PERTURBACIÓN DE SATÉLITES DE COMUNICACIONES

Por Luis Izquierdo Echevarría
y Fernando Davara Rodríguez

Introducción

En los últimos años los satélites de comunicaciones han mejorado sensiblemente el campo de las transmisiones, al aportar flexibilidad, rapidez y seguridad en el enlace. Pero estos conceptos, que son importantes en lo que respecta a las comunicaciones civiles, deben ampliarse cuando se traspasan estos límites y se penetra en el campo de los sistemas de transmisiones militares, por medio de satélites, en el que ya muchos países, y España entre ellos, han hecho acto de presencia.

Este tipo de comunicaciones militares, prácticamente como el resto de ellas, debe responder a unos requisitos que añaden a los propios de cualquier sistema civil —calidad, capacidad...— conceptos tales como seguridad, interoperabilidad y supervivencia. Es tal el consenso en la adopción de requisitos como éstos que se ha generalizado el esquema de valoración de una red de transmisión militar por medio de satélites, a partir de estos factores o criterios: fiabilidad, rapidez, interoperabilidad, seguridad y supervivencia.

Por el primero se garantiza el buen funcionamiento del enlace y la buena recepción de la información por parte del destinatario. Impone la redundancia en los enlaces como medio de paliar los fallos técnicos, de carácter aleatorio, que puedan aparecer en el funcionamiento de la red.

El segundo, rapidez, se traduce en una búsqueda permanente de la solución al problema de cómo hacer frente al flujo constante y creciente de información a transmitir, con unos medios humanos en relativa pero también creciente disminución, manteniendo en todo momento la fiabilidad y rapidez de la transmisión. La respuesta pasa evidentemente por la informática y, claro está, por estos sistemas espaciales.

La interoperabilidad o posibilidad de facilitar la conexión con hombres o máquinas que sirvan a otros sistemas de comunicación, es necesaria en las comunicaciones militares modernas ante la diversificación de los medios propios y de los posibles aliados (comunicaciones tácticas, estratégicas, redes públicas, etc.).

La seguridad, referida a las telecomunicaciones, es necesaria para evitar que otros accedan a las informaciones que transitan por nuestras redes de transmisión (conversaciones, mensajes o datos), o que conozcan nuestros sistemas a través de nuestro nivel y direcciones de tráfico entre equipos.

Finalmente la supervivencia, es decir, la habilidad para asegurar un funcionamiento satisfactorio ante cualquier amenaza, en paz, crisis o guerra.

La creciente generalización en el uso de los sistemas militares de comunicaciones por satélite ha incrementado la importancia de los dos últimos conceptos —seguridad y supervivencia— al aparecer dichos sistemas como posibles objetivos de todo tipo de acciones que busquen su destrucción, neutralización o pérdida de operatividad.

Además, al integrarse en los sistemas nacionales y de alianzas C2 y C3, o bien al depender directamente de ellos, la supervivencia de estos últimos está fuertemente supeditada a la de los primeros, de aquí que se extienda la preocupación por conocer cuál puede ser la amenaza que afecte a estos sistemas espaciales.

Esta preocupación, que en su origen fue exclusivamente militar; hoy en día se contempla también en el ámbito civil, donde el enemigo puede cambiar su nombre, que no su aspecto, por el de adversario comercial o competencia. En este caso, el más importante de los dos conceptos es el de seguridad, necesidad que ha comenzado a expandirse de forma considerable en el mundo de las telecomunicaciones civiles, a causa principalmente, del desarrollo de la telemática y de la naturaleza cada día más mercantil de la información, con las tentaciones y peligros que ello supone.

Desde un punto de vista exclusivamente militar estos dos conceptos pueden contemplarse como las dos grandes vulnerabilidades de las redes de

telecomunicaciones por satélite, que, en resumen, se traducen en la vulnerabilidad física del sistema y en la de la señal. Para poder hacer frente a ellas y defenderse de las posibles amenazas que pretendan aprovecharse de semejantes vulnerabilidades, es preciso conocer cuáles pueden ser las acciones o perturbaciones y así estudiar y poner en práctica las pertinentes medidas preventivas o correctivas que aseguren la continuidad del servicio.

