CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

MONOGRAFÍAS
del
CESEDEN

88

AVANCES EN TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES PARA LA SEGURIDAD Y LA DEFENSA

MINISTERIO DE DEFENSA

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

MONOGRAFÍAS
del
CESEDEN

88

AVANCES EN TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES PARA LA SEGURIDAD Y LA DEFENSA

Julio, 2006

AVANCES EN TECNOLOGÍAS DE LA INFORMACIÓN

Y DE LAS COMUNICACIONES PARA LA SEGURIDAD Y LA DEFENSA

INTRODUCCIÓN

INTRODUCCIÓN

Las Tecnologías de la Información y de las Comunicaciones (TIC) han traído enormes cambios en numerosos aspectos de la economía, la enseñanza, el arte, la política, etc., y, como no podía de otra manera, la seguridad y la defensa. En este campo nuestro de interés, debe observarse, sin embargo, que los potenciales enemigos pueden también beneficiarse, y se han beneficiado, del uso de las TIC.

En esta Monografía*, describimos algunos avances recientes en TIC de especial relevancia en el contexto de la seguridad y la defensa. Para ello, comenzamos describiendo el nuevo contexto global de seguridad y defensa, caracterizado, entre otros, por el fácil acceso a las TIC. Como consecuencia, se analizan algunos de los nuevos modelos de operaciones militares que están empezando a adaptarse y adoptarse a partir de los nuevos modelos de gestión de operaciones empresariales, dada la similitud del entorno nuevo y globalizado que deben enfrentarse tanto las empresas como los ejércitos. En efecto, éstos se caracterizan por su alta incertidumbre, la variedad de clientes a los que se deben enfrentar y la necesidad de responder de manera flexible a nuevas amenazas de índole muy variada. Se adoptan así conceptos como el de operaciones centradas en la red o el de logística de respuesta rápida.*

Después describimos aspectos más específicos de la aplicación de las TIC en la seguridad y la defensa. En tiempos normales de operaciones, resulta conveniente disponer de metodologías basadas en mejores prácticas para la gestión adecuada y eficiente de las TIC. El equipo ha puesto el énfasis en la metodología ITIL (Information Technology Infrastructure Library)*, introducida hace unos 20 años por el Gobierno británico, pero que está empezando a alcanzar niveles casi de estándar en la gestión de las TIC, y en su grado de conocimiento en los centros militares.*

Los tiempos de paz son también de entrenamiento para operaciones. El grupo ha puesto de manifiesto, de nuevo, la enorme relevancia de las TIC en esta tarea, a través de los entornos de simulación y realidad virtual, merced, fundamentalmente, a la mayor velocidad de cálculo y de comunicaciones y a los enormes desarrollos en visualización avanzada. Se pone, sin embargo, de manifiesto la gran heterogeneidad

de estos entornos y la necesidad de definir estándares en este importantísimo campo.

Finalmente, en tiempos de operaciones resulta esencial alcanzar rápidamente la superioridad informativa sobre el enemigo. Para ello, según hemos desarrollado, las nuevas redes ad hoc*, o redes* mesh *o polvo inteligente, pueden ser medios ideales para alcanzar esa ventaja informativa requerida en las primeras fases de las operaciones y facilitar después la consecución de los objetivos propuestos.*

Cubrimos, en definitiva, en esta monografía algunas de las tendencias más recientes y relevantes en TIC para la seguridad y la defensa, con la esperanza de que puedan resultar de interés para nuestros ejércitos.

CAPÍTULO PRIMERO

LOS NUEVOS MODELOS DE OPERACIONES DE SEGURIDAD Y DEFENSA

LOS NUEVOS MODELOS DE OPERACIONES

DE SEGURIDAD Y DEFENSA

Por David Ríos Insua

y José Antonio Valdivieso Dumont

Resumen

En este capítulo, se describe el nuevo contexto global de seguridad y defensa, por similitud con el nuevo contexto global empresarial. Surgen así nuevos modelos de gestión empresarial de respuesta rápida que se han empezado a adoptar en los ejércitos, a través, principalmente, de la logística de respuesta rápida (*sense and respond*) y las operaciones centradas en red orientadas, principalmente, a proporcionar ventaja en el campo de batalla a partir de la superioridad informativa y a apoyar las operaciones en tiempo real.

> *The information domain is the domain where information lives. It is the domain where information is created, manipulated and shared. It is the domain that facilitates the communication of information among warfighters. It is the domain where the command and control of modern military forces is communicated, where commander's intent is conveyed. Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. And, in the all-important battle for information superiority, the information domain is ground zero.*
>
> Office of Force Transformation, NCW Report to Congress.

La gestión de operaciones militares.

Un viaje de ida y vuelta del mundo militar al civil

Aunque, de forma dispersa, se producen antecedentes fundamentales, como la introducción del concepto de valor esperado por Pascal, el método de Newton para encontrar el mínimo de una función, la solución del problema de los puentes de Königsberg por Euler, la resolución de la paradoja de San Petersburgo por D. Bernoulli, la regla de Bayes, los diagramas de Gantt, el concepto de óptimo de Pareto o las cadenas de Markov, la investigación operativa, tal y como hoy la conocemos, no nace hasta la Segunda Guerra Mundial, en la que distintos equipos multidisciplinares se unen a planificadores militares en el Reino Unido (como la U.K. Naval Operational Research, con Lanchester, Blackett y Yates) y en Estados Unidos (con el U. S. Navy Antisubmarine Warfare Operations Research Group, y la U. S. Air Force Operations Research) para buscar formas de tomar mejores decisiones en áreas como logística, secuenciación de operaciones, etc. Proporciona, así, contribuciones esenciales para el triunfo aliado en el uso del radar, la determinación del tamaño óptimo de los convoyes, el despliegue de armamento en aviones, la guerra antisubmarino, los aspectos técnicos de la planificación estratégica, etc. Palmer, veáse Ríos (1953), llega a decir que *La investigación operativa era la mejor arma secreta de los ejércitos aliados.*

Tales éxitos fueron instrumentales para que, una vez acabada la guerra, las metodologías desarrolladas fuesen aplicadas en la Administración Civil y en la industria, con el consiguiente empuje definitivo de este campo, naciendo la Operations Research Society of America en 1952, la Sociedad de Estadística e Investigación Operativa en 1955, la aparición de Departamentos de Investigación Operativa en las universidades, su uso en las grandes consultoras de escala multinacional.

Por otro lado, tales éxitos también motivaron que los ejércitos siguiesen interesados y potenciasen sus actividades de investigación y gestión de operaciones, siempre atentos a los desarrollos del mundo civil. Así, en los últimos años, la globalización de la economía y el auge de las Tecnologías de la Información ha motivado que se hayan desarrollado estrategias de gestión empresarial más flexibles y tecnológicas, que están empezando a penetrar en el mundo militar, revolucionando la forma de acometer las operaciones de seguridad y defensa.

Es nuestro objetivo en este capítulo hacer una breve exposición sobre estos nuevos modelos de gestión de operaciones, poniendo el énfasis en los aspectos tecnológicos y no haciendo, prácticamente, referencia a los aspectos del cambio cultural que en los ejércitos podría conllevar su introducción. Así, tras una breve descripción de por qué han aparecido estos modelos en el epígrafe “La aparición de los nuevos modelos” P. 00, dedicamos dos apartados a los conceptos principales en este campo, a saber, la logística *sense and respond* y las operaciones centradas en la red. Después, en el epígrafe “Un ejemplo” P. 00 describimos brevemente algunos ejemplos de aplicación provenientes de la Operación Libertad Iraquí (OLI), para terminar con una breve discusión.

La aparición de los nuevos modelos

Hemos indicado ya cómo los modelos y conceptos de gestión de operaciones nacidos durante la Segunda Guerra Mundial dieron cuerpo doctrinal a la investigación operativa, que fue evolucionando desde el año 1950, a medida que se producían avances tecno-económicos. Llegamos, así, al final de los años ochenta en los que el paradigma predominante es el de *gestión por excepción*, véase por ejemplo. West y Harrison (1997), en el que se propone emplear un conjunto de modelos para hacer inferencia y predicciones, evaluar alternativas y tomar decisiones de forma estándar, a no ser que se produzca una excepción, en cuyo caso nuestro sistema de gestión debería estar abierto a intervenciones. Un entorno en el que se había producido el cambio de la planificación a largo plazo a la estrategia *just-in-time*, véase Sandras (1989) para una introducción. Se produce en ese periodo el auge y expansión de las Tecnologías de la Información, en general, y de Internet en particular.

