



Universidade de Vigo

Trabajo Fin de Máster

Evaluación de nivel de amenaza asociado a aviones no tripulados intrusos

Luis Enrique Arias Curbelo

Máster en Técnicas Estadísticas

Curso 2022-2023

Propuesta de Trabajo Fin de Máster

Título en galego: Avaliación do nivel de ameaza de drones intrusos
Título en español: Evaluación de nivel de amenaza asociado a aviones no tripulados intrusos
English title: Intruder unmanned aircrafts threat level assessment
Modalidad: Modalidad B
Autor/a: Luis Enrique Arias Curbelo, Universidad de Vigo
Director/a: Marta Sestelo Pérez, Universidad de Vigo
Tutor/a: Silvia Abalo Bóveda, Gradiant
Breve resumen del trabajo: En este trabajo se propone un modelo de asignación de amenaza a aviones no tripulados intrusos y se implementa un módulo que procesa información de tráfico aéreo proveniente de diferentes sensores y asigna un nivel de amenaza a los tráficos intrusos.

Doña Marta Sestelo Pérez, Profesora Ayudante Doctora de la Universidad de Vigo y doña Silvia Abalo Bóveda, Ingeniera-Investigadora Senior de Gradiant informan que el Trabajo Fin de Máster titulado

Evaluación de nivel de amenaza asociado a aviones no tripulados intrusos

fue realizado bajo su dirección por don Luis Enrique Arias Curbelo para el Máster en Técnicas Estadísticas. Estimando que el trabajo está terminado, dan su conformidad para su presentación y defensa ante un tribunal.

En Vigo, a 29 de junio de 2023.

La directora:
Doña Marta Sestelo Pérez

La tutora:
Doña Silvia Abalo Bóveda



El autor:
Don Luis Enrique Arias Curbelo

Declaración responsable. Para dar cumplimiento a la Ley 3/2022, de 24 de febrero, de convivencia universitaria, referente al plagio en el Trabajo Fin de Máster (Artículo 11, [Disposición 2978 del BOE núm. 48 de 2022](#)), **el/la autor/a declara** que el Trabajo Fin de Máster presentado es un documento original en el que se han tenido en cuenta las siguientes consideraciones relativas al uso de material de apoyo desarrollado por otros/as autores/as:

- Todas las fuentes usadas para la elaboración de este trabajo han sido citadas convenientemente (libros, artículos, apuntes de profesorado, páginas web, programas, . . .)
- Cualquier contenido copiado o traducido textualmente se ha puesto entre comillas, citando su procedencia.
- Se ha hecho constar explícitamente cuando un capítulo, sección, demostración, . . . sea una adaptación casi literal de alguna fuente existente.

Y, acepta que, si se demostrara lo contrario, se le apliquen las medidas disciplinarias que correspondan.

A mi esposa.

Agradecimientos

A los amigos que hice en Vigo por hacerme la estancia amena.

Índice general

Resumen	xiii
1. Introducción	1
1.1. Gradient	2
1.2. Problema	3
2. Fundamentos teóricos	5
2.1. Modelos de asignación de amenaza	5
2.1.1. Modelos basados en distancia	7
2.1.2. Modelos basados en tiempo	9
2.2. Fuentes de incertidumbre	11
3. Modelo mixto de asignación de amenaza	15
3.1. Generación de trayectorias	15
3.2. Función de amenaza	16
3.2.1. Función lineal truncada	17
3.2.2. Función exponencial decreciente	17
3.2.3. Comparación entre funciones de amenaza	18
3.3. Asignación de un nivel de amenaza	19
4. Problema práctico	23
4.1. Materiales y métodos	23
4.2. Implementación del módulo de asignación de amenaza	24
4.2.1. Arquitectura	25
4.2.2. Funcionalidades	25
4.3. Experimentación	26
4.3.1. Prueba 1: Funcionamiento	27
4.3.2. Prueba 2: Rendimiento	29
5. Conclusiones	31
5.1. Líneas de trabajo futuras	32
A. Gráficas de las simulaciones de la Sección 4.3.1	33

Bibliografía

49

Resumen

Resumen en español

En escenarios de espacio aéreo compartido entre vuelos tripulados y no tripulados, el riesgo de que una aeronave intrusa pueda ocasionar un peligro a otros vuelos o a estructuras en tierra es mayor, por lo que surge la problemática de proporcionar información complementaria a los controladores de tráfico aéreo que pueda facilitar su reacción ante posibles aeronaves que supongan un peligro.

En este trabajo se propone un modelo de asignación de amenaza a aviones no tripulados intrusos y se implementa un módulo que procesa información de tráfico aéreo proveniente de diferentes sensores y asigna un nivel de amenaza a los tráficos intrusos.

English abstract

In shared airspace scenarios between manned and unmanned flights, the risk that an intruder aircraft could cause a danger to other flights or to structures on the ground is greater. That is why the problem of providing complementary information to air traffic controllers to facilitate their reaction to possible aircraft that pose a danger arises.

This thesis proposes a threat assignment model for intruder unmanned aircraft and a module that processes air traffic information from different sensors and assigns a threat level to intruder traffic is implemented.

Capítulo 1

Introducción

Las operaciones civiles de vehículos aéreos tripulados y no tripulados en espacios aéreos no segregados anticipan grandes expectativas tanto en el terreno económico como en el social. Sin embargo, para alcanzar tal objetivo es necesario afrontar una serie de retos tecnológicos, operativos y regulatorios que garanticen la seguridad, tanto de las aeronaves, como de la población e infraestructuras en tierra.

A lo largo de la última década, los avances tecnológicos en la industria de los sistemas de aeronaves no tripuladas (UASs, del inglés *Unmanned Aircraft Systems*) han habilitado el desarrollo de nuevos modelos de negocio e incrementado extraordinariamente su demanda de operaciones, especialmente de aquellas que tienen lugar en espacio aéreo a muy baja altitud, donde las operaciones de aeronaves tripuladas convencionales están generalmente restringidas o limitadas. Además, se espera que dicha demanda siga creciendo enormemente en los próximos años, por lo que cada vez es más necesario abordar el problema de la integración de este tipo de tráfico en el espacio aéreo actual. Para más información sobre las últimas tendencias en el uso de aeronaves no tripuladas puede consultarse [Herrera et al. \(2017\)](#).

En este sentido, la utilización del modelo tradicional de gestión de tráfico convencional (ATM, del inglés *Air Traffic Management*), en el que el humano está en el epicentro de la toma de decisiones, se ha demostrado como inviable e ineficiente en un contexto de alta densidad de tráfico dentro de un entorno operacional pequeño con una altísima heterogeneidad de operadores (desde entrega de paquetería o vigilancia hasta transporte de pasajeros). En consecuencia, con la finalidad de satisfacer dicha demanda y garantizar operaciones seguras y eficientes, se están llevando a cabo numerosas iniciativas internacionales que buscan la implantación de un sofisticado sistema digital capaz de complementar y, llegado el caso, sustituir al humano. Este sistema se conoce mundialmente con el nombre de UTM (del inglés *UAS Traffic Management*)/U-space.

El sistema UTM/U-space se ha concebido para facilitar la gestión de la movilidad aérea avanzada (AAM, del inglés *Advanced Air Mobility*), proveyendo de los medios y

capacidades necesarios para permitir que aeronaves autónomas, pilotadas en remoto o con un piloto a bordo puedan operar de manera segura, respetando en todo momento la separación mínima entre ellas y el tráfico circundante. Dicho sistema UTM/U-Space se sustenta en la utilización de servicios digitales y tecnologías avanzadas que buscan reducir al máximo posible la intervención humana y aumentar de forma segura el grado de automatización de las operaciones.

En la actualidad existen diferentes iniciativas a nivel mundial que tienen por objeto el diseño e implantación de un sistema UTM/U-Space teniendo en consideración las particularidades regulatorias de sus diferentes áreas geográficas de influencia. En todas ellas, el denominador común es la definición del concepto operacional que se podrá desarrollar en el contexto espacio-temporal seleccionado y que irá evolucionando con el tiempo a medida que las tecnologías maduren y den respuesta a los retos operacionales. Dicho concepto operacional definirá una serie de actores UTM/U-Space, sus roles y sus responsabilidades, de modo que su interoperabilidad permita la planificación y ejecución segura de misiones en contextos AAM.

Para avanzar en el despliegue de estos sistemas, las instituciones aeronáuticas competentes en Europa, Estados Unidos y otras regiones están avanzando hacia el desarrollo del marco regulatorio y los estándares necesarios que garanticen el desarrollo, implementación y despliegue de sistemas UTM/U-Space coherentes y robustos, que puedan así materializar los beneficios económicos y sociales que se esperan. Así, la Agencia de Seguridad Aeronáutica Europea (EASA¹, del inglés *European Union Aviation Safety Agency*) y la estadounidense (FAA², del inglés *Federal Aviation Administration*) están trabajando intensamente para avanzar en la definición de los requisitos tecnológicos, operacionales y regulatorios que se han de observar a la hora de desplegar un sistema UTM/U-Space.

1.1. Gradient

Gradient³ (*Galician Research and Development Center in Advanced Telecommunications*) es un centro de investigación y desarrollo de tecnologías, enfocado en el campo de las Tecnologías de la Información y las Comunicaciones (ICT, del inglés *Information and Communications Technologies*). Tiene como objetivo mejorar la competitividad de las empresas mediante la transferencia de conocimiento y tecnologías en los ámbitos de la conectividad, inteligencia y seguridad. Con más de 140 profesionales y 14 patentes solicitadas, Gradient ha desarrollado más de 340 proyectos diferentes de I+D+i, convirtiéndose en uno de los principales motores de la innovación en Galicia.

El Centro fue creado en 2008 y se conforma a partir de un patronato que agrupa a representantes del sector público y privado. Está formado por las Universidades de A

¹<https://www.easa.europa.eu/>

²<https://www.faa.gov/>

³<https://www.gradient.org/>

Coruña, Santiago de Compostela y Vigo; las empresas Abanca, Altia, Arteixo Telecom, Egatel, Indra, Plexus, R, Telefónica, Televés, y la Asociación empresarial INEO.

El compromiso del Centro con la calidad es una constante desde sus inicios, contando con los siguientes certificados: Sistema de Gestión de Calidad UNE-EN ISO 9001:2015, Sistema de Gestión de Proyectos de I+D+i UNE 166002:2014, Sistemas de Gestión de la Seguridad de la Información UNE-EN ISO/IEC 27001:2013. Además, forma parte del registro estatal de Centros de Innovación Tecnológica (Sello CIT).

Su filosofía es ayudar a las empresas a generar negocio a través del aumento de su competitividad mediante la transformación digital, generando mejoras en sus procesos y facilitando la creación de nuevos modelos de negocio. Integran la transferencia de conocimiento y diseñan soluciones especializadas para la industria, sumando el valor añadido de los profesionales del Centro. Además, siendo completamente independientes, aportan una visión neutral acerca de las mejores soluciones para cubrir los objetivos de las empresas.

En paralelo al proceso de definición del marco regulatorio para el desarrollo, implementación y despliegue de sistemas UTM/U-Space, se requieren esfuerzos de investigación y desarrollo que propongan soluciones que den respuesta a dichos requisitos y que demuestren que las capacidades en tierra y a bordo facilitan la operatividad de aeronaves heterogéneas en espacios aéreos no segregados de manera segura. En este aspecto, Gradient, es partícipe de la iniciativa de desplegar un sistema UTM/U-Space, y se encuentra vinculado, tanto desde el punto de vista investigativo como técnico en el desarrollo del mismo, a través del proyecto U-Sky, que es una subcontratación dentro de un proyecto ministerial subvencionado por el Centro para el Desarrollo Tecnológico y la Innovación (CDTI). De ahí que el Centro haya propuesto la elaboración de este trabajo como parte del desarrollo de dicho proyecto.

1.2. Problema

En escenarios de espacio aéreo compartido entre vuelos tripulados y no tripulados, el riesgo de que una aeronave intrusa pueda ocasionar un peligro a otros vuelos o a estructuras en tierra es mayor. Por tanto, surge la problemática de proporcionar información complementaria a los controladores de tráfico aéreo, que pueda facilitar su reacción ante posibles aeronaves que supongan un peligro. De ahí que este trabajo tenga como **motivación** el desarrollo de un módulo que procese información de tráfico aéreo proveniente de diferentes sensores y la analice.

En particular, desde el proyecto U-Sky, se propone como **problema de investigación** la implementación de un módulo que, a partir de un modelo que considere la cercanía entre aeronaves no tripuladas (UAVs, del inglés *Unmanned Aerial Vehicles*) intrusas y zonas UAS de acceso prohibido, asigne un nivel de amenaza, teniendo en cuenta la estimación, proveniente de sensores, de la posición y velocidad de los UAVs y la

geometría de las zonas.

Para solucionar el problema de investigación se formularon los siguientes objetivos general y específicos:

Objetivo general:

- Desarrollar e implementar el módulo de asignación de nivel de amenaza.

Objetivos específicos:

- Revisar los fundamentos teóricos relacionados con modelos de asignación de amenaza a UAVs.
- Proponer un algoritmo que asigne un nivel de amenaza en función del estado de un UAV.
- Realizar pruebas que permitan evaluar el funcionamiento del módulo implementado, así como su rendimiento.

Teniendo en cuenta las ideas anteriores, mencionaremos los principales conceptos que se involucran en el problema, y qué tratamientos se les darán a lo largo de este trabajo:

- UAV: Denotaremos por UAVs a las aeronaves no tripuladas, de las cuales nos interesa saber si representan o no una amenaza. De estas conoceremos, a partir de información proveniente de sensores, estimaciones de su posición y velocidad.
- Zona UAS: Las zonas UAS son regiones geográficas de interés que pueden indicar o delimitar espacios de tráfico aéreo, aeropuertos, zonas militares o zonas de reserva natural. La geometría de una zona UAS será conocida mediante las coordenadas de un polígono que la represente.
- Zona UAS de acceso prohibido: Las zonas UAS están atributadas según el nivel de acceso que un UAV pueda tener en ellas. Estos niveles de acceso podrían ser: sin restricción, requiere autorización y prohibida⁴. En el caso de las zonas UAS de acceso prohibido significa que bajo ningún concepto un UAV podrá sobrevolar dicha zona.
- Nivel de amenaza: Denotaremos por nivel de amenaza a un número entre 0 y 1, siendo 0 el valor que signifique que un UAV representa poca o ninguna amenaza, y siendo 1 el valor que signifique que la amenaza es máxima porque dicho UAV se encuentra sobrevolando una zona UAS de acceso prohibido.

⁴De aquí en adelante, siempre que se mencione una zona UAS, se asumirá que es de acceso prohibido, salvo que explícitamente se diga lo contrario.

Capítulo 2

Fundamentos teóricos

En este capítulo se da respuesta al primer objetivo específico, de modo que se revisan los fundamentos teóricos relacionados con modelos de asignación de amenaza a UAVs. Para ello, se resumen los diferentes enfoques que tratan el problema y se profundiza en aquellos que resultaron de utilidad para la propuesta en este trabajo.

La mayoría de enfoques previos a este trabajo tratan el problema de asignación de amenaza, sobre todo, desde el punto de vista de un vehículo terrestre (p. ej., un coche), para el cual se desea evitar que sufra colisiones con otros vehículos o el entorno que los rodea (Houénou et al., 2014). Si bien el caso de uso de dichos trabajos es diferente al que en este se aborda, la metodología y enfoques comparten muchos conceptos comunes, tales como: posición y velocidad del vehículo, trayectorias, distancia de seguridad mínima, tiempo de colisión, tiempo de acción, entre otros que se irán introduciendo a lo largo del trabajo. De ahí que las técnicas en tierra sean extrapoladas para resolver problemas en aire, y en particular el de asignar un nivel de amenaza a aeronaves no tripuladas.

2.1. Modelos de asignación de amenaza

En la literatura referente al tema de asignación de amenaza se encuentran disímiles enfoques a la hora de formular un modelo capaz de valorar si un UAV representa una amenaza bajo cierto criterio, y así, catalogarlo como intruso. Dichos enfoques dependen de la información conocida sobre el UAV y también del escenario en que este se encuentre.

Partiendo de que la mayor parte de la información que se puede obtener de un UAV desconocido en circunstancias reales proviene de sensores capaces de estimar posición y velocidad, es común para la mayoría de enfoques utilizar dicha información como base para formular modelos de asignación de amenaza. Otros enfoques también incorporan información derivada de las anteriores, como tiempos para que se complete una acción determinada; por ejemplo, tiempo para que el UAV llegue a sobrevolar un espacio aéreo el cual no debería.