Arquitectura del sistema: segmentos espacial y terreno

Cualquier sistema de comunicaciones por satélite se compone básicamente de un segmento espacial y un segmento terreno.

Segmento especial

Integrado por el satélite, o satélites, en órbita, así como por los centros terrenos que efectúan misiones de telemedida, telemando, seguimiento y apoyo logístico de las plataformas.

En cada satélite debe distinguirse la carga útil, o módulo de comunicaciones, y la plataforma o módulo de servicio.

El módulo de comunicaciones incluye los elementos necesarios para que el satélite actúe como un repetidor de comunicaciones. Estos elementos son principalmente las antenas y los transpondedores, cada uno de los cuales tiene sus correspondientes cadenas receptora y transmisora, de forma que puede funcionar con independencia de los demás transpondedores.

El módulo de servicio incluye los siguientes subsistemas:

— Subsistema de potencia, que genera y distribuye la energía eléctrica necesaria a bordo. Incluye los grandes paneles de células solares y también las baterías necesarias para que el satélite pueda seguir funcionando durante los períodos de eclipse.
— Subsistema de seguimiento, telemedida y telemando, para que en tierra puedan calcularse la posición del satélite en el Espacio, el estado de funcionamiento de los equipos a bordo y para que el satélite ejecute las órdenes que se le envían desde tierra.
— Subsistema de propulsión, formado por el motor de apogeo —que permite pasar de la órbita de transferencia a la geoestacionaria— y los pequeños motores necesarios para llevar al satélite a su posición correcta en el Espacio y mantenerla en ella, corrigiendo los efectos perturbadores de tipo natural que tienden a desplazar el satélite de esa posición.

— Subsistema de control de la orientación o asiento del satélite, para que dicha orientación en el Espacio sea siempre la exacta y las antenas apunten y den servicio a las zonas deseadas. Este subsistema incluye los sensores que detectan si la orientación del satélite en cada momento es o no la correcta y los pequeños motores que corrigen automáticamente las desviaciones que se puedan producir.
— Subsistema de control térmico, que se encarga de que la temperatura de cada equipo esté siempre dentro de unos límites preestablecidos. Sin control térmico podrían alcanzarse temperaturas tan altas como 250 °C o tan bajas como —150 °C.

Los centros de tierra de la componente espacial realizan las operaciones de seguimiento del satélite, de telemando y control, de telemedida de las funciones a bordo y la supervisión de las comunicaciones para garantizar el buen funcionamiento de la red. En algunos casos realizan también funciones de control de la asignación, sincronización, etc.

Estos centros terrestres del segmento espacial son, básicamente, una estación de seguimiento, telemedida y telemando, llamada abreviadamente estación TTC y un centro de control del satélite, que puede situarse junto a la estación TTC o separado de ella.

Segmento terreno

Abarca toda la parte del sistema de comunicaciones constituida por las estaciones en tierra, tanto de transmisión a los satélites como de recepción de los diferentes tipos de señales que éstos transmiten, estaciones que constituyen la conexión con las redes de comunicaciones terrestres.

Están compuestas generalmente de una antena transmisora y receptora, un transmisor, un receptor y unos equipos de modulación, demodulación y transposición de frecuencias.

A caballo entre el segmento espacial y el terrestre se encuentran los enlaces ascendentes y descendentes que aseguran el tráfico de señales de todo tipo y que, como se expondrá posteriormente, son uno de los objetos prioritarios de perturbación.

Órbitas y frecuencias

Para poder estudiar las posibles vulnerabilidades es preciso hacer mención de dos aspectos muy concretos, dentro de estos sistemas espaciales de comunicaciones, tales como las órbitas a utilizar y la parte del espectro

electromagnético más comúnmente usado en este tipo de comunicaciones por satélite, es decir, las bandas de frecuencia.

En la mayor parte de los casos, estos satélites se sitúan en las llamadas órbitas geoestacionarias, que no son más que un caso particular, de las geosíncronas, es decir, aquellas en las que el satélite orbita con igual dirección y velocidad angular que las de la Tierra, por lo que el período orbital es un día sideral (23 horas y 56 minutos).

