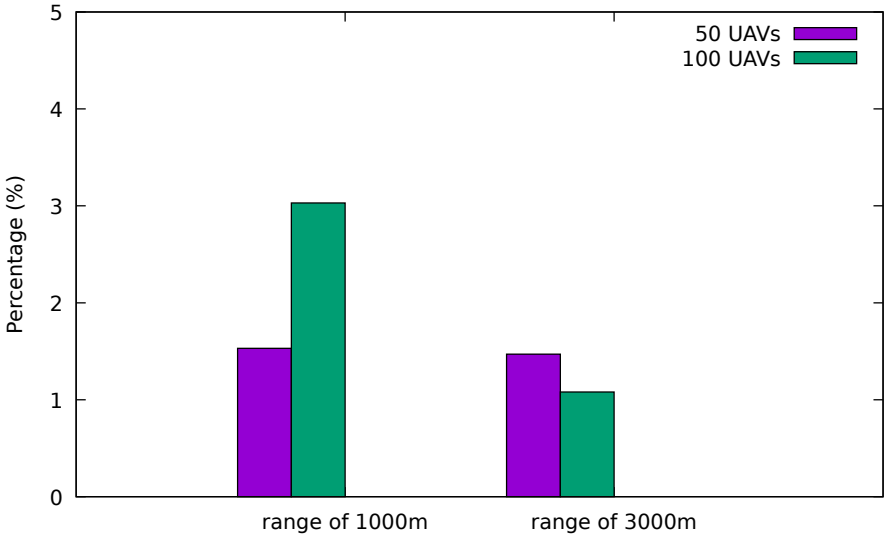
However, the False Positive rate shown in 4.5 shows that the system is filtering non attack cases as if they were attacks. The rate is reduced by switching to wide range of 3000 meters which obviously helps the nodes in communicating with wide range of nearby UAVs. and that reduced the faulty non attack cases filtering. By both increasing the range and number of UAVs, we were able to reduce the error rate to below 10%.

Figure 4.5: False Positive Percentage



For the the attacks correctly detected as illustrated in Figure 4.6, and compared with Figure 4.4. It was possible to detect attacks with an average rate of 80% of the overall only.

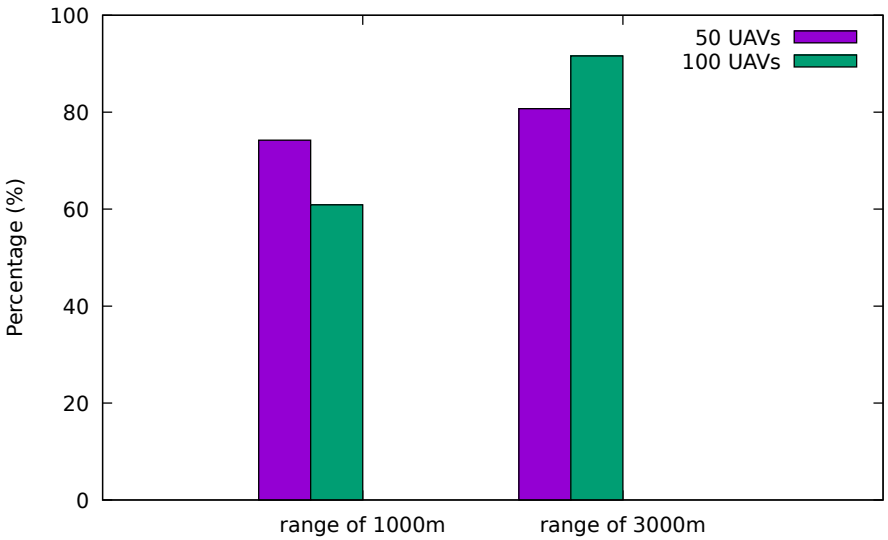
Figure 4.6: True Positive Percentage



As for the rest of non-attack cases, Figure 4.7 demonstrates that trust is sustained between legitimate nodes. and compared with the previous False

Negative rate. We can deduce that a wide communication range between nearby nodes can influence significantly the node trust system and increase the true negative of total cases.

Figure 4.7: True Negative Percentage



Finally, for Figure 4.8. The system can attain higher accuracy with either higher communication range or and increased number of deployed drones. More deployed nodes and higher communication ranges are preferable to guarantee a dependable accuracy rate of the overall system. As shown in Figure 4.9, Increased adjacency and receiving capabilities among nodes lead to a higher volume of packet exchange.

