



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones en un Ejército de Drones

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Gonzalo Lorén Garay

DIRECTOR: José P. González Coma

CURSO ACADÉMICO: 2021-2022

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones en un Ejército de Drones

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

En este trabajo se pretende exponer un caso hipotético, que bien podría ser real, de una determinada operación militar ofensiva. Dicha operación se realizaría en un área de combate de 40 x 40 kilómetros, durante 3 días. No es novedoso que en la actualidad estas operaciones se apoyen en drones. La novedad en este estudio, es realizar este tipo de operación sólo y exclusivamente con drones dentro del área de combate. El número de drones que se calcula para llevar a cabo con éxito esa operación es de unos 5.000. Evidentemente la operación implicaría también una elevada intervención humana, pero sin que ningún humano entrara físicamente en el área de combate. No se espera, por tanto, sufrir ninguna baja propia.

Desde el punto de vista técnico, el objetivo es atender a todos los requerimientos en cuanto a comunicaciones y posicionamiento que una operación de esta índole requeriría.

En la exposición se tocarán también, a modo de ambientación, algunos asuntos puramente militares o de otras técnicas ajenas a este Máster.

Por otro lado se expondrán brevemente, y sin entrar demasiado en profundidad, todas aquellas cuestiones y problemas que requieren una decisión y resolución técnica, y que tienen que ver directamente con diversas asignaturas del Máster.

El estudio ha tenido gran amplitud horizontal a costa de tener una limitada amplitud vertical. En él, se dan unas directrices estratégicas para acometer los diversos problemas técnicos.

Las soluciones aportadas han sido escogidas por el alumno de acuerdo a sus conocimientos (tanto los anteriores que poseía, como los adquiridos en el Máster) y expuestas de forma esquemática y ordenada en un estudio de alto nivel.

Se considera que la tecnología para llevar a cabo esta operación está perfectamente asentada, y el problema principal radica en la consecución de la mezcla e implementación de las diferentes tecnologías de una forma coordinada y realista.

PALABRAS CLAVE

Dron, drones, posicionamiento, UMS, RPAS, UAV, UGV, WiMAX, DTN, GNSS, TACAN, JCOP.

AGRADECIMIENTOS

A José P. González Coma, tutor de este trabajo, por ayudarme a llevarlo a buen puerto.

A mi mujer, Susana, y a mis hijas, Laura e Irene, por soportar mis ausencias con paciencia.

A mi madre, Pilar, a quien debo mucho más que mi existencia¹.

¹ Agradecimiento real, pero además, la cita es un guiño a la dedicatoria de: Michael M. Cirovic (1979) “Electrónica Fundamental: Dispositivos, Circuitos y Sistemas”, de Editorial Reverte [1]. Mi libro de cabecera de estudiante desde 1984 (su madre se llamaba Smilja).

CONTENIDO

Contenido	1
Índice de Figuras	4
1 Introducción.....	5
1.1 Objeto y exposición inicial	5
1.2 Tipo de operación militar	5
1.3 Significado real de “dron” y significado en este trabajo	6
1.4 Distintos tipos de drones	7
1.4.1 Por el Medio donde se desplazan.....	7
1.4.2 Por su sistema de propulsión	7
1.4.3 Por su sistema de alimentación.....	7
1.4.4 Por la autoría del diseño	7
1.4.5 Por su letalidad	7
1.4.6 Por su grado de iniciativa	8
1.4.7 Por sus sistemas de comunicaciones y navegación	8
1.4.8 Por su precio, complejidad e importancia táctica	8
1.5 Distintas funcionalidades de los drones	9
1.5.1 Sensores	9
1.5.2 Apoyo a los sensores. Iluminadores	10
1.5.3 Apoyo al ataque. Designadores	11
1.5.4 Ataque y destrucción. Armamento y munición.	11
1.5.5 Apoyo a las comunicaciones	12
1.5.6 Apoyo al posicionamiento	13
1.5.7 Funcionalidad como señuelo	14
1.5.8 Funcionalidad combinada	14
2 Sistemas de comunicaciones	15
2.1 Introducción a los sistemas de comunicaciones necesarios	15
2.1.1 Primera aproximación.....	15
2.2 Miscelánea de Comunicaciones	16
2.2.1 Introducción	16
2.2.2 Tiempo y sincronía	16
2.2.3 Juegos de claves, aplicaciones e indicativos.....	17
2.2.4 Utilización de SDR y SDN	17
2.3 Sistemas de comunicaciones no guiadas en los drones.....	18
2.3.1 Introducción a los diferentes sistemas	18

2.3.2 Comunicaciones satelitales	18
2.3.3 Comunicaciones por radioenlace micro ondas	19
2.3.4 Comunicaciones VHF y UHF	20
2.3.5 Comunicaciones HF	20
2.3.6 Autorización para el uso de frecuencias	21
2.4 Sistemas de comunicaciones y posicionamiento en el “Área Humana”	21
2.4.1 Introducción al concepto “Área Humana”	21
2.4.2 La JCOP, Joint Common Operational Picture	22
2.4.3 Puestos de mando	23
2.4.4 Zona de cabinas de pilotaje - conducción	23
2.4.5 Estaciones de anclaje de satélite	25
2.4.6 Áreas de antenas de radio	26
2.4.7 Áreas de antenas de radioenlaces	27
2.4.8 Áreas de antenas para apoyo a la localización y navegación	28
2.4.9 Sistema radiogoniométrico de vigilancia de emisiones enemigas y localización propia. 28	
2.4.10 Sistemas de comunicaciones entre las distintas zonas del Áreas Humana	30
2.5 Utilización del WiMAX	31
2.5.1 Introducción al WiMAX	31
2.5.2 OFDMA, MIMO y HARQ	31
2.5.3 Implementación del WiMAX en el ejército de drones	32
2.6 Utilización del DTN	33
2.6.1 Introducción al DTN	33
2.6.2 Historia y descripción del DTN	33
2.6.3 Estudio preliminar de la aplicación del DTN a los enjambres de drones	34
2.6.4 Funcionamiento y ventajas del DTN	35
2.6.5 Posibles aplicaciones militares del DTN	36
2.6.6 Aplicación concreta del DTN en el caso de estudio	37
2.6.7 Conclusiones obtenidas sobre la aplicación del DTN en el caso de estudio	37
3 Sistemas de localización y posicionamiento	40
3.1 Introducción a la localización	40
3.1.1 Sistemas primarios y secundarios	40
3.1.2 Posicionamiento directo e inverso	40
3.1.3 Triangulación y Trilateración	40
3.1.4 La coordenada altura	41
3.2 Sistemas de localización y posicionamiento	41
3.2.1 GNSS: GPS y Galileo	41

3.2.2 TACAN, DME y NDB	42
3.2.3 Sistemas dummies, señuelos y brújulas electrónicas.....	42
3.3 Otros sistemas avanzados.....	43
3.3.1 Otros sistemas avanzados de localización y navegación	43
3.3.2 Conclusiones sobre localización y navegación.....	44
4 Esquema general de interrelación.....	45
4.1 Posicionamiento inicial	45
4.1.1 Otros medios puramente militares	45
4.2 Desarrollo cronológico de la operación	45
4.2.1 Punto de partida	45
4.2.2 Oleada de señuelos	45
4.2.3 Despliegue de drones de comunicaciones	46
4.2.4 Avance de drones de movilidad.....	46
4.2.5 Avance masivo de drones terrestres y aéreos	47
5 Conclusiones finales.....	48
5.1 Cumplimiento de objetivos y conclusiones	48
6 Líneas Futuras	49
6.1 Líneas Futuras	49
7 Bibliografía.....	50
Anexo I: Asignaturas del Máster relacionadas.....	52

ÍNDICE DE FIGURAS

Figura 1-1: Esquema de las distintas zonas de la operación.	6
Figura 1-2: Recreación de drones de comunicaciones terrestres (de cadena y de rueda).	13
Figura 2-1 Típica red de comunicaciones de drones	18
Figura 2-2: En la figura puede verse la distribución del Área Humana, de la banda de seguridad de 10km y del Área de la Operación de 40x40 km.	22
Figura 2-3: Operations Room. Donde puede verse una JCOP “de actualización manual” (Imperial War Museum Duxford). Es de 1940, pero aunque la tecnología ha cambiado, la función que realiza es exactamente la misma.	23
Figura 2-4: Recreación de una cabina de conducción / pilotaje.....	24
Figura 2-5: Recreación de una zona de cabinas de conducción / pilotaje.	25
Figura 2-6: Recreación de una estación de anclaje satélite de instalación fija.	25
Figura 2-7: Recreación de la zona de antenas de radio y radioenlaces.	27
Figura 2-8: Recreación de las antenas de TACAN, DME y NDB. Cada juego situado a derecha e izquierda del frente.	28
Figura 2-9: En la figura puede verse la distribución de las antenas para distintas frecuencias de un emplazamiento de radiogoniometría	29
Figura 2-10: En la figura puede verse la distribución de las distintas zonas del Área Humana. En retaguardia, los distintos routers van unidos mediante fibra óptica.	30
Figura 2-11: Ejemplo de escenario con nodos heterogéneos inalámbricos.	34
Figura 2-12: Ejemplo de red definida por software con drones [5].	38
Figura 4-1: Recreación de red de comunicaciones que se va desplegando a medida que avanzan los drones.	46
Figura 4-2: Recreación de drones para facilitar la movilidad.	47
Figura 5-1 Fotograma de la película “Terminator 3” donde se muestra un particular “ejército de máquinas”.	48

1 INTRODUCCIÓN

1.1 Objeto y exposición inicial

El objeto de este Trabajo de Fin de Máster (TFM) es el diseño, a nivel teórico, de los sistemas de comunicación y posicionamiento de un “Ejército de Drones” para una operación militar de gran envergadura.

No es novedoso el empleo de drones en el campo de batalla como auxiliar del combatiente humano. En este TFM se pretende estudiar una operación donde un bando actúe en un espacio de batalla solamente con drones, de manera que, en teoría, la operación se llevaría a cabo sin bajas humanas propias. Se pretende emplear en la operación de forma coordinada un número masivo de drones. A esto se le llama coloquialmente “enjambre”.

En la exposición del trabajo se mencionarán aspectos relativos a posicionamiento y comunicaciones. Se considera que estos aspectos son importantes, pues representan el *core* de la asignatura del Máster, TEL 3². No obstante, será inexcusable tratar otros aspectos que servirán de “ambientación” para encajar la tecnología descrita en una situación real, lo cual aportará una visión de aplicación práctica de estas tecnologías. No se puede exponer la solución técnica a un problema si no se describe previamente el problema a resolver.

El alumno pretende buscar la originalidad diseñando métodos novedosos que se integrarían con tecnologías ya existentes. Hay que reseñar que aquellas partes que son fruto de la imaginación del alumno carecerán de citas bibliográficas (por propia definición).

1.2 Tipo de operación militar

La operación que se pretende llevar a cabo es una ofensiva convencional en un frente de 40 km con una profundidad de penetración también de 40 km. El número previsto de drones será de 5.000 y la duración de la operación de 3 días. Se supone que se tiene cierta superioridad (aérea y de fuegos, por lo menos) y se pretende sustituir una ofensiva terrestre convencional con una “división humana” por una ofensiva de efectos similares realizada íntegramente con drones.

En el caso de una operación ofensiva convencional, ésta sería llevada a cabo teniendo previstas unas reservas. En este caso, aparte de tener un número de drones en reserva (de los distintos tipos), el diseño se realizará teniendo en cuenta este mismo concepto. Así pues, los cálculos se harán para una ofensiva llevada a cabo por 8.000 drones, durante un máximo de 5 días, en un área de 50 x 50 km.

Al ser una hipotética operación de guerra convencional no habría limitaciones para realizar determinadas acciones (por ejemplo, bombardear todas las instalaciones de telefonía móvil civil que estuvieran emitiendo en el área de la operación militar). La hipótesis es una operación en campo abierto, en una zona sin apenas habitantes. Se estima inviable realizar una operación de este tipo en una zona urbana o con cierta densidad de población. Si este fuera el caso, sería ineludible que el elemento humano participara también en la operación entrando físicamente en la zona.

² Sistemas de comunicaciones vía satélite, de posicionamiento, teledetección y radionavegación (204).

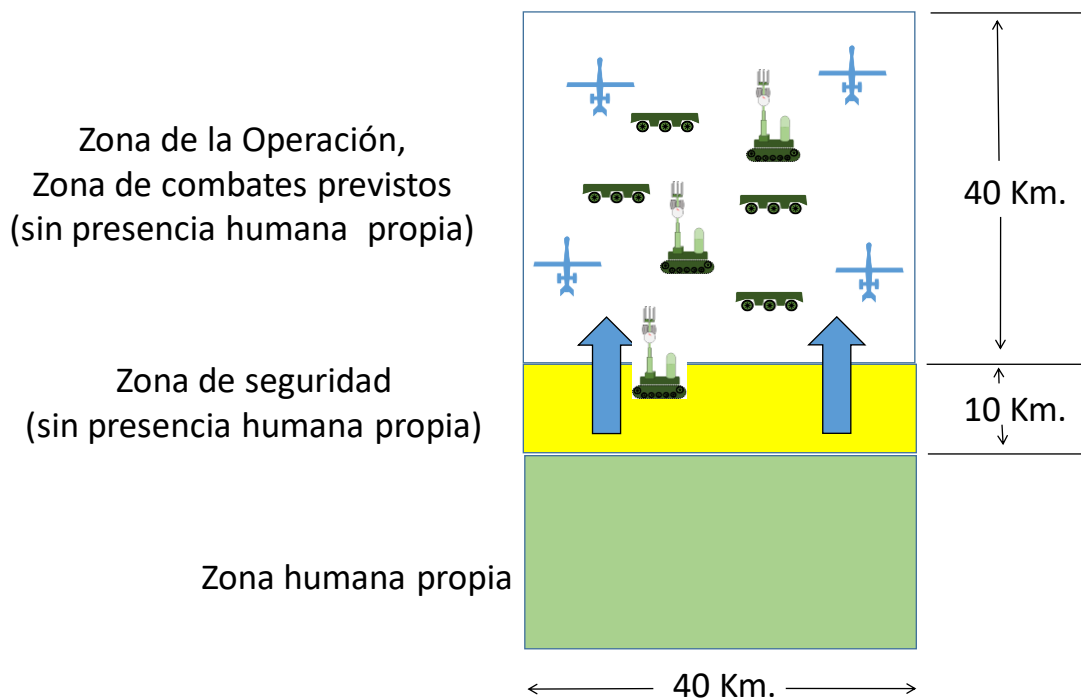


Figura 1-1: Esquema de las distintas zonas de la operación.

1.3 Significado real de “dron” y significado en este trabajo

Según la RAE³, “dron” es: *Aeronave no tripulada. (Del inglés drone)*. Se ha escogido esta palabra por ser la más conocida y de uso más coloquial, aun a sabiendas de que no coincide plenamente con el significado que se le va a dar en este trabajo. En este estudio se amplía el campo semántico y se incluirá también cualquier tipo de sistema NO tripulado⁴ (autónomo, operado remotamente o mixto), terrestre⁵ o aéreo⁶, y con la capacidad de cambiar su trayectoria intencionadamente [19].

Por lo dicho anteriormente se incluirán también bajo la designación de “dron” los misiles⁷ (que podrían considerarse “vehículos kamikaze”) pero no los cohetes (que no tienen capacidad de alterar su trayectoria) [20].

³ Real Academia Española (de la Lengua).

⁴ *Unmanned Systems* (UMS).

⁵ En puridad no existen drones terrestres según la definición de dron. Más correcto sería UGV (*Unmanned Ground Vehicle*).

⁶ UAV (*Unmanned Aerial Vehicle*), también RPAS (*Remotely Piloted Aircraft System*).

⁷ No es habitual considerar a los misiles, ni a las aeronaves por Control Remoto, como UAV, pero en este trabajo sí se incluirán en esta categoría.

1.4 Distintos tipos de drones

En este ejército, tendrán cabida drones de muy diversas características.

1.4.1 *Por el Medio donde se desplazan*

Por el medio por el que desplazan se dividirán entre drones terrestres y aéreos. También podrían utilizarse drones acuáticos y subacuáticos (submarinos), aunque no se han contemplado en este trabajo porque en ese caso habría que analizar el distinto comportamiento de sus sistemas de comunicaciones y localización en el medio acuático.

1.4.2 *Por su sistema de propulsión*

Según su sistema de propulsión, los terrestres pueden desplazarse mediante ruedas o bien con cadenas. Con el primer sistema se obtiene mayor velocidad, pero con el segundo los drones pueden desplazarse por terrenos más accidentados. En cuanto a los aéreos, se contemplan los de ala fija o ala rotatoria. Los de ala fija deben contar con un sistema de despegue y aterrizaje (o asumir su pérdida y contar sólo con un sistema de despegue). El inconveniente del ala rotatoria suele ser su menor velocidad y alcance. En este trabajo los únicos drones de ala rotatoria serán los “drones cautivos”.

Como caso particular de propulsión estaría el “motor cohete”, bien de propergol sólido, líquido o híbridos. Este sería el sistema de propulsión de los misiles (que, como se ha dicho, se consideran drones en este trabajo).

1.4.3 *Por su sistema de alimentación*

Según su sistema de alimentación, los drones podrán extraer su energía de motores de explosión o combustión, o bien estar alimentados por baterías eléctricas. Algunos drones terrestres podrán recargar esas baterías también con placas solares. Esto es especialmente útil en el caso de drones cuya misión requiera una ubicación estática durante un tiempo relativamente largo. Los “drones cautivos” serán alimentados eléctricamente mediante cable desde su “nodriza” terrestre.

1.4.4 *Por la autoría del diseño*

En cuanto al diseño de los sistemas, el alumno pretende diseñar (al menos de forma teórica) un sistema de comunicaciones y otro de localización. Conviviendo con el *Diseño Propio* se describirán sistemas COTS⁸.

1.4.5 *Por su letalidad*

Existirán drones con capacidad letal y sin ella. La capacidad letal será la adecuada a los objetivos sobre los que se quieran producir los efectos, pudiendo ser estos edificaciones y construcciones militares, sistemas defensivos (muros, alambradas, campos de minas...), vehículos con distintos grados de protección (acorazados, semi protegidos o sin protección) o personal al descubierto. Los drones sin

⁸ *Commercial off the shelf*, ya disponibles en el mercado.

capacidad letal serán, por ejemplo los de ISTAR⁹. Este punto estará relacionado con el siguiente punto, iniciativa.

1.4.6 Por su grado de iniciativa

Los drones tendrán distinto grado de iniciativa y autonomía para decidir sus acciones (ALFUS)[2]¹⁰. En el empleo de sus armas letales esta iniciática debería de ser reducida al mínimo. Como máximo el dron podría “sugerir” una acción letal, pero esta acción debería tener que ser refrendada por un humano. La comunicación de esta orden de ataque se considera crítica y por tanto será la de mayor seguridad en todos los sistemas. Según esto, un mismo dron, podrá tener, por ejemplo, un grado de iniciativa en auto navegación, otro en sus funcionalidades ISTAR y otro diferente para el empleo de sus armas letales.

1.4.7 Por sus sistemas de comunicaciones y navegación

El grado de autonomía estará también ligado al sistema de comunicaciones. Cuanto menos autonomía tenga un dron más necesitará recibir órdenes humanas (más órdenes, más detalladas, cada menos tiempo y con menos latencia). Lo mismo sucede con el sistema de posicionamiento, cuanto más capacidad de auto navegación se precise de un dron, su sistema de posicionamiento deberá resultar más efectivo. Se hace evidente por tanto, que los sistemas de comunicación y navegaciones de cada dron no tienen por qué ser iguales (y en algunos casos ni siquiera compatibles).