En este caso particular de las geoestacionarias se sitúa el satélite en una órbita circular con inclinación nula con respecto al Ecuador terrestre y a una altitud de 36.000 km, lo que da como resultado que permanezca inmóvil, con velocidad relativa cero, con respecto a la referencia que es la superficie de la Tierra. Esta característica permite que el satélite proporcione cobertura permanente a una zona determinada, a la vez que simplifica el diseño de las estaciones de tierra al no tener que efectuar seguimientos de satélites en movimiento con velocidades angulares grandes.

Aquí ya aparece un posible objeto de perturbación dado que esta órbita circular es única, por lo que los satélites que la ocupan pueden provocar interferencias entre sí. Cuando los usuarios son civiles la solución se basa en la distribución de esta órbita según una normativa de la ITU (*International Telecomunications Union*), pero en el caso de los sistemas militares la interferencia no sólo puede ser accidental, sino también provocada.

Entre los satélites militares utilizados actualmente se utilizan también otros tipos de órbitas: bajas —tipo MOLNIYA— y geosincrónicas, no estacionarias.

Los sistemas soviéticos sitúan satélites en órbitas bajas para poder operar con equipos de baja potencia o bien en órbitas tipo MOLNIYA con grupos de satélites para conseguir cobertura permanente.

Las órbitas no circulares describen elipses que se caracterizan por su apogeo, o punto de mayor altitud, y su perigeo, o punto de menor altitud. Las MOLNIYA son de esta clase con un apogeo de 40.000 km y un perigeo de 500, con un período de doce horas, una inclinación con respecto al Ecuador de 63° y velocidades variables según el punto de la elipse (bajas en el apogeo y altas en el perigeo). Todo ello permite orbitar a gran altura sobre el hemisferio Norte, facilitando las comunicaciones de los sistemas soviéticos de mando y control, a la vez que se cubre una cara de la Tierra en unas once horas.

Los sistemas de los Estados Unidos son generalmente geoestacionarios, pero en su nuevo desarrollo MILSTAR parte de sus satélites se sitúan en

órbitas con fuerte inclinación con respecto al Ecuador para garantizar una cobertura global.

Al necesitarse grandes capacidades y por tanto grandes anchos de banda, las frecuencias deben ser altas (centimétricas por lo general), cuadro 1.

Cuadro 1.—*Anchos de banda.*

Banda	*Ascendente*	*Descendente*
C (6/4 GHz)	5,925 a 6,425 GHz (500 MHz)	3,700 a 4,200 GHz (500 MHz)
X (8/7 GHz)	7,925 a 8,425 GHz (500 MHz)	7,25 a 7,75 GHz (500 MHz)
Km (13/11 GHz)	12,75 a 13,25 GHz (500 MHz)	10,70 a 11,70 GHz (500 MHz)
Km (14/11 GHz)	14,000 a 14,500 GHz (500 MHz)	10,950 a 11,200 GHz 11,450 a 11,700 GHz (500 MHz)
Km (14/12 GHz)	14,000 a 14,500 GHz (500 MHz)	11,700 a 12,200 GHz (750 MHz)
Km (30/20 GHz)	27,500 a 31,00 GHz (3.500 MHz)	17,700 a 21,200 GHz (3.500 MHz)

El empleo de estas altas frecuencias se justifica también por la menor dimensión de las antenas, disminución de la influencia de las perturbaciones de la ionosfera y, muy importante en este caso, la mayor facilidad para protegerse de las interferencias del adversario.

Tipos de perturbación posible

Definición

Se entiende por perturbación de un satélite de telecomunicaciones a cualquier acción, inteligente o no, que impida o dificulte las comunicaciones normalmente establecidas a través de este satélite.

Tipos de perturbación

De acuerdo con la anterior definición se podrían establecer clasificaciones muy variadas, pero en cualquiera de ellas habrá de contemplarse que las agresiones a un sistema de este tipo siempre serán debidas a una de estas causas: agresión inteligente y agresión no inteligente (por ejemplo, fenómenos naturales).