Otros enfoques utilizan información contextual del escenario en cuestión, reglas basadas en lógica formal y análisis del comportamiento del UAV, así como análisis probabilístico y uso de simulaciones para formular un modelo de asignación de amenaza. Por último, también existen enfoques basados en grandes volúmenes de datos y que utilizan métodos de Aprendizaje de Máquina (ML, del inglés *Machine Learning*) como clasificadores que deciden si un UAV puede ser considerado o no como una amenaza.

En general, los diferentes enfoques de modelos de asignación de amenaza se pueden resumir y agrupar en cuatro grupos, tal y como se muestra a continuación:

- **Único comportamiento** (del inglés *Single Behavior*): En presencia de mediciones perfectas y conocimiento completo de la intención de un UAV (p. ej., su destino), se podría predecir de forma determinista y exacta el estado futuro de dicho UAV utilizando un modelo de propagación de estados. Rara vez este caso se corresponde con la realidad, y por lo general, se introducen simplificaciones en la formulación del problema. Por ejemplo, se asume que las mediciones están libres de ruido. También se suele asumir que la velocidad y dirección en la que se mueve el UAV se mantendrán constantes durante una cierta ventana de tiempo. En este enfoque, los modelos de asignación de amenaza basan sus métricas en dominios de la distancia a un punto o zona objetivo, tiempo hasta alcanzar dicho objetivo, o si se acelera o no en dirección del objetivo para identificar situaciones peligrosas ([Zhang et al., 2006](#); [Ko et al., 2020](#)).
 - Dominio de la distancia
 - Dominio del tiempo
 - Dominio de la aceleración
- **Formales**: La idea de los enfoques formales es realizar un análisis matemático apropiado para proveer sistemas de control robustos (del inglés *correct-by-design*), mediante técnicas de modelado y especificación formal, análisis de riesgos y cumplimiento de estándares y normativas; lo que ayuda a minimizar la probabilidad de errores y fallos, aumentando la confiabilidad y seguridad en general. Los modelos de asignación de amenaza que siguen este enfoque suelen estar basados en lógica, donde los requisitos son traducidos a predicados lógicos con el objetivo de verificar el diseño de un sistema en lugar de especificar requisitos complejos ([Loos et al., 2011](#)); o estar basados en conjuntos, donde los requisitos se formalizan especificando un conjunto de comportamientos aceptables/inaceptables o configuraciones del sistema ([Kowshik et al., 2011](#)).
 - Basados en lógica
 - Basados en conjuntos
- **Probabilísticos**: La idea de los enfoques probabilísticos es aprovechar la información disponible sobre las incertidumbres para tomar decisiones con cierto nivel

de confianza. En términos generales, un modelo probabilístico de evaluación de amenazas asigna probabilidades a diferentes eventos, por ejemplo, qué tan probable es que un UAV sobrevuele una zona en un futuro cercano, dadas algunas suposiciones sobre incertidumbres (Campos et al., 2014). Para realizar el cálculo de probabilidades se suele recurrir a métodos como enfoques bayesianos para modelar las dependencias entre el estado actual del UAV y sus estados futuros posibles (Di et al., 2018). También es común realizar simulaciones de Monte Carlo, a partir de estimaciones de la distribución probabilística de las distintas acciones que el UAV pueda realizar, para calcular la probabilidad de ocurrencia de eventos que suelen ser difíciles de modelar (Eidehall and Petersson, 2008).

- Análisis probabilístico
- Simulación de Monte Carlo
- **Decisión basada en datos** (del inglés *Data driven*): La idea de los enfoques basados en datos, a través de técnicas de ML, es aprender sobre distintos comportamientos a partir de un conjunto denominado datos de entrenamiento. Los algoritmos de ML aproximan relaciones, generalmente complejas o que no están descritas formalmente, entre características de los elementos del conjunto de datos. De esta forma, es usual utilizar como datos de entrada el estado actual o información conocida sobre un UAV para obtener como salida una predicción del estado futuro (Hussein et al., 2017). Otra aplicación importante sería la de directamente clasificar escenarios en distintos niveles de peligrosidad (Gruner et al., 2017).
 - Aprendizaje de Máquina

Puede consultarse Dahl et al. (2019) para más información sobre los distintos enfoques de asignación de amenaza.

En este trabajo se hace hincapié en los enfoques de único comportamiento y en las simulaciones de Monte Carlo, para llegar a un modelo mixto que saque partido de las ventajas que ambos proponen. Atendiendo a las particularidades del problema que se pretende resolver, dichos enfoques se ajustan al tipo de información que se tiene de los UAVs y las zonas UAS. De este modo, se puede formular un modelo de asignación de amenaza que tenga en cuenta tanto las estimaciones de la posición y velocidad del UAV, la incertidumbre que resulta de las mediciones y del proceso en sí, como también la geometría de las zonas.

2.1.1. Modelos basados en distancia

Los modelos de asignación de amenaza cuya variable de decisión pertenece al dominio de la distancia son un caso particular de enfoque de único comportamiento. En estos modelos se da por supuesto que la estimación de la posición y velocidad de un UAV son exactas, y que la trayectoria del UAV se mantendrá constante durante cierto intervalo

de tiempo. De este modo, se puede predecir con precisión el estado futuro del UAV y si, en algún momento entre el estado actual y el futuro, representa una amenaza.

La métrica más intuitiva y sencilla de usar en estos modelos de asignación de amenaza, sería calcular la distancia entre la posición actual del UAV y la zona UAS más cercana a este. Si llamamos $D_{\text{uav-zona}}$ a dicha distancia y d a un cierto parámetro, podremos establecer una regla

$$f(D_{\text{uav-zona}}) = \begin{cases} \text{es una amenaza,} & \text{si } D_{\text{uav-zona}} \leq d \\ \text{no es una amenaza,} & \text{si } D_{\text{uav-zona}} > d. \end{cases}$$

Al parámetro d se le suele llamar Distancia de Seguridad Mínima (del inglés *Minimum Safe Distance*) y representa una distancia mínima que se debe mantener entre el UAV y las zonas UAS (ver Figura 2.1). Esta métrica está destinada a situaciones en las que los márgenes espaciales son importantes. Un caso particular sería cuando $d = 0$, el cual corresponde a una situación en la que se considera a un UAV como una amenaza solo cuando este sobrevuela alguna zona UAS prohibida.

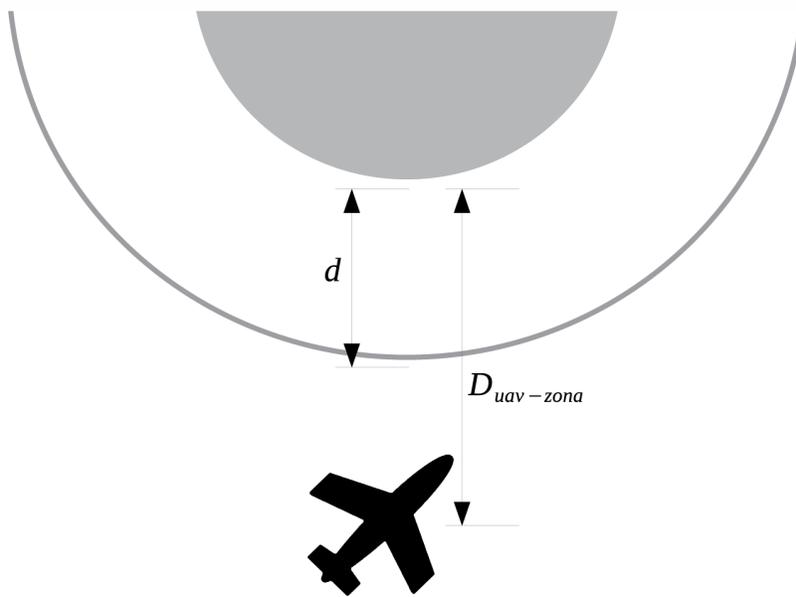


Figura 2.1: La imagen muestra un UAV y una zona UAS (en gris) bordeada por un perímetro. El valor d es la Distancia de Seguridad Mínima y el valor $D_{\text{uav-zona}}$ es la distancia entre el UAV y la zona.

Otra métrica que sigue este enfoque utiliza además la información que se tiene de la velocidad de un UAV. Conociendo la dirección y magnitud en la que este se mueve y, suponiendo que se mantendrá constante durante una ventana de tiempo, se puede

estimar su trayectoria como

$$\text{tray} : p_t = p_0 + vt, \quad t \geq 0,$$

donde p_0 es la posición actual del UAV, v es su velocidad, t es cualquier instante de la ventana de tiempo y p_t es la posición del UAV en ese instante.

Una vez construida la trayectoria, se puede calcular la distancia entre esta y la zona UAS. De igual modo, se puede establecer una regla

$$f(D_{\text{tray-zona}}) = \begin{cases} \text{es una amenaza,} & \text{si } D_{\text{tray-zona}} \leq d \\ \text{no es una amenaza,} & \text{si } D_{\text{tray-zona}} > d, \end{cases}$$

donde $D_{\text{tray-zona}}$ es dicha distancia (ver Figura 2.2). De esta forma, se puede considerar a un UAV como una amenaza, no solo si en el momento actual se encuentra cerca de o sobrevolando una zona UAS, sino además, si este lo estará en el futuro próximo.

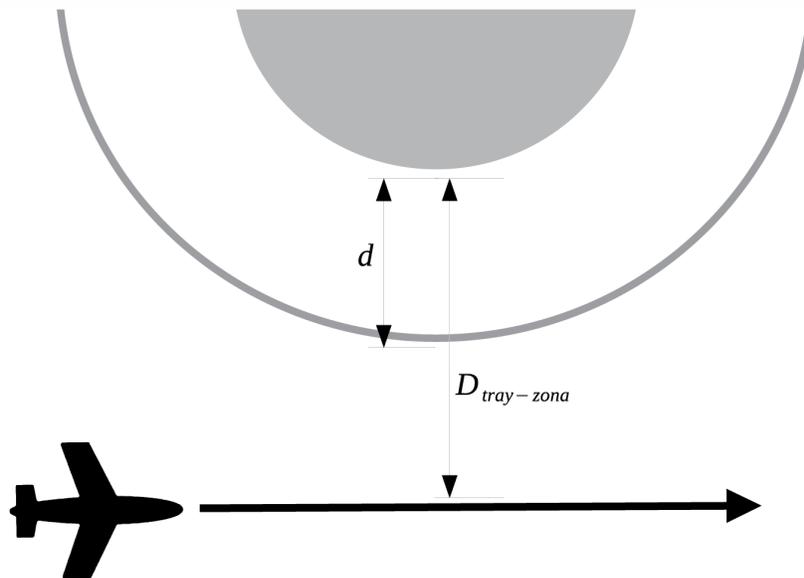


Figura 2.2: La imagen muestra un UAV, su trayectoria (flecha en negro) y una zona UAS (en gris) bordeada por un perímetro. El valor d es la Distancia de Seguridad Mínima y el valor $D_{\text{tray-zona}}$ es la distancia entre la trayectoria y la zona.

2.1.2. Modelos basados en tiempo

Los modelos de asignación de amenaza cuya variable de decisión pertenece al dominio del tiempo son otro caso particular de enfoque de único comportamiento. Estos utilizan la información conocida de posición y velocidad de un UAV, así como su distancia a

las zonas UAS, para calcular el tiempo que tardaría el UAV en acercarse o comenzar a sobrevolar las zonas, suponiendo que mantenga su trayectoria. A este concepto se le suele llamar Tiempo de Colisión (del inglés Time-to-collision).

Si tomamos la trayectoria $tray$ de un UAV y la extendemos a lo largo de una ventana de tiempo, y suponiendo que esta intersecta el área delimitada por una zona UAS, podemos calcular el Tiempo de Colisión como

$$T_{\text{colisión}} = \text{mín}\{t : t \geq 0, p_t \in Z\},$$

donde Z es el conjunto de puntos interiores de la zona UAS (ver Figura 2.3). En el caso, de que, al extender la trayectoria, esta no intersecte con ninguna zona UAS, se puede considerar que el UAV se encuentra suficientemente lejos de cualquier zona, y podemos asignar a $T_{\text{colisión}}$ un valor infinito positivo.

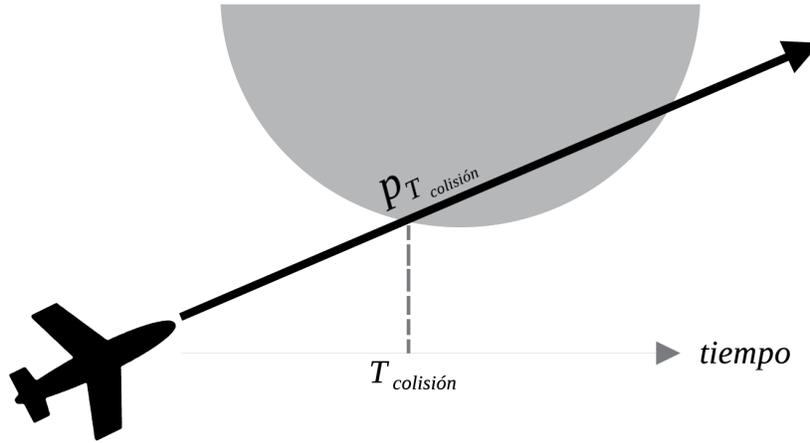


Figura 2.3: La imagen muestra un UAV, su trayectoria (flecha en negro) y una zona UAS (en gris). El valor $T_{\text{colisión}}$ es el Tiempo de Colisión y $p_{T_{\text{colisión}}}$ es el punto por donde el UAV entraría a la zona.

Una vez calculado el Tiempo de Colisión para un UAV, se puede establecer una regla

$$f(T_{\text{colisión}}) = \begin{cases} \text{es una amenaza,} & \text{si } T_{\text{colisión}} \leq t \\ \text{no es una amenaza,} & \text{si } T_{\text{colisión}} > t, \end{cases}$$

donde t es un parámetro que representa el tiempo mínimo que puede ocurrir entre el instante actual y el instante que el UAV se adentra en alguna zona UAS. Al parámetro t se le suele llamar Tiempo de Acción (del inglés Time-to-action), y está relacionado con la idea de ser el tiempo necesario para tomar medidas o acciones en respuesta a una situación determinada; en este caso, evitar que el UAV sobrevuele alguna zona UAS prohibida. Algunos criterios comunes para asignar el valor del parámetro t son:

el tiempo que tarda un UAV en frenar y detenerse antes de comenzar a sobrevolar alguna zona (Chen et al., 2013); el tiempo de maniobra para evadir la zona, desviando la trayectoria del UAV (Eidehall and Madås, 2013); y el tiempo de intercepción del UAV mediante algún tipo de ataque físico o electrónico, que impida el avance del mismo. Puede consultarse Harrison et al. (2020) para más información sobre formas de intercepción de UAVs.

2.2. Fuentes de incertidumbre

Los modelos de asignación de amenaza vistos hasta ahora presentan el principal inconveniente de que simplifican mucho el problema; hacen suposiciones poco flexibles sobre la trayectoria e intención del UAV, además de no tener en cuenta posibles errores en las mediciones. Un modelo que se ajuste más a la realidad debería ser lo suficientemente flexible como para incorporar información sobre la distribución que sigan las mediciones y además considerar variaciones en las trayectorias.

La principal causa de incertidumbre en las mediciones viene dada por la exactitud y precisión que los instrumentos de medición puedan brindar. En el caso de la medición de la posición y velocidad de UAVs se suele utilizar una variedad de sensores, donde los más comunes son: radares, que por su complejidad y robustez suelen ser equipos bastante costosos, pero con la ventaja de brindar información precisa y completa, como la elevación, azimut y rango del objetivo, así como la tasa de cambio de estas magnitudes respecto al sensor; sensores de radiofrecuencia, que son similares a los radares, pero al ser más sencillos solo son capaces de reportar la potencia de las radiaciones intercambiadas entre el objetivo y el sensor, así como la dirección de donde provienen; y por último, las cámaras de vigilancia, ya sean fijadas a alguna estructura en tierra o móviles (p. ej., cámaras instaladas en otros UAVs), son también utilizadas para reportar la elevación y azimut del objetivo respecto al sensor, aunque suelen ser las menos precisas.

Debido a la variedad de fuentes de las que pueden provenir las mediciones, dominios en las que se puedan expresar (p. ej., ángulo, distancia, potencia) e incompletitud de la información que puedan aportar los sensores por separado, es necesario un proceso de fusión de datos con el objetivo de conseguir una única medición que sea suficientemente representativa. Para esto se suelen utilizar técnicas como el filtro de Kalman, que es una técnica de fusión de datos que se utiliza comúnmente en sistemas de control y navegación para estimar el estado de un sistema dinámico a partir de mediciones ruidosas y parciales (Becker, 2023). El objetivo del filtro de Kalman es encontrar la mejor estimación posible del estado del sistema (en este caso, la posición y velocidad de un UAV), teniendo en cuenta tanto la información disponible a través de las mediciones como la dinámica del sistema subyacente (ver Figura 2.4).