Internet trae numerosos cambios socioeconómicos. Por un lado, facilita el acceso a la información, reduciendo, así, las asimetrías de información de la que se beneficiaban numerosas empresas. Un ejemplo claro es la caída de los precios de los seguros de vida, véase Levitt y Dubner (2005): en 1996 *quotesmith.com* pasa a ser el primer sitio *web* que permite a un cliente comparar, en pocos segundos, el precio del seguro de vida ofrecido por docenas de compañías. De esta manera, el proceso de encontrar el producto más barato, siendo las otras características del producto esencialmente idénticas, que hasta ese momento había sido tedioso,

resultaba ser ahora sencillo, con lo que las compañías más caras se vieron abocadas, necesariamente, a reducir sus precios. Se produce, también en parte como efecto de Internet, la globalización de mercados y la necesidad de atender a clientes cada vez más exigentes, de forma que tengamos prácticamente que adaptar nuestra cadena de suministro a las exigencias de cada cliente.

Un entorno, por tanto, con cambios difícilmente predecibles y discontinuos frente a los que, como primera reacción, numerosas grandes compañías se fragmentan en unidades más pequeñas, con mayor rapidez de respuesta. Sin embargo, al hacerlo se pierden las importantes ventajas de las economías de escala. Surge así, con Haeckel (1999), el nuevo paradigma de *empresa adaptativa*, véase también Desai (2005). Haeckel plantea cinco competencias básicas que debe poseer una empresa adaptativa:

1. *Conocer antes* (que tus competidores). Las ventajas de esta capacidad son bastante obvias, pues te permiten tomar la delantera sobre tus competidores y, así, gestionar tu negocio de manera más efectiva. Conocer implica percibir e interpretar, para lo cual debe recurrirse a las tecnologías más recientes. Esto incluye a la nanotecnología que permita a nuestras máquinas ser autoconectadas y automatizadas. Dos ejemplos serían los denominados Sistemas Micro-Electrónico-Mecánicos (MEMS), véase Gardner *et al* (2001), que integran elementos mecánicos, sensores, actuadores y electrónica en un sustrato común de silicio, y el polvo inteligente, descrito en el capítulo cuarto de esta *Monografía*, que consiste en microsensores que se autoconfiguran y comunican entre sí en una red ad hoc desplegada de forma aleatoria. También incluye los RFID´s (*Radio Frequency Identification Tags*), que pueden describirse como códigos de barra que actúan a distancia. Inicialmente se emplearon para control de inventario y movimientos, pero se están empleando ya para la gestión de micropagos y seguridad y defensa. Su uso será especialmente útil cuando se reduzca su costo y se combinen con Sistema de Posicionamiento Global (GPS) o Galileo. Finalmente, por lo que respecta a la interpretación de datos, resulta especialmente prometedor el empleo de herramientas de minería de datos, véase Giudici (2003), que integran herramientas estadísticas tradicionales, con herramientas de aprendizaje de máquina, véase Hastie *et al* (2003), para poder extraer información y hacer predicciones a partir de grandes masas de datos.

2. *Gestión mediante cable*. Puesto que la complejidad del entorno hace extremadamente complicada la gestión, se pasaría a la gestión de una representación informatizada de las organizaciones, esto es, a emplear un modelo que represente el comportamiento de toda la organización, conectado a todas las fuentes relevantes de información, que aporte memoria e inteligencia institucional para aumentar la capacidad del gestor para dirigir un negocio. Una tecnología especialmente útil es la logística autónoma, que permite predecir fallos en sistemas operativos, controlar niveles de inventarios en consumibles, informar automáticamente de fallos inminentes y solicita los pedidos sin intervención humana. También son útiles aquí los sistemas de diagnóstico remoto, posiblemente basados en las tecnologías descritas en el capítulo cuarto, fundamentalmente con el objeto de anticipar requisitos de mantenimiento y controlar equipamiento de alto valor, cualquiera que sea el lugar donde esté y en todo momento. Igualmente, aquí es fundamental la interconexión de los sistemas para promover la compartición de información. Un ejemplo sería imbuir a las herramientas de gestión de la cadena de suministro con, por un lado, agentes o sensores en nodos clave de la organización que alimenten al sistema integrado de gestión con la información necesaria y, por otro, con herramientas de inteligencia de negocio que permitan anticipar, más que reaccionar. Un ejemplo sería el Sistema *SAR Blue Enterprise* de IBM, véase Lin *et al* (2002).

3. *Diseñar una organización como un sistema*, con el objeto de que se adapte mejor a un entorno de difícil predicción y rápidamente cambiante. Implica integrar todas las funciones de la organización para crear un sistema optimizado, eficiente y coordinado que cree sinergias entre las mismas y, por tanto, se centre en las interacciones, más que en las acciones, definiendo bien el propósito último de la organización, al que debe estar orientado, en conjunto y de forma coherente, el propósito de cada una de sus unidades. Es también importante proporcionar un modelo en el que se pueda improvisar.

4. *Despliegue de capacidades en respuesta a las demandas de clientes.* Tal como se ha descrito, al diseñarse la organización como un sistema adaptativo, potencialmente cada nuevo cliente podría conllevar la reconfiguración de la organización. La responsabilidad se refiere ahora al cliente, con lo que el poder se desplaza de los proveedores a los clientes, de manera que los resultados se

revisan y renegocian con los clientes: el éxito se define en función de los efectos producidos sobre el cliente y se expresa en términos del incremento en satisfacción del cliente.

5. *Liderazgo aportador de contexto*. En esta situación, se daría a los empleados el propósito de su papel, sus principios de gobierno, sus principios de guía y un diseño estructural de roles y responsabilidad. Después, los líderes poblarían los roles principales con gente competente y confiarían en ellos para realizar las operaciones sin interferencias, de nuevo centrándose más en las interacciones que en las acciones a desarrollar. Se conseguiría así una descentralización hasta el mayor nivel de detalle posible.

Existen ya diversos conceptos relacionados disponibles como estrategias organizativas, como serían los de *Adaptive Enterprise de Hewlett Packard*, o *Business on Demand* o *Sense and Respond Value Net* de IBM, que, esencialmente, integran un modelo de gestión, un sistema de ayuda a la decisión en tiempo real, un sistema de gestión de riesgos y recursos, la optimización de la cadena de suministro y la automatización de los procesos de negocio, para monitorizar y analizar resultados del negocio y su entorno en tiempo real, alinear las operaciones con la estrategia y los requisitos del cliente, detectar sucesos proactivamente, aliarse con los socios para tomar decisiones colaborativamente y, finalmente, adaptarse constantemente al entorno de negocio

En este estado de cosas, diversos ejércitos, especialmente el norteamericano, han seguido atentos esta evolución en la gestión empresarial y están intentando adaptarlos, dado el nuevo contexto de seguridad y defensa mundial: los Estados deben ahora enfrentarse a un número creciente de adversarios repentinos y oportunistas que pueden ir desde otros estados hostiles hasta organizaciones terroristas transnacionales. Estos adversarios pueden emplear ataques por sorpresa, no convencionales, para crear daños a gran escala sobre objetivos débiles para maximizar el caos sobre la estabilidad y la geopolítica mundial. Los ejércitos deben estar preparados para enfrentarse a sus enemigos en cualquier instante y lugar, bajo cualquier circunstancia, rápida y decisivamente. Más aún, las organizaciones militares deben además enfrentarse a un número creciente de misiones

humanitarias, operaciones de paz y de actuaciones en catástrofes. Así, los retos en el nuevo entorno de seguridad global serían:

- Contemplar la nación como un campo de batalla potencial, que requiere sistemas de defensa.
- Preparar un conjunto diverso y complejo de capacidades de fuerza, con alta disponibilidad para responder a los retos y las amenazas reales y potenciales.
- Prepararse para el posible uso de armas de destrucción masiva por el enemigo.
- Mantener simultáneamente conciencia, integración y acomodación de todos los niveles de guerra (estratégico, operacional y táctico).
- Adaptarse continuamente a la sofisticación evolutiva de las amenazas de los enemigos.

En resumen, como en el mundo civil, las organizaciones militares deben afrontar retos cada vez más irregulares, disruptivos y catastróficos, además de la guerra tradicional.

Estos cambios en el entorno de la misión militar y los avances en la Tecnología de la Información y de las Comunicaciones (TIC) han llevado a varios países a afrontar estos nuevos retos, por reflexión sobre los nuevos modelos de gestión empresarial. Aquí nos fijaremos en dos aproximaciones clave que emanan del Gobierno norteamericano, como son la logística *sense and respond* y las operaciones centradas en la red.

Logística *sense and respond*

Tradicionalmente, la logística relacionada con la defensa se ha basado en el despliegue masivo de recursos, con el consiguiente coste elevadísimo y pérdida de eficacia. Aunque esta aproximación puede ser útil en las situaciones en las que la demanda es estable y fácilmente predecible, el nuevo contexto ya descrito, exige mucha más flexibilidad. Específicamente, entre los retos logísticos que se deben afrontar se incluyen:

- Eliminación de los cuellos de botella logísticos inter e intra ejércitos y agencias.