Entre las primeras destacan:

— Perturbación electromagnética para impedir o dificultar el uso del espectro.
— Decepción.
— Escucha de la señal por parte del adversario.
— Destrucción física de los equipos y medios de transmisión.
— Destrucción lógica (electromagnética) del *software* y/o *hardware*.
— Ataque físico a una estación o parte del sistema.
— Ataque electromagnético a estación o parte del sistema.

Entre los segundos tenemos:

— Perturbación electromagnética, como por ejemplo descargas eléctricas, perturbaciones atmosféricas.
— Deficiente propagación atmosférica.
— Meteorología adversa.
— Degradación ambiental de los componentes físicos del sistema.

Puntos vulnerables en un sistema de comunicaciones vía satélite

Las diferentes acciones que pueden llevarse a cabo o afectar a un sistema de telecomunicaciones por satélite deberán hacerlo sobre alguno de sus componentes anteriormente especificados. Así se pueden diferenciar las siguientes:

a) Acciones sobre el satélite.
b) Acciones sobre las estaciones tierra de control y explotación.
c) Acciones sobre los enlaces entre el satélite y tierra.

Acciones sobre el satélite

Las principales formas de actuar sobre el satélite son las armas antisatélite, las armas de energía dirigida, con base en la Tierra o el Espacio, y los efectos de las armas nucleares, próximas o lejanas.

Las armas antisatélites tal y como se conciben actualmente sólo pueden actuar sobre los satélites en órbitas bajas, por lo que puede desecharse su utilización sobre este tipo de sistemas. Pero dado que la evolución de la técnica es cada vez más rápida y ante la importancia creciente de las telecomunicaciones espaciales, no se descarta que en un futuro muy próximo este tipo de armas se encuentre al alcance al menos de las grandes potencias.

El sistema que los Estados Unidos está desarrollando en la actualidad contempla el ataque al satélite por medio de proyectiles que incidan

directamente en él o por medio de los fragmentos proyectados por explosiones convencionales o nucleares realizadas en sus proximidades.

También pueden utilizarse armas de energía dirigida que producen en el satélite efectos de destrucción o neutralización. Entre ellas destacan los haces de partículas neutras, los láser y las emisiones de microondas de gran potencia.

Estas armas de energía dirigida (no nucleares), utilizan un haz de energía muy intenso y de pequeña divergencia que se dirige con precisión hacia el blanco. Dicho haz puede estar constituido por partículas atómicas que se propagan a velocidad próxima a la de la luz (caso del haz de partículas neutras), por fotones (caso del láser) o por radiaciones de RF de alta potencia (caso del haz de microondas de gran potencia).

Respecto al primero (partículas neutras) de los dos tipos de partículas que pueden actuar sobre un satélite, electrones o neutras (hidrógeno o deuterio) sólo las segundas pueden actuar con eficacia, dado que los electrones sufrirían el efecto de repulsión de las fuerzas electroestáticas y el haz sería divergente. Además deberían abrirse camino hacia el blanco hasta distancias muy considerables, por lo que, en este tipo de sistemas de telecomunicación espacial, los estudios sobre ellos prácticamente se han abandonado.

Al contrario las partículas sin carga pueden actuar eficazmente contra los satélites. Basándose en la técnica de los aceleradores de partículas, un haz de iones negativos (deuterones y protones) se acelera, posteriormente se neutraliza y se envía hacia el satélite, donde penetran profundamente.

Por ejemplo, utilizando protones en un haz de 400 MeV se consiguen penetraciones de más de 40 cm en aluminio, lo que supone para el satélite protecciones tan grandes que, por cuestión de peso, no pueden transportar.

En lo que respecta a los láser, éstos presentan unas propiedades que los hacen muy útiles a la hora de atacar a los satélites. Algunas de ellas son su propagación a la velocidad de la luz, la pequeña divergencia del haz o la posibilidad de ser reflejados en espejos adaptados a su longitud de onda. Todas ellas hacen posible la concentración de energía a gran distancia en tiempos muy pequeños, por lo que se les considera una de las armas de energía dirigida de mayor eficacia contra satélites de comunicaciones.