1.4.8 Por su precio, complejidad e importancia táctica

Un factor muy a tener en cuenta es el precio del dron. Para obtenerlo hay que sumar los precios de todos sus subsistemas así como el precio de integración de los mismos. Por simplificar, el precio de un subsistema sería la suma de los costes de diseño, fabricación y coste durante su etapa de uso (aquí se incluiría control de configuración, actualizaciones, modificaciones, mantenimiento...). Normalmente los precios son proporcionales a la complejidad de los sistemas. Hay que valorar la iteratividad¹¹ dado que el coste del diseño será el mismo independientemente de los elementos iguales a fabricar. Por tanto, desde el punto de vista económico (y de facilidad para el mantenimiento) se tenderá a aprovechar el mismo subsistema para el máximo número posible de drones. Por otro lado, según el principio de especialización, puede ser conveniente que cada necesidad operacional distinta sea resuelta con un diseño técnico distinto. Esto se resume en la frase: “Si algo es capaz de hacer varias cosas, seguramente no hará ninguna bien”¹².

Este factor del coste económico, en este tipo de guerra sin bajas (en teoría), es fundamental. Véase el siguiente ejemplo. Si tenemos un país A capaz de fabricar un misil a un coste de X € la unidad y por otro lado tenemos un país B capaz de fabricar un antimisil a un coste de 2X € la unidad, se llega fácilmente a la conclusión de que el país A podría estar lanzando misiles indefinidamente contra el país B aunque todos ellos fueran interceptados por sus antimisiles.

⁹ Inteligencia, Reconocimiento, Vigilancia y Adquisición de Objetivos (*Intelligence, Surveillance, Target Acquisition, and Reconnaissance*).

¹⁰ Huang, Hui-Min. *Autonomy Levels for Unmanned Systems (ALFUS) Framework*. National Institute of Standards and Technology. (Octubre 2008 v 2.0.) Volumen I: *Terminology* / (diciembre 2007 v 1.0) Volumen II: *Framework Models*.

¹¹ El número de veces que se repite un subsistema dentro del conjunto total de drones a fabricar.

¹² Sobre este principio es muy ilustrativa la película *The Pentagon Wars*, en español “Juguetes de Guerra”. 1998. Sobre el diseño del Vehículo de combate Bradley.

Así mismo se adivina que la velocidad de fabricación es también importante (aplíquese al ejemplo anterior). La velocidad de fabricación depende de la capacidad industrial del país (que puede considerarse constante a estos efectos) y de la sencillez del diseño. Normalmente, sencillez y precio, irán también unidos. Por tanto, el objetivo del diseño de los sistemas y subsistemas, aparte de cumplan la funcionalidad deseada, será alcanzar un producto fácil de fabricar, sencillo y barato (o por lo menos que tenga estas características en el mayor grado posible, siempre que se cumpla la de funcionalidad).

Otro ejemplo, si se consigue que un dron completo del modelo A, sea capaz de tener una probabilidad de impacto del 50 % a un precio de X €, y modificando el sistema de puntería conseguimos un dron modelo B, que aumente esa probabilidad al 70 % pero con un precio de 2X €, habría que evaluar si se implementa la mejora o no. Ya que si fabricamos dos drones de tipo A entre los dos obtendrían una probabilidad de impacto del 75 %, teniendo el mismo precio que uno del modelo B.

Si lo que se precisa es un dron para un ataque individual “tipo quirúrgico” seguramente serían necesarios muchos subsistemas complejos y caros, porque no deben fallar. Sin embargo, en el escenario propuesto en este trabajo, los ingenieros de diseño no deben perder de vista que la optimización principal debe recaer en un diseño sencillo y barato, cumpliendo siempre, el mínimo de funcionalidad requerida.

Muchos de los drones de este ejército tendrían una misión de señuelo. Su objetivo sería provocar que el enemigo activará sus radares y demás sensores activos para detectarlos, descubriera su origen de fuegos y consumiera munición (inteligente o no) para destruirlos. Sería absurdo desarrollar subsistemas complejos y caros para este tipo de drones señuelo.

Entre los drones señuelo y los drones de vital importancia táctica, hay una serie de niveles de criticidad, los cuales deberían ser proporcionales al coste de fabricación de los drones que desarrollan estas misiones. A mayor importancia táctica, drones más caros.

1.5 Distintas funcionalidades de los drones

Todos los subsistemas que se incorporan a un dron tienen un fin último que es la utilidad o misión que desarrolla ese dron (o misiones en plural). Aquí entraría el concepto de *payload* o “carga útil”, es decir, aquellos elementos del dron que sirven de manera directa para realizar la misión para la que ha sido diseñado. En el concepto de *payload* no entrarían, por ejemplo, ni su sistema motor, control y guiado, comunicaciones (a menos que fuera específicamente un dron cuya función fuera las comunicaciones)...

Para agrupar algunas de estas misiones se explicarán a continuación los conceptos de ISTAR, apoyo a los sensores (iluminadores), apoyo al ataque (designadores), ataque (con capacidad letal), apoyo a las comunicaciones (repetidores y nodos) y apoyo al posicionamiento (radiofaros).

1.5.1 Sensores

En este epígrafe se hablará de drones que reciben información. No hay otra manera de recibir información que captándola con distintos sensores. En realidad también se llaman “transductores” porque convierten una energía de entrada en otra diferente de salida. Entre estos sensores podemos encontrar:

Sensores de luz (transductores fotoeléctricos):

Con los sensores de luz se captan imágenes. Estas imágenes pueden ser fotos fijas o bien imágenes en movimiento (video). En combinación con lo anterior, cada cámara se especializa y capta un tipo de luz. Dicha luz puede ser infrarroja (cámaras termográficas), espectro visible o ultravioleta.

Sensores radioeléctricos:

Los sensores radioeléctricos se encargan de recibir distintas frecuencias de radio y microondas (pudiendo llegar casi al límite del infrarrojo). Dichos sensores pueden especializarse en una banda de frecuencias. Esta especialización se debe principalmente a la relación de la longitud de onda de la radiación que se busque con la longitud de la antena del receptor. Algunos tendrán capacidad de medir la intensidad de la señal recibida, demodularla o definir su dirección de procedencia. En el último caso se habla de DF¹³. También estos receptores pueden medir diferencias de tiempo de forma muy precisa. En el penúltimo caso podría conseguirse la localización de la fuente emisora por triangulación y en el último por trilateración, en este apartado se incluirían los receptores de radar¹⁴ o de GNSS¹⁵.

Sensores de distancia (EDM)¹⁶:

Con este tipo de sensores se pueden medir distancias. Pueden ser mediante radar (en este caso sería un caso particular de sensor incluido en el punto anterior), por sonido o por láser. En el entorno de este trabajo se utilizaría el telémetro láser (con luz dentro del espectro visible o no) y por radar.

Sensores de movimiento externo:

Se basan en la detección de la diferencia de los sensores anteriores de luz o microondas. Detectan cambios en la recepción de determinada radiación.

Sensores de movimiento, giro y aceleración propia (interna):

Detectan y cuantifican la aceleración propia mediante acelerómetros y giróscopos, de manera que colaboran en la localización propia.

Sensores de orientación magnética:

Son las conocidas brújulas, pero con la capacidad transductora a señal eléctrica incorporada.

1.5.2 Apoyo a los sensores. Iluminadores

La misión de los iluminadores es conseguir que los sensores anteriores puedan detectar el reflejo de su radiación. Pueden estar ubicados en el mismo dron que el sensor o en otro diferente. En el campo de batalla son vulnerables porque su emisión los hace detectables por el enemigo. Los sensores puros no son detectables por ser sensores, sino por ser un ente físico.

¹³ *Direction Finder*, o radiogoniómetros.

¹⁴ *Radio detection and ranging*, o detección y medición de distancias por radio.

¹⁵ *Global Navigation Satellite System*, o sistema global de navegación por satélite.

¹⁶ *Electronic distance meter*, o medidor de distancia electrónico.

Suelen recibir el nombre de iluminadores, y se clasifican según el tipo de radiación que emane de ellos. Cada tipo de radiación está pensada para ser recibida por su sensor correspondiente.

Según lo visto anteriormente las radiaciones iluminantes pueden ir desde las ondas de radio de baja frecuencia hasta la luz ultravioleta.

La señal radiada puede llevar a su vez implícita algún tipo de modulación¹⁷.

El objetivo de la iluminación puede ser el de incidir en algún elemento enemigo (para que el sensor capte su reflejo) o bien que se capte la radiación directa del iluminador en sí mismo. Un radiofaro sería un ejemplo de esto último.

Siguiendo el ejemplo del radiofaro (emisor de una radiación determinada), éste puede ser el propio dron (aéreo o terrestre) o bien un radiofaro inerte que otro dron lanza o deposita en un punto determinado del terreno.

1.5.3 Apoyo al ataque. Designadores

La misión de este tipo de drones es “señalar” un objetivo para que sea destruido con mayor facilidad por otro dron u “otro medio”. El condicionante autoimpuesto en este trabajo es que ningún ser humano transite el espacio de batalla durante la operación. Por tanto, cuando se habla de destrucción “por otro medio” (que no pertenezca al ejército de drones) se está hablando, por ejemplo, de artillería (convencional o lanzacohetes) que queda relativamente alejada de la zona de la operación. A esta unidad de artillería le servirían una coordenada y el detalle del tipo de objetivo para poder batirlo.

El ejemplo más típico de “apoyo al ataque” es un designador laser, que podría ser la *payload* de un dron terrestre o aéreo.

El “apoyo al ataque” también puede realizarse mediante balizas emisoras. Pueden emitir en una radiofrecuencia determinada junto al objetivo para que luego el medio de ataque pueda utilizarla como guía en la última fase de su trayectoria.

La baliza puede soltarse en caída libre desde un dron aéreo encima del objetivo o bien tratarse de un dron terrestre que se situara en el punto deseado.

Los parámetros de la transmisión de la señal (frecuencia, modulación, etc.) tienen que estar bien prefijados y en coordinación con el medio de ataque que, evidentemente, debe tener un sistema para seguir precisamente esa señal. Es de vital importancia asegurarse de que el medio de ataque no confunde una señal de uno de los drones propios con una baliza designadora, porque en ese caso se lanzaría a destruirlo.

1.5.4 Ataque y destrucción. Armamento y munición.

La misión final de estos drones es provocar daños físicos. Normalmente éstos se producirán por medio de municiones y explosivos. Se ha hablado brevemente de ellos en el punto 1.4.5.

En determinadas operaciones, en las que los drones apoyan y acompañan al ser humano, puede que esta capacidad no sea decisiva. Pero en este tipo de operación en la que se pretende expulsar (o neutralizar) a un enemigo de una amplia zona, el peso táctico de estos drones es muy importante.

No es objeto de este trabajo la descripción de los efectos letales de las municiones, pero podrían dividirse entre proyectiles inertes o explosivos. Los inertes son proyectiles que causan efectos sólo mediante el choque físico a alta velocidad. No serán muy utilizados por los drones expuestos en este trabajo. En cuanto a los explosivos, pueden especializarse para destruir determinados tipos de objetivos.

¹⁷ Por ejemplo el *chirping* (frecuencia modulada pulsada) en algunos sistemas de radar.

Para edificaciones y fortificaciones se utilizarían los anti búnker (con poder de penetración en hormigón). Similares serían los anti blindaje, pero en este caso su poder de penetración estaría especialmente diseñado para atravesar el blindaje metálico de los vehículos acorazados. Los rompedores y los incendiarios estarían destinados a neutralizar a grupos de tropas poco protegidas.

Para atravesar las defensas enemigas, en un ataque “humano” se emplea a los zapadores. Estas unidades se encargan de “abrir brecha” en las alambradas y demás dispositivos defensivos con el objeto de dejar libre el acceso a las tropas de infantería que participan en el ataque. Como podrá imaginarse estos zapadores sufren un gran número de bajas ya que las defensas siempre deben estar batidas por el fuego enemigo por definición. Los “drones zapadores” tendrían una misión fundamental. Por lo general serían drones terrestres y su munición será la misma que la que utilizan los zapadores humanos. Los drones se encargarían de depositar la pértiga explosiva para abrir alambradas o la manguera explosiva para abrir campos de minas. Es a través de estas brechas por donde pasarán el resto de los drones terrestres que participarán en el ataque.

Hay casos en los que el propio dron es la munición. En este caso se incluirían los misiles. También se incluirían aquellos drones destinados a ser destruidos en el momento y lugar de la explosión. A ambos podría llamárseles “Drones kamikazes”.

Hay que recordar que la orden ejecutiva para llevar a cabo la destrucción debe recaer en un ser humano y la comunicación de esta orden debe producirse a través de un medio y protocolo especialmente seguro. Podría dejarse en manos de la Inteligencia Artificial (IA) pero en opinión del autor de este trabajo, ni es conveniente, ni es ético.

1.5.5 Apoyo a las comunicaciones

En el escenario que se describe existirán drones con la misión de apoyar los sistemas de comunicación. Las comunicaciones en esta operación serán de tipo satélite, radioenlace (punto a punto) o de difusión por radio mediante antenas omnidireccionales. No se contemplan comunicaciones por medio guiados (cable o fibra óptica) en el escenario de batalla. Tampoco se contemplan comunicaciones de medios luminosos no guiados (laser o infrarrojos).

En los casos de satélite y radioenlace existe el hándicap del apuntamiento de las antenas sin poder contar con un ser humano “in situ”. Por tanto estos drones tendrán capacidad de auto apuntamiento o bien posibilidad de apuntamiento remoto. La mayoría de los drones contarán con algún tipo de sistema de comunicaciones (algunos drones señuelo no). Un dron con un sistema de comunicaciones para sí mismo no se considera un dron de apoyo a las comunicaciones. Para que pueda ser llamado con ese nombre, deberá contar con la posibilidad de facilitar las comunicaciones a otros drones. Un ejemplo sería un dron que recibe un mensaje por señal satélite y lo transmite por radio (o a la inversa, o en ambos sentidos). Otro caso podría ser un repetidor de radioenlace que se consigue colocando un dron terrestre con esta funcionalidad en un lugar elevado.

En la mayoría de los casos los drones de apoyo a las comunicaciones que cuenten con antenas direccionales que deban apuntarse serán drones terrestres. La mayoría de los drones aéreos de apoyo a las comunicaciones funcionarán con antenas omnidireccionales.

Como la supervivencia y disponibilidad en las comunicaciones se considera un factor clave en este tipo de operación se tendrá en cuenta una gran cantidad de drones de reserva con estas funcionalidades al objeto de sustituir de inmediato a cualquier dron que sufriera avería o destrucción (intencionada por parte del enemigo o fortuita).

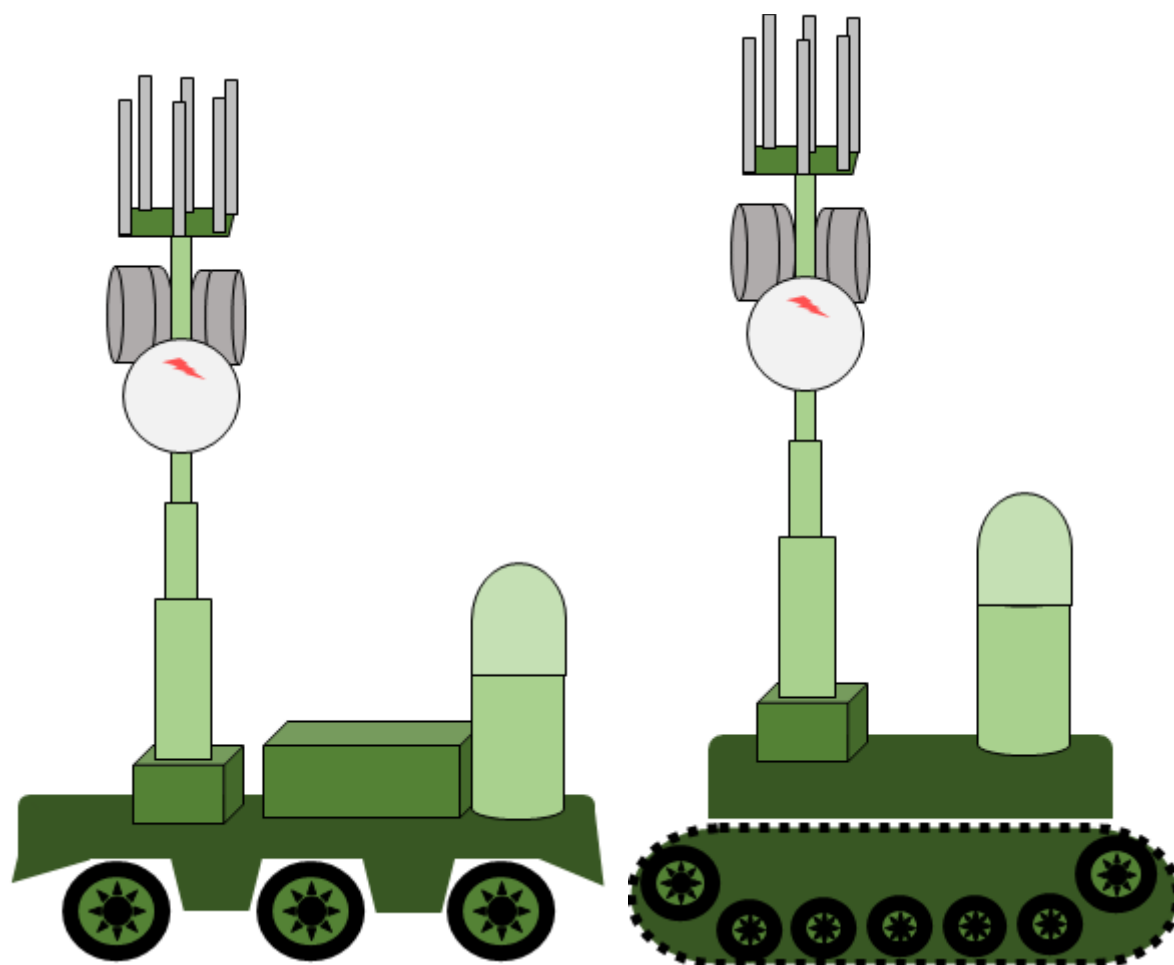


Figura 1-2: Recreación de drones de comunicaciones terrestres (de cadena y de rueda).

1.5.6 Apoyo al posicionamiento

Al objeto de apoyar al posicionamiento y navegación de los drones, existirán drones que transmitirán una señal con este fin. Normalmente los drones utilizarán para posicionarse los sistemas GNSS pero, como en el caso de las comunicaciones, la supervivencia y disponibilidad de los sistemas de posicionamiento es vital. Por lo anterior la mayoría de los drones (o por lo menos los más importantes) utilizarían un sistema principal y uno o varios alternativos. En retaguardia se situarían NDB¹⁸, VOR¹⁹, DME²⁰, TACAN²¹, LORAN²² e ILS²³. Al estar en retaguardia y poder ser operados por humanos, estos elementos no formarían parte del “ejército de drones” (aunque servirían de apoyo al posicionamiento y navegación de los mismos). Sin embargo, otros drones sí que avanzarán con algunas de estas radioayudas dentro del campo de batalla. Se estima que no es conveniente ni factible habilitar en los drones de apoyo

¹⁸ *Non-Directional Beacon*, o baliza no direccional

¹⁹ *VHF Omnidirectional Range*, o radiofaro omnidireccional VHF

²⁰ *Distance Measuring Equipment*, o equipo medidor de distancia.

²¹ *Tactical Air Navigation System*, o sistema de navegación aérea táctica.

²² *Long Range Navigation*, o navegación de largo alcance.

²³ *Instrument Landing System*, o sistema de aterrizaje instrumental. Al objeto de que los drones puedan tomar (aterrizar) en pista a su regreso de la misión.

al posicionamiento todas estas funcionalidades. Sólo se tienen previsto para este trabajo drones con emisiones para DME (sin VOR).

1.5.7 Funcionalidad como señuelo

Los drones señuelo servirán para que el adversario se delate tratando de detectarlos y/o destruirlos. Se pretende que encienda sus sensores activos (como los radares) para poder detectarlos, o desvele el origen de fuegos de sus armas. Por tanto los drones señuelos deben cumplir dos características:

- Ser lo más similares posible a los drones reales (ante cualquier tipo de sensor del adversario).
- Cumpliendo lo anterior, tener un precio lo más reducido posible.

Las cargas tipo de estos drones serán simuladores de emisión de señales de comunicaciones, iluminadores, radiofaros o simplemente su sola presencia en movimiento (ninguna carga). Sus sistemas reales de comunicaciones y de posicionamiento serán muy pobres o a veces carecerán totalmente de ellos. Normalmente se utilizarán en masa al comienzo de la operación y también acompañando a drones de gran importancia táctica.