Por otro lado, la incertidumbre del sistema en sí puede ser difícil de modelar, sobre todo cuando se tienen en cuenta variables con una alta variabilidad. Tales son el caso del viento y la intención de un UAV. Las ráfagas de viento son cambios bruscos en la

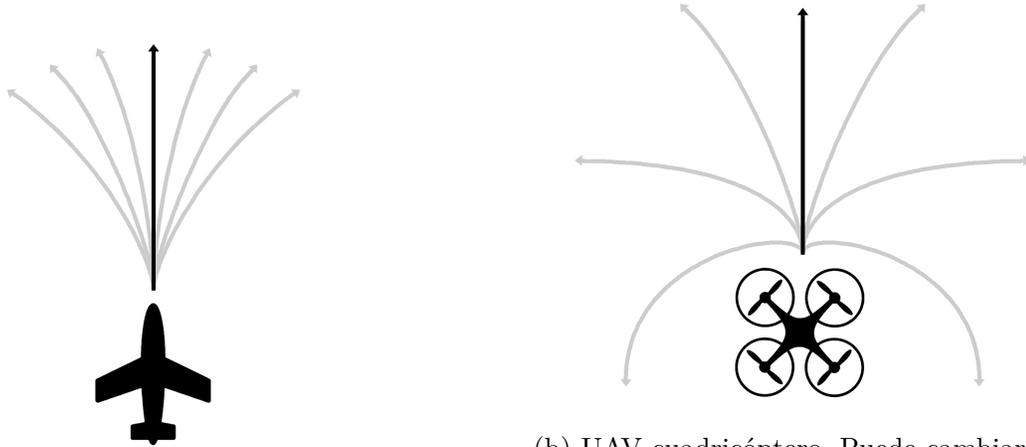


Figura 2.4: Distintos sensores detectan un UAV y realizan mediciones por separado. Luego, un módulo de fusión de datos utiliza un filtro de Kalman para lograr una única medición más precisa y exacta, a partir de las anteriores.

velocidad o dirección del viento, y pueden ser causadas por condiciones meteorológicas adversas, como frentes de tormenta o cambios en la topografía del terreno; mientras que, las turbulencias son causadas por corrientes de aire irregulares, que pueden ser creadas por la velocidad del viento, las condiciones atmosféricas, la topografía del terreno, y otros factores. Por otra parte, la intensidad de un UAV también puede cambiar, sobre todo de manera instantánea, y en dependencia de la maniobrabilidad que este posea, los cambios serán más pronunciados (ver Figura 2.5). Todo lo anterior en conjunto hace que las trayectorias se vuelvan poco predecibles.

En la literatura podemos encontrar alternativas a la hora de formular trayectorias, con el objetivo de ganar en flexibilidad y que un modelo se ajuste más a la realidad (Wang et al., 2019). En general, los tipos de trayectoria se resumen a continuación (ver Figura 2.6):

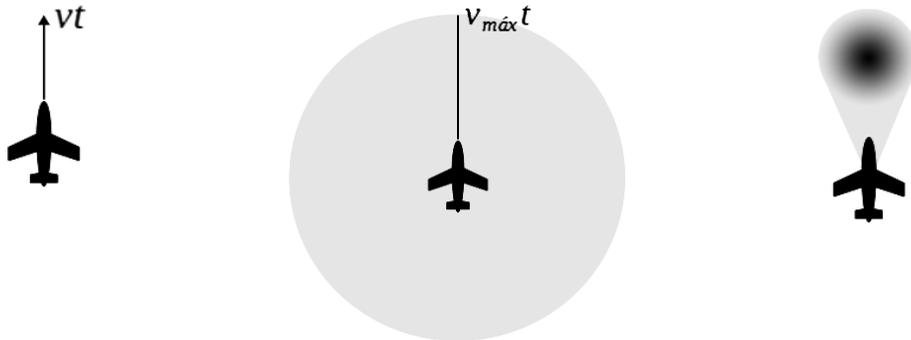
- Nominal: La trayectoria se obtiene a partir de extrapolar la posición del UAV en dirección de su movimiento, asumiendo que mantendrá constante su velocidad.
- Peor caso: Se toma como velocidad de referencia la velocidad máxima que pueda alcanzar el UAV (pudiendo depender del modelo), y se calcula un volumen de todas las posiciones que podrá alcanzar a esa velocidad.
- Probabilística: La trayectoria se obtiene a partir de estimaciones de la distribución de la posición y velocidad del UAV, a partir de las cuales se calcula la distribución de las posiciones futuras.



(a) UAV ala fija. Para cambiar de dirección necesita seguir avanzando hacia adelante.

(b) UAV cuadricóptero. Puede cambiar de dirección (vertical, horizontal y lejanía) de forma independiente.

Figura 2.5: Imagen comparativa de la maniobrabilidad de un UAV ala fija (2.5a) y un UAV cuadricóptero (2.5b).



(a) Trayectoria nominal. El valor v es la velocidad actual del UAV. La flecha indica la posición que el UAV tendrá si mantiene su velocidad constante durante un tiempo t .

(b) Trayectoria peor caso. El valor $v_{\text{máx}}$ es la velocidad máxima que puede alcanzar el UAV. La zona gris representa todas las posiciones a las que el UAV podría llegar durante un tiempo t .

(c) Trayectoria probabilística. El cono representa la probabilidad de las posiciones futuras del UAV. El color negro indica las posiciones más probables.

Figura 2.6: Imagen comparativa de los distintos tipos de trayectoria.

Capítulo 3

Modelo mixto de asignación de amenaza

En este capítulo se da respuesta al segundo objetivo específico, de modo que se propone un algoritmo que asigna un nivel de amenaza a un UAV en función de su cercanía a las zonas UAS.

La idea general del modelo de asignación de amenaza que se propone en este trabajo es un modelo mixto que tenga en cuenta la distancia $D_{\text{uav-zona}}$ entre la posición actual de un UAV y las zonas UAS, y también el Tiempo de Colisión $T_{\text{colisión}}$. De modo que al utilizar la regla de asignación de amenaza de los enfoques basado en distancia y basado en tiempo se puedan cubrir diferentes necesidades a la vez. Además, se pretende aprovechar la información sobre las estimaciones, no solo utilizando valores puntuales, sino también la estimación que ofrecen los sensores sobre las varianzas y covarianzas de las mismas. Para ello, mediante una simulación de Monte Carlo, se pueden generar varias trayectorias, y para cada una de ellas evaluar una cierta función de nivel de amenaza basada en las reglas anteriores. Puede consultarse el trabajo de [Kim et al. \(2007\)](#) sobre generación de trayectorias 3D para UAVs.

3.1. Generación de trayectorias

Para poder realizar la simulación de Monte Carlo es necesario generar un número n de trayectorias a partir de la estimación de la posición y velocidad del UAV. Partiendo de que dicha estimación proviene de un filtro de Kalman, podemos asumir que sigue una distribución Normal Multivariante, con vector de medias μ y matriz de covarianzas Σ .

$$\mu = \begin{bmatrix} p_0 \\ v \end{bmatrix}, \quad \Sigma = \begin{pmatrix} \sigma_{p_0}^2 & \sigma_{p_0,v} \\ \sigma_{p_0,v} & \sigma_v^2 \end{pmatrix},$$

donde p_0 y v son las estimaciones de la posición y velocidad del UAV, y $\sigma_{p_0}^2$, σ_v^2 y $\sigma_{p_0,v}$ son las estimaciones de las varianzas y covarianza.

Utilizando el Algoritmo 1 se pueden generar tantas trayectorias como se desee para la simulación de Monte Carlo (ver Figura 3.1).

Algoritmo 1 Generación de trayectorias: $\text{tray}(\mu, \Sigma, n)$

Entrada: μ, Σ, n

Salida: tray

- 1: $\text{tray} \leftarrow$ lista de n trayectorias
 - 2: **para** $i \leftarrow 1, n$ **hacer**
 - 3: $\tilde{p}_0, \tilde{v} \leftarrow$ muestraNormMultiVar(μ, Σ)
 - 4: $\text{tray}[i].p_0 \leftarrow \tilde{p}_0$
 - 5: $\text{tray}[i].v \leftarrow \tilde{v}$
 - 6: **fin para**
 - 7: **devolver** tray
-

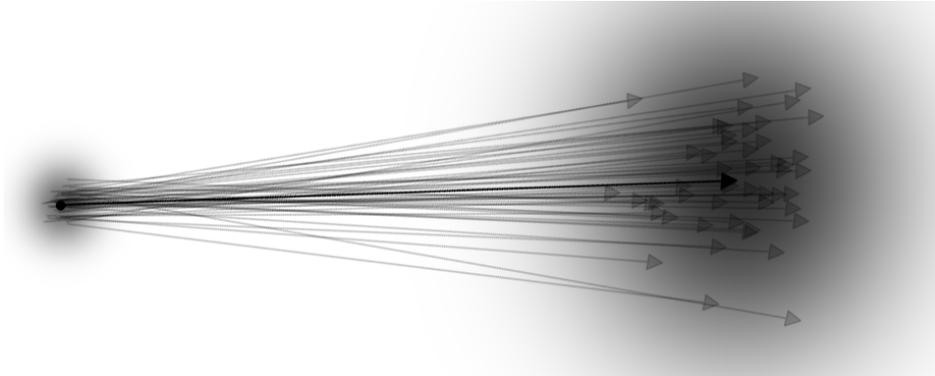


Figura 3.1: La imagen muestra ejemplos de trayectorias generadas por el Algoritmo 1. A la izquierda se observa la distribución de p_0 y a la derecha la distribución de p_t , para algún t específico.

3.2. Función de amenaza

Para la función de asignación de un nivel de amenaza se desea que tome valores entre 0 y 1. Intuitivamente, tanto para valores de $D_{\text{uav-zona}} \gg 0$ como para valores de $T_{\text{colisión}} \gg 0$ (lo que representaría un UAV lejano de cualquier zona UAS, en cuanto a distancia y tiempo), la función debe devolver un valor cercano a 0. Por el contrario, si $D_{\text{uav-zona}} \approx 0$ o $T_{\text{colisión}} \approx 0$ (lo que representaría un UAV cercano a alguna zona UAS, en cuanto a distancia o tiempo), entonces debe devolver un valor cercano a 1. También se desea que la función valga $\frac{1}{2}$ cuando, según el caso, $D_{\text{uav-zona}} = d$ (Distancia de Seguridad Mínima) o $T_{\text{colisión}} = t$ (Tiempo de Acción).

En las Secciones 3.2.1 y 3.2.2 se proponen dos variantes de la función y en la Sección 3.2.3 se comparan con el objetivo de seleccionar la que mejor se ajuste al problema de asignación de amenaza.

3.2.1. Función lineal truncada

Una primera función que se propone es la función lineal truncada

$$f(x; m) = \max\{mx + 1, 0\},$$

donde m es el valor de la pendiente de la función lineal, de forma tal que

$$f(x_{1/2}; m) = \frac{1}{2} \Rightarrow m = -\frac{1}{2x_{1/2}},$$

donde $x_{1/2}$ es, según el caso, d o t (hablaremos de m_d y m_t respectivamente) (ver Figura 3.2).

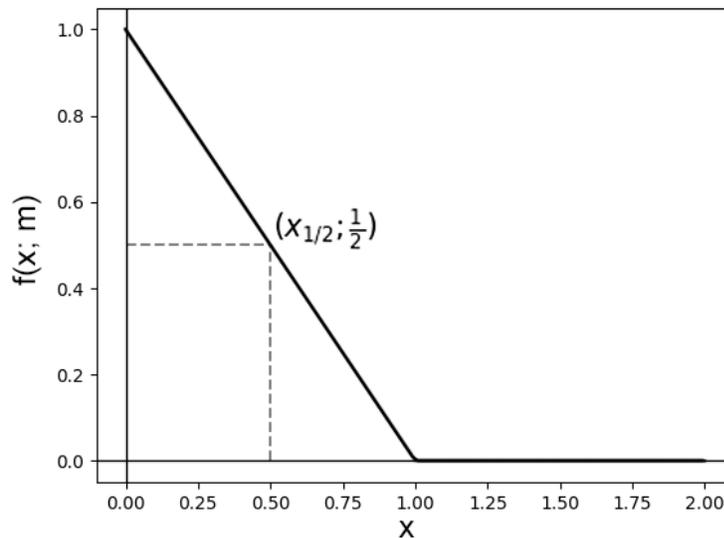


Figura 3.2: Función de amenaza lineal truncada $f(x; m) = \max\{mx + 1, 0\}$, con $m = -1$ y $x_{1/2} = 0.5$.

3.2.2. Función exponencial decreciente

La segunda función que se propone es la función exponencial decreciente

$$f(x; \sigma) = e^{-x/\sigma},$$

donde σ es un parámetro de escala tal que

$$f(x_{1/2}; \sigma) = \frac{1}{2} \Rightarrow \sigma = \frac{x_{1/2}}{\ln 2},$$

donde $x_{1/2}$ es, según el caso, d o t (hablaremos de σ_d y σ_t respectivamente) (ver Figura 3.3).

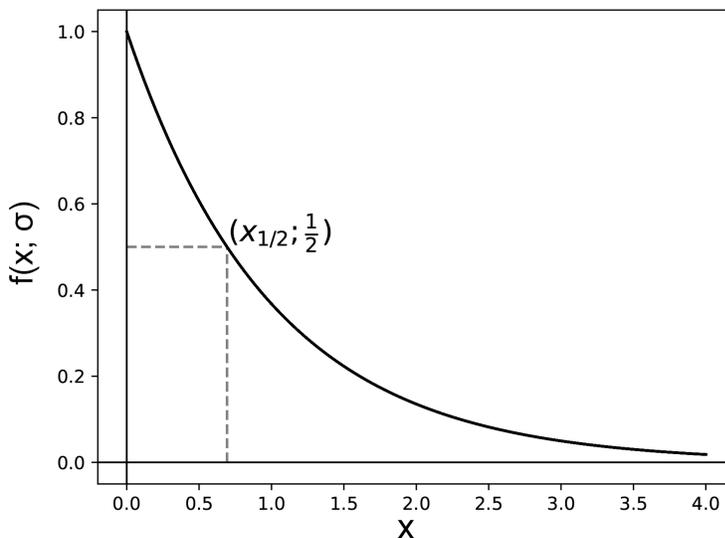


Figura 3.3: Función de amenaza exponencial decreciente $f(x; \sigma) = e^{-x/\sigma}$, con $\sigma = 1$ y $x_{1/2} = \ln 2$.

3.2.3. Comparación entre funciones de amenaza

Con fines comparativos y por simplicidad, tomemos el valor $x_{1/2} = \ln 2$. De este modo, los valores de los parámetros de las funciones lineal truncada y exponencial decreciente serían $m = -1/(2 \ln 2)$ y $\sigma = 1$. En la Figura 3.4 podemos observar el comportamiento de ambas funciones a la vez.

Una primera observación es que la función lineal truncada tarda en comenzar a asignar valores de nivel de amenaza mayores que cero. Esto es, a medida que los valores de x van disminuyendo, la mayoría de valores para el nivel de amenaza, que asigna la función, son cero. Este comportamiento no cambia hasta que las x comienzan a tomar valores menores que $2 \ln 2$ (aproximadamente 1.39).

Por otro lado, la función exponencial decreciente siempre asigna un valor para el nivel de amenaza mayor que cero. Este valor va aumentando paulatinamente según disminuyen las x , lo cual permite detectar desde momentos tempranos que un UAV se está acercando, ya sea espacial o temporalmente, y se tenga en cuenta como potencial amenaza futura.

En general, la función lineal truncada subestima el nivel de amenaza para valores de x mayores que $x_{1/2}$.

Otra observación es que la función lineal truncada tiene una pendiente más pronunciada que el ritmo de crecimiento de la función exponencial decreciente, haciendo que, para pequeños cambios en el valor de la variable x se vean reflejados grandes variaciones en el nivel de amenaza asignado. Dicho de otra forma, la función exponencial decreciente es más robusta a cambios en el valor de las x .

Por los motivos anteriores, para este trabajo, se decidió tomar la función exponencial decreciente como función de nivel de amenaza, ya que su comportamiento en general es más deseable que el de la función lineal truncada. En adelante, siempre que nos refiramos a la función f se estará haciendo referencia a $f(x; \sigma) = e^{-x/\sigma}$.