Finalmente, en lo que respecta a las armas del tipo haz de microondas de gran potencia, en la actualidad se las sitúa en el apartado de las armas de interferencia, pero los desarrollos actuales pueden conducirnos a fuentes de

muy alta energía que causen daños permanentes a los equipos electrónicos de los satélites, en nuestro caso principalmente a los receptores.

El arma nuclear, de difícil utilización, por los efectos políticos que conlleva, produce sobre el sistema dos tipos de efectos, debido ambos a la dispersión de rayos gamma y consiguiente retroceso de electrones tras la explosión nuclear (efecto Compton). El primero, a la altura del satélite, es de la forma de un impulso electromagnético de muy corta duración y de gran radio de acción, que puede neutralizar el satélite a miles de kilómetros de distancia, incluso en zonas donde no llegan el resto de los efectos de la explosión.

El segundo, producido al interaccionar los rayos gamma con la atmósfera, genera un campo eléctrico radial que afecta principalmente a los equipos de comunicaciones e instalaciones de superficie.

Acciones sobre las estaciones terrestres

Las estaciones en tierra de estos sistemas, tanto las del sector espacial como las del terreno, constituyen, como todos los puntos sensibles militares, objetivos para actos de sabotaje, acciones terroristas o, en caso de conflicto o crisis grave, de agresiones convencionales o nucleares. La forma de destruirlas o neutralizarlas puede ser por medio de ataques directos, indirectos (por ejemplo, a las fuentes de potencia) o por acciones terroristas.

Otro tipo de acciones a llevar a cabo sobre los centros de tierra son aquellas que utilizando medios electromagnéticos, intentan la inutilización de los sistemas automáticos o no de mando y control, alterando su proceso normal de funcionamiento. Este punto, que hasta hace poco tiempo no se consideraba preocupante, dado que protegiendo el acceso al centro se aseguraba también contra estas acciones, está adquiriendo una importancia considerable ante la tendencia a la automatización que proporciona un camino de acceso de más difícil control.

Los posibles ataques por medio de esta clase de acciones pueden ser:

— Introducción de *software* o datos cuya apariencia física está de acuerdo con las normas, pero que provocan un mal funcionamiento e incluso un bloqueo, al saturar los sistemas, con la consiguiente falta de operatividad de parte o todo el equipo. Este tipo de acción es muy conocido actualmente a través de una de sus más sencillas versiones: «los virus».
— Alteración del proceso lógico sobre todos en los casos en que el equipo es crítico y con ello se afecta a la integridad del sistema (por ejemplo, los equipos de telemando).

— Destrucción total o parcial de los equipos por acciones físicas del tipo electromagnético dirigidas principalmente a aquellos componentes que se encargan de la protección del sistema.

Estas acciones dirigidas a los equipos adecuados, en especial los críticos, pueden llevar a una inutilización total del sistema sin riesgo alguno por parte del adversario.

También deben señalarse las acciones debidas a las explosiones nucleares, tanto en su aspecto mecánico (ondas de presión, choque, etc.) como en el electromagnético ya mencionado en el apartado dedicado al satélite.

Acciones sobre los enlaces satélite-tierra (enlaces descendentes)

Este tipo de interferencia ha sido siempre considerada como difícil de realizar y, por lo tanto, no se estima que sea una amenaza tan seria como la que actúa sobre los enlaces ascendentes. Los mejores efectos podrían conseguirse por medio de estaciones aerotransportadas por sus características de cubrir amplias zonas, movilidad y facilidad de despliegue.

Respecto a las acciones sobre los enlaces descendentes desde estaciones espaciales, sólo serían eficaces en el caso de situarse en la órbita geoestacionaria y próximas al satélite a interferir.

Existe un tipo de agresión que no aparece como tal, pero de la que es necesario protegerse por afectar directamente al concepto anteriormente expresado de seguridad. Esta intervención «pasiva» consiste en la escucha por parte del enemigo de nuestras informaciones y su utilización para conocer nuestras posibilidades y vulnerabilidades.