1.5.8 Funcionalidad combinada

Se trata de drones que tengan más de una funcionalidad, por ejemplo un dron que realice al mismo tiempo apoyo a las comunicaciones y al posicionamiento. Otro caso habitual será el dron que cuente con un apoyo al sensor (iluminador), el propio sensor y el armamento.

2 SISTEMAS DE COMUNICACIONES

2.1 Introducción a los sistemas de comunicaciones necesarios

2.1.1 Primera aproximación.

Para el ejército de drones de este trabajo serían necesarios varios sistemas de comunicaciones. En principio puede pensarse en un solo sistema con compatibilidad total, pero parece más oportuno una pléyade de sistemas especializados (no necesariamente compatibles entre ellos), dadas las diferentes necesidades de comunicación. Las principales diferencias en estas necesidades serán marcadas por las características mínimas requeridas para cada tipo de comunicación.

2.1.1.1 Velocidad mínima de transmisión.

A veces se le conoce coloquialmente como “ancho de banda”, ya que, a igualdad de las demás condiciones (tipo de modulación, relación S/R...), la velocidad de transmisión es directamente proporcional al ancho de banda utilizado. Se mide en bits transmitidos por segundo. Un ejemplo de necesidad de alta velocidad de transmisión sería la transmisión de imágenes en tiempo real. El número de bits/s (o bps) generados por la cámara dependerá de su calidad y de su sistema de compresión. La mínima calidad para transmitir vídeo es de 32 Kbps y correspondería a la calidad de un video portero. La máxima calidad de vídeo prevista en este trabajo se correspondería a una velocidad de transmisión de 2 Mbps. A su vez, la calidad requerida dependerá del uso que se le vaya a dar a las imágenes. Aquellas imágenes cuyo fin sea obtener inteligencia (ISTAR) deberán tener más calidad (aunque por otro lado puede que no requieran muchos fotogramas por segundo o puedan ser incluso fotos fijas), sin embargo aquellas imágenes destinadas a facilitar la conducción remota sólo requerirán la suficiente nitidez para identificar los obstáculos.

2.1.1.2 Latencia máxima permitida [3]²⁴.

La latencia es el retardo total del mensaje a transmitir y, como es lógico, es la suma de los retardos intermedios de transmisión y procesamiento de las etapas intermedias entre el emisor y el receptor. En el caso de los drones los requerimientos máximos de latencia corresponden a la conducción remota. Tanto para drones aéreos como terrestres la conducción remota se basa en que un humano (situado en los puntos de control de la zona segura de retaguardia) recibe el vídeo del dron y controla su conducción en tiempo real. En el mejor de los casos el propio dron contará con una cámara y con los medios para transmitir el vídeo a la zona segura. En otros casos, la cámara también podrá encontrarse en otro dron diferente (que lógicamente apuntará al dron que se pretende conducir a distancia).

Este proceso de que el piloto remoto reciba el vídeo de la zona inmediata por donde se pretende que el dron se desplace, debe contar con una latencia mínima. Pero las comunicaciones en el camino de vuelta son igual de importantes y requieren la misma premura. El piloto remoto accionará el cuadro de mandos y esas órdenes deben ser transmitidas y llegar al dron con el mínimo retardo. Así mismo, el dron debe procesarlas y dar las órdenes a sus servomecanismos de conducción en el menor tiempo posible.

Otro proceso que requiere una latencia lo más baja posible es el control sobre el apuntamiento. El control remoto sobre un designador (ver punto 1.5.3.) debe ser casi instantáneo sobre todo si lo que se pretende destruir es un blanco en movimiento.

²⁴ *Coordinating multiple agents for workflow-oriented process orchestration*. M. Brian Blake. Information Systems and e-Business Management Springer-Verlag. 2003. Consultado 19/10/2021 en: https://web.archive.org/web/20060901073108/http://www.cs.georgetown.edu/~blakeb/pubs/blake_ISEB2003.pdf

2.1.1.3 Por su grado de seguridad requerida.

Según la ONS²⁵ la seguridad de la información se divide en tres vertientes: Confidencialidad, integridad y disponibilidad [4]²⁶.

Todos los sistemas de comunicaciones del ejército de drones requieren asegurar el cumplimiento de estos tres preceptos en un alto grado. No obstante, algunos en concreto, por su criticidad, requieren un nivel superlativo de seguridad, mayor, si cabe, que el resto.

Se pondrán un par de ejemplos críticos:

La transmisión de las coordenadas de ataque y la orden ejecutiva a un misil en vuelo deberá mantener la integridad, puesto que en caso contrario el enemigo podría alterar el mensaje cambiando las coordenadas para que misil impactara en un objetivo propio.

La transmisión de imágenes de ISTAR deberá mantener la confidencialidad, porque el enemigo podría deducir que determinado objetivo está siendo observado. Sobre este punto, se muestra un enlace a noticia real²⁷.

2.1.1.4 Por el alcance requerido y el medio de transmisión empleado.

Ya se ha dicho que el escenario de actuación será un área de 40 x 40 km. Teniendo en cuenta estas medidas ya se vislumbra que no se podrá utilizar cualquier medio de transmisión. Todos los medios de transmisión utilizados en el ejército de drones serán “no guiados” a excepción de uno, los drones cautivos. Estos drones se comunican con el dron terrestre al que están anclados mediante un cable de datos (por ejemplo Ethernet), por el que además discurriría la alimentación. Se muestra un ejemplo COTS en este enlace²⁸. Salvo esta excepción del dron cautivo, todas las demás comunicaciones entre drones, o entre el control “humano” y los drones serán por medios no guiados. Se describen en el punto siguiente. Cada uno de los distintos medios tendrá en cuenta los cuatro requerimientos de este punto 2.1 velocidad de transmisión necesaria, latencia requerida, seguridad y alcance.

2.2 Miscelánea de Comunicaciones

2.2.1 Introducción

En este apartado se introducirán algunos conceptos relacionados con las comunicaciones pero que afectan de forma transversal a diferentes sistemas.

2.2.2 Tiempo y sincronía

Todos los drones que transmitan o reciban algún tipo de señal (es decir, todos menos algunos drones señuelo) contarán con relojes para la sincronía. La sincronía de los relojes de todo el ejército de drones y de las instalaciones en la zona humana se producirá justo antes de iniciar la operación. Antes del inicio de la operación, también se dotará a todos los drones con la secuencia temporal de eventos en los

²⁵ Oficina Nacional de Seguridad del Centro Nacional de Inteligencia español.

²⁶ *Normas de la Autoridad Nacional para la Protección de la Información Clasificada*. 2016. Ministerio de la Presidencia. Punto 9. Pg. 123. La norma UNE-EN ISO/IEC 27001:2017 utiliza el mismo criterio. Punto 0.1. Pg. 8.

²⁷ Irán asegura que 'hackeó' drones de EE.UU (publicado: 22 feb 2019, consultado 28/10/2021):

<https://actualidad.rt.com/actualidad/306340-iran-hackeado-drones-eeuu>

²⁸ Dron Cautivo TS150 (consultado 28/10/2021):

<https://www.embention.com/es/producto/dron-cautivo-ts150/>

próximos cinco días (aunque como se ha dicho sólo se tiene previsto utilizar los eventos de las primeras 72 horas). Entre estos eventos programados estarán incluidos los momentos de los 7.200 silencios de emisión de un segundo (en los que se aprovechará para localizar emisiones enemigas), los 120 instantes en que desde la zona humana se mandará una señal de sincronismo (entre 1 y 119 minutos) y las 7.200 ventanas de un segundo destinadas a señales de servicio (órdenes especiales, solicitudes prioritarias, etc.).

Si un dron pierde la sincronía puede enviar una señal de servicio en la próxima ventana (una cada minuto de media) o bien recibir la señal de sincronía general (una cada hora de media). La señal de sincronía podría incluso enviarse mediante HF en alta potencia para determinados drones. Aquellos drones “enganchados” a su Estación de Abonado (SS) de WiMAX, recibirían la sincronía por este sistema.

2.2.3 Juegos de claves, aplicaciones e indicativos

La secuencia de ventanas de tiempo descrita en el apartado anterior, ya es en sí un juego de claves. Como además están previstos 7.200 silencios sincronizados se pueden implementar 7.200 juegos de claves distintos que cambien automáticamente en todos los sistemas de comunicaciones tras cada silencio. Determinados sistemas COTS tienen su propia estructura de claves por lo que no se verán afectados por las claves descritas anteriormente, que se utilizarán sólo en sistemas propietarios. Las aplicaciones deberían ser adaptadas o creadas *ad hoc* para cumplir con las necesidades. Sería necesaria una aplicación para comunicar los posicionamientos de los drones al objeto de formar y actualizar la JCOP. Con esta misma aplicación se gestionaría la actualización de los posicionamientos enemigos y modificaciones del terreno (por ejemplo: “puente destruido”). Cada dron estará identificado por un ID, utilizando bits sobrantes para realizar la función “resumen con clave”²⁹. No obstante, tanto este ID como cualquier otra parte del mensaje sería codificado con la clave vigente en ese minuto³⁰.

2.2.4 Utilización de SDR³¹ y SDN

Para las comunicaciones del ejército de drones se empleará con profusión las SDR, que implementan mediante software características (frecuencia, tipo de modulación, etc.) que tradicionalmente eran definidas mediante el hardware. Ahondando en este concepto se llega a la “radio cognitiva” que además dota al sistema de radio de cierta inteligencia y capacitada de decisión para cambiar los parámetros de la comunicación con intención, por ejemplo, de evadirse de interferencias. No se tiene previsto utilizar para este ejército de drones de manera sistemática radios cognitivas, debido a que el otorgar iniciativa a la IA en un despliegue tan grande y masivo podría hacer perder cierto control que convendría quedara en manos humanas. Sí en cambio, el uso de equipos SDR será lo habitual. Por otro lado, además de las radios, también existen las SDN³². Estas redes se definen en el estándar RFC 7149 del IETF y en ellas pueden definirse los servicios de red sin necesidad de que un administrador los gestione a bajo nivel ya que la propia red lo hace de una forma dinámica. El plano de control queda centralizado. En la siguiente figura, extraída de un estudio monográfico [5] de aplicación de estas redes al control de drones³³, puede verse un ejemplo de una red de drones con estaciones de control terrestres GAU³⁴ y satélite.

²⁹ Keyed hash function.

³⁰ Función OR exclusiva para encriptar y desencriptar con una de las 7.200 claves temporales.

³¹ Software Defined Radio, o Radio definida por software.

³² Software Defined Networking, o Redes Definidas por Software.

³³ McCoy, James and B. Rawat, Danda (2019) *Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey*. En *Electronics* 2019, 8, 1468.

³⁴ Ground Data Acquisition Unit.

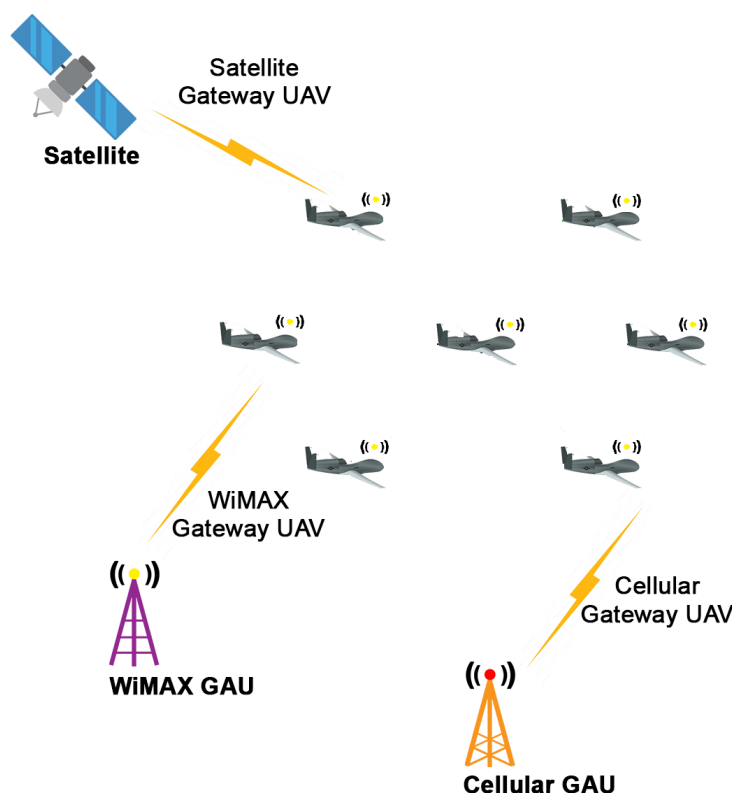


Figura 2-1 Típica red de comunicaciones de drones³⁵

2.3 Sistemas de comunicaciones no guiadas en los drones

2.3.1 Introducción a los diferentes sistemas

Como se ha dicho en el punto anterior, todas las comunicaciones entre el “Área Humana”³⁶ y cualquier dron, o entre drones entre sí, se realizará por medios no guiados³⁷. Cada uno de los sistemas será elegido para que cumpla con las condiciones del punto 2.1. para cada caso. Se describen a continuación los diferentes sistemas de comunicaciones utilizados. En el punto 2.3 se describirá lo que se conoce como “Área Humana” que es la zona de retaguardia desde donde las personas controlarán el ejército de drones.

2.3.2 Comunicaciones satelitales

Determinados drones tendrán equipos de comunicación por satélite. Un hándicap a superar será la orientación de la antena del dron teniendo en cuenta que no existirá ningún humano “in situ” para tal operación. Los drones terrestres que se determinen irán equipados con terminales de tipo SOTM³⁸ o ATHQ³⁹.

³⁵ *Ibidem*.

³⁶ Que se tratará en el punto 2.3

³⁷ Con la sola excepción de los “drones cautivos”.

³⁸ *Satcom On the Move*, o Comunicaciones satélite en movimiento.

³⁹ *Satcom At The Quick Halt*, o Comunicaciones satélite desplegadas en parada rápida.

El primer sistema permite a los drones (terrestres o aéreos) establecer y mantener la conexión vía satélite, aun estando en movimiento, mediante una antena con receptor de baliza y seguimiento automáticos.

El segundo sistema suele tener mayor capacidad de transmisión de datos pero, por el contrario, no puede funcionar mientras el dron está en movimiento. El sistema ATHQ sólo se aplicaría a drones terrestres que tuvieran previsto mantenerse la mayor parte de la operación en una posición estacionaria. La forma de solventar la necesidad de movimiento es contar con dos (o más) drones equipados con este sistema por cada itinerario, de manera que mientras un dron cubre el servicio satélite el otro se desplaza. Una vez el dron que se ha desplazado llega a su destino y activa el enlace (entre 10 y 30 minutos desde la parada, dependiendo del modelo) el que estaba dando el servicio puede proceder al plegado de la antena y comenzar su movimiento (y así sucesivamente).

Los drones equipados con terminales satélites serán los que requieran mayor capacidad de transmisión de datos. Se tratará principalmente de aquellos que deban transmitir imágenes o bien de aquellos que deban tener una función de enlace troncal (backbone) y deban ser nodo de comunicaciones para varios drones situados en zona celular (que a su vez pueden demandar la transmisión de imágenes).

La seguridad ante fallos en la disponibilidad (intencionada mediante perturbación) tiene ciertas garantías por una cuestión de ganancia y orientación de antenas. La forma de perturbar su recepción sería situando un perturbador en su vertical (en la dirección donde se encontraría el satélite emisor). La forma de perturbar su señal de transmisión sería apuntar la perturbación directamente al satélite. Esto podría soslayarse por el tipo de medio de acceso (por ejemplo CDMA⁴⁰). Los terminales satélites previstos son todos TCP/IP y COTS. Con respecto a esto, hay terminales ATHQ COTS desde el punto de vista de las comunicaciones, pero no se conocen terminales en el mercado que desplieguen de forma automática (todos requieren de humanos “in situ”).

Los inconvenientes principales son la latencia elevada con respecto a otros sistemas de comunicación, así como el elevado precio.

2.3.3 Comunicaciones por radioenlace micro ondas

Para complementar a los enlaces satélites en su misión de backbone troncal se establecerán radio enlaces de micro ondas. Todos estos radioenlaces estarán situados sobre drones terrestres. Como en el caso de los satélites uno de los problemas es la necesidad de orientación de las antenas en ambos extremos del radioenlace, teniendo en cuenta que esta operación debe realizarse en remoto. Las órdenes para orientar la antena del radioenlace deben darse por otro sistema diferente ya que evidentemente la comunicación del radioenlace no funciona todavía. Existe la opción de apuntamiento automático (detectando el nivel de la señal del correspondiente) pero debe de existir algún sistema de control principal o alternativo. Para esto pueden ser de utilidad los mensajes cortos de HF que se describen en el punto 2.2.5.

Al declarar que los radioenlaces se implementarán sólo en drones terrestres, y teniendo en cuenta que un radioenlace necesita LoS⁴¹, será obligado salvar los obstáculos del terreno. Además, dependiendo de la frecuencia (esto aunque la operación se desarrollara en una llanura) las distancias (que podrían ser de hasta 50 km.) no permitirían (o lo harían de forma muy ajustada) realizar un enlace directo desde el “Área Humana” hasta el radioenlace más avanzado. Por tanto, se hace necesario el uso de repetidores. En el caso del ejército de drones, algunos de ellos tendrían la función de repetidor de radioenlace. Algunos radioenlaces serían TCP/IP y COTS pero otros podrían implementar otros sistemas no comerciales. Aquellos drones con tecnología IP portarían además los correspondientes *routers* (enrutadores). El despliegue de estos enlaces se realiza desde atrás a adelante. Es decir, a medida que la

⁴⁰ Code Division Multiple Access, o Acceso múltiple por división de código.

⁴¹ Line of Sight, o línea de visión directa.

operación y los drones penetran en territorio enemigo, nuevos radioenlaces se van desplegando hacia vanguardia para tejer la red que de soporte en cada célula. Combinando enlace satélite y radioenlace (muchos drones terrestres dispondrán de ambos para mayor versatilidad) se pretende cubrir toda el área de la operación de forma celular.

2.3.4 Comunicaciones VHF y UHF⁴²

Como se ha dicho en los dos puntos anteriores el esqueleto (backbone) de las comunicaciones con mayor capacidad de datos se forma con los enlaces satélites y de micro ondas. Los drones equipados con estos medios distribuyen y se comunican con el resto de los drones en las bandas de VHF y UHF.

Dentro de estas bandas, cuanto mayor sea la frecuencia, mayor podrá ser el ancho de banda [6] y por tanto mayor la capacidad de transmisión de datos⁴³. Por otro lado, cuanto mayor sea la frecuencia el alcance será menor, los obstáculos influirán en mayor medida y las antenas direccionales deberán estar mejor orientadas (pero serán más pequeñas).

Estos conceptos serán un punto de decisión clave, pues nos aportan la distancia a la que se puede alejar un dron ISTAR para transmitir imágenes a un dron backbone. Esta distancia nos dará el radio que tiene que tener cada célula y, por tanto, el número de células necesarias para cubrir toda el Área de Operaciones. Con el número de células se obtendrá el número requerido de drones de comunicaciones backbone. Con las premisas ya descritas, al número de drones de comunicaciones obtenido se le sumaría un 30% para garantizar la supervivencia del enlace en todo momento (a pesar de fallos fortuitos y destrucciones por parte del enemigo). El concepto de “reserva” sigue siendo igual de vital en las operaciones militares.

2.3.5 Comunicaciones HF

Este tipo de comunicaciones cuenta con el inconveniente principal de que la capacidad de datos es la más baja con diferencia (debido a la lógica limitación del ancho de banda en estas frecuencias, visto en el punto anterior).

Otro inconveniente es que por las frecuencias (3 a 30 MHz.), la longitud de las antenas requeridas hace muy difícil su implementación sobre los drones. En el caso de drones aéreos se podría situar el dipolo sobre las propias alas, teniendo aquí el inconveniente de la orientación (la comunicación se realizaría mejor hacia delante y detrás pero sería mínima hacia los lados). En el caso de los drones terrestres sería aplicable una antena de cuarto de longitud onda (de “varilla” y con acoplador de sintonía para poderla alargar/acortar). Por ello se estima que sería mejor utilizar la parte alta de la banda (de 25 a 30 MHz. con lo que las antenas necesarias serían más cortas).