- El apoyo a operaciones expedicionarias a través de bases flexibles.
- Ensanchamiento de la base de recursos logísticos entre ejércitos, aliados y recursos propios.
- Reducción del riesgo de pausa operativa de origen logístico.
- Sostenimiento rápido y adaptable de fuerzas para apoyar la rapidez de decisión y calidad de efectos
- Apoyo cognitivo a la toma de decisiones logísticas, especialmente para la predicción y anticipación de las necesidades logísticas
- Puesta en red de todos los recursos y activos logísticos.
- No acumulación masiva de los recursos logísticos.
- Priorización global y optimización local del apoyo logístico
- Alineación de las operaciones logísticas con la intención, situación, fuerza, estatus y entorno cambiante del mando.
- Apoyo logístico a todas las operaciones militares.

Se ha intentado emplear la logística *just-in-time*, véase Sandras (1989), en los ejércitos para aligerar los inventarios y, en general, hacer más eficientes los sistemas logísticos. Los resultados han sido aceptables, pero se tiende a crear una cadena de suministro demasiado frágil con un nivel de riesgo demasiado alto en entornos dinámicos, debido a su inflexibilidad, su vulnerabilidad a los ataques y su potencial incapacidad para dar servicio priorizado a las necesidades generadas por un entorno cambiante. Así, algunos de los ERP´s (*Enterprise Resource Planners*) que han funcionado adecuadamente en el sector comercial, no han operado demasiado bien en el entorno militar, cada vez más dinámico: no se trata de mejorar la eficiencia de las operaciones de dominio, sino de transformar la logística para responder a un mosaico de necesidades con velocidad y efectividad.

Surge así el concepto de logística, S&R (*Sense and Respond*) ([1]) definida por la Office of Defense Transformation, en un contexto militar, como sigue:

> La logística S&R es un concepto innovador centrado en la red que posibilita operaciones conjuntas basadas en efectos y proporciona apoyo preciso y ágil. Se fundamenta en procesos altamente adaptativos, autosincronizados y dinámicos. Predice, anticipa y coordina acciones que proporcionan ventaja competitiva que abarca todo el rango de operaciones militares en los niveles estratégico, operacional y táctico de la guerra. Promueve la transformación doctrinal y organizativa y apoya la coherencia escalable del mando y control, las operaciones, la logística, la inteligencia, el reconocimiento y la seguridad.
>
> Implementada como un servicio horizontal en toda la organización, proporciona una red de recursos y capacidades logísticas de punto de efecto a origen de apoyo. Bajo este esquema, cualquier entidad, sea militar, gubernamental o comercial, pasa a ser tanto un cliente potencial, como un proveedor potencial. Proporciona flexibilidad, robustez y escalabilidad para la guerra conjunta expedicionaria a través de redes adaptativas, sensibles, de tiempo real, para las operaciones estadounidense, aliadas y en coalición.

Así, la logística S&R se centra en las siguientes cuestiones:

- *Adaptabilidad y velocidad.* Puesto que la demanda es altamente impredecible, el apoyo efectivo dependerá, esencialmente, de la adaptabilidad y velocidad de respuesta. Así, las redes logísticas deberían autosincronizarse sobre un entorno común y un conjunto de objetivos compartidos, para proporcionar la satisfacción de los requisitos operativos en el punto de aplicación.

- *Efectividad.* El apoyo logístico debe centrarse en conseguir el propósito del mando, que puede evolucionar en función de la situación estratégica, operacional y táctica, el entorno de las operaciones militares y el estado de las fuerzas. Debe reconocerse y mitigarse el riesgo operativo debido a la logística. Además,

---

[1] Lo podemos traducir por el concepto de Logística de *"Respuesta Rápida".*

deberán proporcionarse distintas opciones para las tareas militares en función del análisis de las capacidades de apoyo.

- *Flexibilidad.* El apoyo a las operaciones militares es más eficaz a partir de una cadena de suministro altamente flexible, más que a partir de una cadena altamente optimizada. De hecho, deberían promoverse las negociaciones por recursos y capacidades logísticas para apoyar tareas que evolucionan rápidamente y operaciones basadas en efectos. La distribución y el transporte de apoyo debería ser independiente de las restricciones geográficas.

- *Modularidad.* El apoyo debería organizarse por módulos de capacidades, en lugar de por elementos tradicionales de servicio.

- *Integración.* El empleo de TIC sofisticadas permitirá compartir datos, una perspectiva común del campo de batalla, una percepción rápida del consumo y las necesidades de recursos, el seguimiento del plan logístico y el apoyo a su eventual reconfiguración

El cuadro 1, tomado de la Office of Defence Transformation, resume cómo debería ser la logística antes y después de las transformaciones requeridas.

Antes	**Después**
Lineal	No lineal
Cadenas	En red
Basada en uso	Basada en efectos
Preplanificada	Planificación y ejecución continua
Reactiva	Proactiva

Jerárquica	En red
Monolítica	Distribuida, Modular
Pobre escalabilidad	Dinámicamente escalable
Inflexible	Flexible
Basada en consumo	Adaptativa y cognitiva
Masiva	De efecto rápido
Agotamiento	Basada en efectos
Perspectiva de servicio	Coherencia conjunta
Eficiencia	Efectividad
Altamente optimizada	Efectiva
Cadenas de suministro frágiles y rígidas	Redes de demanda robustas y flexibles
Hazlo más rápido	Hazlo más inteligentemente

En algo más de detalle, un sistema logístico S&R, aprovechando la infraestructura nacional de información, incluiría los siguientes elementos:

- *Base de conocimientos logísticos,* que relaciona los recursos logísticos con las operaciones logísticas para todo el espectro de visibilidad de activos. Acumula la experiencia y el conocimiento proporcionado por sistemas de ayuda a la decisión.

- *Base de reglas de decisión y de negocio adaptables*, que ajusta la ejecución logística de forma precisa y se adaptan dinámicamente al propósito del mando en función de la situación estratégica, operacional o táctica y del entorno del campo de batalla.

- Un *conjunto de agentes software inteligentes* que:
  - Representan recursos, consumidores y distribuidores logísticos.
  - Monitorizan la evolución del propósito del mando; la situación; el entorno del campo de batalla; el estatus de las fuerzas aliadas.
  - Representan las prioridades del mando.
  - Controlan la distribución de los recursos escasos.
- Un *conjunto de sistemas de ayuda a la decisión cognitivos* que:
  - Analizan la información proporcionada por los agentes.
  - Adaptan la ejecución del sistema, a medida que cambien las condiciones.
  - Apoyen la toma de decisiones para la planificación logística.
  - Proporcionan recomendaciones sobre misiones y tareas a realizar para reducir el riesgo de no alcanzar los objetivos del mando debido a cuestiones logísticas.
  - Identifiquen patrones de actividad que requieran el ajuste de la planificación y ejecución logística (anticipación y predicción).
  - Identifiquen y procesen sucesos en la red de suministro.
- El *conjunto de interfaces, aplicaciones y portales logísticos*, incluidos los vínculos con la infraestructura de red, las funciones logísticas, los agentes y los sistemas de ayuda a la decisión.

Dentro de esta arquitectura, conviene destacar el concepto de *agente software inteligente*, véase Padgham y Winnikoff (2004) para más información. Los agentes *software* son programas que actúan como agentes para otros programas en una relación de agencia, en el sentido económico del término.

Como ejemplo, algunos agentes implementarán la asignación de valores operacionales, que pueden interpretarse como la aplicación del análisis de valor

multiatributo, véase Ríos *et al* (1988), a la evaluación de tareas, misiones y efectos, bien en un área de operaciones en un campo de batalla; bien durante el marco de tiempo de una operación; bien en relación con la evaluación del riesgo frente a fallos logísticos, etc.

Operaciones centradas en la red

> *It allowed us to make decisions and execute those decisions faster than any opponent.*
>
> Lt. Gen. David D. McKiernan
>
> Combined Forces Land Component Commander, OIF

El otro concepto importante es el de *operaciones centradas en la red*, que viene a ser la vía militar, en la Sociedad de la Información y del Conocimiento, para explotar una nueva fuente de poder, como es compartir la información. Se refiere, en definitiva, al empleo de las TIC para conseguir una superioridad informativa que se traduzca en superioridad en el campo de batalla, habiendo recibido diversos nombres en distintas partes del mundo incluyendo la *guerra centrada en la red* y la *defensa centrada en la red*. En esencia, la premisa básica es que compilar la información proporcionada por sensores orgánicos en una vista integrada, conectada en red en tiempo real del campo de batalla proporciona superioridad en el conocimiento a las unidades del frente, que posibilita la toma de mejores decisiones, por ejemplo, facilitando el despliegue de una fuerza más letal y enfocada en las áreas más críticas, de forma que se maximicen los efectos.