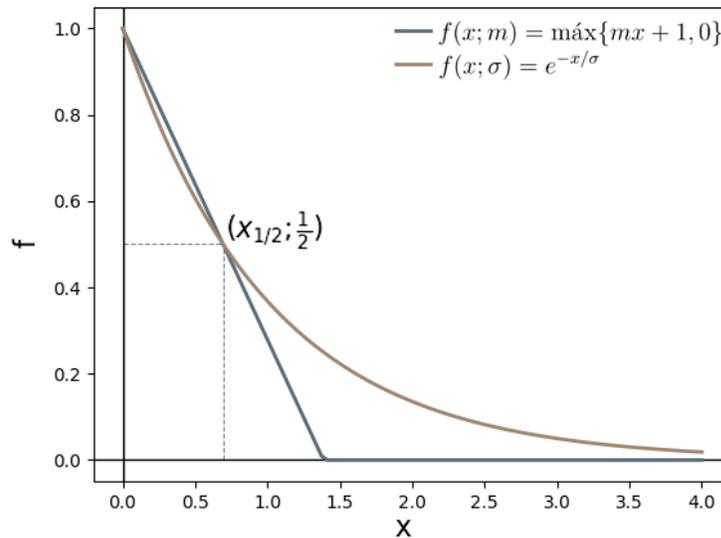


Figura 3.4: Comparación entre las funciones de amenaza lineal truncada y exponencial decreciente, con $m = -1/(2 \ln 2)$, $\sigma = 1$ y $x_{1/2} = \ln 2$.

3.3. Asignación de un nivel de amenaza

Dada una trayectoria, del conjunto generado por simulación, se pueden calcular sus respectivos valores de $D_{\text{uav-zona}}$ y $T_{\text{colisión}}$ respecto al conjunto Z de puntos pertenecientes a las zonas UAS. Posteriormente, habiendo fijado valores para d y t , se calculan los niveles de amenaza $f(D; \sigma_d)$ y $f(T; \sigma_t)$, correspondientes a los criterios de distancia y tiempo. El nivel de amenaza que se asigna a la trayectoria es el máximo entre ambos valores (ver Figura 3.5).

Finalmente estamos en condiciones de describir una serie de pasos para asignar un nivel

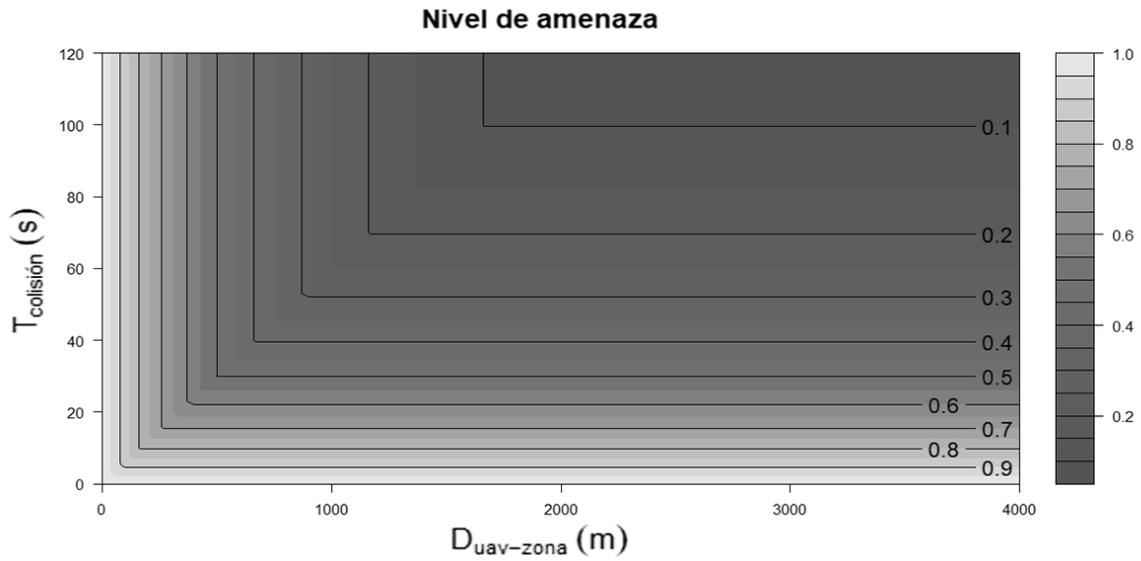


Figura 3.5: Ejemplo de nivel de amenaza: $d = 500$ m, $t = 30$ s. Los grises claros indican un nivel de amenaza mayor al que indican los grises oscuros.

de amenaza a un UAV, basado en el conjunto de trayectorias generadas por simulación. El Algoritmo 2 consiste en iterar por las n trayectorias, y para cada una evaluar la función de amenaza f según los criterios de distancia y tiempo, obteniendo $f(D; \sigma_d)$ y $f(T; \sigma_t)$ respectivamente, y consecutivamente el máximo entre ambos valores. El resultado del algoritmo es el promedio de los niveles de amenaza de cada trayectoria.

Algoritmo 2 Asignación de un nivel de amenaza: $\text{amenaza}(\mu, \Sigma, n, Z, \sigma_d, \sigma_t)$

Entrada: $\mu, \Sigma, n, Z, \sigma_d, \sigma_t$

Salida: amenaza

- 1: $\text{tray} \leftarrow \text{tray}(\mu, \Sigma, n)$
 - 2: $f_{\text{máx}} \leftarrow$ lista de n valores de nivel de amenaza
 - 3: **para** $i \leftarrow 1, n$ **hacer**
 - 4: $D \leftarrow \text{dist}(\text{tray}[i].p_0, Z)$
 - 5: $T \leftarrow \text{mín}\{t : t \geq 0, \text{tray}[i].p_t \in Z\}$
 - 6: $f_D \leftarrow f(D; \sigma_d)$
 - 7: $f_T \leftarrow f(T; \sigma_t)$
 - 8: $f_{\text{máx}}[i] \leftarrow \text{máx}\{f_D, f_T\}$
 - 9: **fin para**
 - 10: $\text{amenaza} \leftarrow \bar{f}_{\text{máx}}$
 - 11: **devolver** amenaza
-

Capítulo 4

Problema práctico

En este capítulo se da respuesta al objetivo general del trabajo y al tercer objetivo específico, de modo que se describe la implementación del módulo de asignación de amenaza y también las pruebas que se realizaron para su validación.

4.1. Materiales y métodos

Para la implementación del módulo de asignación de amenaza se utilizó el lenguaje de programación Python 3.9 ([Van Rossum and Drake Jr, 2021](#)) a través de un entorno Conda ([Anaconda, Inc., 2022](#)), el cual permite orquestrar los diferentes paquetes del lenguaje utilizados.

Los principales paquetes del lenguaje Python utilizados en este trabajo para la implementación del módulo se enuncian a continuación y se comenta, brevemente, el uso que se les dio durante la resolución de los distintos problemas que se afrontaron desde un punto de vista técnico.

- `numpy` ([Harris et al., 2020](#)): Paquete de cómputo numérico con una gran variedad de funciones y características para el trabajo con *arrays* multidimensionales de forma eficiente, así como operaciones vectoriales, matriciales y generación de variables y vectores aleatorios. Este paquete se utilizó principalmente durante la generación de trayectorias a partir de vectores aleatorios y posteriormente para el tratamiento de las mismas.
- `pymap3d` ([Hirsch et al., 2019](#)): Paquete para la conversión de coordenadas geográficas en distintos sistemas de referencia, tales como el sistema geodésico (latitud, longitud y altitud), el sistema ENU (del inglés *East-North-Up*) y el sistema ECEF (del inglés *Earth-centered Earth-fixed*). Este paquete se utilizó para transformar los datos geoespaciales, de forma que fuera más fácil su tratamiento, tanto en operaciones de almacenamiento y consulta como en operaciones geométricas.

- **shapely** (Gillies et al., 2022): Paquete para la manipulación y análisis de objetos geométricos planos. Este paquete se utilizó para la representación geométrica a partir de polígonos de las zonas UAS, donde los vértices de los mismos correspondían a coordenadas geográficas. También se utilizó para representar a partir de líneas poligonales las trayectorias generadas de los UAVs.
- **geopandas** (Jordahl et al., 2020): Paquete para el tratamiento de conjuntos de datos geoespaciales, así como facilitar la realización de operaciones geométricas sobre los datos. Este paquete fue utilizado para acelerar las distintas operaciones geométricas que se realizaron sobre las zonas UAS y las trayectorias de los UAVs, tales como hallar uniones, intersecciones y el cálculo de distancias.
- **rtree** (Gilles and Butle, 2022): Paquete que provee un número de funcionalidades avanzadas para realizar indización de datos espaciales. Este paquete se utilizó para crear una estructura de datos eficiente donde almacenar en memoria las zonas UAS, para luego, durante el cálculo de asignación de amenaza, filtrar el conjunto de todas las zonas y obtener las zonas cercanas a los UAVs.
- **multiprocessing** (The Python team, 2022): Adicionalmente, se utilizó este paquete, el cual está diseñado para permitir la ejecución de tareas en paralelo. De esta forma, se ideó una arquitectura de tareas distribuidas, que en su conjunto, se encargan de aportar funcionalidad al módulo de asignación de amenaza.

4.2. Implementación del módulo de asignación de amenaza

En esta sección se describe la arquitectura y las funcionalidades del módulo de asignación de amenaza implementado. En general, el módulo es capaz de recibir información de tráfico aéreo e información sobre zonas UAS para asignar niveles de amenaza utilizando el modelo propuesto en la Sección 3. La información es recibida desde y hacia la red mediante el uso de conexión WS (del inglés *Web Sockets*). Puede consultarse Hixie et al. (2011) para más información sobre dicho protocolo de comunicación.

La información recibida por el módulo conteniendo datos sobre los UAVs la denominaremos **tracks**. Cada UAV, para el cual se desea que se le asigne un nivel de amenaza, tiene asociado un **track** único, el cual lo describe. Dentro de la información relevante podemos encontrar las coordenadas geodésicas de la posición del UAV, la velocidad en coordenadas ENU y la estimación de los errores de medición.

Por otro lado, la información recibida sobre zonas UAS contiene datos como el nivel de acceso de la zona y su geometría, descrita por un polígono cuyos vértices se encuentran en coordenadas geodésicas.

La información recibida por el módulo se estructura como se muestra a continuación:

- `track`
 - posición
 - velocidad
 - error de medición
- `zona UAS`
 - nivel de acceso
 - geometría

4.2.1. Arquitectura

El módulo de asignación de amenaza se implementó siguiendo una arquitectura distribuida. El objetivo de dicha arquitectura fue ganar en modularidad y en capacidad de procesamiento en paralelo. Puede consultarse [Mertens \(2011\)](#) para más información sobre procesamiento en paralelo con Python. El proceso completo de asignar un nivel de amenaza a un UAV, que va desde recibir un `track` hasta enviar el resultado asociado, se dividió en cuatro tareas puntuales, las cuales intercambian información entre sí (ver Figura 4.1):

- `tracksListener`, se encarga de esperar a que lleguen `tracks` desde la red, a través de WS. Una vez que un `track` es recibido es almacenado en una cola de espera para su posterior procesamiento.
- `zonesManager`, se encarga de gestionar las zonas UAS. Recibe desde la red a través de WS actualizaciones, consistentes en agregar o eliminar zonas del espacio aéreo¹. Las zonas UAS recibidas son almacenadas en una estructura de datos eficiente para su posterior consulta.
- `inferenceWorker`. Esta tarea puede tener varias réplicas (tantas como el equipo de cómputo lo permita). Cada `inferenceWorker` es encargado de procesar, a la vez, un `track` pendiente en la cola del `tracksListener`. Para esto, realiza una consulta al `zonesManager` sobre las zonas UAS cercanas al UAV indicado por el `track`, y utilizando el Algoritmo 2 le asigna un nivel de amenaza.
- `threatsSender`, se encarga de recibir los resultados conteniendo los niveles de amenaza de los `tracks` procesados. Finalmente los envía a la red a través de WS.

4.2.2. Funcionalidades

El módulo de asignación de amenaza cuenta con funcionalidades internas que permiten a las tareas `tracksListener`, `zonesManager`, `inferenceWorkers` y `threatsSender` realizar las operaciones necesarias para manipular datos. Las funcionalidades más relevantes son:

- Indizado de zonas UAS: Las zonas UAS son almacenadas en una estructura de datos `r*-tree`, la cual es especializada para la consulta eficiente de datos

¹La acción de eliminar zonas UAS no fue objetivo de implementación durante la entrega del proyecto.

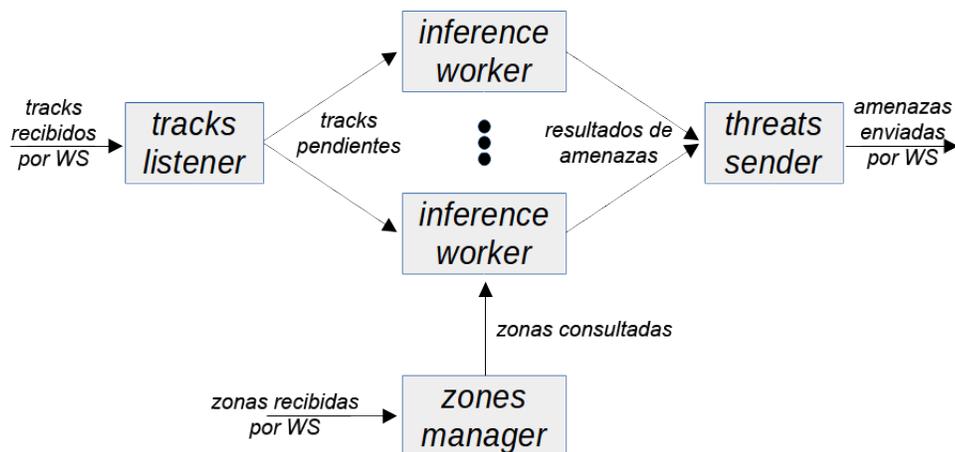


Figura 4.1: Arquitectura del módulo de asignación de amenaza. En la imagen se muestran las tareas del módulo (el `tracksListener`, el `zonesManager`, los `inferenceWorkers` y el `threatsSender`) y el flujo de información entre ellas.

geoespaciales. Esto permite a los `inferenceWorkers` obtener rápidamente, dentro del conjunto de todas las zonas UAS, solo las que son cercanas a los UAVs que se están procesando, dados sus posiciones y un radio de búsqueda (ver Figura 4.2). Puede consultarse [Beckmann et al. \(1990\)](#) para más información sobre la estructura de datos `r*-tree`.

- Transformación entre sistemas de coordenadas: El módulo es capaz de convertir coordenadas desde el sistema geodésico hacia los sistemas ECEF y ENU. El caso de la conversión hacia ECEF es utilizado por el `zonesManager` para convertir los polígonos que representan a las zonas UAS y poderlos almacenar en el `r*-tree`. El caso de la conversión hacia ENU es utilizado por los `inferenceWorkers` para convertir las coordenadas de los polígonos de las zonas a coordenadas locales, donde los centros de referencia son las posiciones de los UAVs. Puede consultarse [Hirt and Featherstone \(2008\)](#) para más información sobre conversión entre los sistemas de coordenadas geodésicas, ECEF y ENU.
- Asignación de nivel de amenaza: Es la principal funcionalidad del módulo. Es una implementación directa del Algoritmo 2 de asignación de amenaza.

4.3. Experimentación

En esta sección se describen una serie de pruebas realizadas para ilustrar las distintas funcionalidades del módulo de asignación de amenaza, así como para chequear, corregir y validar el correcto funcionamiento del mismo. La etapa de experimentación permitió además, valorar la utilidad del módulo implementado y observar si los resultados daban respuesta a las interrogantes objeto de estudio.

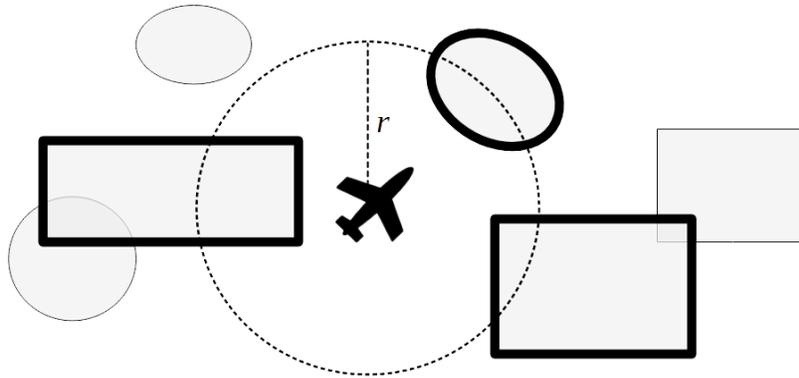


Figura 4.2: La imagen muestra un UAV y varias zonas UAS. Las zonas marcadas en negro están contenidas en el radio r de búsqueda.