La confidencialidad e integridad sólo podría asegurarse con un cifrado robusto de los mensajes a transmitir. La disponibilidad se aseguraría evitando la perturbación por medios físicos como se verá más adelante⁴⁴.

Por lo dicho anteriormente este sistema se utilizaría sólo para comunicaciones “de último recurso”, para mensajes cortos y concisos, especialmente en la dirección “Área Humana – Drones” y raramente al revés.

⁴² HF (High Frequency: 3 a 30), VHF (Very High Frequency: 30 a 300), UHF (Ultra High Frequency: 300 a 3000) y SHF (Super High Frequency: 3000 a 30.000), unidades en megaherzios. Recomendación UIT-R V.431-8 (08/2015) *Nomenclatura de las bandas de frecuencias y de las longitudes de onda empleadas en telecomunicaciones*. Publicación electrónica UIT. Ginebra, 2016.

⁴³ Briceño Márquez, José E. (2005) Transmisión de Datos. Departamento de Electrónica y Comunicaciones de la Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Los Andes. Mérida (Venezuela). Pg. 498.

⁴⁴ Ver *Sistema radiogoniométrico de vigilancia de perturbaciones* (2.3.8).

Para la comunicación descrita no necesariamente hay que respetar el límite de clasificación de 30 MHz como si fuera una línea fronteriza. La misma funcionalidad podría conseguirse hasta 40 MHz. (aunque en teoría se considerara VHF).

2.3.6 Autorización para el uso de frecuencias

Independientemente de los requerimientos técnicos para la elección de frecuencias, habrá que tener en cuenta los requerimientos legales. Para este asunto la legislación vigente en España queda establecida por la Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias (CNAF) [16]. En dicha Orden se dice que:

... el Ministerio de Energía, Turismo y Agenda Digital, aprobará el Cuadro Nacional de Atribución de Frecuencias para los diferentes tipos de servicios de radiocomunicación, de acuerdo con las disposiciones de la Unión Europea, de la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), y del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), definiendo la atribución de bandas, subbandas, frecuencias y canales, así como las demás características técnicas que pudieran ser necesarias⁴⁵.

No se ha realizado en este trabajo un estudio a fondo de las frecuencias autorizadas, no obstante, una vez definidas técnicamente las frecuencias idóneas para cada tipo de enlace, con el requerimiento de cumplir los condicionantes del punto 2.1, se debe elegir dentro de las posibles frecuencias de uso autorizado. Así mismo, se deberá solicitar autorización para aquellas con esta consideración. Esta operación también puede hacerse a la inversa, ver que frecuencias pueden usarse legalmente y ver después las que mejor se adecuan técnicamente a los fines perseguidos (de hecho lo razonable sería hacer esto último).

Por otro lado, podría pensarse que dado el tipo de operación definida, y tratándose de una “guerra convencional” en Territorio Nacional, este tipo de normativas podrían soslayarse en interés de la Seguridad Nacional. Esto es cierto, pero sólo en parte. Si bien la operación en sí podría llevarse a cabo sin estar sujeta a estos condicionantes limitativos legales, hay un detalle a tener en cuenta. Para tener disponible un “ejército de drones” llegado el caso de tener que hacer uso del mismo, habría que tenerlo construido y probado desde tiempo de paz. Los operadores y técnicos deberían de entrenarse asiduamente en maniobras y ejercicios. Por esta razón no se puede diseñar unos sistemas que no cumplan con la legalidad del CNAF, porque no podría realizarse el entrenamiento en tiempo de paz.

2.4 Sistemas de comunicaciones y posicionamiento en el “Área Humana”

2.4.1 Introducción al concepto “Área Humana”

En este trabajo se pretende que en la zona de la operación propiamente dicha, no despliegue ningún ser humano. En teoría las bajas sólo se producirían en esa zona y, por tanto, la operación se desarrollaría sin ninguna baja propia. Esto no quiere decir que no intervengan humanos en la operación, sí que lo hacen (alguien tiene que dar las órdenes a las máquinas), pero desde una zona en retaguardia alejada de todo peligro. Evidentemente esta zona sí que debe contar con medios de transmisión que también serán expuestos en este trabajo (y concretamente en este punto 2.3). Se ha denominado a esta zona “Área Humana”.

⁴⁵ Ministerio de Energía, Turismo y Agenda Digital «BOE» núm. 259, de 27 de octubre de 2017. Referencia: BOE-A-2017-12318. Consultado en el TEXTO CONSOLIDADO. Última modificación: 21 de julio de 2020

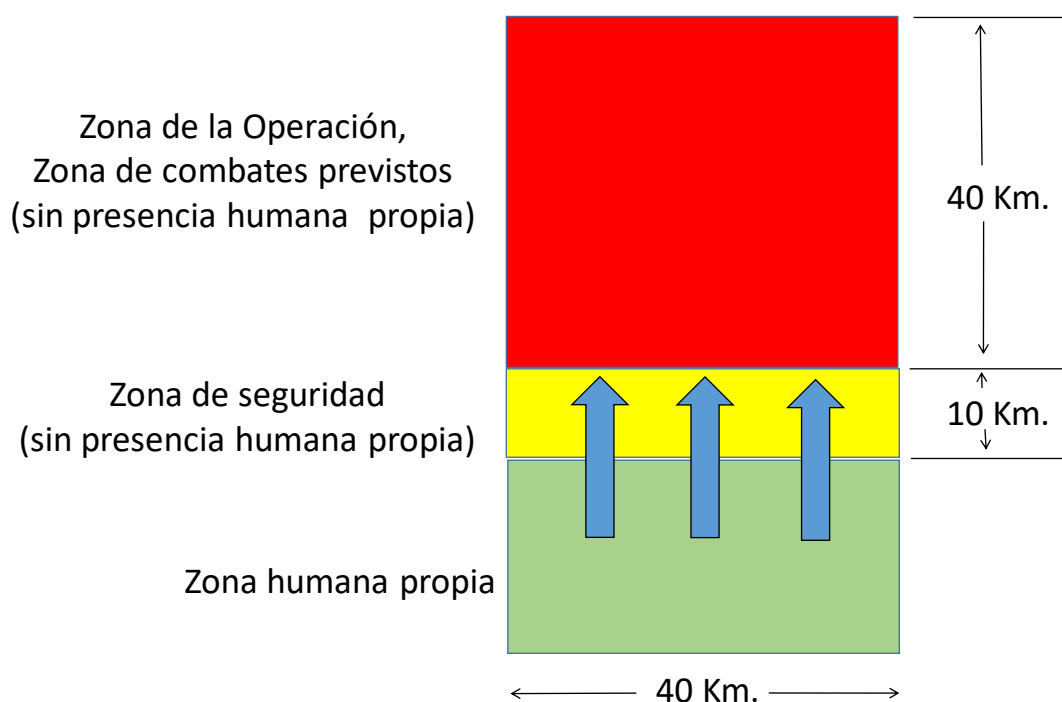


Figura 2-2: En la figura puede verse la distribución del Área Humana, de la banda de seguridad de 10km y del Área de la Operación de 40x40 km.

2.4.2 La JCOP, Joint Common Operational Picture⁴⁶

El concepto de JCOP consiste en un “mapa” (actualmente electrónico) donde son representados las Unidades o medios propios⁴⁷ así como los enemigos. El grado de detalle dependerá del tipo de operación. Esta JCOP se actualiza con las posiciones del enemigo a medida que van llegando informes de inteligencia. La actualización de las unidades propias puede realizarse en modo automático (transfiriendo las coordenadas que los medios propios pueden enviar). La “C” es de *Common*, e indica que si hay varios puestos de mando, la imagen que ven todos ellos es la misma porque se comparte. En el caso que se describe en este trabajo, en ella se representará la localización de los distintos tipos de drones propios, así como un esquema de su información más relevante (nivel de combustible, funcionamiento, nivel de munición...). También se representará toda la información disponible acerca del enemigo. Estos sistemas tienen unos filtros a aplicar para resaltar u ocultar temporalmente determinadas informaciones, al objeto de no saturar la imagen y dar al analista la oportunidad de centrarse en la información que en ese momento sea más importante. Por ejemplo, puede hacerse que se vean sólo los drones repetidores de comunicaciones, o sólo los drones de ataque, o sólo la información del enemigo⁴⁸.

⁴⁶ Allied Command Operations Comprehensive Operations Planning Directive COPD interim V2.0. PG 2-9, punto f.

⁴⁷ *Blue force tracking*, sistemas que posicionan y representan las fuerzas propias.

⁴⁸ En esta página web se muestra una JCOP. En el video se indica además como se tabulan e introducen las órdenes a las unidades propias. En este caso se trata de un simulador (JTLS) pero una JCOP real tendría el mismo funcionamiento: https://www.rolands.com/jtls/j_over.php



Figura 2-3: Operations Room. Donde puede verse una JCOP “de actualización manual” (Imperial War Museum Duxford⁴⁹). Es de 1940, pero aunque la tecnología ha cambiado, la función que realiza es exactamente la misma.

2.4.3 Puestos de mando

Al objeto de garantizar la supervivencia de este vital elemento siempre existirán como mínimo dos. En ellos podrá verse la JCOP representada. Uno será del puesto de mando principal y otro el alternativo. El principal podrá delegar algunas funciones en el alternativo o podrán relevarse por horas. Desde ellos se darán las órdenes al ejército de drones, pero no directamente. Los dos puestos de mando estarán enlazados para esto con el área de cabinas para pilotaje o conducción al detalle de los drones. El enlace de los puestos de mando con la zona de cabinas se producirá mediante fibra óptica. Este enlace es vital para la operación, por tanto se cubrirá con fibras por distintos trayectos a través de zonas controladas y vigiladas de retaguardia.

2.4.4 Zona de cabinas de pilotaje - conducción

Aunque los puestos de mando son el “corazón militar” de la operación, el “corazón técnico” está en la zona de cabinas. Salvo los drones que sean totalmente autónomos, el resto serán conducidos o pilotados (se utilizará esta segunda palabra independientemente sean terrestres o aéreos) por sendos humanos desde cabinas. Hay que tener en cuenta que se van a desplegar unas 5.000 cabinas. El número de pilotos ascendería a 8.000 (ya que las máquinas no duermen pero los humanos sí).

Cada una de estas cabinas tendrá también acceso a la JCOP. Cada piloto, como es lógico, aplicará el filtro y se centrará en la parte de la JCOP que le afecte (aunque tendrá toda la JCOP disponible). De hecho la JCOP se conformará en esta zona, y sus actualizaciones se enviarán tanto a los dos puestos de mando, como a cada una de las cabinas de pilotaje. La información de interés que reciba de los drones que controla cada piloto, la transmitirá a los servidores que conforman la JCOP. Parte de esta información se transmitirá de forma automática (por ejemplo las coordenadas donde se encuentra un dron).

⁴⁹ <https://dokodemodoorblog.com/2014/11/17/imperial-war-museum-duxford-un-trozo-de-la-historia-de-la-aviacion/>

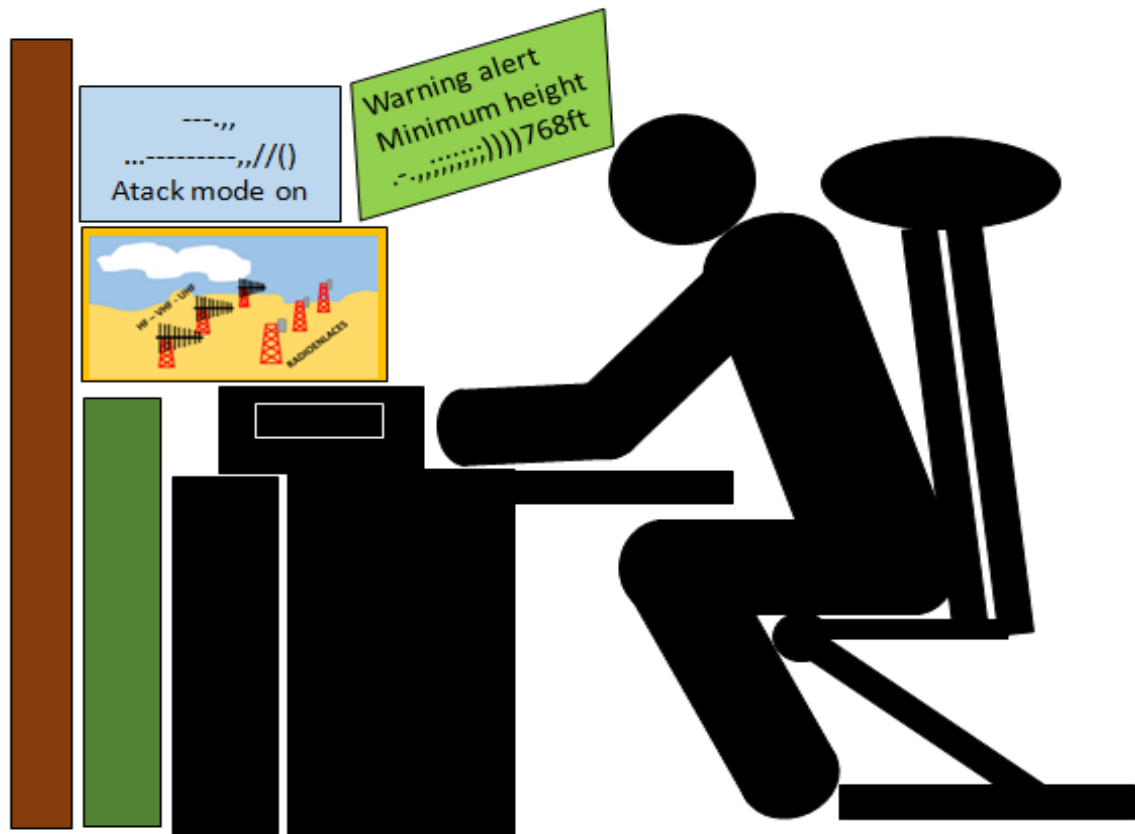


Figura 2-4: Recreación de una cabina de conducción / pilotaje

La capacidad de dar órdenes a los drones estará jerarquizada. Un ejemplo, desde el puesto de mando se ordena abrir una brecha en un punto de las alambradas enemigas. Para esto se manda una “compañía de drones” (20 drones). En una de las cabinas de control se encontraría el “capitán de la compañía” que será el único que reciba las órdenes del puesto de mando y las transmitiría en detalle a cada uno de sus 20 pilotos. Es evidente que es inviable que desde el puesto de mando se den las órdenes de forma individual a 5.000 pilotos de drones. La zona de cabinas se extenderá en unos 3 Km².

En la zona de cabinas estará la zona de servidores y computación donde residirá el peso de la capacidad de proceso de toda la operación.



Figura 2-5: Recreación de una zona de cabinas de conducción / pilotaje.

2.4.5 Estaciones de anclaje de satélite

Como se ha dicho en el punto 2.2.2. Algunos drones tendrán comunicación vía satélite. En el caso que se presenta, dado que la operación se desarrollaría en España, los satélites geoestacionarios a utilizar serían los Spainsat y Xtar-eur (de Hisdesat). En un futuro (previsto 2024) se utilizarían los SpainSat NG I y II (actualmente en desarrollo).

Las estaciones de anclaje satélite de las Fuerzas Armadas se encuentran en Torrejón, Bermeja y Hoyafría⁵⁰ y ofrecen comunicaciones en la banda Ku y X.

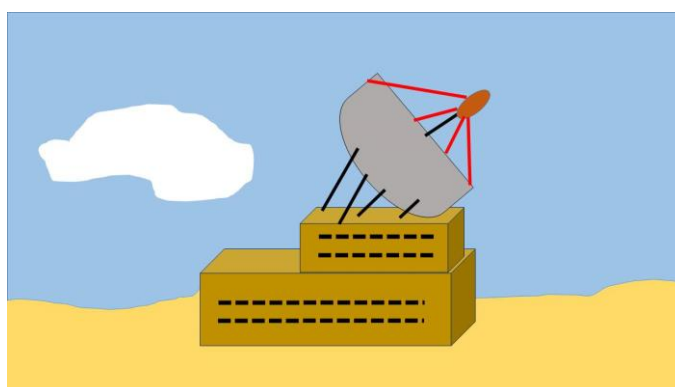


Figura 2-6: Recreación de una estación de anclaje satélite de instalación fija.

⁵⁰ Torrejón de Ardoz (Madrid), Bermeja – Valdilecha (Madrid) y Hoya Fría (Santa Cruz de Tenerife).

2.4.6 Áreas de antenas de radio

Hasta aquí, las partes descritas del “Área Humana” podían encontrarse a la distancia necesaria de la zona de la operación para garantizar su seguridad. En el caso de los campos de antenas, se debería de sopesar el alcance máximo, teniendo en cuenta que, por motivos tácticos, cuanto más alejadas de la zona de la operación estuvieran, mejor. Sin embargo por motivos técnicos, la profundidad de la zona de la operación sumado la distancia de la antena al borde de la misma debería de ser menor que el alcance.

Para calcular el alcance de cada enlace hay que tener en cuenta diversos factores⁵¹. Así, es muy posible que determinados enlaces más críticos tuvieran que situarse a pocos kilómetros del borde de la zona de operaciones mientras que otros pudieran alejarse hasta situarse en la zona de cabinas de pilotaje. En el caso de que la antena tuviera que situarse alejada de la zona de cabinas de pilotaje (para estar más cerca de la zona de operaciones), los sistemas de radio se situarían junto a la antena, produciéndose la comunicación entre la zona de cabinas y la zona de antenas mediante fibra óptica.

Además de las distancias, hay que tener en cuenta el terreno que, como normal general, afecta más cuanto más altas son las frecuencias. En ese apartado se incluyen los enlaces en los que por su frecuencia pueden ser NLoS⁵². Por realizar una aproximación *grosso modo*⁵³ un terreno ondulado no dificulta mucho la banda de HF, presenta una dificultad intermedia en VHF y dificulta en gran medida o impide las comunicaciones en UHF.

Las antenas serán direccionales, ya que todos los drones a controlar estarán a vanguardia, en la zona de operaciones. No obstante el ancho del lóbulo de radiación horizontal no deberá ser demasiado estrecho ya que debe cubrir todo el espacio de la operación previsto.

Las antenas en esta zona no tendrán un único receptor sino que funcionaran en modo *broadcast* (para todos los destinatarios, aunque sólo desde el punto de vista radioeléctrico; no es un enlace “punto a punto”).

Se estudiará el terreno de la operación así como la posible ubicación (más bien ubicaciones) de las distintas antenas de cada enlace. Se debe tener en cuenta que si bien la antena de la “zona humana” estará fija durante toda la operación, las antenas de los drones corresponsales podrán situarse en cualquier punto de la zona de operaciones. Si el dron es aéreo, no se prevén problemas con el terreno, pero en ese caso, la direccionalidad de la antena de la zona humana, tendrá que tener en cuenta el ancho en vertical del lóbulo de radiación.

Si el alcance se estima escaso para determinado enlace, se puede pensar en aumentar la potencia del transmisor. Así podría asegurarse el trayecto de los mensajes “zona humana hacia dron” pero no se solucionaría el problema en el sentido contrario (“dron hacia zona humana”). No se tiene previsto habilitar repetidores para estas bandas (en ninguno de los dos sentidos de la comunicación), por tanto la comunicación “dron hacia zona humana” se produciría por otros medios (satélite o radioenlaces) cuando el alcance no pueda ser cubierto.

La mayoría de los mensajes transmitidos por estos enlaces serán órdenes cortas desde la zona de cabinas a los drones. Un dron terrestre no puede conducirse con órdenes cortas, sin embargo un dron aéreo sí puede pilotarse con órdenes cortas durante su vuelo de crucero.

⁵¹ Un ejemplo de calculador automático:

https://wni.mx/index.php?option=com_content&view=article&catid=37:tools&id=66:freespace-loss&Itemid=80

⁵² *Non Line of Sight*, o Sin Línea de Visión necesaria. Pueden existir obstáculos de terreno entre las antenas emisora y receptora. Aunque no impiden totalmente el enlace, sí que lo dificultan.

⁵³ Estimación muy simplificada y subjetiva del autor. Y Briceño (2005), Pg. 498.