De manera esquemática, las nuevas reglas asociadas a las operaciones en red, serían:

- Luchar primero por la superioridad en la información.
- Rapidez en la decisión.
- Acceso a la información global: atención compartida.
- Fuerzas dispersas: operaciones no contiguas.

- Mitigar el despliegue masivo de recursos.
- La autosincronización.
- Alcance profundo de sensores.
- Alterar las condiciones iniciales a tasas mayores de cambio.
- Comprimir los niveles de guerra.

En algo más de detalle, con las Operaciones Centradas en la Red (OCR) se describe el conjunto de tácticas, técnicas y procedimientos emergentes que una fuerza parcial o completamente conectada a la red puede emplear para crear una ventaja militar decisiva. Así:

- OCR es un concepto de operaciones basado en la superioridad en la información que describe cómo una nación puede organizarse y luchar en la era de la información.
- OCR incrementa el poder de combate poniendo en red sensores, decisores, y multiplicadores para conseguir una atención compartida, mayor rapidez de decisión, mayor ritmo de las operaciones, mayor letalidad y mayor capacidad de supervivencia y autosincronización.
- OCR traslada la superioridad en la información mediante la conexión efectiva de las fuerzas amigas en el campo de batalla, proporcionando una percepción mejorada y compartida de la situación, posibilitando una toma de decisiones más rápida y efectiva.

Los beneficios de las OCR se derivan de que, claramente, las fuerza conectadas dominarán a las no conectadas, si el resto de las condiciones son iguales, puesto que disponen de capacidades muy superiores para compartir, acceder e intercambiar información. Así:

- Una fuerza estrechamente conectada a la red, comparte mejor la información.
- La información compartida, potencia la calidad de la misma y la percepción compartida de la situación.

- La percepción compartida de la situación, a su vez, posibilita la colaboración y la auto-sincronización y potencia el sostenimiento y la rapidez de la toma de decisiones.

- Finalmente, éstas incrementan, sustancialmente la efectividad de la misión.

Para su implementación, algunos elementos clave serían:

- Refinar las nuevas reglas de la guerra en la era de la información y la teoría de la OCR a través de la simulación, el contraste, la experimentación y las experiencias reales de combate, véase capítulo tercero.

- Aplicar la teoría OCR a todo el ejército.

- Acelerar la conexión en red de todas las fuerzas en los niveles estratégico, operacional y táctico.

- Acelerar el despliegue y empleo de los nuevos conceptos y capacidades basados en la red.

- Experimentar con los nuevos conceptos y capacidades para desarrollar nuevas y mejores formas de implementar operaciones centradas en la red.

- Afrontar los retos asociados con las operaciones (basadas en red) de aliados y coaliciones.

- Desarrollar doctrina, tácticas, técnicas y procedimientos para las OCR.

Un ejemplo

Quizá el ejemplo más notable de aplicación de los conceptos antes descritos es el de la primera fase de la OLI. Para la mayor efectividad de su diseño, se tuvo en cuenta:

- El gran incremento del ancho de banda en las comunicaciones.

- Los ejercicios de ensayo de misiones.

- La experiencia de la operación *Libertad Duradera* en Afganistán.

- Los trabajos del grupo de observación Norte-Sur, durante doce años.
- Los cuarteles generales existentes.
- Los procedimientos de mando y control existentes.
- Las mejoras en el transporte aéreo.
- La superioridad de combate, basada en la superioridad en la información, la rápida supremacía en aire y mar, la velocidad y profundidad de las maniobras y los instantes y lugares de ataque perfectamente determinados.

Como consecuencia de ello se diseñó un plan altamente flexible y maduro, se contó con capacidades conjuntas robustas, bien entrenadas y rápidamente adaptables, mejores servicios y se pudo poner énfasis en los imperativos estratégicos, pronto y de forma continuada.

Entre los elementos más populares para apoyar las OCR, estuvieron y están los FBCB2 (*Force XXI Battle Command Brigade and Below*) que forman parte del entorno del comando de maniobras e incluye, además, un Sistema de Control de Maniobras (que representa la situación del campo de batalla con las localizaciones de los enemigos y las propias fuerzas), el Sistema de Análisis de todas las fuentes de información (de satélites y radares para determinar la localización de las fuerzas enemigas), el sistema avanzado de datos tácticos de artillería de campaña (que selecciona objetivos y pasa la información pertinente a los sistemas de disparo de artillería y cohetes), el sistema de planificación de misiones de aviación, el sistema de integración del *software* y un sistema de administración.

EL FBCB2 es un Sistema de Información que proporciona percepción de la situación e información de las tropas amigas desde nivel brigada hasta nivel soldado. También conocido como BFT (*Blue Force Tracker) (*o seguimiento de fuerzas propias), incluye en los vehículos de combate un ordenador portátil reforzado, sobre un tablero de instrumentos, con un receptor/transmisor sobre el techo para emitir información vía satélite al cuartel General y a los otros vehículos, que permite tener una representación permanente, casi en tiempo real y bajo cualquier condición atmosférica del campo de batalla, con la posición del portador y de sus compañeros.

Combinado con un mapa digital que incluya las posiciones enemigas y que permite determinar dónde está el enemigo.

Los FBCB2 se instalaron en helicópteros, tanques, carros de combate y vehículos (*Hummer)* americanos y en algunos británicos. Dado su éxito, se está estudiando, por un lado, el compartirlo con otros aliados y, por otro, añadir ancho de banda para poder transmitir más datos sobre unidades enemigas y amigas, soportar imágenes 3D, y permitir paso de mensajes extendidos. Se está desarrollando, además, una versión portátil, para llevar en la mano. Debe mencionarse, además, que durante OLI, se probaron más de sesenta dispositivos diferentes, surgiendo así la necesidad de desarrollar estándares apropiados, una situación que volverá a tratarse en el capítulo tercero.

Las ventajas principales obtenidas con los FBCB2 serían:

- Un dibujo operativo común.
- Una percepción situacional compartida, mucho mejor para el mando, los mandos intermedios y los soldados, con lo que se reduce la carga cognitiva necesaria para obtener tal percepción situacional.
- Un propósito de mando basado en una mayor, y más compartida, comprensión de la situación, potenciado, además, por capacidades adicionales para la colaboración en tiempo real.
- Una toma de decisiones más rápida y de más calidad.
- Una mayor agilidad táctica.
- Riesgos reducidos.

Por comparación con la operación *Tormenta del Desierto*, realizada con actores y condiciones similares, nos gustaría destacar que OLI conllevó:

- Menos fuerzas aéreas y de tierra.
- Uso extensivo de operaciones especiales.

- Costes mucho menores.
- Menos munición empleada.
- Menos pozo de petróleo destruídos.
- Menos lanzamientos de misiles iraquíes.
- Mayores distancias en las maniobras.
- Un esfuerzo de planificación colaborativo robusto.

Conclusiones

Hemos realizado una breve descripción de algunos de los nuevos modelos de operaciones militares que están empezando a adaptarse y adoptarse a partir de los nuevos modelos de gestión de operaciones empresariales, dada la similitud del entorno nuevo y globalizado con que deben enfrentarse tanto las empresas como los ejércitos, caracterizado por su alta incertidumbre, la variedad de clientes a los que se deben enfrentar y la necesidad de responder, de manera flexible, a la variedad de nuevas amenazas. Desde luego deberá pasar aún algo de tiempo, hasta que se produzca la adopción definitiva de estos modelos y se desarrollen los sistemas de gestión correspondientes. No debemos soslayar tampoco el profundo cambio cultural que estos nuevos modelos tendrán en los ejércitos, cuestión que apenas hemos tocado, por habernos centrado principalmente en temas tecnológicos. Así, los individuos se formarían y entrenarían como *guerreros centrados en la red*, con la ética adaptativa primero y, después, como especialistas funcionales o técnicos. Debe quedar claro, en cualquier caso, el profundo papel que las TIC deben tener en los nuevos ejércitos, modificando su concepción como antes han hecho en la economía, la educación o la política.

Es por ello que los restantes capítulos de esta monografía se centran en aspectos más puntuales de la aplicación de las TIC en la seguridad y la defensa. En tiempos normales de operaciones, resulta conveniente disponer de metodologías basadas en mejores prácticas para la gestión de las TIC, según describen Eugenio Fernández e Isaías Peral en el capítulo segundo «Implantación ITIL para la gestión TIC en centros militares», en el que ponen el énfasis en la metodología ITIL. José Miguel

Castillo y Luis Pastor describen la preparación frente a posibles operaciones militares que los entornos de simulación y de realidad virtual posibilitan, en el capítulo tercero «Operaciones militares y entornos de realidad virtual». Finalmente, en el capítulo cuarto «Las Redes *ad hoc* para seguridad y defensa», Javier Ramos y Carlos Alberich ilustran, entre otras ideas, como las nuevas redes *ad hoc* pueden ser medios ideales para alcanzar esa ventaja informativa requerida en las primeras fases de las operaciones a que hemos aludido en este capítulo primero.