La realización de las pruebas se hizo en conjunto con un tercer Centro mediante una plataforma de simulación y gestión de tráfico aéreo². Dicho Centro se encargó de la configuración de los vuelos realizados por los UAVs, la configuración de las zonas UAS y el envío de `tracks` para que el módulo de asignación de amenaza los procesara.

4.3.1. Prueba 1: Funcionamiento

La primera prueba consistió en probar el funcionamiento del módulo de asignación de amenaza. Para esto, se simularon 13 vuelos de UAVs alrededor de una zona UAS. La zona se configuró como un rectángulo de lados 1000 y 500 metros. Los parámetros σ_d y σ_t de la función de amenaza se establecieron a $500/\ln 2$ metros y $30/\ln 2$ segundos respectivamente. La duración de cada vuelo fue de 10 minutos. Para cada vuelo se registró el nivel de amenaza que el módulo le asignaba según el UAV se movía en el tiempo.

Los resultados de la prueba de funcionamiento se muestran en las gráficas del Apéndice A. Para cada vuelo simulado, se muestran tres gráficas. La primera gráfica muestra la posición de la zona UAS (en rojo) y la posición del UAV a lo largo del tiempo (en verde la posición real y en azul la posición estimada por sensores). La segunda gráfica muestra la distancia desde el UAV a la zona UAS, $D_{\text{uav-zona}}$ (en magenta) y el Tiempo de Colisión, $T_{\text{colisión}}$ (en anaranjado), en función del tiempo transcurrido. Por último, la tercera gráfica muestra la evolución del nivel de amenaza asignado al UAV en función del tiempo transcurrido.

En la Figura 4.3 se muestra, a modo de ejemplo, las gráficas con los resultados del primer vuelo simulado. En la primera de estas gráficas se puede observar que el vuelo del UAV se inicia en las cercanías de la zona UAS, y su rumbo se dirige hacia la zona. Esto se ve reflejado en las siguientes dos gráficas donde se observa, en la segunda, que tanto la

²Por motivos de privacidad no se mencionan los nombres del Centro ni de la plataforma.

distancia entre el UAV y la zona como el Tiempo de Colisión disminuyen gradualmente, y en la tercera gráfica, se observa que consecuentemente el nivel de amenaza aumenta, hasta hacerse máximo una vez que el UAV se adentra en la zona. Finalmente, tras el UAV abandonar la zona UAS, los niveles de amenaza asignados comienzan a disminuir.

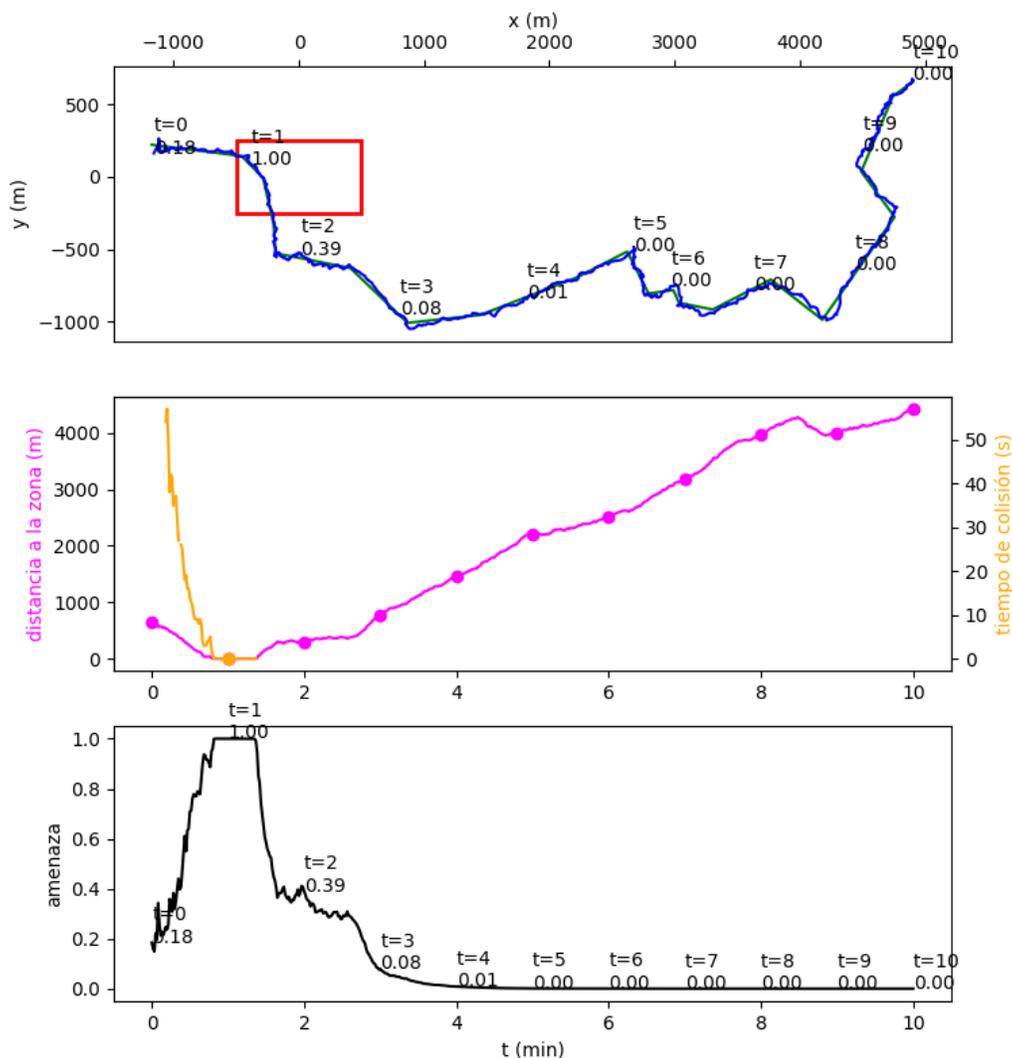


Figura 4.3: Ejemplo de simulación de un UAV y asignación de amenaza.

De los resultados de la prueba, podemos concluir que el comportamiento del módulo de asignación de amenaza fue el esperado. A cada uno de los trece UAVs simulados se les fue asignando un nivel de amenaza para cada instante de tiempo. Los niveles de amenaza iban aumentando gradualmente según los UAVs se acercaban a la zona UAS,

llegando a ser máximos cuando estos sobrevolaban la zona. Finalmente, los valores iban disminuyendo si los UAVs tomaban una dirección que los alejara de la zona.

4.3.2. Prueba 2: Rendimiento

La segunda prueba consistió en medir el rendimiento del módulo de asignación de amenaza. Para esto, se cronometró el tiempo de ejecución durante el cómputo de las operaciones más costosas: la obtención mediante el r^* -tree de las zonas UAS cercanas al UAV recibido en un `track` y el correspondiente cálculo del nivel de amenaza. Para cada operación se registró el tiempo medio y desviación típica que tardaron en completarse. El número de `inferenceWorkers` se estableció a 4, el número n de trayectorias generadas se estableció a 1000 y el número total de zonas UAS fueron 1254.

Los resultados de la prueba de rendimiento se muestran en el cuadro a continuación.

Operación	Tiempo medio (s/track)	Desviación típica (s/track)
obtención de zonas UAS	0.000	0.000
cálculo del nivel de amenaza	0.126	0.002

Cuadro 4.1: Resultados de la prueba de rendimiento.

Respecto a los resultados obtenidos para la prueba, podemos observar en el Cuadro 4.1 que el tiempo medio, por `track`, que tardan en completarse las operaciones de obtención de zonas UAS y cálculo del nivel de amenaza es 0.000 y 0.126 segundos respectivamente.

Para el nivel de precisión con el que se cronometraron las operaciones (milésimas de segundo), podemos deducir que el tiempo que tarda en ejecutarse la operación de obtención de las zonas UAS es despreciable. Este resultado es favorable, ya que nos permite concluir que la carga computacional de dicha operación no impacta negativamente en el rendimiento general del módulo de asignación de amenaza.

Por otro lado, para la operación de cálculo del nivel de amenaza, podemos observar que cada `inferenceWorker` tarda en media 0.126 segundos en procesar un solo `track`; esto es, cada 1 segundo, cada `inferenceWorker` es capaz de asignar un nivel de amenaza al menos a 7 UAVs. Teniendo en cuenta que la prueba se realizó con 4 `inferenceWorkers` trabajando en paralelo, podemos concluir que el módulo de asignación de amenaza es capaz de procesar al menos 28 UAVs cada segundo.

Capítulo 5

Conclusiones

Este capítulo presenta las conclusiones derivadas del desarrollo de este trabajo, cuyo objetivo principal fue implementar un módulo de asignación de amenaza a aeronaves no tripuladas intrusas. A lo largo de esta investigación se abordaron diversos aspectos relacionados con el tema, con el fin de obtener una comprensión más profunda y avanzada en esta área de conocimiento.

En primer lugar, se llevó a cabo una revisión de la literatura científica y de las fuentes relevantes, lo que permitió establecer una base teórica sólida y un marco conceptual para el estudio. Se identificaron los principales enfoques y modelos utilizados en el tema de asignación de amenaza a aeronaves no tripuladas, lo que facilitó el diseño de la investigación y la interpretación de los resultados obtenidos.

En segundo lugar, se propuso un modelo mixto de asignación de amenazas, combinando las principales ideas de los enfoques de único comportamiento, específicamente las ideas de los modelos basados en distancia y basados en tiempo. También se tuvo en cuenta las fuentes de incertidumbre, agregando flexibilidad al modelo propuesto, de modo que se ajustase más a la realidad.

En tercer lugar, la interrogante se centró en la implementación del módulo de asignación de amenaza y en comprobar sus prestaciones para ser integrado a un sistema UTM/U-Space. Para responder a este objetivo, se emplearon herramientas del lenguaje de programación Python para implementar el módulo. También se realizaron pruebas de comportamiento y rendimiento para evaluar dicho módulo. Los resultados obtenidos indicaron que el módulo de asignación de amenaza presenta el comportamiento esperado y es capaz de dar respuesta rápida ante las peticiones realizadas por los controladores de tráfico aéreo. Estos resultados podrán ser relevantes para el posterior desarrollo de sistemas UTM/U-Space.

5.1. Líneas de trabajo futuras

Habiendo comprobado el correcto funcionamiento del módulo de asignación de amenaza con datos simulados, una primera recomendación como línea de trabajo futura sería probar el módulo con un flujo de datos reales, proveniente de maniobras realizadas por un UAV teledirigido por un humano.

De igual modo, se recomienda la realización de un trabajo comparativo, donde se compare la propuesta de modelo de asignación de amenaza de este trabajo con los modelos propuestos en otros.

Apéndice A

Gráficas de las simulaciones de la Sección 4.3.1

Descripción de las gráficas: Para cada vuelo simulado, se muestran tres gráficas. La primera gráfica muestra la posición de la zona UAS (en rojo) y la posición del UAV a lo largo del tiempo (en verde la posición real y en azul la posición estimada por sensores). La segunda gráfica muestra la distancia desde el UAV a la zona UAS, $D_{\text{uav-zona}}$ (en magenta) y el Tiempo de Colisión, $T_{\text{colisión}}$ (en anaranjado), en función del tiempo transcurrido. Por último, la tercera gráfica muestra la evolución del nivel de amenaza asignado al UAV en función del tiempo transcurrido.

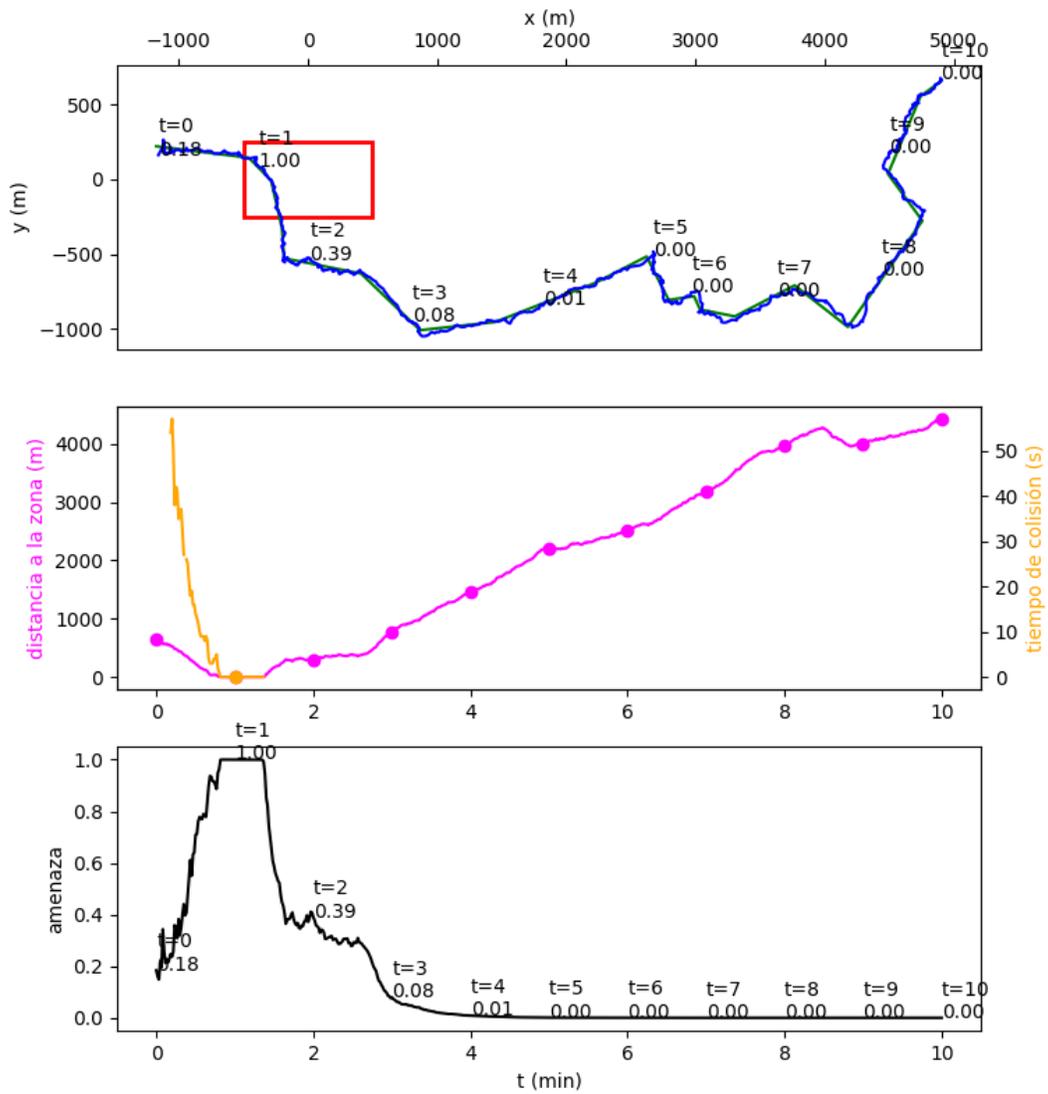


Figura A.1: Simulación de UAVs y asignación de amenaza.