2.4.7 Áreas de antenas de radioenlaces

En este punto son válidas las consideraciones del punto anterior con las diferencias que se indicarán a continuación.

Las frecuencias de los radioenlaces son superiores a las frecuencias de radio, situándose en las bandas de UHF y SHF. Las antenas son más pequeñas y más direccionales, por tanto el apuntamiento debe ser más preciso. Los enlaces son LoS⁵⁴ y son más afectados por el terreno y por la lluvia que los anteriores. Los enlaces son “punto a punto” y se puede dar la comunicación dúplex (en ambos sentidos al mismo tiempo) utilizando la FDM⁵⁵.

La diferencia principal en este caso, está en la existencia (por necesidad) de repetidores. En la zona de la operación, todos los repetidores serán drones terrestres que se situarán en zonas determinadas (puntos elevados para salvar las elevaciones del terreno). Estos drones dispondrán de sistemas de apuntamiento de antenas tanto en remoto como automáticos.

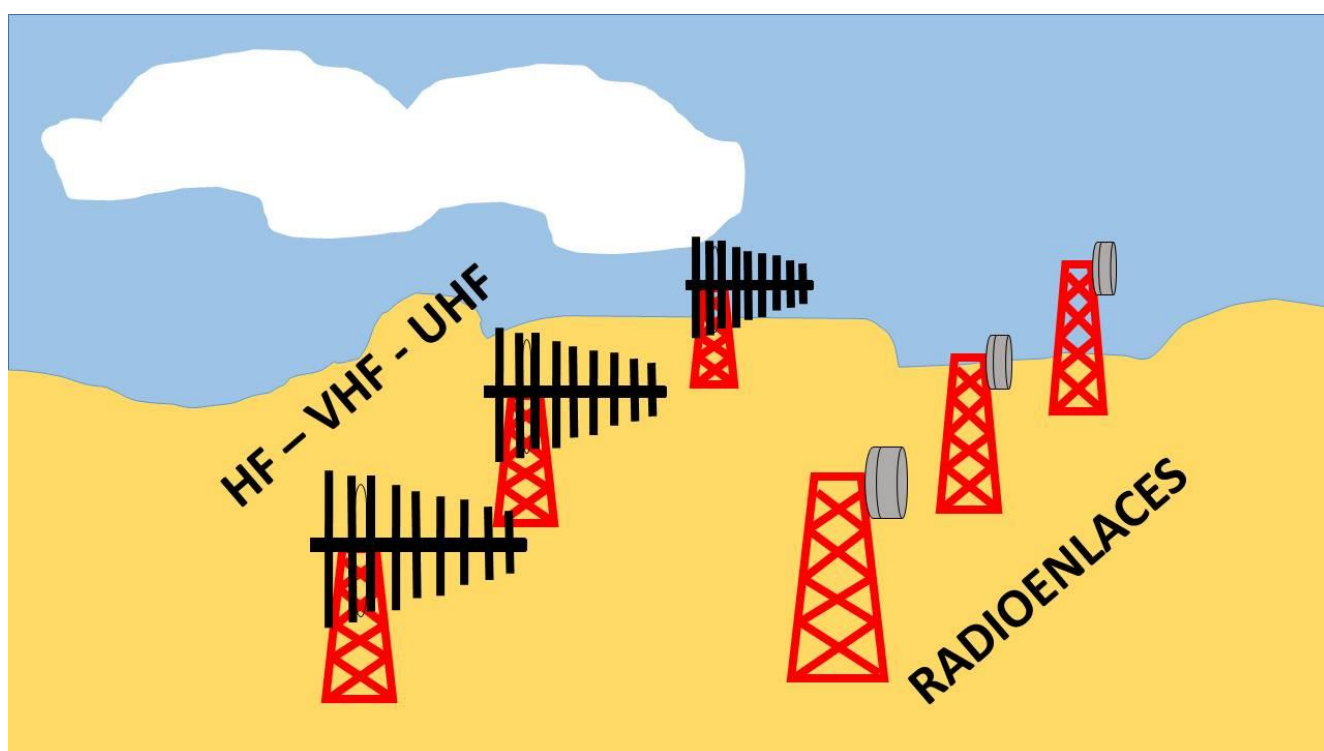


Figura 2-7: Recreación de la zona de antenas de radio y radioenlaces.

⁵⁴ Line of Sight, o necesaria Línea de Visión. No pueden existir obstáculos de terreno entre las antenas emisora y receptora. Esto no es exacto, especialmente a las frecuencias más bajas, se puede establecer la comunicación por las otras zonas de Fresnel del lóbulo de radiación aunque habría pérdidas por difracción. Lo ideal es que haya línea de visión directa en este tipo de enlaces pero no significa que si no la hay no se produzca la comunicación. Se quiere remarcar la contraposición a los enlaces radio de HF y VHF en los que los obstáculos influyen mucho menos que en los radioenlaces.

⁵⁵ Frequency-division multiplexing, o multiplexación por división de frecuencia.

2.4.8 Áreas de antenas para apoyo a la localización y navegación

En esta zona se situarán las antenas de las radiobalizas emisoras para apoyo a la navegación. Se considerarán estos sistemas como alternativos (el sistema principal serán los GNSS comerciales cuyos emisores se encuentran en los satélites correspondientes). No se instalará LORAN por ser este sistema diseñado para distancias más largas. Tampoco se instalará VOR ya que sus funciones serán realizadas por TACAN. El emisor de ILS se instalará sólo en las pistas de toma y despegue para aquellos drones aéreos que lo necesiten. En cuanto al TACAN y el NDB, se instalará una antena de cada sistema en los dos extremos de la zona de operaciones. El emisor TACAN contará al mismo tiempo con emisor DME.

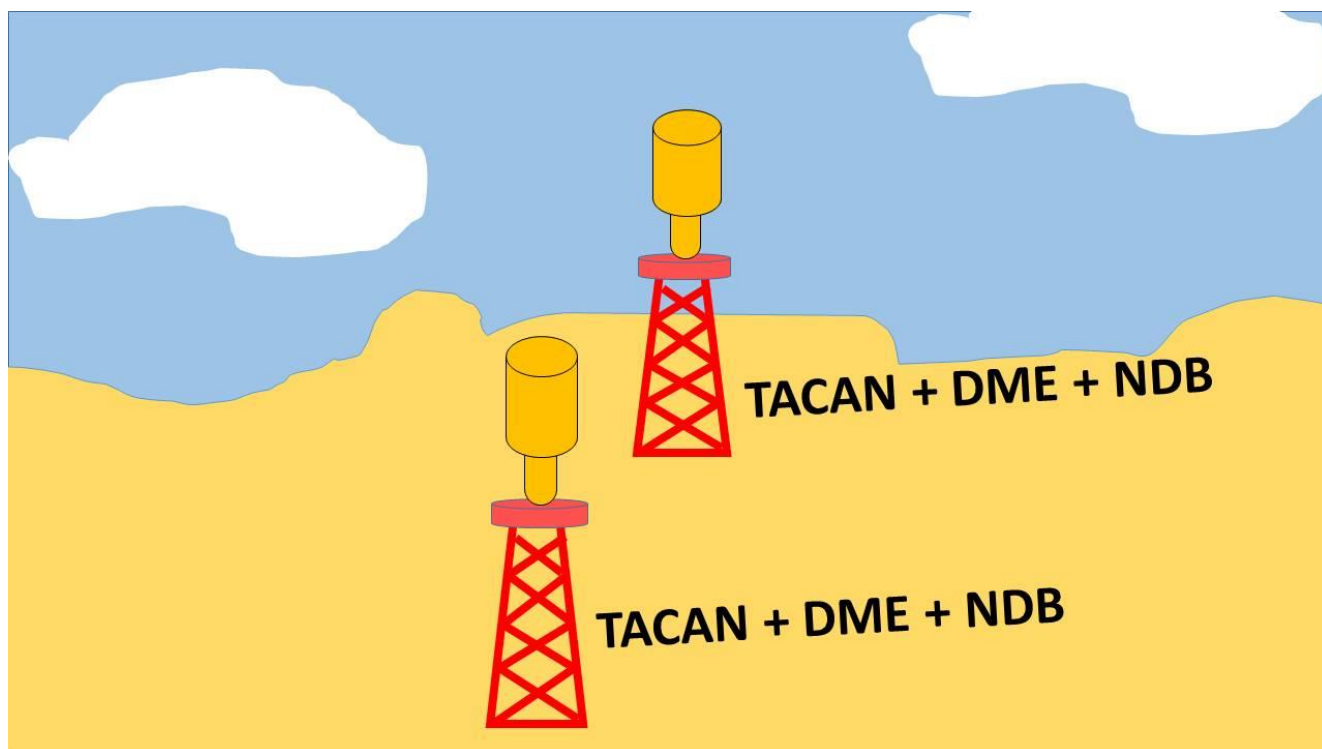


Figura 2-8: Recreación de las antenas de TACAN, DME y NDB. Cada juego situado a derecha e izquierda del frente.

2.4.9 Sistema radiogoniométrico de vigilancia de emisiones enemigas y localización propia.

En esta zona se situarán los campos de antenas para realizar radiogoniometrías. Las antenas que miden la dirección de la emisión por la amplitud son tremendamente inexactas, por tanto quedan descartadas en esta zona (lo que no implica descartarlas en algunos drones). Las antenas utilizadas serán de grupos de pares de elementos que restan sus señales recibidas. Esto puede conseguirse con un mínimo de cuatro monopolos o dipolos verticales (usualmente ocho para mayor precisión). Los elementos están separados media longitud de onda de la señal esperada (por lo que se hace necesario montar distintos arrays de antenas según las frecuencias) de manera que se resta la señal recibida por los elementos opuestos. El resultado de la amplitud recibida es mayor para la pareja que se encuentra perpendicular al emisor (restar una señal desfasada 180°, es sumarla) mientras que resta la misma señal en fase (caso de

la pareja que se encuentra a igual distancia del emisor) da como resultado una amplitud nula. Este tipo de antenas reciben el nombre de *Adcock*.

Pero con este sistema se puede averiguar sólo la dirección por donde llega la emisión. Para averiguar las coordenadas del emisor se necesitan, como mínimo, dos emplazamientos de antenas goniométricas. En este trabajo se tiene previsto instalar un emplazamiento central y uno a cada extremo del espacio de batalla, teniendo un total de tres arrays de antena por grupo de frecuencias. Se muestra a continuación un ejemplo gráfico.

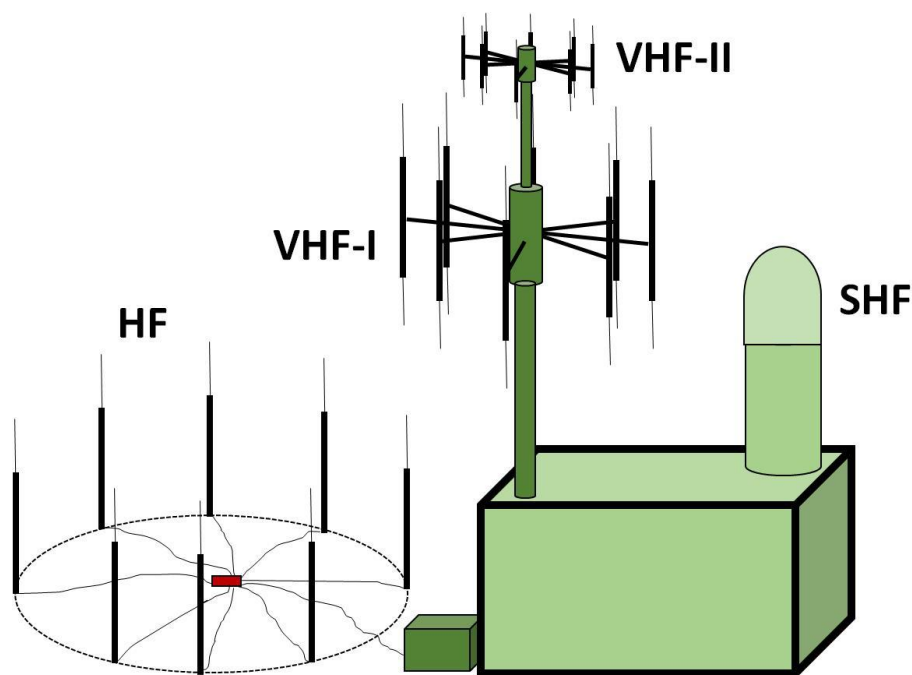


Figura 2-9: En la figura puede verse la distribución de las antenas para distintas frecuencias de un emplazamiento de radiogoniometría

Junto a cada array se encontrará una estación de goniometría con los receptores y procesadores de señal correspondientes que sean capaces de recibir una orden de goniometría en una frecuencia concreta a realizar en un momento concreto o bien explorar cierto margen de frecuencias en cierto margen de tiempo. Una vez realizada la orden, la estación devolverá la información de la frecuencia, ángulo y momento de la detección a la estación de radiogoniometría maestra. Dicha estación contará con un sistema de análisis donde se habrá introducido previamente el mapa de la zona, sus propias coordenadas y las coordenadas de las otras dos estaciones que hacen goniometrías en su banda de frecuencias. La estación maestra enviará las coordenadas de origen (realizando una triangulación) a la zona de cabinas de pilotaje, concretamente al sistema de procesamiento donde se forma la JCOP. Esta localización puede tratarse a su vez tanto de un dron propio como de una emisión enemiga sin identificar (que puede ser una señal de comunicaciones, la señal de un iluminador o bien una perturbación intencionada). De hecho, el objetivo del sistema radiogoniométrico es doble, vigilancia y localización de emisiones enemigas y también como apoyo a la localización de los drones propios. El dron propio emitirá una baliza (con su

ID codificado) bien a requerimiento del piloto o bien por iniciativa de su IA propia (al detectar alguna inconsistencia en sus sistemas de localización).

Para poder localizar sin confusión las diferentes emisiones en este campo de batalla tan prolífico en señales radioeléctricas, se hace imprescindible una disciplina de tiempos.

Para poder detectar las emisiones enemigas, cada cierto tiempo (entre 1 y 119 segundos) se producirá un silencio de emisiones propias de 1 segundo de duración. Todos los drones tendrán programada una serie de ventanas de tiempo donde se realizará cada silencio, desde el inicio de la operación hasta el final. La operación durará tres días pero, como se ha dicho, todos los cálculos se han realizado para cinco. Por tanto cada dron lleva programados 7.200 instantes donde realizará un silencio de un segundo. Los radiogoniómetros realizarán dos localizaciones en cada una de esas ventanas temporales, una a las dos décimas de segundo del comienzo del silencio y otra a las ocho. Aquellas emisiones detectadas en ambos instantes serán calificadas automáticamente como emisiones enemigas. Con las emisiones detectadas sólo en un instante se realizará un análisis concreto particularizado, ya que pueden ser drones propios que se hayan desincronizado.

2.4.10 Sistemas de comunicaciones entre las distintas zonas del Área Humana



Figura 2-10: En la figura puede verse la distribución de las distintas zonas del Área Humana. En retaguardia, los distintos routers van unidos mediante fibra óptica.

Los enlaces entre las distintas zonas se realizarán por fibra óptica. La mayoría de los enlaces estarán duplicados para garantizar su supervivencia en caso de fallo. Esta duplicidad implicará caminos separados (un mínimo de dos km.) así como dispositivos de electrónica de red igualmente duplicados.

Las radios y balizas emisoras se encontrarán en la misma zona de la antena y recibirán y transmitirán la información por fibra óptica en banda base.

2.5 Utilización del WiMAX

2.5.1 Introducción al WiMAX⁵⁶

Sobre WiMAX [17] puede obtenerse información relevante en *WiMAX Forum*⁵⁷. En esta página se declara que la misión de este foro es desarrollar especificaciones técnicas basadas en estándares abiertos y perseguir un entorno regulatorio favorable al objeto de lograr la interoperabilidad mundial. Este foro otorga la certificación de los desarrollos que cumplen las premisas anteriores.

Por otro lado la TIA⁵⁸ editó en 2011 tres normas (1140, 1143 y 1164) que cubren parte de los aspectos fundamentales de WiMAX.

La tecnología WiMAX⁵⁹ podría ser de utilidad y aplicación para las comunicaciones en el área de batalla. Se cuenta con que no hay instalaciones de comunicaciones en esta área previamente al inicio de la operación. Se ha escogido WiMAX en lugar de WIFI porque la segunda cuenta con menores alcances y menor escalabilidad. Las especificaciones técnicas de WiMAX se recogen en el estándar inalámbrico IEEE 802.16 [18].

La norma IEEE 802.16 cuenta a su vez con diversos subestándares. No obstante, sobre la misma norma puede desarrollarse también una “solución propietaria” *ad hoc* que cubra las necesidades específicas del ejército de drones para el control de “última milla”. Esta solución propietaria podría estar muy cercana a IEEE 802.16m (del 2011)⁶⁰, que cuenta con velocidades de 100 Mbps para enlaces en movimiento y 1 Gbps para enlaces fijos [7]. Se conoce también como *Wireless MAN-Advanced Mobile* [8] o *WiMAX Release 2*⁶¹.

2.5.2 OFDMA, MIMO y HARQ

Dentro de cada célula, el sistema de acceso elegido es OFDMA⁶², en el que varios usuarios (en este caso los drones a los que da servicio cada célula) comparten el espectro dividido en subportadoras. También cuenta con modulación adaptativa, es decir, a corta distancia y con buena cobertura de señal, utiliza QAM64. Cuando la distancia aumenta y la señal se recibe en peores condiciones, utiliza QAM16. Por último, en las peores condiciones de recepción, utiliza QPSK. Cada uno de estos tipos de modulación tiene una velocidad de transmisión de datos diferente para un mismo ancho de canal, de forma que a mejores condiciones de recepción, la velocidad de transmisión aumenta (y viceversa).

⁵⁶ *Worldwide Interoperability for Microwave Access*, o Interoperabilidad mundial para acceso por microondas.

⁵⁷ <https://wimaxforum.org/home>

⁵⁸ *Telecommunications Industry Association*, o Asociación de la Industria de Telecomunicaciones.

⁵⁹ Apuntes de la asignatura TEL 1 (Sesión 4).

⁶⁰ Ahmadi Sassan (2011) “Mobile WiMAX: A Systems Approach to Understanding IEEE 802.16m Radio Access Technology”. Elsevier. Burlington (MA, USA).

⁶¹ Aunque según documento WMF-T23-001-R030v02_MSP (actualización de R021v02 de 20 mayo 2021) de WiMAX Forum air interface system profile, ya ha sido publicada recientemente la *Release 3*.

⁶² *Orthogonal Frequency-division Multiple Access*, o Acceso por multiplexación por división de frecuencias ortogonales.

Otro concepto a tener en cuenta es el acceso de los drones a través de la antena de la base. El MIMO⁶³, técnica que puede ser soportada por el IEEE 802.16m, incluye las versiones de usuario único (SU-MIMO) o multiusuario (MU-MIMO). En el caso mostrado, con una gran cantidad de drones transmitiendo video la tecnología adecuada, sería deseable MU-MIMO (sin olvidar *massive MIMO* que puede utilizar decenas de antenas, aumentando así el número de drones a los que puede dar servicio).

Los equipos de radio podrían usar la *mmWave*⁶⁴ y la antenas ser del tipo *beam steering*⁶⁵.

Por último hay que nombrar el HARQ⁶⁶ que es un sistema de corrección de errores que consiste en una combinación entre el FEC⁶⁷ y el ARQ. Como en el ARQ estándar, los bits redundantes se agregan a los datos y se transmiten mediante un código de detección de errores como un CRC⁶⁸, por lo que puede decirse que el HARQ es un híbrido entre ambos sistemas.

2.5.3 Implementación del WiMAX en el ejército de drones

Como se ha dicho anteriormente, sería conveniente implementar una solución propietaria adaptada a los requerimientos previstos, muy similar a la descrita en la norma IEEE 802.16m. En esta norma se detallan los niveles físico y de enlace, pero WiMAX debe desarrollar también la capa de red.

Como la premisa es que ningún humano penetre en la zona de la operación y, además, no se cuenta con ninguna infraestructura de comunicaciones propia en esta zona, todas las estaciones base⁶⁹ se implementarán sobre drones específicos para comunicaciones.