BIBLIOGRAFÍA

Alberts, D., Gartska, J., Stein, F. (2004) *Network Centric Warfare,* CCRP

Desai, A. (2005) Adaptive complex enterprises, *Communications of the ACM,* 48, 33-35.

Gardner, J., Varadan, V., Awadelkarim, O. (2001) *Microsensors, MEMS and Smart Devices*

Gartska, J. (2004) Network Centric Operations, presentación disponible en www.oft.osd.mil

Gass, S. (2002) Great Moments in HistORy, *OR/MS Today,*

Giudici, P. (2003) *Applied Data Mining : Statistical Methods for Business and Industry,* Wiley.

Gouré, D. (2004) Standardize Blue-Force Tracking, disponible en http://www.defensenews.com/story.php?F=494578&C=

Haeckel, S. H. (1999) *Adaptive Enterprise: Creating and Leading Sense-And-Respond Organizations.* Harvard Business School Press.

Hastie, T., Tibshirani, R., Fiedman, J. (2003) *The Elements of Statistical Learning, Springer.*

Levitt, S., Dubner, S. (2005) *Freakonomics : A Rogue Economist Explores the Hidden Side of Everything,* Harper Collins.

Lin, G., Luby, R., Ko-Yang, W. (2004) New Model for Military Operations, *OR/MS Today,* 12, 78-83.

Lin, G., Buckley, S., Cao, H., Caswell, N., Ettl, M., Katircioglu, K., Nigam, A., Ramachandran, B. (2002), *OR/MS Today,* 10, 26-31.

Menotti, M. (2004) The Sense-and-Respond Enterprise, *OR/MS Today,* 8.

Network Centric Warfare Education home page, http://www.oft.osd.mil/initiatives/ncw/presentations/ncw.cfm

Office of Force Transformation (2004). *Operational sense and respond logistics: Coevolution of an adaptive enterprise capability,* Concept document.

Office of Force Transformation (2003). *Sense and respond logistics: Enabling concept,* Concept document.

Office of Force Transformation (2003). *Joint Operational sense concepts,* Concept document.

Office of Force Transformation (2003). *Network Centric Warfare,* Concept document.

Padgham, L., Winikoff, M. (2004) *Developing Intelligent Agent Systems : A Practical Guide***,** John Wiley.

Ramnath, R., Landsbergen, D. (2005) IT-Enabled sense-and-respond startegies in complex public organizations, *Communications of the ACM,* 48, 59-64.

Ríos, S. (1953) Métodos Estadísticos, experimentación industrial e investigación operativa, *Revista del Instituto Nacional de Racionalización del Trabajo,* 3-12.

Ríos, S., Ríos Insua, S., Ríos Insua, M.J. (1988) *Procesos de Decisió Multicriterio,* EUDEMA.

Ruengert, M., Gannon, S. (1999) *A2C2S MCE/Communications Tutorial,* presentación disponible en http://www.fas.org/man/dod-101/sys/ac/equip/docs/A2C2S_Tutorial_RevA1a/sld001.html

Sandras, W. (1989) *Just-in-Time: Making It Happen : Unleashing the Power of Continuous Improvement,* John Wiley.

West, M., Harrison, J. (1997) *Bayesian Forecasting,* Springer.

CAPÍTULO SEGUNDO

IMPLANTACIÓN DE ITIL PARA GESTIÓN TIC EN CENTROS MILITARES

IMPLANTACIÓN DE ITIL PARA LA GESTIÓN TIC EN CENTROS MILITARES

Por Eugenio Fernández Vicente

e Isaías Peral Puebla

Resumen

Las Tecnologías de la Información y de las Comunicaciones (TIC) se han convertido con el paso del tiempo en un elemento indispensable para la mayoría de las organizaciones, sin el cual muchas de ellas no podrían desarrollar su actividad diaria. A pesar de esto, tradicionalmente ha sido relegado su papel dentro de la organización a un segundo plano, y las áreas de tecnologías han sido consideradas como meras proveedoras de infraestructuras. Sin embargo, en los últimos años se ha tomado conciencia de que una adecuada gestión y un buen gobierno de estas tecnologías que las alinee adecuadamente con los objetivos de la organización, producirá unos beneficios reales y tangibles para la misma. Es por tanto necesario disponer de marcos de actuación como metodologías o estándares apropiados para llevar a cabo estos procesos de gestión y gobierno, y en este sentido ITIL (*Information Technology Infraestructure Libray*) se configura como el referente a seguir. En los centros de ámbito militar, como en muchos otros, la llegada de modelos de este tipo es inminente por la propia dinámica del trabajo que en ellos se desarrolla, y deben ponerse los mecanismos necesarios para abordar con éxito una gestión y un gobierno de las TIC, para lo cual se han sentado ya las bases correctamente a través del Plan Director del Centro de Investigaciones Sociológicas (PD SIC).

Introducción

Las TIC se han hecho omnipresentes en mayor o menor grado en la dinámica de la mayoría de las organizaciones independientemente del sector de actividad de éstas, de sus dimensiones, o de su carácter público o privado, lo que ha provocado una dependencia de estas tecnologías tan fuerte que algunos autores como Carr (2003)

plantean que su uso ya no constituye ninguna ventaja competitiva, sino que más bien las TIC han pasado a ser una *commodity* como puede ser la luz eléctrica. Al margen del debate las posiciones de estos autores, lo cierto es que si miramos a nuestro alrededor en nuestro ámbito de trabajo, y reflexionamos sobre la posibilidad de un *apagón tecnológico* momentáneo que dejase no operativos todos los sistemas informáticos (ordenadores, impresoras, programas de gestión, etc.) y de comunicaciones (Internet, centralitas digitales, etc.), nos será difícil imaginar la actividad de nuestra organización en el día a día, y seguramente concluyésemos que un incidente de este tipo abocaría seguramente a un colapso en el funcionamiento habitual de la organización. En este sentido es inmediato deducir que es necesaria una buena administración de las TIC con el objeto de que no ocurran incidentes de esa magnitud, e incluso de magnitudes menores que dejasen no operativos por ejemplo sólo una parte de los sistemas.

Debemos considerar además que en este entorno de dependencia de las TIC por parte de las organizaciones que usan éstas para la gestión, el desarrollo y la comunicación de activos intangibles como son la información y el conocimiento, el éxito pasa por que estos sean seguros, exactos, fiables, entregados a la persona correcta, y en el momento y lugar correctos, lo cual se consigue tratando adecuadamente el denominado *factor riesgo* que viene dado habitualmente por multitud de amenazas (errores u omisiones, abusos, cibercrimen, fraudes, etcétera), y minimizando la vulnerabilidad que es inherente a estas tecnologías, paradójicamente mediante el aumento de nuestra dependencia de las TIC incorporando nuevas tecnología y nuevos usos. En definitiva, podemos concluir que una adecuada administración de las TIC redundará en una mejora de aspectos como la calidad o la eficiencia en nuestra organización aportando valor al negocio de la misma (sea este del tipo que sea: económico, social, etc.), y ayudando a esta a conseguir sus objetivos minimizando los riesgos.

Este planteamiento es conocido y válido desde hace más de dos décadas. Entonces, ¿por qué no se ha producido en este tiempo un reconocimiento apropiado de las TIC y se ha trabajado en su alineamiento con los objetivos del negocio, y se habla ahora de administrar adecuadamente las TIC en la organización? En respuesta a esta pregunta podemos apuntar dos factores clave que han supuesto un

lastre en este camino, y permiten clarificar el contexto de las TIC en las organizaciones:

- En primer lugar debemos considerar que una adecuada administración en materia TIC alineada con los objetivos de negocio de las organizaciones implica involucrar activamente a sus órganos directivos, cuyos miembros se enfrentan generalmente a una tarea para la que no suelen están preparados, ya que no han recibido formación adecuada y cuentan a lo sumo con experiencia en materia de gestión pero no tecnológica, y en las últimas décadas han confiado, una y otra vez, en que la solución a sus problemas venga de la mano de las empresas de tecnología, las cuales sabedoras de esta situación, anuncian una y otra vez la panacea tecnológica definitiva que resolverá los problemas de cualquier organización, provocando en los órganos directivos de las organizaciones un ciclo que pasa año tras año de la euforia a la decepción profunda, generando una cultura directiva escéptica en las soluciones tecnológicas, y en general en las TIC.

- En segundo lugar debemos considerar un aspecto que tiene como base la conocida *paradoja de la productividad*, introducida en el año 1987 por Steven Roach, analista de Morgan Stanley, asegurando que había observado que durante las décadas de los años setenta y ochenta la inversión en TIC por trabajador había crecido substancialmente, mientras que la productividad se había mantenido constante, de lo cual concluyó que, en principio, el incremento de la inversión en tecnología tenía un efecto casi nulo en la productividad de los trabajadores, abriendo un debate sobre si es necesario o no adquirir estas tecnologías, que sigue abierto y aún no tiene una única solución, existiendo opiniones a favor y en contra.