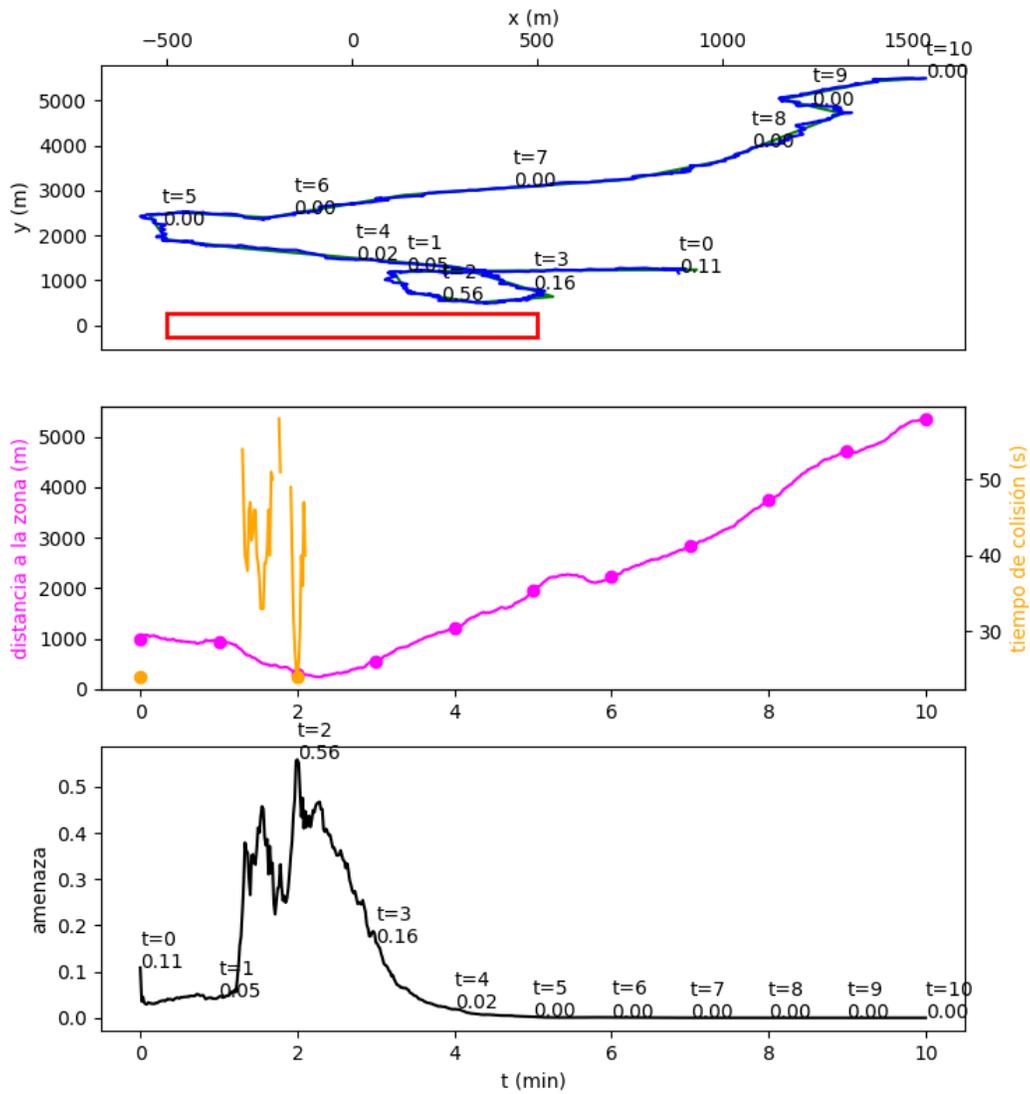


Figura A.2: Simulación de UAVs y asignación de amenaza.

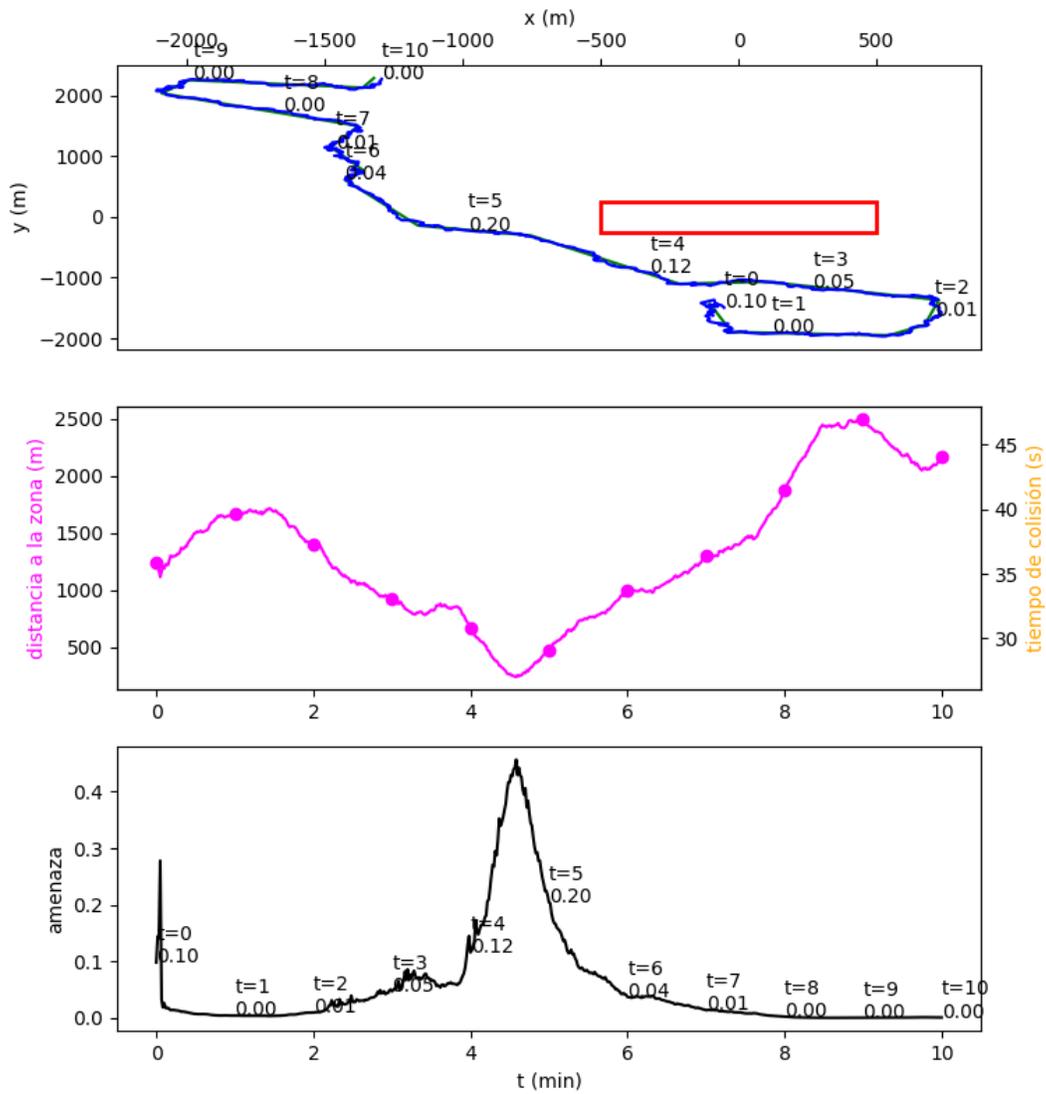


Figura A.3: Simulación de UAVs y asignación de amenaza.

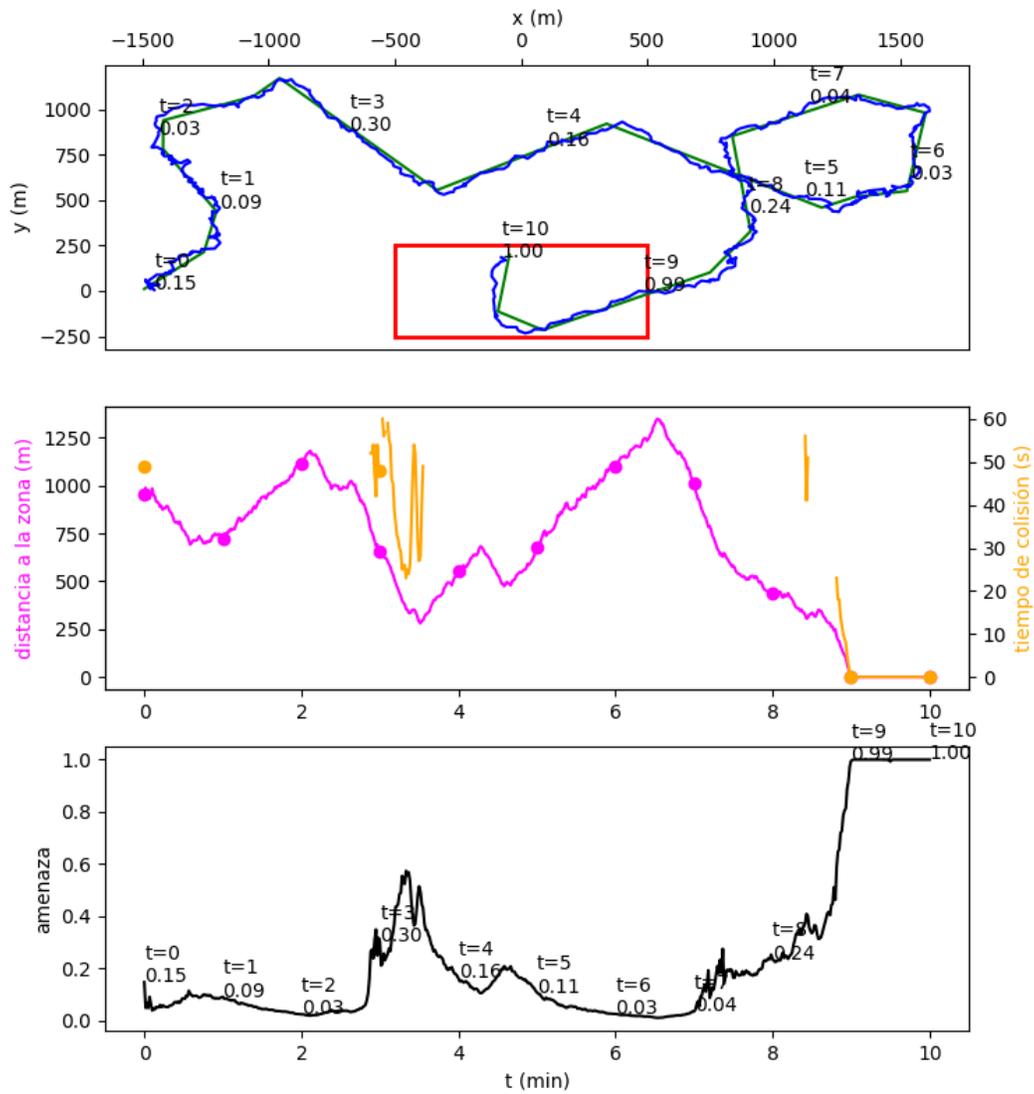


Figura A.4: Simulación de UAVs y asignación de amenaza.

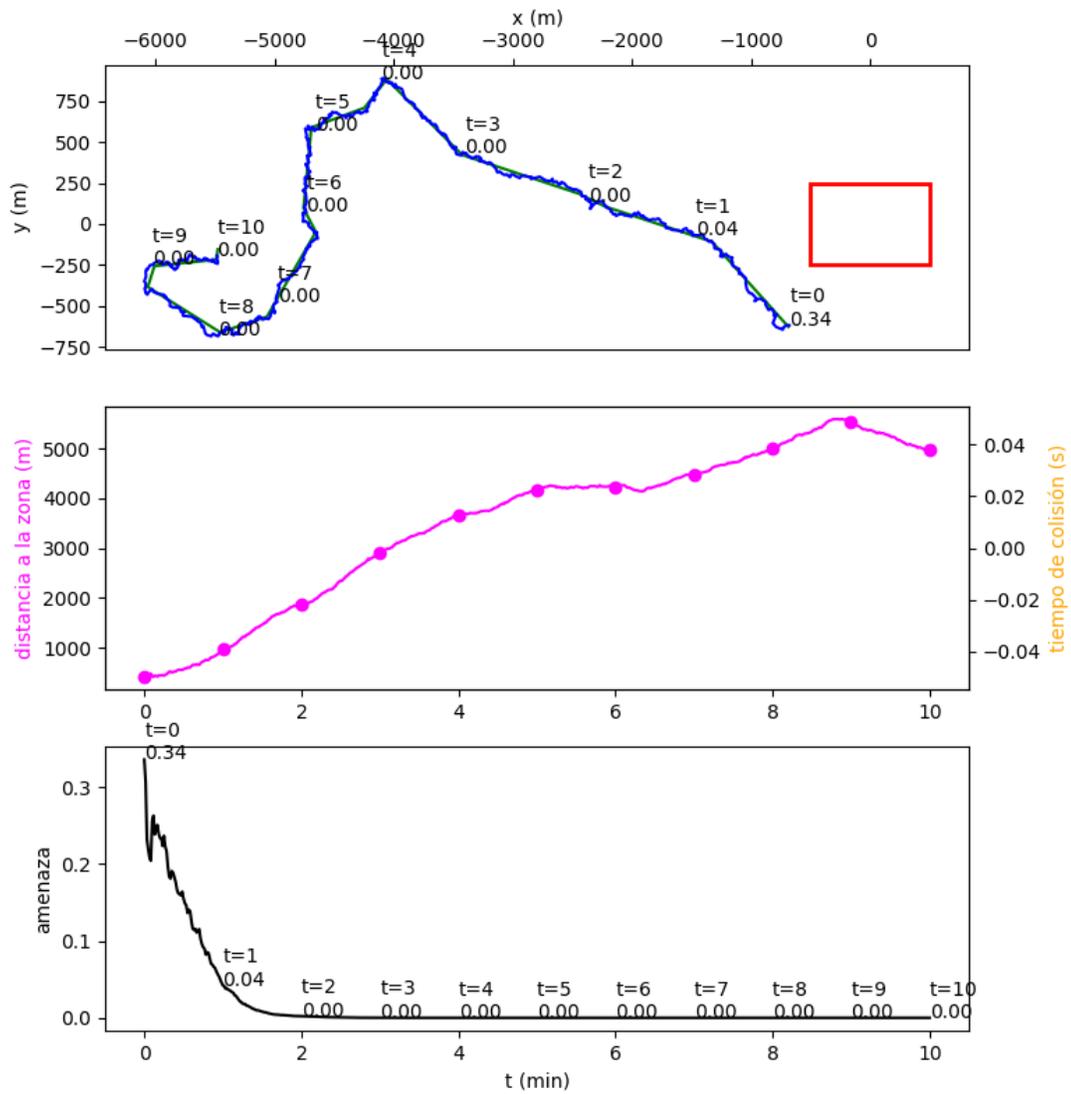


Figura A.5: Simulación de UAVs y asignación de amenaza.

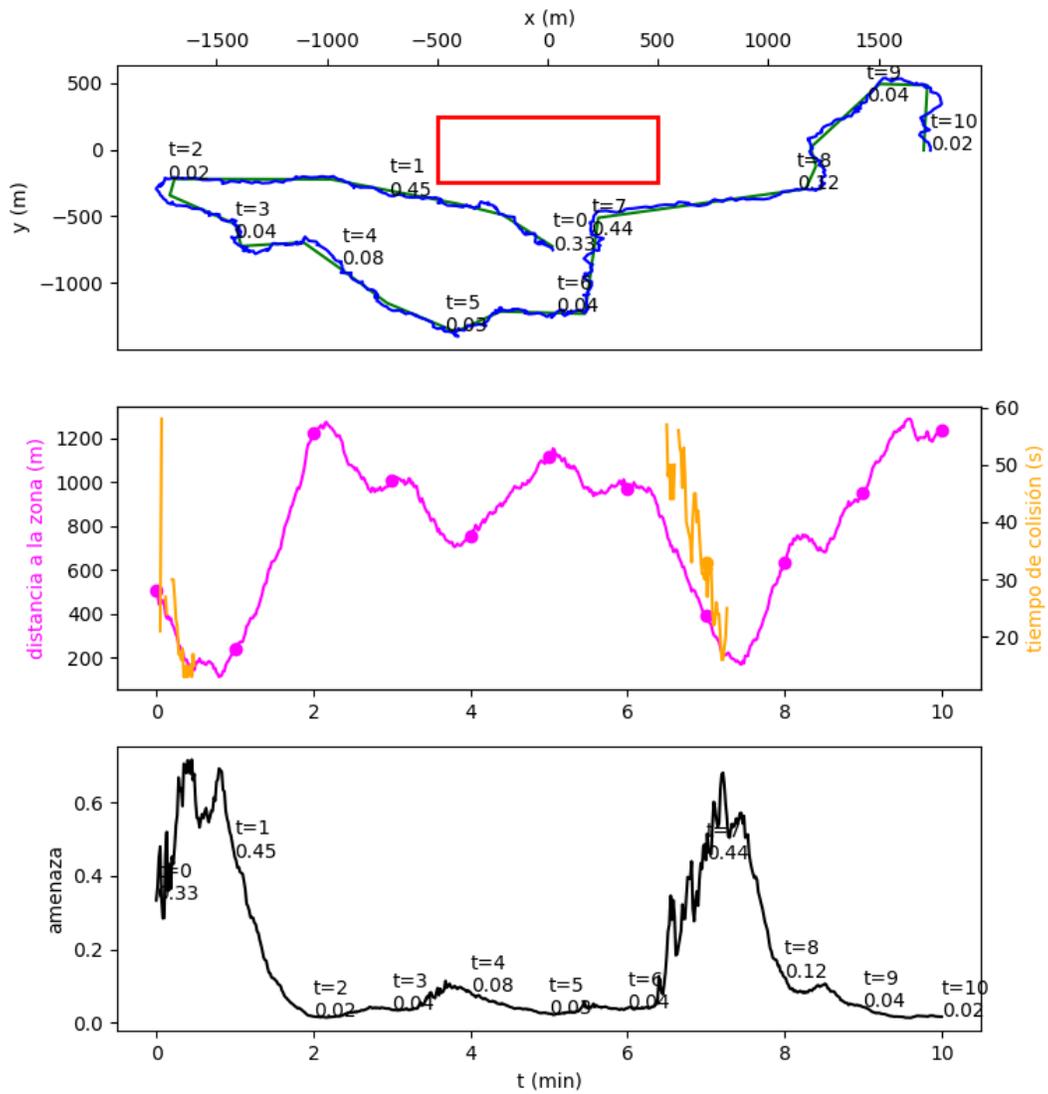


Figura A.6: Simulación de UAVs y asignación de amenaza.