Las estaciones que forman el *backhaul*⁷⁰ estarían montadas sobre drones terrestres. Está previsto que una vez ubicado el dron en su posición, despliegue sus antenas y quede estático durante el resto de la operación. Estas estaciones contarían con antenas tanto para el *uplink* (conectadas a otras estaciones *backhaul* en una red), como para dar conectividad de gran ancho de banda a la “última milla”. Las antenas para *uplink* son radioenlaces direccionales (y con conexiones redundantes) y las de la última milla son omnidireccionales.

Las estaciones de la última milla también estarían montadas sobre drones, aunque en este caso también puede tratarse de drones aéreos además de terrestres. Cada estación de última milla estará asociada a una estación *backhaul*, pero las estaciones *backhaul* estarán desplegadas de tal forma que si se produjera un fallo en una de ellas, otra podría asumir su función para esa zona. La salida de las estaciones de última milla se realizará a través de las de *backhaul*. Se ha de tener en cuenta la dificultad añadida que produce que muchos de los usuarios sean drones aéreos, con lo que la cobertura de las antenas debe contemplar esta circunstancia. Cuando se habla de antenas omnidireccionales para la última milla, normalmente se consigue con un grupo de antenas direccionales dispuestas para cubrir los 360° a su alrededor. Con lo dicho sobre los drones aéreos, la cobertura debe contar también con la tercera dimensión, añadiendo dificultad al problema de la cobertura.

Otro problema a resolver es la asimetría inversa. Es decir, las velocidades de subida y de bajada no son similares (asimetría). En el caso típico de un domicilio también se produce esta asimetría, debido a que las plataformas multimedia aportan mucho más caudal de información a un hogar que a la inversa.

⁶³ Multiple-Input Multiple-Output.

⁶⁴ Ondas milimétricas, cercanas a 26 GHz, mayor frecuencia, más canales, más usuarios a más velocidad de transmisión. Aunque hay tener en cuenta que estas ventajas se ganan a costa de perder alcance. Habría que sopesar si merece la pena utilizar estas antenas en el caso descrito.

⁶⁵ Antenas que pueden cambiar la dirección del lóbulo y su diagrama de radiación mediante software, sin que ello implique cambios físicos.

⁶⁶ *Hybrid Automatic Repeat Request*, o Híbrido ARQ (solicitud de repetición automática).

⁶⁷ *Forward Error Correction*, o Corrección de Errores hacia Adelante.

⁶⁸ *Cyclic Redundancy Check*, o Verificación de Redundancia Cíclica.

⁶⁹ Tanto las BTS: *Base Transceiver Stations*, como las SS: *Subscriber Stations*.

⁷⁰ Esqueleto o *backbone* principal de la red.

La buena noticia es que WiMAX está pensado para este tipo de asimetría. La mala noticia es que en el ejército de drones la asimetría se produce a la inversa que en el hogar, el caudal información de subida, procedente de los videos de los drones, es mucho mayor que el de bajada (principalmente las órdenes para el control remoto).

2.6 Utilización del DTN

2.6.1 Introducción al DTN

Las Redes Tolerantes a Retardos e Interrupciones (DTN, del inglés, *Delay- and Disruption-Tolerant Networking*) [9]⁷¹ han surgido como respuesta a aquellos casos en los que las premisas que se supone deben cumplir las redes TCP/IP no se cumplen o se cumplen con carencias. Las comunicaciones por los protocolos de internet asumen que el entorno de las mismas es relativamente estable. Se presupone que existe un camino entre el origen de los datos y el destinatario así como que el tiempo transcurrido no es excesivo y además la pérdida de paquetes es mínima. Pero esto no siempre es así [10]⁷².

Las DTN nacieron inicialmente para cumplir la necesidad de movilidad, bien de host o de routers (o ambos), pero también para paliar otros inconvenientes, como fallos en la alimentación (que provocan inexorablemente un fallo en las comunicaciones) o bien un entorno con muchas interferencias. Algunos ejemplos de estos entornos son redes terrestres móviles, redes “exóticas” (como enlaces satélites o en el “espacio profundo”), redes específicas o *Ad Hoc* (aquí entraría el concepto de redes militares, expuestas a interferencia intencionada o *Jamming*) y redes de sensores (caracterizadas por tener limitadas la capacidad de proceso, la memoria y el consumo de alimentación)⁷³.

En este punto se tratará el caso de utilidad de DTN en redes *Ad Hoc* para fines militares.

2.6.2 Historia y descripción del DTN

A finales de la década de los 90 la comunidad científica comenzó a explorar el aprovechamiento de los protocolos de internet para las comunicaciones planetarias y en el espacio exterior. Así comenzó el IPM (*Interplanetary Internet Project*)⁷⁴. Poco antes ya se había extendido el uso de protocolos inalámbricos (*wireless*) y se había creado el MANET (*Mobile Ad-Hoc Networking*)⁷⁵. En los cálculos de un enlace Tierra - Marte, usando TCP, por la limitación de los tiempos de transmisión, la velocidad era de 1,6 a 250 Kbps [11]⁷⁶. Si se añaden las temperaturas extremas, los movimientos de órbitas de los planetas y de las naves espaciales y el enorme retraso entre la ida y la vuelta se aprecia que las tasas de error son muy altas.

En 2002 Kevin Fall comenzó a adaptar ideas del IPM para el diseño de redes terrestres. Él fue quien acuñó el término y su acrónimo DTN⁷⁷. Ese mismo año el IETF⁷⁸ creó el *DTN Research Group* (DTNRG) que tenía el objetivo de extender el concepto de una arquitectura de redes tolerantes a retardos e interrupciones. En realidad la aplicación del DTN es similar en las comunicaciones espaciales y

⁷¹ VVAA (2009) “Delay-/Disruption-Tolerant Networking: State of the Art and Future Challenges”. Surrey, UK. Center for Communication Systems Research (CCSR).

⁷² Estas premisas se dan tanto en los apuntes de la asignatura TEL 2 como en: VVAA (2012) *Delay Tolerant Networks: Protocols and Applications*, Boca Ratón, USA. CRC Press Tylor & Francis Group, LLC. (Pg. V, Preface).

⁷³ Ibidem, (Pg. VI, Preface).

⁷⁴ Proyecto de la NASA con varios colaboradores, entre ellos, Vinton Cerf.

⁷⁵ Ibidem, (Pg. 2).

⁷⁶ Voyiatzis, Artemios G. (2012) “A Survey of Delay- and Disruption-Tolerant Networking Applications”. En *Journal of Internet Engineering*, Vol. 5, No. 1.

⁷⁷ VVAA (2012).

⁷⁸ *Internet Engineering Task Force* o Grupo de Trabajo de Ingeniería de Internet.

terrestres, con la diferencia que las interrupciones y retrasos en el espacio son en gran parte predecibles con precisión⁷⁹.

Los protocolos DTN se fueron desarrollando y en 2007 se publicaron por el IETF los RFC 4838 y RFC 5050⁸⁰. El IETF desarrolló el protocolo *Bundle BPv7*⁸¹ (hay seis implementaciones).

Los protocolos de *Bundle* desarrollados por el CCSDS⁸² son los BPv6 y entre ellos puede mencionarse el DTN-2⁸³ (específicos para misiones en el espacio).

2.6.3 Estudio preliminar de la aplicación del DTN a los enjambres de drones

Entre los casos de uso descritos en la bibliografía consultada⁸⁴ se mencionan (entre otras) las *Pocket Switched Networks* (Redes conmutadas de bolsillo) o las “Redes metropolitanas con nodos heterogéneos”. Las primeras toman el concepto de extender las redes más allá de los puntos de acceso incluyendo, por ejemplo, enlaces *peer-to-peer* tales como conexiones *Bluetooth*. Las segundas están en cierto modo relacionadas con las primeras. Se muestra un ejemplo esquemático:

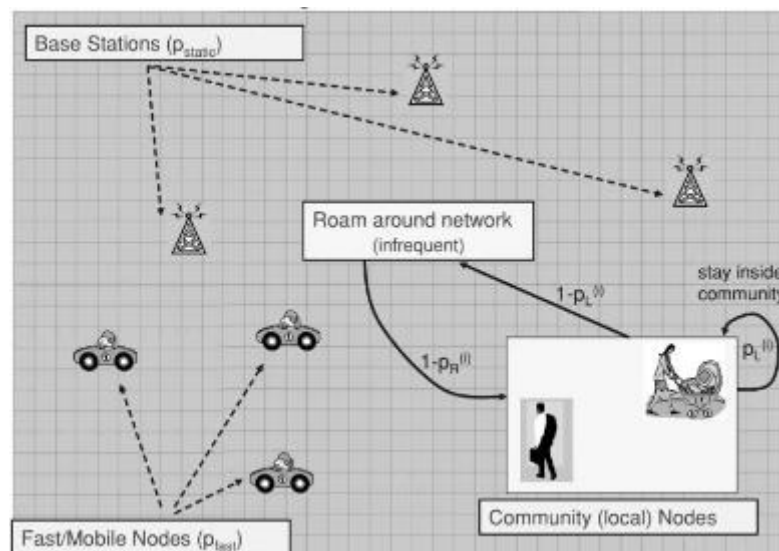


Figura 2-11: Ejemplo de escenario con nodos heterogéneos inalámbricos⁸⁵.

No obstante este trabajo está enfocado al posible uso de las DTN en el ámbito militar pero hay que decir que, desde el punto de vista de las comunicaciones, sería muy parecido. La diferencia más sustancial es que en el ámbito militar habría que prevenir especialmente acciones intencionadas de los adversarios contra la integridad, confidencialidad y disponibilidad de la información.

⁷⁹ Voyiatzis (2012).

⁸⁰ <https://datatracker.ietf.org/wg/dtn/documents/>

⁸¹ <https://datatracker.ietf.org/doc/html/draft-ietf-dtn-bpbis-27.html>

<https://tools.ietf.org/pdf/draft-sipos-dtn-bpv7-admin-iana-00.pdf>

⁸² Consultative Committee for Space Data Systems: <https://public.ccsds.org/default.aspx>

⁸³ <https://github.com/delay-tolerant-networking/DTN2>

⁸⁴ VVAA (2012). Pg. 57, punto 2.6.

⁸⁵ *Ibidem*.

2.6.4 Funcionamiento y ventajas del DTN

Cómo se ha dicho las DTN son usadas en aquellos casos en los que por determinadas circunstancias las comunicaciones aportan menores prestaciones que en otros entornos más estables. Se asume pues un cierto retardo, o la posibilidad de que el mismo no sea incompatible con la finalidad de la aplicación. Si se necesitara una aplicación con una latencia permitida mínima y las comunicaciones fueran inestables, la única solución sería mejorar las comunicaciones o cambiar de aplicación. Implementar una DTN no solucionaría el problema en este caso. El DTN intenta minimizar la pérdida de información por pérdida de paquetes con una idea ingeniosa que lo diferencia del TCP/IP tradicional: Los nodos almacenan información y la envían cuando las comunicaciones están disponibles (no la pierden).

Es decir, la arquitectura es una red de redes. Cada una de estas redes se denomina “Región DTN” y tiene (o puede tener) distinta naturaleza. En cada Región hay Host y Routers. Para conectarse con otras regiones se emplean las pasarelas (gateways). El almacenamiento persistente en el Gateway es necesario, mientras que en los host y routers es opcional (aunque muy conveniente).

Como ya se ha anticipado anteriormente, en los RFC 4838 and RFC 5050 el IETF desarrolló el *Bundle Protocol BPv7*.

Bundle podría traducirse por paquete, pero no se utilizará esta palabra para evitar confusión con los paquetes del protocolo TCP/IP. *Bundle* también puede ser haz, manojo, fajo, bulto, ramillete o envoltorio.

Este protocolo define una serie de bloques de datos contiguos como un envoltorio, donde cada envoltorio contiene suficiente información semántica para permitir que la aplicación funcione donde un bloque individual quizá no lo haría. Los envoltorios se enrutan para que se produzca el almacenamiento y reenvío entre los distintos nodos a través de diversas tecnologías de transporte de red (incluidas tanto las basadas en TCP/IP como aquellas que no se basan en estos protocolos).

Las capas de transporte que llevan los paquetes a través de sus redes locales se denominan capas de convergencia de envoltorios. Por lo tanto, la arquitectura de envoltorio funciona como una red superpuesta, lo que proporciona una nueva arquitectura de nombres basada en identificadores de extremos (EID⁸⁶) y ofertas de servicios.

Las capas del protocolo ofrecen seis tipos de servicios en el envoltorio:

Transferencia de custodia: La responsabilidad de la retransmisión se negocia y traspasa entre el nodo que envía y el que recibe. El nodo que recibe devuelve un reconocimiento de custodia al nodo emisor. Hasta que esto no se produce, el emisor sigue teniendo la responsabilidad de la custodia.

Acuse de recibo: El receptor confirma que ha recibido el envoltorio (*bundle*). Esto se produce en último término por parte de la Aplicación de destino.

Notificación de transferencia de custodia: Se produce cuando un nodo acepta la transferencia de custodia del envoltorio.

Notificación de reenvío de envoltorios: Notificación de que el envoltorio ha sido reenviado a otro nodo.

⁸⁶ Endpoint Identifiers

Prioridad de entrega: Se indica Poca, Normal o Acelerada⁸⁷

Autenticación: Método de firma digital que verifica tanto la identidad del emisor como la integridad del envoltorio.

Con respecto al funcionamiento de las aplicaciones con DTN, hay que decir que no todas las aplicaciones pueden funcionar con este tipo de redes. En muchos casos los tiempos de retardo de la DTN sobrepasan los *timeouts* de ejecución de la aplicación.

Lo normal es adaptar aplicaciones existentes o bien desarrollar otras nuevas *ad hoc*. Otra solución es utilizar *Proxys*, pero esto sólo puede hacerse en algunas aplicaciones (por ejemplo el correo electrónico, la transferencia de ficheros o la navegación web).

2.6.5 Posibles aplicaciones militares del DTN

La inestabilidad de las comunicaciones en un entorno bélico es evidente y no necesita de mucha demostración. Ahora bien, sí que se requiere una puntualización: La inestabilidad no es igual en todos los niveles.

Se definen los niveles Estratégico, Operacional y Táctico. En el primero pueden imaginarse grandes puestos de mando en edificios de retaguardia, el táctico correspondería a las unidades de primera línea, muy móviles y en contacto directo con el enemigo. El nivel operacional correspondería a un estatus intermedio entre los dos anteriores⁸⁸.

Por lo anterior puede deducirse que las redes más inestables se encuentran en los niveles táctico, operacional y estratégico (precisamente por ese orden de inestabilidad).

Por otro lado, para la toma de decisiones es vital la información (que debe llegar a tiempo). Una vez tomada la decisión, ésta debe llegar cuanto antes a quien deba ejecutar la acción. Así que el retardo, o latencia admitida, tampoco será la misma dependiendo del nivel. En el nivel estratégico las decisiones se toman a medio y largo plazo. En el táctico a corto y cortísimo plazo. Como se ha dicho antes, el nivel operacional siempre es el intermedio, o puente entre los otros dos.

Con lo que aparece aquí una especie de paradoja: Las redes que, por su inestabilidad, más necesitarían DTN, son también las que menos retardo admiten y, por tanto, donde menos aplicación tendría ésta.

Por el tipo de medios, las redes cuyos medios de transmisión se sitúan en plataformas aéreas (aviones, drones o helicópteros) tienen una topología de naturaleza dinámica que encajaría muy bien con DTN. Las redes navales incluyen múltiples enlaces heterogéneos con lo que también son un escenario ideal para un enfoque DTN, ya que la capa del paquete puede actuar como la capa unificadora sobre las capas de convergencia y las redes específicas con enlaces de distintas tecnologías.

Un ejemplo de demostración real del concepto es el proyecto CONDOR⁸⁹ (del Cuerpo de Marines estadounidense).

La unidad prototipo del *gateway* consta de un enrutador Cisco 3725, una Radio EPLRS, un módulo de encriptación de enlaces, otro enrutador de acceso Cisco, y una terminal de comunicaciones por

⁸⁷ Bulk, Normal o Expedited.

⁸⁸ Explicación del autor, destinada a legos en material militar.

⁸⁹ Command and Control On-The-Move Network Digital Over-The-Horizon Relay.

satélite. El software DTN2 se transfiere a CONDOR y se carga en el módulo IDS de Cisco. El proyecto CONDOR también añadió soporte para el Protocolo de comunicación espacial, incluyendo un Protocolo de transporte estándar (SCPS-TP) en el módulo, e implementó un proxy web habilitado para DTN.

2.6.6 Aplicación concreta del DTN en el caso de estudio

La inestabilidad y dificultad de la red descrita en este trabajo se hace evidente debido a que no contaría con ninguna instalación fija, su heterogeneidad de sistemas, las influencias del terreno y del clima y la acción enemiga (posibles destrucciones físicas y perturbaciones).

Por tanto se hace necesario estudiar en qué casos y qué tipos de datos podrían transitar por DTN y cuáles no.

Un servicio de comunicaciones necesario para el control de drones es el que tiene por misión recibir en tiempo real el vídeo para poder realizar la conducción. Así mismo, a raíz de las imágenes que el piloto contempla, éste transmite al dron las señales que servirán para accionar sus servomecanismos de movimiento (y en algunos casos, de ataque). No es preciso tener grandes conocimientos para intuir que ambos servicios requieren una latencia mínima. No obstante, los drones aéreos pueden contar con cierta latencia en ambas señales (video desde el dron hacia el piloto y órdenes en sentido inverso) si el dron aéreo cuenta con cierta IA (Inteligencia Artificial) para la autonavegación. En el caso de los drones terrestres, se haría necesario implementar un sistema de frenado automático en el caso de que se detectara una latencia (o interrupción) en alguno de los dos enlaces.

El video grabado por un dron para obtener ISTAR (sin capacidad letal), podría ser muy apto para ser transmitido a través de una red DTN hasta los analistas de inteligencia que evaluarían ese vídeo.

Determinadas órdenes hacia los drones y respuestas de los sensores de los mismos podrían ser perfectamente transmitidas por los envoltorios del DTN. Las localizaciones de posicionamiento de los drones, pueden ser un caso a utilizar. Simplemente se deberá tener en cuenta que la coordenada de la posición debe “formar pareja” con la coordenada tiempo, porque puede que el retardo en la recepción sea considerable y, por tanto, se necesite ubicar al dron en relación a un momento determinado.

Si se ha decidido utilizar DTN como red de datos para determinadas aplicaciones, habrá que tener en cuenta que para su correcto funcionamiento serán necesarias algunas adaptaciones. Una opción es desarrollar una nueva aplicación (o aplicaciones en plural, según la necesidad) que funcione con DTN. La segunda alternativa es utilizar un proxy para que adapte y haga compatible la aplicación con la DTN.

2.6.7 Conclusiones obtenidas sobre la aplicación del DTN en el caso de estudio

Tras el estudio se considera que el DTN tiene ciertas aplicaciones pero “no hace milagros”. Si el problema es que la red de la que se dispone tiene graves carencias, el DTN podrá soslayar algunas de ellas, pero no todas. Para cumplir algunos objetivos o que funcionen de determinada forma ciertas aplicaciones, el único camino será mejorar la red.

En una operación militar ofensiva convencional, los medios de telecomunicaciones estables y fiables solo están en retaguardia. Si además se habla de una operación a realizar sólo con drones, y añadiendo la utilización de un número masivo de estos (con los problemas de saturación del espectro que eso conlleva), las dificultades se multiplican. Se estima que para solventar estas dificultades las opciones más viables son aumentar el número de nodos, hacer uso extensivo de comunicaciones satélite (aunque estas añaden cierta latencia por sí mismas), así como incrementar los radioenlaces de alta

capacidad (en “primera línea” sólo los enlaces “no guiados” son posibles, no se puede contar con cable ni fibra óptica a partir de determinada distancia al enemigo). En las siguientes figuras puede verse esquemas de comunicaciones típicas entre drones y fuerzas terrestres. Los mensajes se transmitirían de forma asíncrona entre los nodos de red.