Estos dos aspectos, la desconfianza en las TIC generada en estos años en los órganos directivos de las organizaciones, y la falta de métodos que permitiesen alinear adecuadamente las TIC con los objetivos del negocio y posteriormente tomar mediciones que demostrasen a estos órganos directivos los beneficios de una adecuada administración de las TIC, ha provocado un retraso sustancial en el posicionamiento de estas tecnologías dentro de la organizaciones; y si bien muchas organizaciones han ignorado el papel relevante de las TIC y han evitado tomar decisiones en materia de administración de las mismas debido a estos factores, en

la actualidad es algo impensable para la mayoría de ellas que de una forma u otra han asumido la importancia de una adecuada administración de las TIC.

El gobierno y la gestión de las TIC

De lo expuesto en la introducción anterior podemos extraer cuatro factores:

1. La dependencia de las organizaciones de sus TIC.
2. La necesidad de controlar y disminuir el riesgo.
3. La poca o nula confianza en las TIC por parte de los órganos directivos.
4. La falta de indicadores que permitan relacionar las TIC con la productividad y los objetivos del negocio de las organizaciones.

Estos factores han incrementado en los últimos años la búsqueda de soluciones que permitan administrar las TIC de manera adecuada obteniendo métricas de medición y valoración que obtengan la confianza necesaria de los órganos directivos y aseguren que las inversiones en TIC generan el correspondiente valor de negocio con el mínimo riesgo. Así, poco a poco han aparecido marcos de actuación concretos en forma de metodologías, estándares o buenas prácticas que han supuesto avances significativos en ese sentido.

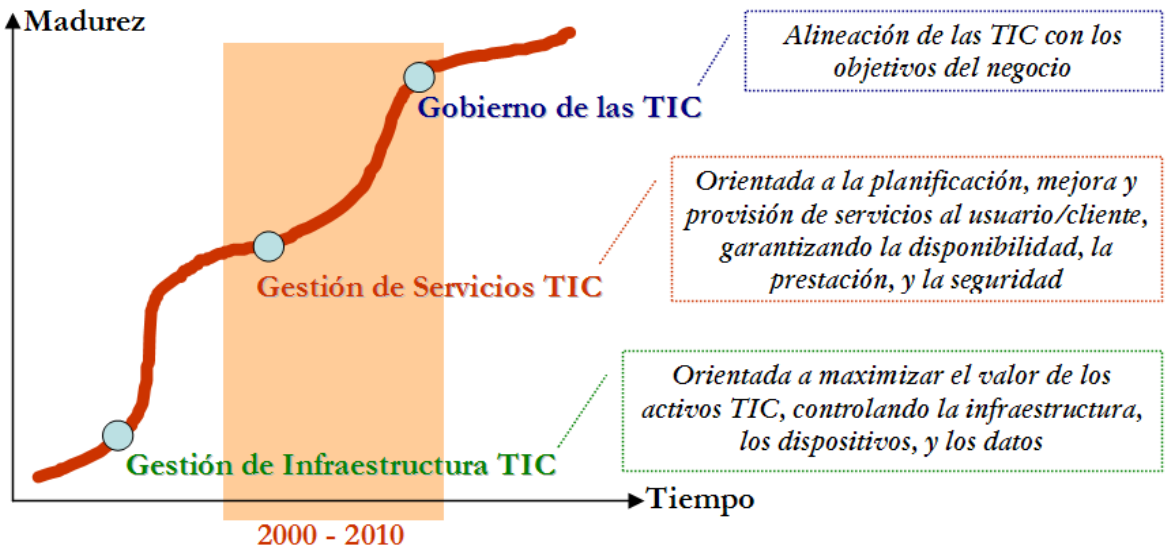


Figura 1 *Evolución de la administración de las TIC*

De esta forma, y mediante la adopción de estos marcos, en la última década las organizaciones están consiguiendo superar una fase de gestión puramente orientada a la infraestructura existente y evolucionar hacia una gestión de los servicios, en el camino hacia un adecuado gobierno de las TIC (figura 1). Esta primera fase (en la que aún se encuentran muchas organizaciones) estaba basada en un modelo reactivo en el que el área TIC se dotaba de la infraestructura necesaria para satisfacer las necesidades constantes del negocio, sin recibir la más mínima información por parte de la organización respecto a los objetivos perseguidos, los beneficios para el negocio o aspectos similares, y por tanto sin una visión de negocio. Se practicaba por tanto una política que no permitía obtener ninguna valoración sobre la influencia de las TIC en la organización, y ni siquiera valorar si la inversión en materia TIC era adecuada o no, produciendo comportamientos perniciosos como la compra desmesurada de infraestructura en previsión de posibles demandas no planificadas.

Esta visión del poco o nulo control sobre las TIC dio lugar a la implantación de modelos de gestión racionales que permitiesen de alguna manera avanzar en la dirección correcta mediante la utilización de mecanismos adecuados para la gestión de las TIC, y que los diferentes marcos de actuación como COBIT o ITIL, de los que expondrá posteriormente, ven en términos de procesos, de tal manera que se obtienen guías o buenas prácticas sobre seguridad, gestión financiera, continuidad, gestión de incidencias de usuario, etcétera. De esta manera, y con buenos procesos de gestión es posible además empezar a medir de manera individual aspectos relevantes de las TIC que pueden aportar luz a los órganos directivos, como puede ser la satisfacción de los usuarios, tiempos de respuestas en la resolución de incidencias, o aspectos similares, por poner algunos ejemplos básicos. En esta fase podemos establecer el estado actual de las organizaciones en materia TIC de manera general, de manera que más o menos asentada, la política a seguir es la implantación de mecanismos adecuados en materia de *gestión de las TIC*.

Sin embargo, aún es necesario un nivel mayor de abstracción si se quiere lograr un adecuado alineamiento de las TIC con los objetivos del negocio que ofrezca resultados medibles e interpretables, surgiendo así un nuevo concepto para dirigir y controlar las TIC en las organizaciones: el *gobierno de las TIC*, que entenderemos como parte integral del *gobierno corporativo* para las organizaciones en su conjunto,

y que de forma básica podemos definirlo como el liderazgo, los procesos, y las estructuras que aseguran que las tecnologías de la organización apoyan los objetivos y estrategias de la organización. En este sentido, este concepto es mucho más amplio que el de *gestión de las TIC* y se centra en la interpretación y la transformación de las TIC para satisfacer las demandas presentes y futuras del negocio y de sus clientes y usuarios. Una revisión de estos conceptos puede encontrarse en (Peterson, 2003).

Centrándonos en la gestión y el gobierno de las TIC, y dejando a un lado la gestión de la infraestructura que se entiende como una fase superada por la gran mayoría de las organizaciones, y que en su defecto es susceptible de ser abordada de manera adecuada en la actualidad, podríamos enumerar una serie marcos de actuación (modelos, metodologías, estándares, o guías de buenas prácticas) que pueden utilizarse para abordar tanto una buena gestión como un buen gobierno, y en lo que sigue utilizaremos el término de *marco* en referencia a los *marcos de actuación* para unificar un criterio pues entendemos que define a cualquiera de los otros por su generalidad.

La cuestión es decidir *cuáles y para qué,* partiendo de la base de que se admite que el uso de estos marcos tiene numerosas ventajas, como un menor coste de adopción, no reinventar lo mismo una y otra vez, facilitar la externalización, la auditoría y control, etc. Ante la primera cuestión (*cuáles*), debemos considerar un conjunto de marcos muy referenciados en la literatura: COBIT, ITIL e ISO 17799, así como otros menos conocidos como MOF o BS15000. La segunda cuestión (*para qué*) es preciso abordarla en términos de *¿gobierno o gestión?,* de manera que debemos seleccionar el o los marcos apropiados para desarrollar un gobierno de las TIC adecuado o una gestión de las mismas. Este no es un aspecto sencillo, ya que muchos de estos marcos pueden ser utilizados para abordar ambos dominios, como por ejemplo COBIT. Lo cierto es que algunos de ellos están más focalizados hacia el gobierno como es COBIT, otros hacia la gestión como es ITIL, y otros a procesos muy particulares como la seguridad como ISO 17799. Además la tendencia actual *IT Governance Institute* (ITGI, 2005*a*) es la integración de marcos de actuación que permita la utilización conjunta de estos de manera eficiente, como es el caso de los tres mencionados y representado en la figura 2.