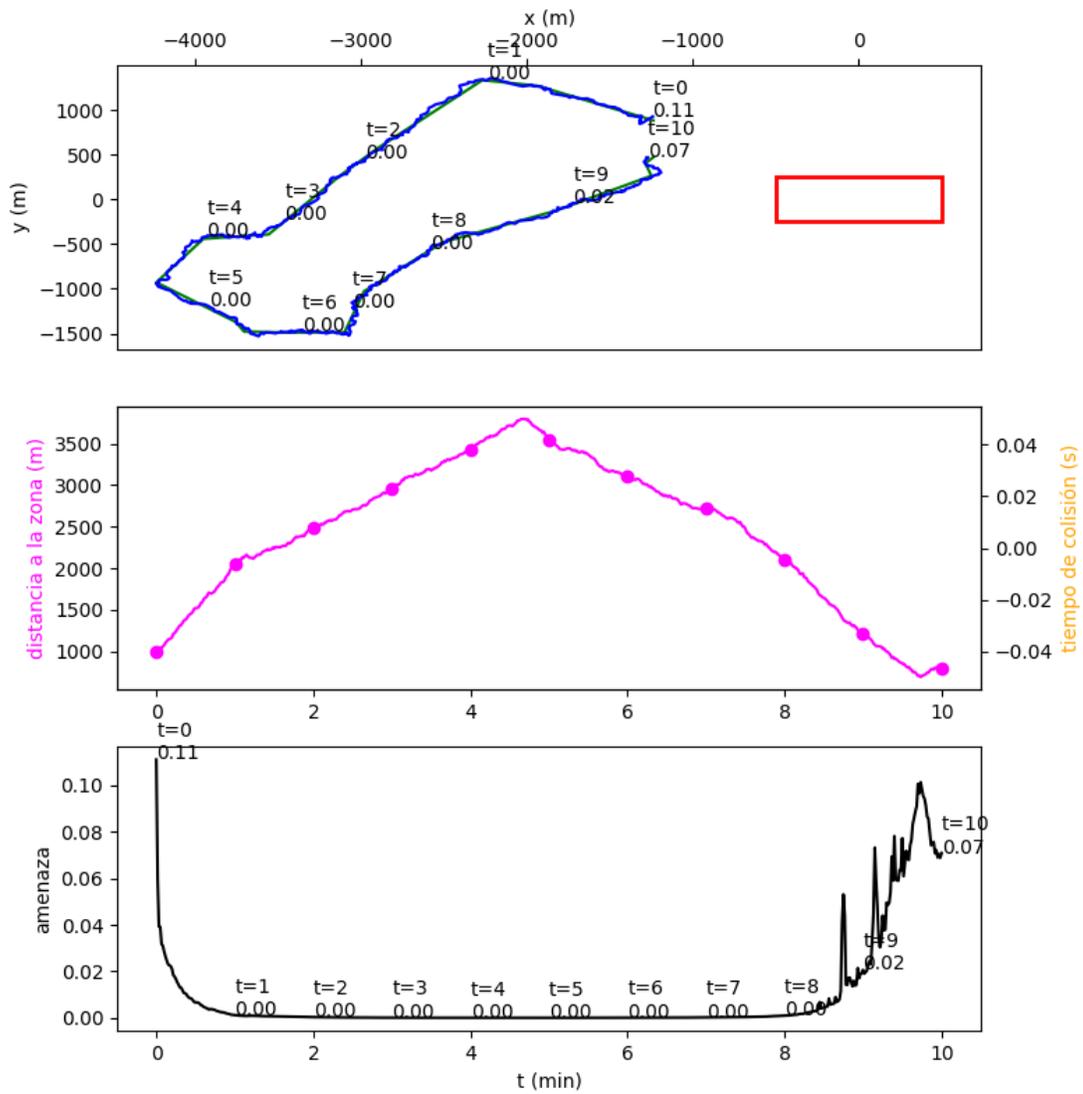


Figura A.7: Simulación de UAVs y asignación de amenaza.

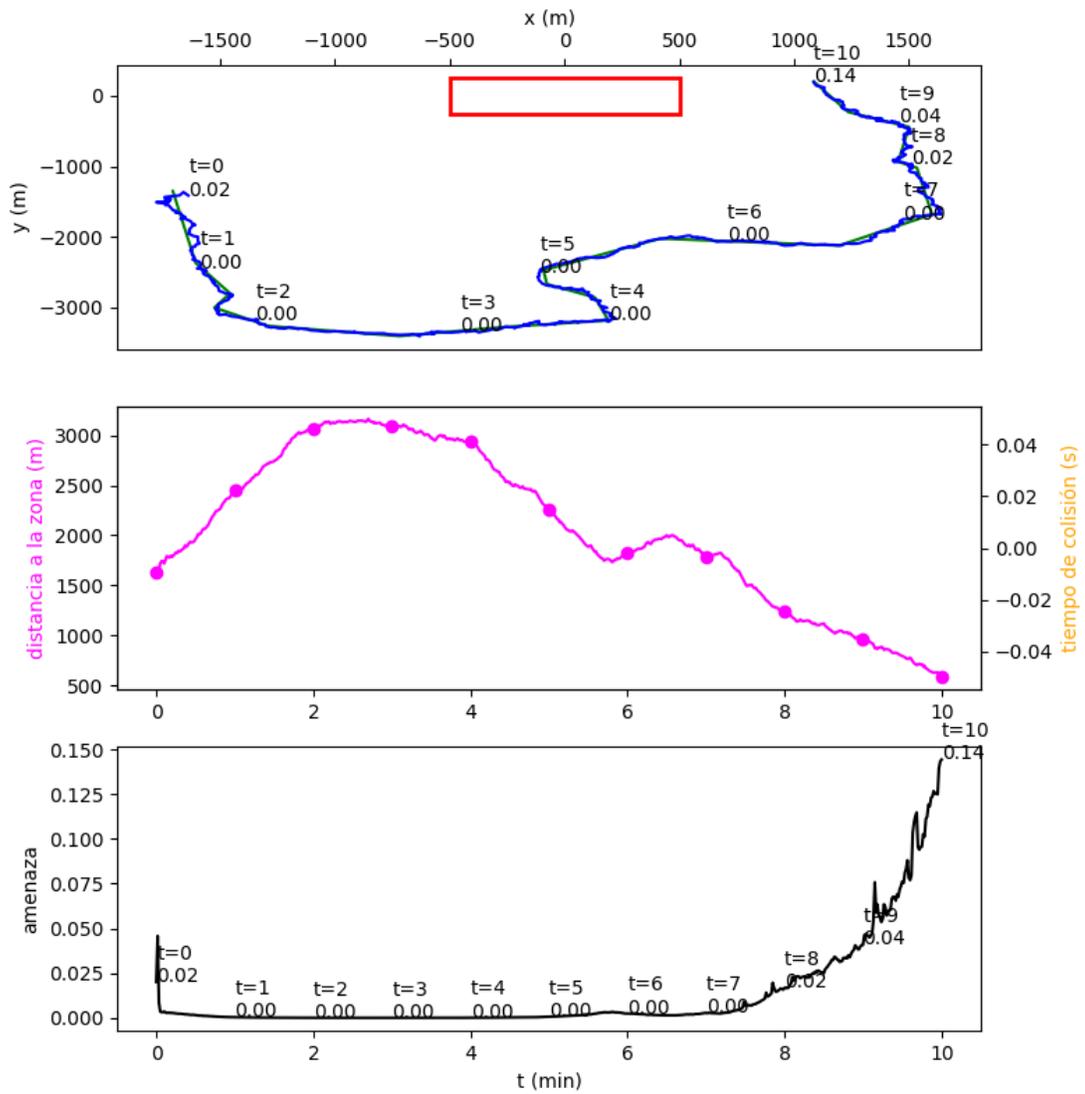


Figura A.8: Simulación de UAVs y asignación de amenaza.

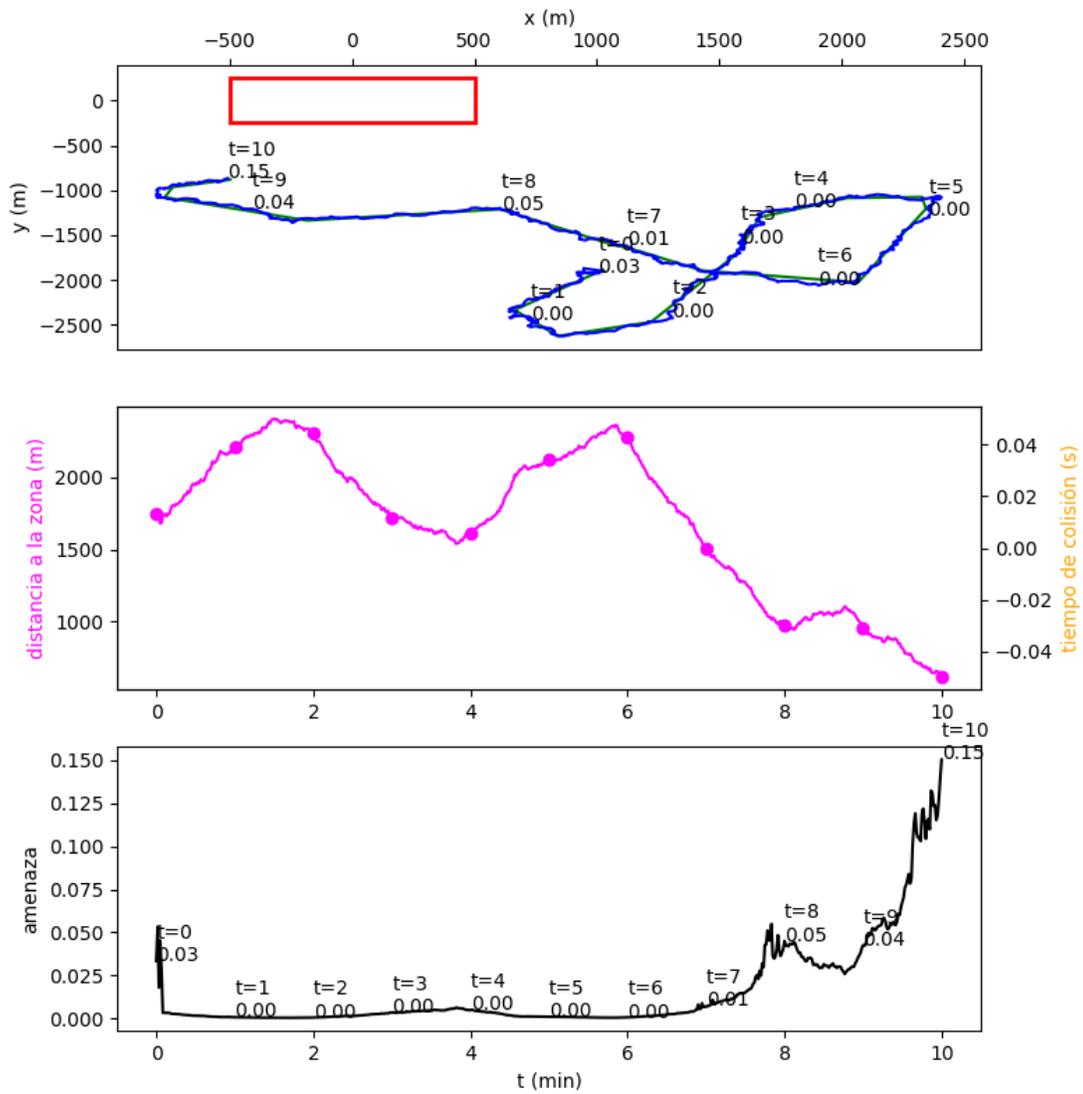


Figura A.9: Simulación de UAVs y asignación de amenaza.

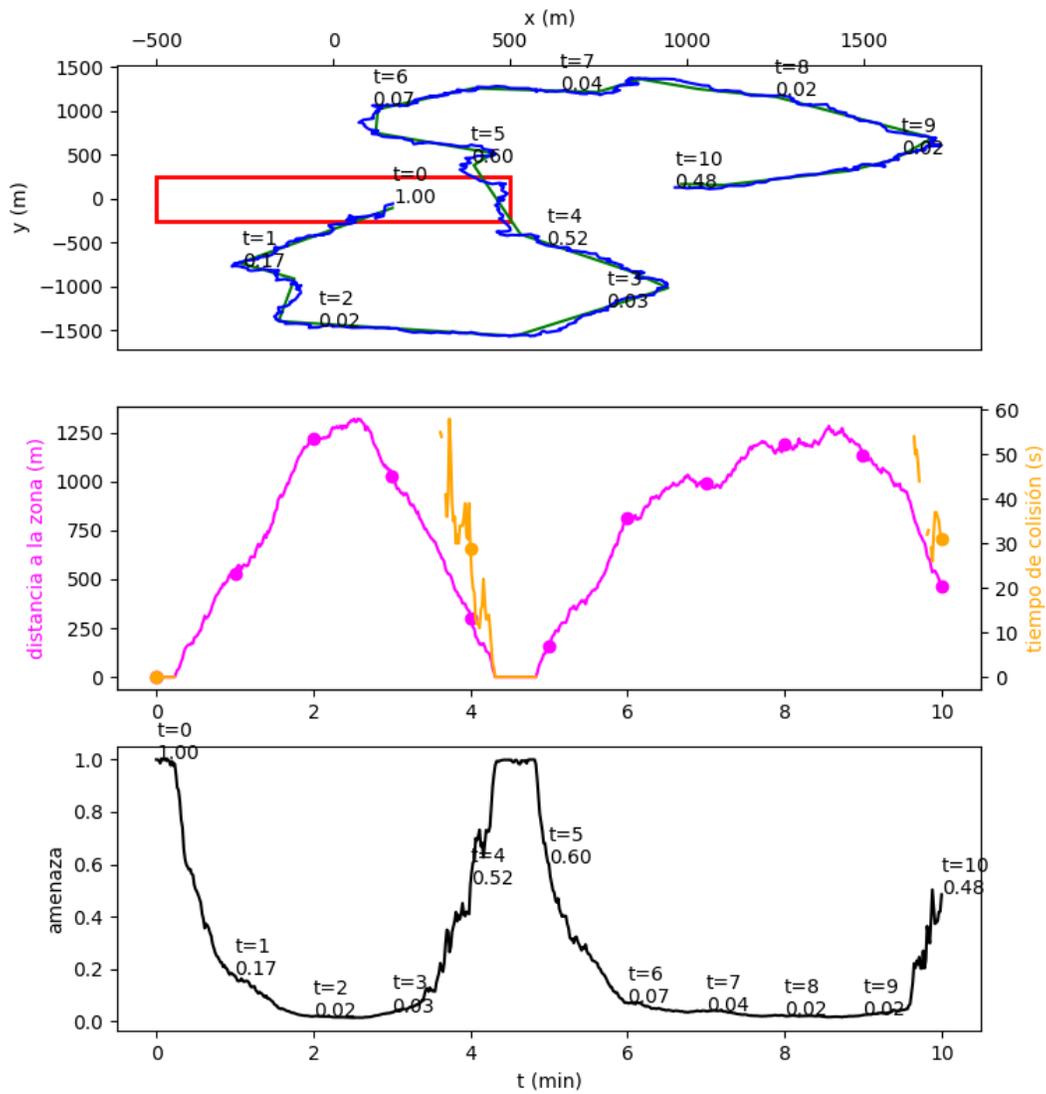


Figura A.10: Simulación de UAVs y asignación de amenaza.