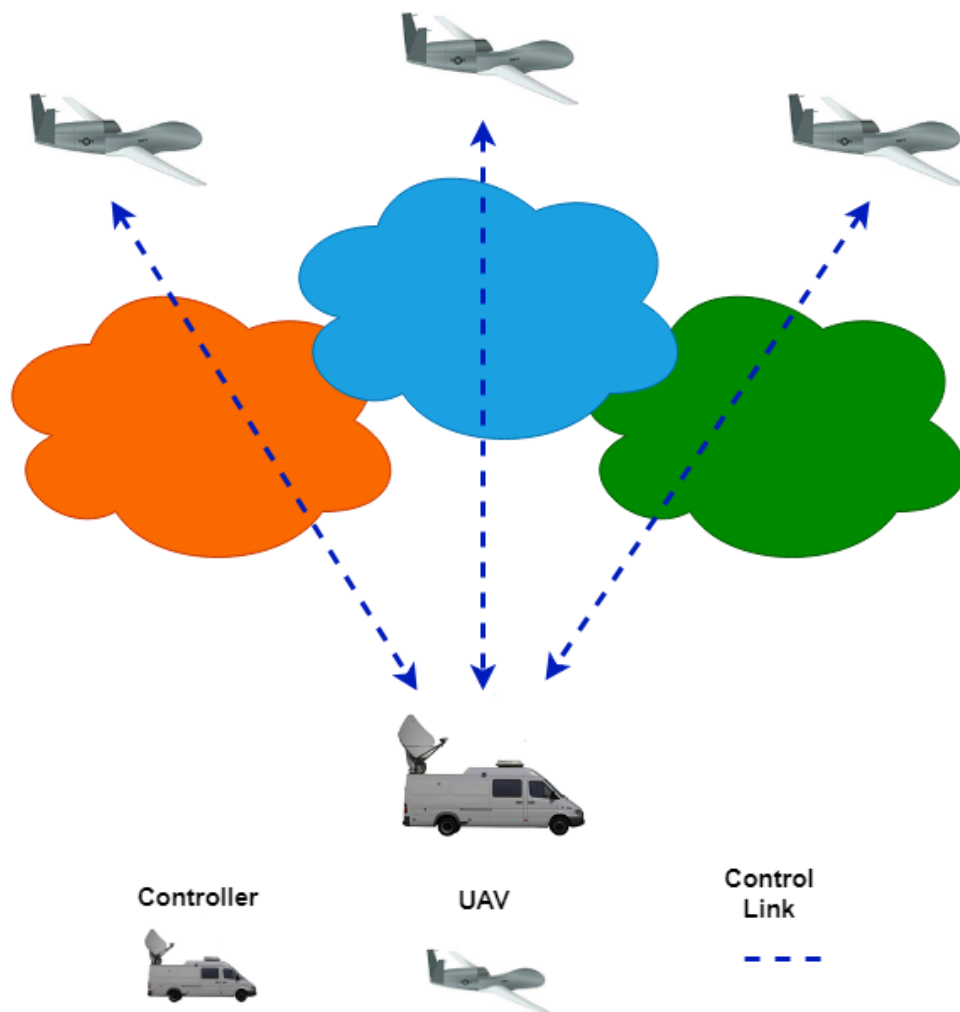


Figura 2-12: Ejemplo de red definida por software con drones [5].

Las conclusiones del estudio de la validez de DTN para ser utilizado en una operación masiva de drones han sido las siguientes:

Determinados servicios, como la transmisión de vídeo para la conducción de los drones terrestres, o las órdenes para este fin dadas a los mismos, deberían de enviarse por otro tipo de redes (o bien en

comunicaciones punto a punto si fuera posible).

Algunos servicios, que puedan admitir ciertas latencias y a la vez requieran capacidad de supervivencia, sí que son candidatos ideales para utilizar DTN.

Por lo anterior, la piedra angular es la correcta decisión de qué servicios circularán por DTN y cuáles por redes TCP-UDP/IP (sin implementación DTN).

La siguiente decisión es buscar el esquema de adaptación de las aplicaciones a DTN, bien mediante proxy o bien adaptando (o realizando *ad hoc* desde cero) cada una de las aplicaciones. Se debe tener en cuenta que puede escogerse una solución diferente para cada aplicación.

3 SISTEMAS DE LOCALIZACIÓN Y POSICIONAMIENTO⁹⁰

3.1 Introducción a la localización

3.1.1 Sistemas primarios y secundarios

El sistema principal para el posicionamiento de los drones serán las señales de GNSS. La mayoría (aquellos que lo necesiten) de los drones aéreos y terrestres contarán con un sistema multireceptor de GNSS capaz de obtener localización del GPS NAVSTAR (Standard y WAAS) y del Galileo. Caso de que estos sistemas resultaran degradados (intencional o accidentalmente), o aparecieran contradicciones o inconsistencias con respecto a la localización, se utilizarían los sistemas TACAN / DME y, en último caso, NDB. Se ha estudiado utilizar radares para la localización de drones propios. Este sistema se ha desechado por el número masivo de drones intervinientes. Aunque determinados radares son capaces de discriminar y diferenciar distintos objetos móviles, se ha desestimado este uso para el ejército de drones.

3.1.2 Posicionamiento directo e inverso

Por posicionamiento se entenderá la asociación de un determinado dron a unas coordenadas. En el caso de los drones terrestres serán necesarias dos coordenadas pero en el caso de los aéreos se añadirá la altura. Esta información de localización será de utilidad, tanto para los sistemas de navegación automática del dron como para el piloto del dron y el puesto de mando (en el Área Humana). Si la información de la localización de un dron sólo estuviera en un extremo (bien en el dron, bien en el Área Humana) se podrían transmitir las coordenadas con un sencillo sistema de mensajes, por ejemplo:

“Dame tus coordenadas, te he perdido / Mis coordenadas son estas xxyy”

“Dame mis coordenadas, me he perdido / Tus coordenadas son estas xxyy”

“Te he perdido, transmite con tu radiobaliza tu indicativo en x segundos”

“Mi posición es dudosa. Transmite con TACAN – NDB en x segundos”

Como dato a tener en cuenta el posicionamiento directo se realiza tanto para ubicar a los drones propios, como a los medios emisores enemigos. El posicionamiento inverso sólo se utiliza para posicionar los drones propios.

3.1.3 Triangulación y Trilateración

Ambos sistemas pueden determinar la posición del dron que nos interese y pueden hacerlo, a su vez de forma directa y de forma inversa. Se verá en primer lugar la triangulación.

Si el dron emite una señal de radiofrecuencia baliza con una frecuencia determinada, en un momento determinado y con un indicativo (ID) determinado, los tres radiogoniómetros reciben esa señal, la demodulan (para confirmar que el ID es el correcto) y miden el ángulo con respecto al norte. Como en el radiogoniómetro maestro se encuentran los datos de posición de él mismo y de los otros dos, es relativamente sencillo calcular automáticamente el punto donde se cortan las tres semirrectas. Esta triangulación podría hacerse con sólo dos radiogoniómetros. De hecho al realizarla con tres, el resultado no es un punto, sino un triángulo. Dependiendo del tamaño y forma de ese triángulo se produce una zona de indeterminación, donde el dron se encontrará con cierta probabilidad. Luego esta información se

⁹⁰ Localización y posición son términos casi sinónimos. Podría decirse la posición de un objeto serían sus coordenadas, y su localización la situación relativa con respecto a otro de posición conocida. La RAE no arroja mucha luz sobre esta diferencia y el significado de ambas que se da en este trabajo probablemente sea un anglicismo. Debido al estrecho matiz, se emplearán indistintamente.

transmite a los servidores que conforman la JCOP así como al propio dron (como ayuda a la navegación). En el caso de un emisor enemigo, el proceso sería el mismo, con la diferencia de que su transmisión no es intencionada para que pueda ser localizado.

En la triangulación inversa son las antenas del área humana (TACAN y NDB) las que emiten secuencialmente (no a la vez) y es cada dron el que estará equipado con un sistema para medir el ángulo de esas transmisiones. El propio dron también tendrá introducido en su sistema, un procesador para posicionamiento y las coordenadas de los emisores para poder realizar los cálculos.

En el caso de la trilateración, aunque el objetivo que se busca es el mismo (recuérdese que en este caso no se persigue la localización de medios enemigos, sólo los drones propios) los datos obtenidos en primer término no son ángulos, sino distancias desde el emisor hasta el móvil (a raíz de medir el tiempo de retardo). La trilateración inversa por señales GNSS será el sistema prioritario para la localización de un dron propio. No está prevista la trilateración directa (que el dron emita la señal y un dispositivo ajeno mida el tiempo y la distancia).

La trilateración inversa alternativa la formarán los equipos DME.

3.1.4 La coordenada altura

Esta coordenada no es lo suficientemente precisa con los medios de GNSS, y una falta de precisión podría devenir en que el dron, en vuelo automático, colisionara contra el suelo.

Se ha sopesado utilizar un sistema alternativo con un emisor embarcado en un globo cautivo (a una altura fija y conocida) y situado en el área humana. El dron realizaría con esta señal proveniente del globo y otra al nivel del suelo, una triangulación o trilateración inversas. Esto es técnicamente posible pero se ha estimado más oportuno equipar a los drones aéreos que lo necesiten con un radioaltímetro⁹¹.

Hay que tener en cuenta que el radioaltímetro expresa la altura en pies o metros AGL⁹². Esto es precisamente lo que interesa para la autonavegación o el apoyo al control remoto (incluyendo el TAWS⁹³). Para saber la coordenada sobre el nivel del mar sería necesario la suma de la altura del terreno en ese punto, aunque tampoco parece muy crucial esta información en este caso.

3.2 Sistemas de localización y posicionamiento

3.2.1 GNSS: GPS y Galileo

Gran parte de los localizadores GNSS actuales cuentan con multireceptores compatibles con los sistemas GPS [12]⁹⁴, Galileo y GLONASS⁹⁵, para obtener redundancia en las medidas y, por tanto, mayor fiabilidad y precisión. Dependiendo del tipo de conflicto sería conveniente desechar las medidas del GLONASS (e incluso del GPS). En los sistemas GNSS el posicionamiento del dron se calcula por trilateración inversa. Para aumentar ciertas características (disponibilidad, integridad, continuidad y precisión), esos sistemas cuentan con posibilidades de “aumentación”. Estos sistemas pueden estar

⁹¹ Recomendación UIT-R M.2059-0 (02/2014). *Características técnicas y de funcionamiento y criterios de protección de altímetros radioeléctricos que utilizan la banda de frecuencias 4.200-4.400 MHz.*

⁹² Above Ground Level, o sobre el nivel del suelo.

⁹³ Terrain Awareness and Warning System, o sistema de aviso de colisión contra el suelo.

⁹⁴ VVAA (2008), *Global Positioning System Standard Positioning Service Performance Standard*. 4th Edition. Department of Defense (USA).

⁹⁵ *Global'naya Navigatsionnaya Sputnikovaya Sistema*, es un GNSS hoy gestionado por la Federación Rusa (antes URSS).

implementados en propio dron⁹⁶, con apoyo de estaciones terrestres (en este caso se encontrarían todas en el área humana y ninguna en la zona de operación) o en los propios satélites (sistemas WAAS [13]⁹⁷ o EGNOS⁹⁸). Para que todos los sistemas alternativos a los GNSS tuvieran utilidad, es vital que los drones cuenten con un sistema de detección de funcionamiento anómalo (intencionado o fortuito) y capacidad de decisión para tener en cuenta los posicionamientos que les marquen los sistemas secundarios que se verán a continuación.

3.2.2 TACAN, DME y NDB

Como se ha explicado en el apartado de 2.3 (Sistemas de comunicaciones y posicionamiento en el “Área Humana”) existirán transmisores y antenas de los tres sistemas mencionados para apoyo al posicionamiento. Los drones de mayor importancia táctica contarán con los equipos necesarios para trabajar con estos sistemas⁹⁹, como opción de posicionamiento alternativa. Las coordenadas y características de las instalaciones en tierra deben estar introducidas en los drones con estos sistemas antes del inicio de la operación.

En el DME es el dron el que primero transmite unos pulsos con su emisor interrogador, que son devueltos con un determinado retardo (12 y 36µs. y entre 1.025 y 1.150 MHz)¹⁰⁰ por el emisor en tierra. De esta forma puede medirse la distancia entre el dron y la baliza de tierra. Teniendo dos DME en tierra como se ha explicado, puede el dron conocer su posición por trilateración inversa.

Las instalaciones del DME pueden (y suelen) aprovecharse para hacerlas coincidir con las del TACAN [14]. El TACAN¹⁰¹ aporta una señal al dron que le hace ser capaz de medir su dirección relativa. Podría decirse, *grosso modo*, que un TACAN es como un VOR militar con algo más de precisión. Dicho esto, puede deducirse que con una sola instalación de TACAN y DME sería suficiente para la localización del dron. Teniendo las coordenadas de la instalación combinada en tierra, la dirección y la distancia, se puede determinar un punto de localización del dron. Con esta duplicidad se busca eliminar inconsistencias que pudieran producirse. El resultado sería una “figura de incertidumbre” en cuanto a la posición.

En cuanto a los dos emisores NDB, podrían considerarse “el alternativo del alternativo”. Es mucho menos preciso que el TACAN pues la emisión de tierra no lleva implícita ninguna información de dirección y ésta debe ser medida por el ADF¹⁰² embarcado en el dron. Para realizar la localización inversa por triangulación deben desplegarse dos emisores (como se ha previsto).

3.2.3 Sistemas dummies, señuelos y brújulas electrónicas.

Determinados drones, por las misiones que realizan, no requieren de un sistema de posicionamiento sofisticado. Los drones señuelo, principalmente aéreos, estarán programados para realizar un vuelo con un rumbo fijo. Para mantener ese rumbo, por medio de su piloto automático, tan sólo necesitan una brújula electrónica que les indique que están volando en la dirección correcta. Esta brújula será de tres

⁹⁶ RAIM y FDE (Receptor con Supervisión Autónoma de la Integridad y Detección de Fallos y Exclusión) en el caso de GPS.

⁹⁷ VVAA (2008) *Global Positioning System Wide Area Augmentation System (WAAS) Performance Standard*. 1th Edition. Department of Transportation (USA).

⁹⁸ European Geostationary Navigation Overlay Service, es un servicio que cuenta con tres satélites suplementarios y además una red de estaciones en tierra (4 de ellas en España).

⁹⁹ Antenas, receptores, sistemas de cálculo y en algunos casos, emisores de balizas.

¹⁰⁰ Overview of Distance Measuring Equipment (DME), 2012. www.richardsonrfpd.com Consultado 01/12/2021.

¹⁰¹ VVAA (2016) *Manuals Combined: ELECTRONICS TECHNICIAN, VOLUMES 01 – 08*. Capítulo 2, TACAN. Center for Surface Combat Systems, U.S. Navy.

¹⁰² *Automatic Direction Finder*, o buscador de dirección automática.

ejes¹⁰³, para comprobar que además de la dirección, el dron mantiene una trayectoria ligeramente ascendente.

Existirán drones terrestres que podrán ser controlados desde otro dron “nodriza”. La visión de cámaras será la vista desde el dron nodriza y también desde éste se transmitirán las órdenes. Este dron terrestre de “avanzadilla” tan sólo contará con un receptor que le permita transmitir las órdenes recibidas a sus servomecanismos (tanto de movimiento como de ataque). Este sistema será especialmente utilizado en las primeras fases de apertura de brecha donde se espera que el enemigo todavía tenga capacidad de destrucción física de algunos drones.

3.3 Otros sistemas avanzados

3.3.1 Otros sistemas avanzados de localización y navegación

Hasta ahora se han descrito los sistemas de posicionamiento primarios (GNSS) y los secundarios (TACAN, DME y NDB), así como sistemas de bajas prestaciones como una brújula electrónica. No obstante existen sistemas más sofisticados que podrían actuar también en el caso de fallo de los sistemas primarios [15]¹⁰⁴.

Un caso particular sería el utilizado por los misiles HARM¹⁰⁵. El AGM-88¹⁰⁶ es un ejemplo de este tipo de misil que utiliza un sistema de guiado peculiar; detecta las emisiones SHF y UHF de radar (o telecomunicaciones) enemigas y utiliza esa misma emisión para su guiado terminal. Este no sería un caso de posicionamiento, pero sí de navegación (relativa a la fuente emisora).

Como variante de este sistema, se puede utilizar un dron propio y situarlo en la zona de impacto deseada, a continuación, ordenarle transmitir una radiobaliza y enviar un HARM (o un dron con el mismo sistema de navegación) contra esa señal propia.

Otro caso de interés son los sistemas de navegación del misil Taurus KEPD 350¹⁰⁷. Este misil no sería usado en el ejército de drones, ya que por su alcance de 500 km estaría infrutilizado. No obstante sus sistemas sí que podrían adaptarse a algunos drones. Utiliza el MIL-GPS- SAASM¹⁰⁸ (con resistencia a las perturbaciones). También INS¹⁰⁹, por el que mediante sensores de rotación (giróscopos) y de movimiento (acelerómetros) calcula la orientación y velocidad sin tener referencias externas.

El mismo misil Taurus cuenta con TRN¹¹⁰ que mide las alturas del terreno y las compara con un mapa de elevaciones que se ha cargado previamente en el navegador. Este sistema es un complemento perfecto del INS anterior.

Por último, se incorpora el IBN¹¹¹. Este sistema tiene varias versiones. En unas compara las imágenes captadas por el dron con las imágenes esperadas del terreno según el mapa, y en otras compara las imágenes captadas en un momento con las captadas en el momento siguiente (corrección de imágenes sucesivas)¹¹².

¹⁰³ Por ejemplo, el chip comercial AK8973S (Asahi Kasei).

¹⁰⁴ VVAA, (2013) *Navegación en condiciones de denegación de señal GNSS*. En Nº 13 de Monografías del SOPT (Sistema de Observación y Prospectiva Tecnológica). Secretaría General Técnica del Ministerio de Defensa.

¹⁰⁵ *High-speed Anti-Radiation Missile*, o Misil de alta velocidad anti radiación.

¹⁰⁶ Fabricado en la actualidad por Raytheon Corporation.

¹⁰⁷ *Target Adaptive Unitary and Dispenser Robotic Ubiquity System / Kinetic Energy Penetrator and Destroyer*.

¹⁰⁸ *Selective Availability Anti-Spoofing Module*.

¹⁰⁹ *Inertial Navigation System*, o Sistema de Navegación Inercial.

¹¹⁰ *Terrain Referenced Navigation*, o Navegación referenciada al terreno.

¹¹¹ *Image Based Navigation*, o Navegación Basada en Imagen.

¹¹² VVAA, (2013) *Navegación en...* puntos 6.1.10 y 6.2.

3.3.2 Conclusiones sobre localización y navegación

Hasta ahora se ha mostrado una diferente panoplia de sistemas para posicionamiento. Sus objetivos son, en resumen, obtener una coordenada de posicionamiento para que el dron con sistemas de navegación automática sepa dónde está y qué servomecanismos de guiado tiene que activar para llegar a su destino. Así mismo es útil (necesario o vital en algunos casos) que el puesto de mando sepa dónde está determinado dron en determinado momento, y que la posición de los drones - o de un dron en concreto - aparezca en la JCOP si se desea.

Por tanto se deberá valorar la elección del sistema, o sistemas (normalmente lo segundo), a implementar en cada dron. En aquellos drones con varios sistemas de posicionamiento, será de suma importancia la parte de computación e IA que decida a qué sistema otorga mayor credibilidad, existiendo unas prioridades por defecto y unos eventos (como detección de degradación de la señal o perturbaciones) que decidan cambiar esa prioridad o incluso pedir automáticamente confirmación externa de la posición.

4 ESQUEMA GENERAL DE INTERRELACIÓN

4.1 Posicionamiento inicial

4.1.1 Otros medios puramente militares

Dada la naturaleza de la operación, y tratándose de un entorno de guerra convencional en la que el bando propio cuenta con superioridad (no se realiza un ataque cuando no se cuenta con superioridad), está previsto proceder a la destrucción física de los medios enemigos. Los principales medios que deben destruirse son los que más pueden oponerse a nuestro ejército de drones. Se trataría principalmente de medios de Guerra Electrónica (CEMA)¹¹³. La única condición autoimpuesta es que ningún humano entre (ni se acerque a menos de 10 km.) en la zona del combate definida. Para realizar las destrucciones se situarían a la distancia oportuna las unidades de artillería de largo alcance¹¹⁴ o de lanzacohetes¹¹⁵. Estas unidades sólo necesitarían la coordenada a batir, el tipo de objetivo (para adecuar la munición) así como una evaluación de daños posterior (para corregir el tiro, repetirlo o detenerlo). El resto de las destrucciones serían provocadas por los propios drones. Pueden utilizarse desde drones “suicidas” (que llevan adosada la carga explosiva) o, por ejemplo, drones lanzadores de bombas de tipo *Paveway* o misiles AGM-114 *Hellfire*, ambos con versiones guiadas por designadores laser. Estos designadores laser podrían estar instalados en el mismo dron que los lanza o en otro diferente.