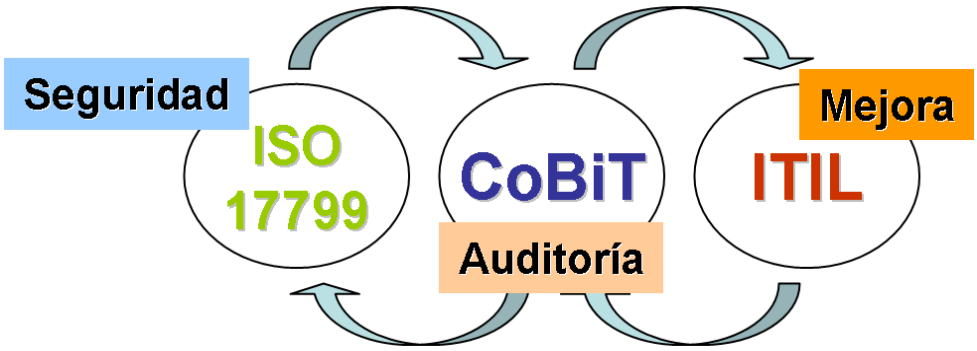


Figura 2 *COBIT-ITIL-ISO 17799*

Es importante establecer que no existe una respuesta única a la hora de seleccionar los marcos a utilizar en cada momento. En principio diremos que no hay una aproximación que abarque todo, desde el gobierno de las TIC a la implementación de los procesos concretos como el de seguridad, y más bien existe un conjunto de aproximaciones que se complementan unas con otras para abarcar todo el escenario. Existen otros marcos de actuación que podríamos enumerar (cuadro 1), si bien la consideración de los tres anteriores cubre sobradamente la mayoría de las pretensiones en materia de gobierno y gestión de las TIC en una organización. Lo importante en todo caso es realizar una buena selección de éstos y saber por cual de ellos empezar.

	Estándar Internacional	Estándar Nacional	Estándar de Organizaciones
Gestión TIC		BS 15000	COBIT ITIL MOF
Gestión de Proyectos			PMBOK PRINCE2 APMs
Gestión de la Seguridad	ISO 13335 ISO 13569 ISO 17799 ISO 15408	NIST - 800 series BS 7799-2 GAO's FISCAM German BSI	ACSI-33 COBIT ISF ENV12924 SEI's OCTAVE SEI's SW-CMM Baseline_ Production_ Manual
Desarrollo de Software	ISO 12207 ISO 15504	TickIT	CMMI Bootstrap
Gestión de la Calidad	ISO 9001	EFQM Baldrige_National_ Quality_ Plan	
Gobierno TIC		AS 8015 COSO	COBIT
Gestión de Riesgos		AS/NZS 4360 COSO	
Gestión de la Continuidad		PAS-56 AS/NZS 4360 HB 221-2004	
Auditoría	ISO 19011		COBIT

Cuadro 1 *Marcos de actuación*

Además de estos marcos de actuación concretos que suelen ser los más conocidos e implementados por las organizaciones, existen trabajos más amplios que los recogen y que cubren aspectos más metodológicos en la implementación tanto de la gestión como del gobierno de las TIC. En el ámbito del gobierno de las TIC, uno de los trabajos más completos es el del (ITGI, 2001, 2005*b*), que junto con los trabajos de Guldentops (2004), abordan el Gobierno de las TIC de una manera práctica y centrada en COBIT, pero con un enfoque muchísimo más amplio que el propio marco.

Otros trabajos se basan en la aproximación al gobierno de las TIC y su posterior gestión mediante el estudio del *alineamiento de las TIC con los objetivos del negocio* como pieza fundamental, y en este sentido abordan distintas aproximaciones y modelos para conseguir un alineamiento adecuado. La base para la mayoría de las aproximaciones en este sentido proviene del trabajo de Henderson y Venkatraman (1993) que establece las bases del modelo SAM (*Strategic Aligment Model*), y las aportaciones más importantes han sido las desarrolladas por Luftman (2002), si bien puede encontrarse una excelente y completa revisión en Avison *et al* (2004). Un tercer enfoque lo ofrecen los trabajos centrados en los *modelos de madurez* que de la mano otra vez del ITGI (2001) y otros autores como Duffy (2002) proponen modelos de madurez que permiten a una organización obtener una valoración del estado de la alineación de las TIC con los objetivos del negocio, y en última instancia del estado del gobierno de sus TIC. Una aproximación más pragmática para la implementación de modelos de gobierno de las TIC propone trabajos basados en una idea global que establece que el gobierno de las TIC puede ser dirigido utilizando una mezcla de estructuras, procesos y mecanismos de relación, y en este sentido los trabajos de Peterson (2003) y de Van Grembergen *et al* (2004) constituyen una excelente aproximación práctica para la implementación de un modelo de gobierno de las TIC, y establecen una bases seguidas por numerosos autores para desarrollar modelos específicos. Y centrándonos el aproximaciones prácticas encontramos un conjunto de trabajos desarrollados en el *Center for Information Systems Research* del MIT fundamentalmente por dos autores, Weill and Ross (2004) que proponen modelos de gobierno de las TIC basados en experiencias a lo largo de muchos años en implantaciones reales en empresas, así como en trabajos basados en encuestas y entrevistas realizados en numerosas empresas.

En el ámbito de la gestión de las TIC si bien son aplicables muchos de los trabajos anteriores, pues el gobierno de las TIC en su última instancia converge hacia la gestión y muchos de los modelos y trabajos mencionados acaban abordando ambas facetas, como es el caso de COBIT, los trabajos específicos de gestión giran en torno a ITIL. Los orígenes de los modelos de gestión de las TIC los podemos datar en la década de los años ochenta cuando IBM documenta los conceptos de gestión de sistemas en un modelo denominado ISMA *(Information Systems Management Architecture)*, y áreas como la gestión de redes y la gestión de aplicaciones llaman la atención de la comunidad de expertos en esta materia apareciendo modelos específicos como el SNMP *(Simple Network Management Protocol)* en el año 1988. Sin embargo, las primeras aproximaciones formales a la gestión de servicios TIC, conocida internacionalmente como ITSM *(Information Technology Service Management)*, fueron realizadas en la década de los ochenta, cuando la CCTA (*British Government.s Central Computer &Telecommunications Agency*), puso en marcha un proyecto denominado GITIMM (*Government TIC Infrastructure Management Method*) cuyo objeto era profundizar en la fase de operación del ciclo de vida del software, siendo el resultado final de este proyecto ITIL, un conjunto de libros que ofrecían una guía que constituyen las mejores prácticas en la provisión de servicios TIC en base a los requerimientos del cliente, que ya en el año 2000 lanzó su segunda versión, y que está a punto de editar la tercera. En relación a ITIL hay que mencionar el desarrollo de BS15000, el estándar inglés para ITSM en el año 2002. La versión ISO (*Internatitonal Standardization*) del mismo verá pronto la luz bajo el nombre de ISO 20000. Por último, es preciso mencionar los modelos de referencia basados en ITIL que distintas organizaciones han sacado al mercado, como es el caso de MOF (*Microsoft Operations Framework*) en su versión 3.0 en 2004; del HP ITSM (*IT Service Management Reference Model*) también en su versión 3.0; o del SMSL *(Systems Management Solution Lifecycle)* de IBM.

Ante este elenco de soluciones para abordar el gobierno de las TIC, su gestión, o ambas, en el que se entrecruzan marcos de actuación concretos y trabajos que proponen modelos teóricos y prácticos basados en diferentes aproximaciones, es difícil para una organización decidir el camino a adoptar, dejando en la mayoría de los casos la decisión a empresas externas que le ayudan a abordar esta cuestión, y que irremediablemente se decantarán por unas u otras aproximaciones por sus

propios criterios de negocio marcados por tecnologías, dependencias de empresas colaterales con las que mantienen acuerdos, especialización de su personal, y en definitiva un sinfín de factores que a menudo no tienen en cuenta la realidad de la organización sobre la que se va a actuar y las necesidades de éstas.

De manera general, tras un análisis detallado de todos los modelos mencionados y de todas las propuestas existentes tanto en la literatura científica como en el sector privado, y con el objeto de proponer una recomendación básica estándar, estableceríamos la adopción de un modelo de gestión de las TIC basado en COBIT e ITIL, haciendo énfasis en este último y utilizando el esquema de relación entre ambos modelos e ISO 17799 recientemente publicado (ITGI, 2005*a*) para relacionar los procesos de ambos modelos de manera que mediante ITIL se aborde la gestión en un sentido más práctico, y mediante la relación con los procesos de COBIT se inicie el camino hacia un modelo de gobierno de las TIC. En todo caso, es preciso matizar que no a todas las organizaciones les es válido ese modelo, que por lo general requiere de la definición y diseño de un plan en materia de gobierno y gestión de las TIC *ad hoc* para la organización, que finalmente establecerá (o no) como mecanismos de implementación los marcos mencionados.