Figure 4.8: Accuracy Percentage

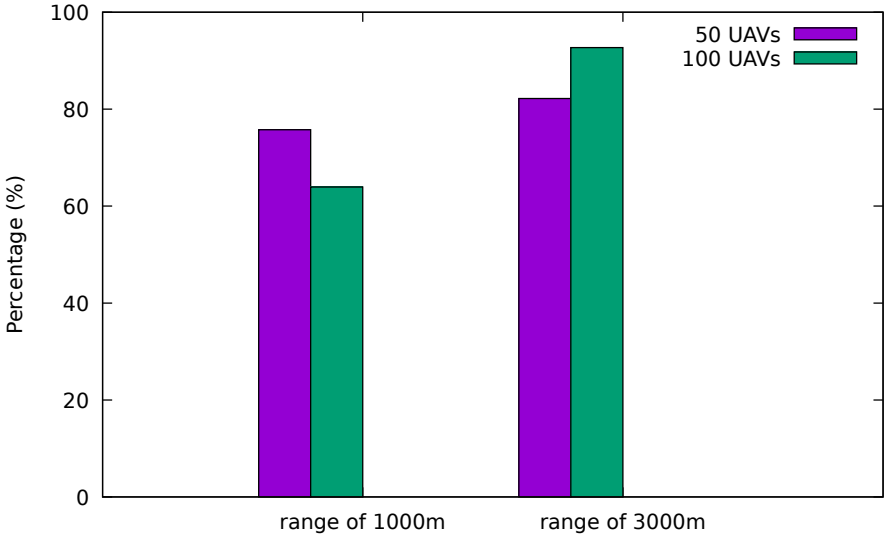
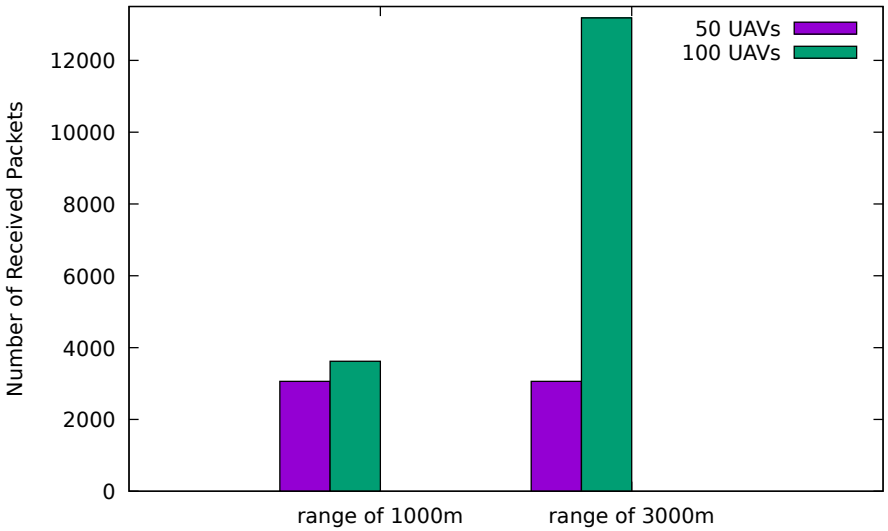


Figure 4.9: Received Packets



4.5 Conclusion

This chapter concluded our proposed method and performance results in the detection of GPS signal attack. The proposed approach can benefits UAVs due to its simple calculations and may reduce battery consumption compared

to intensive computational methods. Although it has limitations for smarter attack cases, where the attacker takes good manner mode then change it to attacker mode.

Chapter 5

Conclusion and Future Perspectives

5.1 Summary of our Work

In this work we presented the UAVs and its different aspects, then we also presented the different localization methods commonly known and different technologies used in localization. We summarized related work in the detection of GPS spoofing attacks. and their performance results. We proposed a trust system to enhance decision making in our simulation of GPS spoofing attacks and finally we presented a simulation of our approach alongside a discussion to analyse the impact and contribution

5.2 Future Perspectives

As a future proposition, we would combine trust system with other techniques for efficient data filtering and normalization. The inclusion of additional sensitive parameters is crucial for optimizing performance and achieving optimal results.

Bibliography

[1] A. Sabitha Banu and G. Padmavathi. *Taxonomy of UAVs GPS Spoofing and Jamming Attack Detection Methods.*, pages 167–201. Springer International Publishing, Cham, 2022.

[2] ChineseGovernment. Beidou navigation satellite system. Last accessed 16 September 2024.

[3] Yongchao Dang, Chafika Benzaïd, Bin Yang, and Tarik Taleb. Deep learning for gps spoofing detection in cellular-enabled uav systems. In *2021 International Conference on Networking and Network Applications (NaNA)*, pages 501–506, 2021.

[4] GalileoGNSS. Galileo — european global navigation satellite system. Last accessed 16 September 2024.

[5] GNUPlot. Gnuplot homepage. Last accessed 16 September 2024.

[6] Tahar ISSAAD. Ns3 simulation code. Last accessed 19 September 2024.

[7] Ahmad Y Javaid, Farha Jahan, and Weiqing. Sun. Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation. *SIMULATION: Transactions of The Society for Modeling and Simulation International*, 93:427–441, 2017.

[8] LefanCoLtd. Signal detector app. Last accessed 16 September 2024.

[9] Mohammad Majidi, Alireza Erfanian, and Hamid Khaloozadeh. A new approach to estimate true position of unmanned aerial vehicles in an ins/gps integration system in gps spoofing attack conditions. *International Journal of Automation and Computing*, 15:747–760, 2018.

[10] Mohsen Riahi Manesh, Jonathan Kenney, Wen Chen Hu, Vijaya Kumar Devabhaktuni, and Naima Kaabouch. Detection of gps spoofing attacks

on unmanned aerial systems. In *2019 16th IEEE Annual Consumer Communications and Networking Conference (CCNC).*, pages 1–6, 2019.

[11] NS3. What is ns-3. Last accessed 16 September 2024.

[12] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè. A svm-based detection approach for gps spoofing attacks to uav. In *2017 23rd International Conference on Automation and Computing (ICAC)*, pages 1–11, 2017.

[13] RussianGovernment. Glonass navigation satellite system. Last accessed 16 September 2024.

[14] USGovernment. Gps navigation satellite system. Last accessed 16 September 2024.