No se va a extender más este punto ya que no entra directamente en las asignaturas del Máster, pero se trata de tener presente que para que el ejército de drones fuera efectivo debe de estar equipado y respaldado por los medios militares tradicionales que deberían desplegar en zona próxima a la operación, pero a salvo de ataques enemigos.

4.2 Desarrollo cronológico de la operación

4.2.1 Punto de partida

Para el inicio de la operación será necesario ubicar los drones aéreos en sus pistas de despegue, los drones terrestres ante la zona de la operación, y ubicar todas las instalaciones del área humana en su lugar. Se procederá a la carga en los drones de las distintas claves, combustible, programaciones y munición. Todo esto, que dicho así parece sencillo, conlleva una complejidad logística mayor, si cabe, que si de una operación humana equivalente se tratara. Para el desarrollo de toda esta operación previa sería necesario, a su vez, utilizar sistemas de comunicación. Si se emplearán algunos de los sistemas descritos hasta ahora, antes del comienzo de la operación de ataque, sería imprescindible el cambio de claves previo.

4.2.2 Oleada de señuelos

Como primera acción se lanzaría, en los 40 km de frente, un grupo de drones señuelo (la mayoría aéreos). Además de internarse en la zona de la operación se lanzarían varios en zonas alejadas de la misma para no delatar precisamente la zona del ataque. En ese punto los sistemas de localización de emisiones enemigas descritos trabajarían en toda su plenitud, así como los medios de destrucción. Una vez se viera el silencio de emisiones enemigas se pasaría a las siguientes fases del ataque. Si el enemigo reactivara las emisiones se volvería a la fase de “señuelos – localización de emisiones enemigas – destrucción sistemática”.

¹¹³ *Cyber and Electro Magnetic Activities*, este concepto incluye tanto la EW (*Electronic Warfare*, Guerra Electrónica propiamente dicha), como los ciberataques.

¹¹⁴ Que podrían utilizar municiones M712 Copperhead, guiadas por láser.

¹¹⁵ O lanzamisiles, por ejemplo, el MGM-140 ATACMS (*Army Tactical Missile System*) tiene un alcance de 300 km.

4.2.3 Despliegue de drones de comunicaciones

El sistema mallado de comunicaciones TCP/IP a través de WiMAX estará formado por drones terrestres que contarán también con terminal satélite (sistema SOTM) y antenas elevadas para radioenlaces. Cada uno de estos drones hará la función de Estación Base para los drones de su zona / célula. Cada dron avanzará por un itinerario y será seguido por los drones necesarios para no perder la LoS (línea visual) con el anterior y posterior. Si el terreno lo permitiera se procuraría mantener el radioenlace con los seis “vecinos” de célula, para ello, cada uno de estos drones contará con seis antenas. El sistema podría funcionar sin radioenlaces pero en ese caso el satélite (con un ancho de banda limitado) podría no ser capaz de atender la demanda de todas estas estaciones. El número de estaciones deberá ser tal, que además de cubrir los enlaces con línea visual (cuanto más accidentado sea el terreno, más drones Estación Base serán necesarios), tendrá que ser capaz de atender a todos los drones usuarios de su célula.

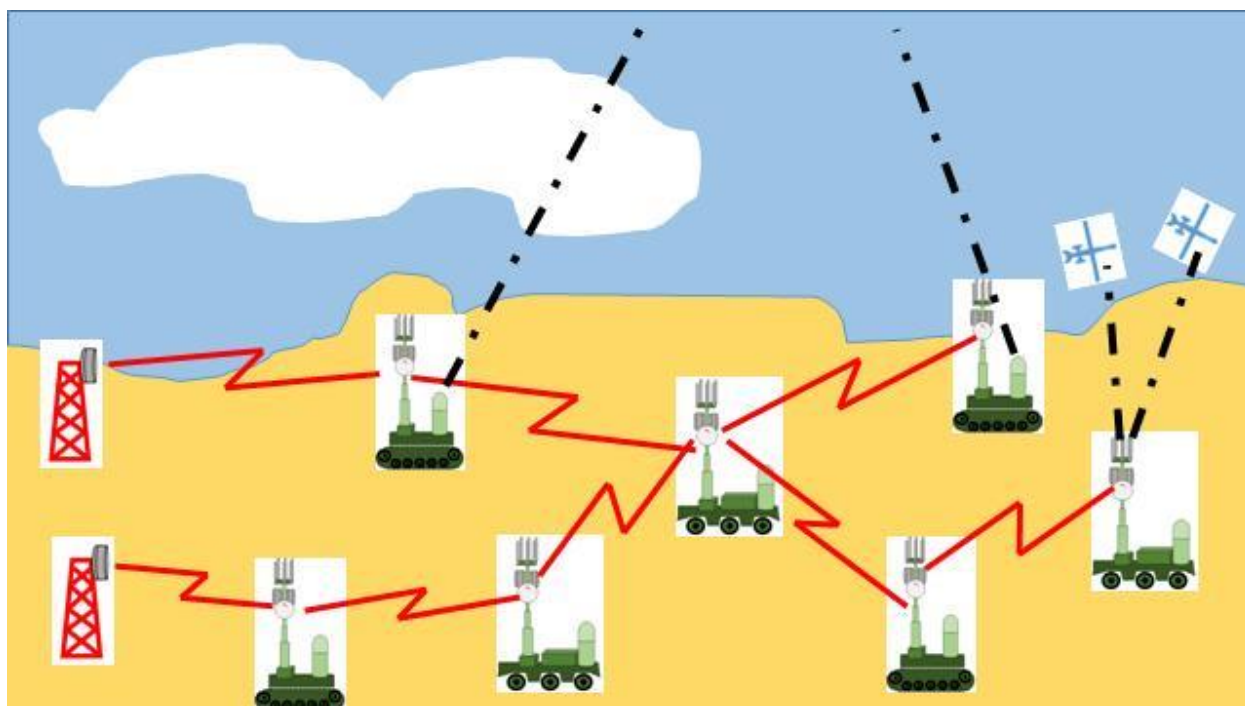


Figura 4-1: Recreación de red de comunicaciones que se va desplegando a medida que avanzan los drones.

4.2.4 Avance de drones de movilidad

La misión de este tipo de drones es facilitar la movilidad del resto de los drones terrestres. Se trata de drones “lanzapunto” con la utilidad de que otros drones terrestres puedan salvar pequeños ríos o zanjas. También drones de destrucción de obstáculos (como *erizos checos* o alambradas), o también para limpiar campos de minas. Este tipo de operaciones de “apertura de brecha” son las que más vidas humanas suelen costar, por tanto este tipo de drones, una vez diseñados y contruidos, participarían asiduamente también en operaciones “mixtas” en combinación con soldados en otros escenarios. No se ha hablado de ellos en el apartado sobre “funcionalidades” ya que su tecnología militar para la destrucción de obstáculos no se incluye en las asignaturas del Máster.

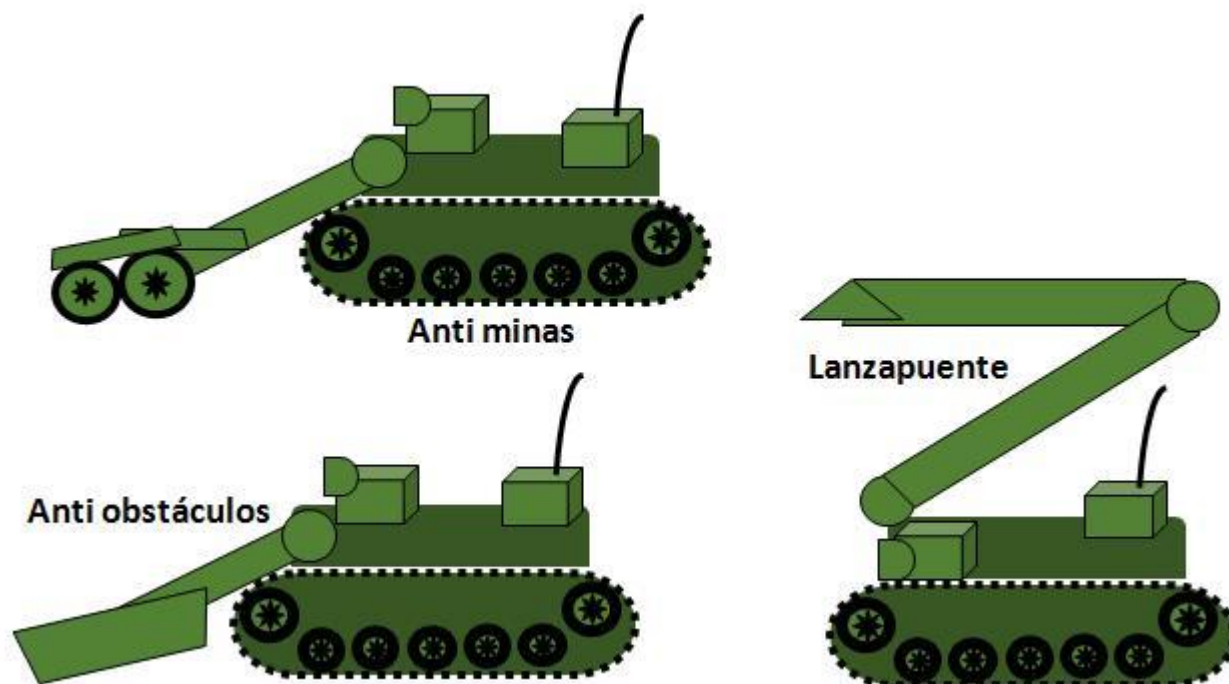


Figura 4-2: Recreación de drones para facilitar la movilidad.

4.2.5 Avance masivo de drones terrestres y aéreos

Desde el puesto de mando se darán las órdenes generales a la zona de conducción de manera que los distintos capitanes darán a su vez las órdenes de detalle a los pilotos de drones bajo sus órdenes. La coordinación será especialmente importante en esta fase por la dificultad que conlleva la cantidad masiva de drones utilizada. El orden de avance de los drones con distintas funcionalidades será fundamental (señuelos, ISR, movilidad, ataque, comunicaciones...). Los drones deberán tener una correcta distribución en los espacios del campo de batalla. Además de por los mismos motivos tácticos que tendría un ejército humano, hay que tener en cuenta que una densidad muy alta de drones por cada célula, podría sobrecargar el tráfico de la misma (de igual modo que un grupo de humanos demasiado numeroso que se concentra en un punto, puede provocar problemas con la telefonía móvil).

5 CONCLUSIONES FINALES

5.1 Cumplimiento de objetivos y conclusiones

Con respecto al objetivo de:

El alumno pretende buscar la originalidad diseñando métodos novedosos que se integrarían con tecnologías ya existentes.

Se ha de reconocer que ha tenido que adaptarse a medida que el trabajo ha ido avanzando. Al comienzo del trabajo se buscaba aportar soluciones creativas para solventar determinados problemas. Algunos de estos problemas eran el alargamiento de la distancia de comunicaciones, saturación por concentración de drones, supervivencia y seguridad en las comunicaciones o supervivencia ante perturbaciones intencionadas en los sistemas GNSS.

Una vez que se buscaron soluciones a estos problemas, se constató que algunas tecnologías ya existentes solventaban de forma satisfactoria estos problemas. Estas tecnologías eran WiMAX, DTN, TACAN, DME o NDB.

Se ha preferido mantener el objetivo en su lugar original, para demostrar la importancia de la flexibilidad a la hora de adaptarse a circunstancias no previstas, en este caso, la utilización del sentido común al no tratar de “inventar” algo que “ya estaba inventado”.

De hecho, al hilo del comentario anterior, el autor del presente trabajo defiende que todas las tecnologías individuales y concretas para llevar a cabo este proyecto, están perfectamente en uso y han superado con creces las fases de investigación y desarrollo. Lo que queda pendiente es el trabajo de integración de todas ellas para llevar a cabo este proyecto.

La integración de estas tecnologías ha sido descrita en este trabajo de forma muy somera y a muy alto nivel. Si se pretendiera llevar a la práctica este proyecto se prevé que la complejidad crecería conforme se bajara de nivel y se produjera el acercamiento a lo tangible.

La información en fuentes abiertas sobre este ejército de drones es nula, pudiendo deberse esto a que ningún país está dedicando recursos a esta integración y empleo masivo, o bien a que sí lo están haciendo, pero los resultados están cubiertos y etiquetados como materias clasificadas (que sería lo lógico en este caso). Debido a esto no se ha podido completar la situación actual del estado del arte a este respecto.



Figura 5-1 Fotograma de la película “Terminator 3” donde se muestra un particular “ejército de máquinas”¹¹⁶.

¹¹⁶<https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Articulos-Selectos-de-Nuestra-Coleccion/2019/La-subelevacion-de-las-maquinas/>

6 LÍNEAS FUTURAS

6.1 Líneas Futuras

Una vez dicho que todas las tecnologías a aplicar tienen actualmente superada la fase de investigación y desarrollo, el siguiente paso sería la materialización de los prototipos de los diferentes drones. Tras probar individualmente cada uno, y asegurarse del correcto desempeño, tanto de su movilidad, como de la funcionalidad respectiva, se deberá pasar a la siguiente fase.

Esta es la fase más delicada, pues se trata de hacer funcionar simultáneamente una gran cantidad de drones cuyo único nexo de unión con la zona humana sería el espectro electromagnético. El volumen principal de la información dentro de la zona humana, discurriría por una red de fibra óptica, sin embargo, el reto está en evitar las interferencias en el espectro electromagnético en la zona de combate, que podrían provenir, tanto de perturbaciones intencionadas del enemigo, como de interferencias por la saturación de emisiones propias.

Para ello se utilizarían las tecnologías de WiMAX y DTN, la primera para recibir el video y dar las órdenes que permitan la conducción en tiempo real de los drones y la segunda para recibir información de los diferentes sensores y transmitir aquellas órdenes y datos que por su naturaleza puedan tolerar un cierto retardo.

Se ha dicho que las tecnologías a utilizar ya están desarrolladas, sin embargo la mayoría de ellas tendrían que sufrir adaptaciones ad hoc que permitieran, mediante soluciones propietarias, cumplir con los requerimientos específicos que primarán por encima de todo la integridad, confidencialidad y disponibilidad en tiempo útil de todos los intercambios de información.

7 BIBLIOGRAFÍA

- [01] M. Cirovic, Michael (1979) “Electrónica Fundamental: Dispositivos, Circuitos y Sistemas”. Editorial Reverte, S.A.
- [02] Huang, Hui-Min (2007/2008) *Autonomy Levels for Unmanned Systems (ALFUS) Framework. National Institute of Standards and Technology. Volumen I: Terminology / Volumen II: Framework Models.*
- [03] Blake, M. Brian (2003) *Coordinating multiple agents for workflow-oriented process orchestration. Information Systems and e-Business Management Springer-Verlag*¹¹⁷.
- [04] VVAA (2016) Normas de la Autoridad Nacional para la Protección de la Información Clasificada. Ministerio de la Presidencia.
- [05] McCoy, James and B. Rawat, Danda (2019) *Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey.* En Electronics 2019, 8, 1468.
- [06] Briceño Márquez, José E. (2005) *Transmisión de Datos.* Departamento de Electrónica y Comunicaciones de la Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Los Andes. Mérida (Venezuela).
- [07] AHMADI SASSAN (2011) “Mobile WiMAX: A Systems Approach to Understanding IEEE 802.16m Radio Access Technology”. Elsevier. Burlington (MA, USA).
- [08] Documentos de WiMAX Forum¹¹⁸:
- Release 3: WMF-T23-001-R030v02_MSP (actualización R021v02 de 20 mayo 2021).
 - Release 2: Mobile Radio Conformance Tests: WMF-T25-002-R020v01 (03/08/2012)
 - Release 2: Mobile Inter Operability Test: WMF-T25-003-R020v01 (03/08/2012)
- [09] VVAA (2009) “Delay-/Disruption-Tolerant Networking: State of the Art and Future Challenges”. Surrey, UK. Center for Communication Systems Research (CCSR).
- [10] VVAA (2012) Delay Tolerant Networks: Protocols and Applications, Boca Ratón, USA. CRC Press Tylor & Francis Group, LLC.
- [11] Voyiatzis, Artemios G. (2012) “A Survey of Delay- and Disruption-Tolerant Networking Applications”. En Journal of Internet Engineering, Vol. 5, No. 1
- [12] VVAA (2008) *Global Positioning System Wide Area Augmentation System (WAAS) Performance Standard.* 1th Edition. Department of Transportation (USA).
- [13] VVAA (2008), *Global Positioning System Standard Positioning Service Performance Standard.* 4th Edition. Department of Defense (USA).
- [14] VVAA, (2016) *Manuals Combined U.S. Navy ELECTRONICS TECHNICIAN, VOLUMES 01 – 08.* Center for Surface Combat Systems.

¹¹⁷ Consultado 19/10/2021 en:

https://web.archive.org/web/20060901073108/http://www.cs.georgetown.edu/~blakeb/pubs/blake_ISEB2003.pdf

¹¹⁸ <https://wimaxforum.org/home>

- [15] VVAA (2013) *Navegación en condiciones de denegación de señal GNSS*. En N° 13 Monografías del SOPT (Sistema de Observación y Prospectiva Tecnológica). Secretaría General Técnica del Ministerio de Defensa.
- [16] Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias. Ministerio de Energía, Turismo y Agenda Digital. BOE 259 (27/10/2017)
- [17] Torres Portero, Felipe Ariel (2015) *Estudio de WiMAX2 (IEEE 802.16m) y la factibilidad de implementación en el Ecuador*. Facultad de Ingeniería de Quito.
- [18] VVAA (2013)¹¹⁹ Performance and Capacity Evaluation for Mobile WiMAX IEEE 802.16m Standard. En Wireless and Mobile Technologies¹²⁰.
- [19] Cole, C. (2014) *Rise of the Reapers: A brief history of drones*¹²¹.
- [20] Haulman, D. (2003) *U.S. Unmanned Aerial Vehicles in Combat, 1991-2003*¹²².

¹¹⁹ Hala B. Nafea, Fayez W. Zaki y Hossam E. Moustafa

¹²⁰ Science and Education Publishing: <http://pubs.sciepub.com/wmt/1/1/3>

¹²¹ <https://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones>

¹²² <http://www.dtic.mil/dtic/tr/fulltext/u2/a434033.pdf>

ANEXO I: ASIGNATURAS DEL MÁSTER RELACIONADAS

El presente trabajo tiene relación directa con la siguiente asignatura del Máster:

TEL 3. “Sistemas de comunicaciones vía satélite, de posicionamiento, teledetección y radionavegación”.

En dicha asignatura se encuadran los temas:

Tema 1: Comunicación vía satélite.

Tema 2: Sistemas de radionavegación.

Tema 3: Sistemas de posicionamiento.

Tema 4: Sistemas de teledetección.

Tema 5: Sistemas de aplicación al ámbito militar.

Todos ellos han sido tratados (en mayor o menor medida) en este trabajo. Por otro lado se ha tocado partes de los temarios de las siguientes asignaturas:

TEL 1. “Sistemas de comunicaciones ópticos e inalámbricos”.

TEL 2. “Redes de banda ancha”.

COM 6 “Transformación digital e innovación”.

Y también (aunque algo menos):

COM 8. “Redes y sistemas de telecomunicación”.

COM 9. “Sistemas de información”.

COM 10. “Seguridad de la información”.

COM 11. “Gestión de la seguridad y análisis de riesgos”.

TEL 4. “Seguridad en sistemas de telecomunicaciones”.

Se ha utilizado también como bibliografía de consulta todos los apuntes de las mencionadas.