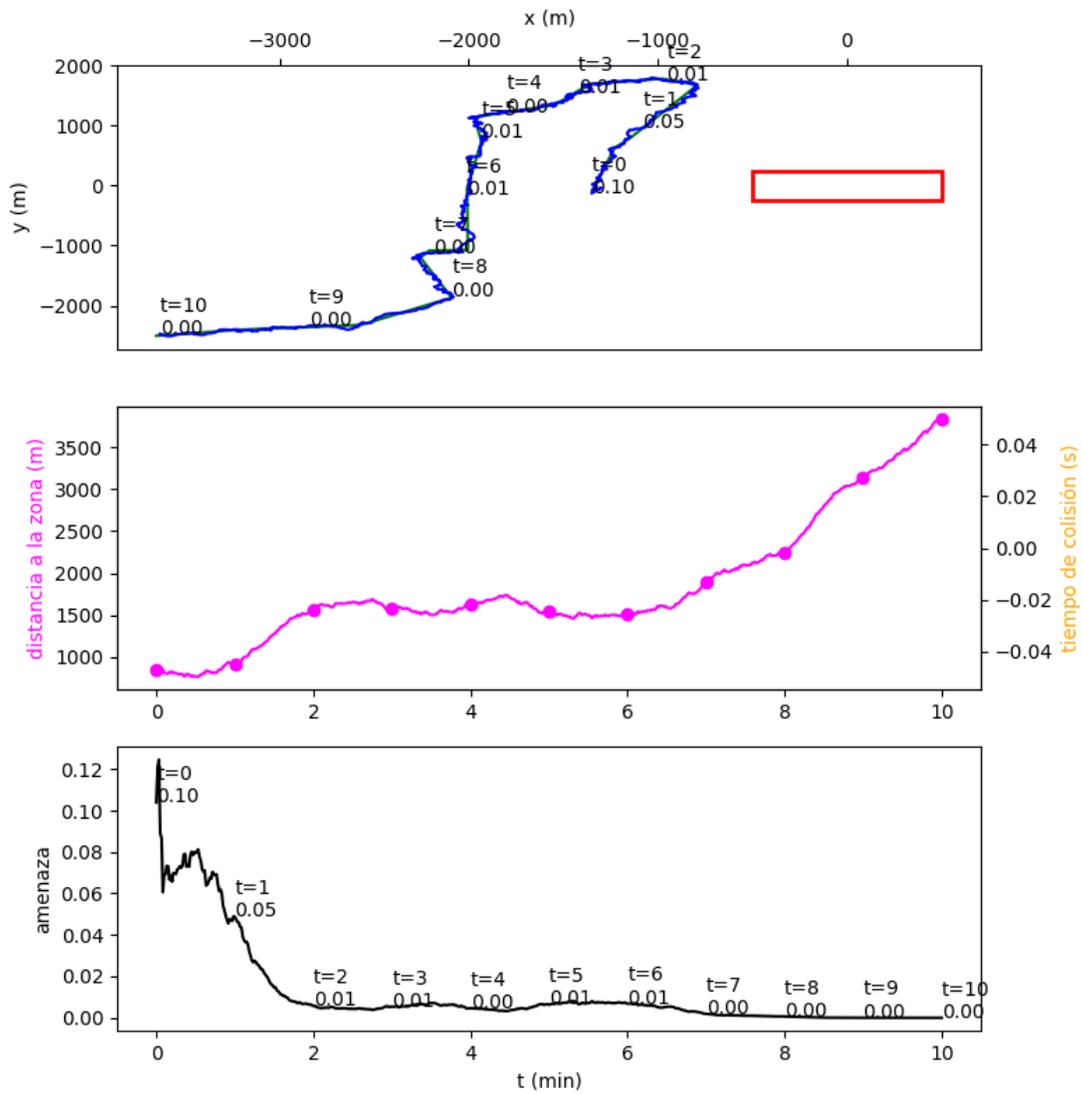


Figura A.11: Simulación de UAVs y asignación de amenaza.

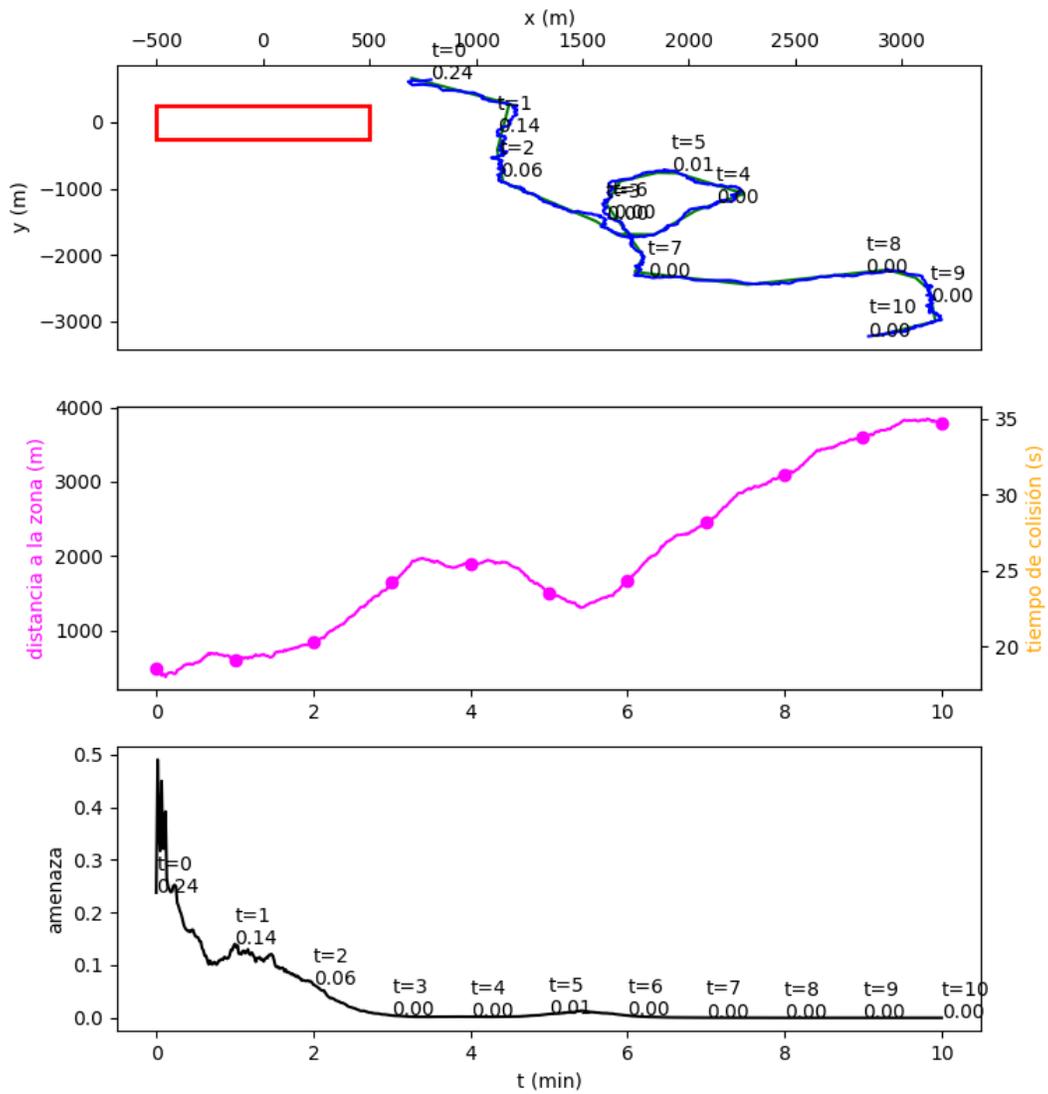


Figura A.12: Simulación de UAVs y asignación de amenaza.

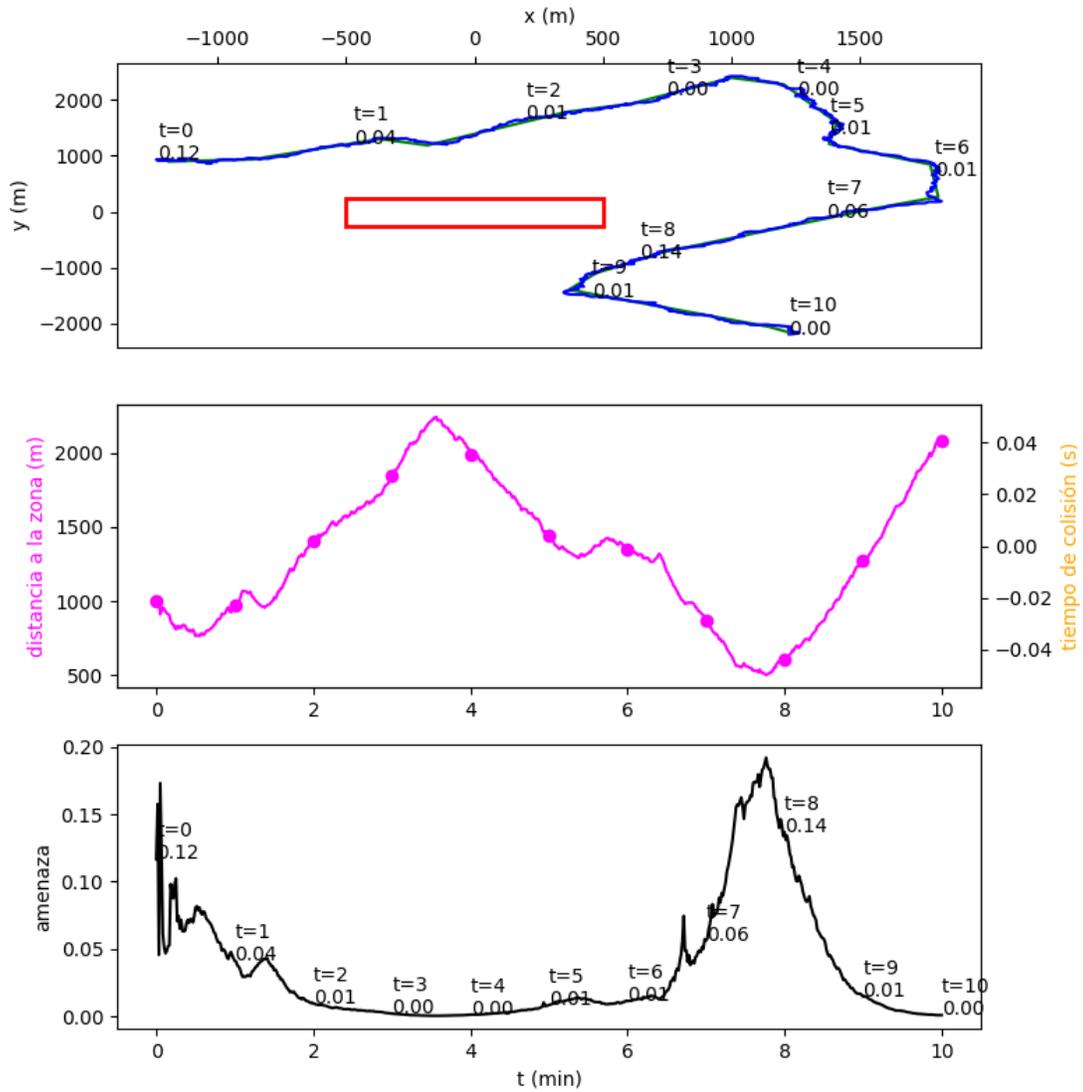


Figura A.13: Simulación de UAVs y asignación de amenaza.

Bibliografía

- [1] Anaconda, Inc. (2022). *Conda: Package, dependency, and environment management for any language*. Versión 22.9.0, <https://conda.io>.
- [2] Becker, A. (2023). Kalmanfilter.net. <https://www.kalmanfilter.net/>. Accedido 2022-11-15.
- [3] Beckmann, N., Kriegel, H., Schneider, R., and Seeger, B. (1990). The r*-tree: An efficient and robust access method for points and rectangles. *ACM SIGMOD Record*, 19:322–331.
- [4] Campos, G. R. D., Runarsson, A. H., Granum, F., Falcone, P., and Alenljung, K. (2014). Collision avoidance at intersections: A probabilistic threat-assessment and decision-making system for safety interventions. *17th IEEE International Conference on Intelligent Transportation Systems*, pages 649–654.
- [5] Chen, Y., Shen, K., and 8th Conference on, S. W. . I. (2013). Forward collision warning system considering both time-to-collision and safety braking distance. *ieeexplore.ieee.org*, pages 972–977.
- [6] Dahl, J., Zenuity, G. R. D. C., Zenuity, C. O., Fredriksson, J., de Campos, G. R., and Olsson, C. (2019). Collision avoidance: A literature review on threat-assessment techniques. *ieeexplore.ieee.org*, 4:101–113.
- [7] Di, R., Gao, X., Guo, Z., and Wan, K. (2018). A threat assessment method for unmanned aerial vehicle based on bayesian networks under the condition of small data sets. *Mathematical Problems in Engineering*, 2018:1–17.
- [8] Eidehall, A. and Madås, D. (2013). Real time path planning for threat assessment and collision avoidance by steering. *16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013)*, pages 916–921.
- [9] Eidehall, A. and Petersson, L. (2008). Statistical threat assessment for general road scenes using monte carlo sampling. *IEEE Transactions on Intelligent Transportation Systems*, 9:137–147.
- [10] Gilles, S. and Butle, H. (2022). *Rtree: Spatial indexing for Python*. Versión 1.0.1, <https://rtree.readthedocs.io/en/latest/>.

- [11] Gillies, S., van der Wel, C., Van den Bossche, J., Taves, M. W., Arnott, J., and Ward, B. C. (2022). *Shapely: Manipulation and analysis of geometric objects in the Cartesian plane*. Versión 2.0.1, <https://shapely.readthedocs.io/en/stable/>.
- [12] Gruner, R., Henzler, P., Hinz, G., Eckstein, C., and Knoll, A. (2017). Spatio-temporal representation of driving scenarios and classification using neural networks. *IEEE Intelligent Vehicles Symposium*, page 1782–1788.
- [13] Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., Gérard-Marchant, P., Sheppard, K., Reddy, T., Weckesser, W., Abbasi, H., Gohlke, C., and Oliphant, T. E. (2020). Array programming with NumPy. *Nature*, 585(7825):357–362.
- [14] Harrison, T., Johnson, K., Moye, J., and Young, M. (2020). Space threat assessment 2020. *CSIS Aerospace Security Project’s annual flagship report on counterspace weapons developments*.
- [15] Herrera, G., Dechant, J., Green, E., and Klein, E. (2017). Technology trends in small unmanned aircraft systems (suas) and counter-uas: A five-year outlook. *INSTITUTE FOR DEFENSE ANALYSES*.
- [16] Hirsch, M., Pavlick, R., cchuravy, Marks, S., and Rivière, P. (2019). *Pymap3d: pure-Python (Numpy optional) 3D coordinate conversions for geospace ecef enu eci*. Versión 1.8.1, <https://github.com/geospace-code/pymap3d>.
- [17] Hirt, C. and Featherstone, W. (2008). Conversion of geodetic coordinates to the local east, north, up coordinate system and vice versa. *Journal of Geodesy*, 82:425–435.
- [18] Hixie, I., Thewlis, I., McManus, P., and Robinson, D. (2011). WebSocket: A communication protocol for web applications. *World Wide Web Consortium (W3C)*.
- [19] Houénou, A., Bonnifait, P., and Cherfaoui, V. (2014). Risk assessment for collision avoidance systems. *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pages 386–391.
- [20] Hussein, A., Gaber, M. M., Elyan, E., and Jayne, C. (2017). Imitation learning: A survey of learning methods. *ACM Computing Surveys*, 50(2):1–35.
- [21] Jordahl, K., Van den Bossche, J., Fleischmann, M., Wasserman, J., and McBride, J. (2020). *Geopandas: Python tools for geographic data*. Versión 0.8.1, <https://geopandas.org/>.

- [22] Kim, K.-Y., Park, J.-W., and Tahk, M.-J. (2007). Uav collision avoidance using probabilistic method in 3-d. *2007 International Conference on Control, Automation and Systems*, pages 826–829.
- [23] Ko, Y. L., Ho, K. E., Matson, E. T., Ko, Y., Ho, E., and Lee, M. (2020). Uav threat level assessment based on the velocity and distance from collision. *ieeexplore.ieee.org*, pages 495–500.
- [24] Kowshik, H., Caveney, D., and Kumar, P. R. (2011). Provable system wide-safety in intelligent intersections. *IEEE Transactions on Vehicular Technology*, 60(3):804–818.
- [25] Loos, S., Platzer, A., and Nistor, L. (2011). Adaptive cruise control: Hybrid, distributed, and now formally verified. *Lecture Notes in Computer Science, Springer*, 6664:42–56.
- [26] Mertens, B. (2011). Multiprocessing in python. *ACM SIGPLAN Notices*, 46:45–50.
- [27] The Python team (2022). *Multiprocessing: Process-based parallelism*. Versión 3.9.16, <https://docs.python.org/3.9/library/multiprocessing.html>.
- [28] Van Rossum, G. and Drake Jr, F. L. (2021). *Python: A dynamic, open-source programming language*. Versión 3.9.6, <https://www.python.org/>.
- [29] Wang, C. H., Tan, S. K., and Low, K. H. (2019). Collision risk management for non-cooperative uas traffic in airport-restricted airspace with alert zones based on probabilistic conflict map. *Transportation Research Part C: Emerging Technologies*, 109:19–39.
- [30] Zhang, Y., Antonsson, E. K., and Grote, K. (2006). A new threat assessment measure for collision avoidance systems. *IEEE Intelligent Transportation Systems Conference*, pages 968–975.