Acciones sobre los enlaces tierra-satélite (enlaces ascendentes)

Los enlaces radio eléctricos de tierra con el satélite han sido muy estudiados dadas sus ventajas con respecto a los descendentes, entre las que destaca la posibilidad de afectar simultáneamente a una variada gama de enlaces.

Estos enlaces pueden perturbarse por medio de interferencia o intrusión, acción que permitiría, por ejemplo, hacer aceptar al satélite una orden anormal. Otro tipo de agresión sería la interferencia de los enlaces de mando emitiendo desde tierra en la misma frecuencia, enviando órdenes de mando falseadas e incluso haciéndose cargo del control del satélite.

También puede actuarse sobre los enlaces de telecomunicación interfiriendo o enviando informaciones falsas. Para todo ello se necesitan estaciones capaces de radiar una cantidad importante de energía, lo que implica

grandes antenas y equipos muy voluminosos. Esto nos lleva a considerar que en este caso las verdaderamente eficaces son las estaciones terrestres en oposición a las aerotransportadas, que no pueden afectar en forma eficaz a estos satélites a altitudes muy grandes por las mencionadas razones de tamaño de antena y equipos.

No es éste el caso de las estaciones espaciales cuya pequeña potencia radiada puede aprovecharse eficazmente si se sitúan como en el caso anterior, en las proximidades del blanco, dentro de la órbita única geoestacionaria.

Acciones de protección

Ante este tipo de acciones de perturbación es necesario enfrentar otras de protección que eviten o aminoren los efectos de las primeras. Según la actitud que se tome a la hora de ponerlas en práctica, se pueden clasificar en acciones de protección pasivas, como por ejemplo la evasión, y activas, como la autodefensa.

Para evitar las acciones sobre el satélite se pueden hacer maniobras de evasión o bien utilizar técnicas de engaño de los autodirectores evidentemente específicos de los sistemas militares. El éxito de éstas depende de la capacidad de poner en evidencia un intento de agresión y del tiempo del que se dispone entre el momento de la detección de la agresión y el momento en el que se puede ser destruido.

El estudio de la vulnerabilidad de los satélites a los haces láser da lugar a un amplio espectro de contramedidas tales como la discrección, para evitar ser localizados, el engaño, para hacer desperdiciar el número limitado de disparos láser y las técnicas de blindaje posibles, aun limitando las características del satélite.

Respecto a las armas nucleares, la técnica de protección, conocida como endurecimiento, se ha desarrollado y se fabrica ya para muchas aplicaciones militares; en particular para los cohetes balísticos que deben ser capaces de despegar en ambiente nuclear y cuyas ojivas deben resistir una agresión nuclear directa.

La Unión Soviética ha previsto una forma de defenderse de todos estos tipos de agresiones, consistente en poner en órbita un elevado número de satélites, lo que unido a una suficiente capacidad de lanzamiento produce el efecto de permanencia del sistema, a pesar de la destrucción o inutilización de alguno de sus efectivos.

Las técnicas de protección contra las acciones intrusivas —filtrado de personas, control de accesos— necesitan un estudio muy detallado para asegurar, además de la seguridad de las instalaciones, la protección de las informaciones clasificadas y de los enlaces de mando. La búsqueda de una autonomía cada vez mayor en los satélites y el crecimiento de la robustez del sistema, por una prudente elección del número de estaciones y de su implantación deben permitir garantizar el cumplimiento de la misión a pesar de la pérdida provisional o definitiva de una parte de las estaciones terrestres.

Las técnicas de EW que se desarrollan para proteger los sistemas militares sirven para defenderse de las agresiones contra los enlaces. Así contra la escucha podemos utilizar las variadas técnicas de cifrado y contra el resto, emplearemos métodos como el salto de frecuencia, escalonamiento del espectro, cifrado de alta seguridad, firmas digitales en las señales ciertas, etc.

Otra de las protecciones a buscar es que en caso de pérdida temporal de enlace con el satélite, debe conseguirse una suficiente autonomía en las funciones vitales y operativas del satélite.