Las ITIL

Dado el eco que ha tenido ITIL en dos últimos años, algunas de las más prestigiosas firmas de análisis y sondeos de mercado han realizado estudios de opinión y encuestas al respecto cuyos resultados merece la pena exponer, ya que reflejan la situación de ITIL en el sector de las TIC. Así, la prestigiosa firma de análisis de mercados Forrester dijo a finales del año 2004 que después de 15 años ITIL finalmente se convertiría en el año 2005 en la metodología estándar de facto para la gestión interna de procesos TIC, y que la adopción de este estándar duraría hasta 2008. TechRepublic realizó recientemente un estudio sobre 200 profesionales del mundo de las TIC en organizaciones de más de 1.000 empleados con el objeto de evaluar el grado de implantación de ITIL, evaluando en concreto la implementación de prácticas en ITIL, y los resultados establecieron que si bien la adopción de ITIL estaba ganado adeptos, esta era lenta, y solo el 19% habían adoptado procesos ITIL, asegurando el 81% tener la intención de adoptar ITIL, si bien aún estaban en los primeros pasos. Por otro lado, la firma Gartner afirmaba en 2004 que la

adopción de ITIL como estrategia puede suponer a una organización la reducción de su gasto en Tecnologías de la Información en un 50%. Estos datos y muchos otros que pueden encontrarse fácilmente en la literatura muestran como ITIL es el deseo de todos pero la realidad de unos pocos, y casos prácticos como el referenciado por Gartner en 2004 sobre una organización Europea que recuperó la inversión de la adopción e implementación de ITIL en 12 meses mejorando los beneficios en el segundo año, demuestran el éxito de implantar ITIL pero aún hoy son una excepción, ya que las implantaciones de ITIL existentes no alcanzarán la madurez suficiente como para poder evaluar los resultados desde el punto de vista del negocio hasta dentro de un par de años al menos.

Lo cierto es que existe un consenso generalizado en el sector sobre la pertinencia de adoptar ITIL y los resultados después de 25 años de experiencias lo demuestran. La paradoja se da en que a la vez que ITIL se ha puesto de moda (basta con preguntar a cualquier proveedor de servicios TIC al respecto y asegurará saber y tener toda la experiencia necesaria, tener sus herramientas perfectamente adaptadas para soportar los procesos, y contar con varios empleados certificados) se ha generado una decepción inicial en las organizaciones al comprobar que si bien una gran mayoría de ellas han manifestado su intención de implantar ITIL, pocas son las que lo han conseguido. ¿Por qué? Algunas de las razones son:

- ITIL expone fundamentalmente qué se debe hacer, pero no el cómo, de manera que las organizaciones deben desarrollar ellas mismas su propia manera de implementar los procesos.

- ITIL es complejo en el sentido de que toca *todas* las disciplinas, desde la seguridad a la gestión financiera, generando fracasos de implantación al querer abordar todos de una vez.

- ITIL tiene procesos muy interrelacionados entre sí y no es secuencial en el sentido de que pueda implementarse uno a uno de manera independiente, sino que deben implementarse subconjuntos de estos.

- ITIL no se ha convertido en un estándar todavía, lo que genera algunas reticencias, y provoca que algunos proveedores de servicios lo utilicen para implementar y vender su propia aproximación basada en ITIL, lo cual no deja de

ser un foco de confusión. Afortunadamente, con la aparición de la ISO 2000 se paliará este problema.

- ITIL debe ser implementado por equipos internos bien formados y certificados o bien por organizaciones de servicios externas expertas en la materia que se involucren de forma muy activa en toda la organización. No puede externalizarse la definición, el diseño y la implementación de la gestión de las TIC, sólo algunas de sus actividades. Se necesita que la organización se involucre activamente.

En resumen, ITIL no es difícil de implantar, como aducen algunas organizaciones decepcionadas en sus inicios tras intentos fallidos en la implementación, lo que ocurre es que hablamos de un nivel de abstracción distinto al de la gestión de infraestructuras a la que están habituadas la áreas TIC que implica además a otras áreas de la organización a medida que avanzamos de la gestión al gobierno de las TIC. Los puntos expuestos anteriormente que las organizaciones argumentan como freno a su implantación son precisamente las grandes ventajas de ITIL, el error proviene de la forma de entender su aplicación.

Pero, ¿qué es ITIL? ITIL fue originalmente un producto de la CCTA que era la Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido. Desde el 1 de abril de 2001, la OGC (*Office of Government Commerce*) absorbió a la CCTA y ahora es la propietaria de ITIL. El objetivo de la OGC es ayudar a sus clientes del sector público en el Reino Unido a actualizar sus actividades de provisión y a hacer el mejor uso posible de TIC y demás instrumentos, procurando modernizar la provisión de TIC en el gobierno, y conseguir un valor sustancial por el dinero invertido, de manera que promueve el uso de mejores prácticas en muchas áreas, entre ellas la gestión de servicios TIC, y publican gran cantidad de colecciones de libros escritos por expertos internacionales, siendo ITIL una de ellas. ITIL ofrece un marco común para abordar todas las actividades que desarrolla el área TIC estructurado en procesos de forma que podemos decir que aborda en su completitud la gestión de servicios TIC dentro de una organización. ITIL no es un método, sino que ofrece un marco de trabajo para planificar los procesos, los roles y las actividades más comunes, indicando los nexos entre ellos y los flujos de comunicación necesarios. Parte de la filosofía TIC tiene su base en los sistemas de calidad, como la serie ISO 9000, y los marcos de

trabajo de calidad total, como el EFQM. ITIL sustenta tales sistemas de calidad y ofrece una clara descripción de los procesos y las mejores prácticas en la gestión de servicios TIC. Los primeros libros de ITIL fueron publicados en el año 1989, y desde entonces estos han sido revisados y ampliados en diversas paulatinamente. En principio, ITIL consistía en un gran número de libros de forma que cada uno de los cuales describía un área específica de mantenimiento y operación de la infraestructura TIC. Estos fueron refundidos con posterioridad en un conjunto más homogéneo, de forma que las publicaciones que conforma ITIL en la actualidad y que definen sus procesos son: *Soporte del servicio, provisión del servicio, gestión de la seguridad, gestión de infraestructuras TIC, gestión de aplicaciones, planificación para implementar la gestión de servicios,* y *perspectiva del negocio*. Adicionalmente, existen otra serie de libros considerados como complementarios a los anteriores tales como: *Dirección y la organización,* y *gestión de activos software*. La estructura básica de ITIL se ilustra en la figura 3, en la que se refleja de forma clara cada uno de los libros de ITIL y su situación respecto al resto, además de la intención clara de ITIL en proveer una fuerte unión entre el negocio y la inversión en las TIC.

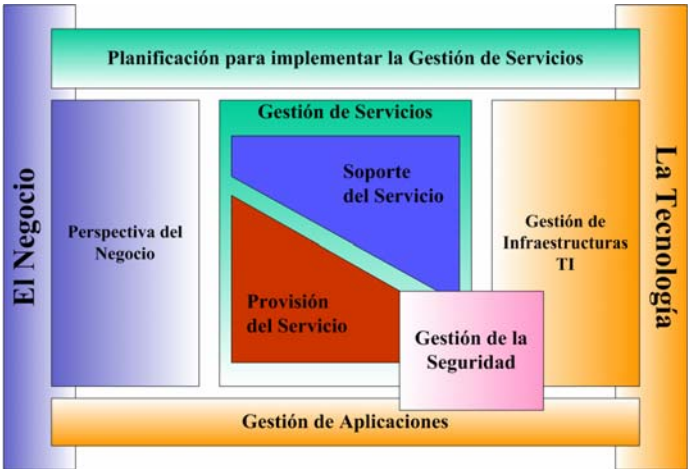


Figura 3. *ITIL*

Las TIC en Defensa

Las TIC en el Ministerio de Defensa español alcanza una complejidad y volumen que configuran unos de los contextos de actuación en este ámbito más ricos y a la vez complejos y problemáticos de abordar, y por ende más interesantes para los profesionales de las TIC. Esto es debido fundamentalmente a la multitud de áreas de competencia abarcadas por el Ministerio (*gestión de personal civil y militar, economía, armamento y material, logística, infraestructura, justicia, gestión hospitalaria, enseñanza, cultura y acción social*), las relaciones con otros entes como el Mando y Control de operaciones militares, tanto en el marco nacional como en las derivadas de su pertenencia a organizaciones internacionales –Organización del Tratado del Atlántico Norte (OTAN), Unión Europea Occidental (UEO), etc.,- la gran variedad de servicios comunes (*cartografía, informática, investigación operativa, psicología y estadística, etc.*), y su propia estructura y constitución, ya que además de las Fuerzas Armadas y el propio Órgano Central, tiene otros siete organismos autónomos (*Instituto Nacional de Técnica Aeroespacial* (INTA)*, Instituto Social de las Fuerzas Armadas* (ISFAS), *Instituto de la vivienda para las Fuerzas Armadas* (INVIFAS), *Gerencia de Infraestructura y Equipamiento de la Defensa* (GIED), *etc.*).

Desde un punto de vista tecnológico se ha venido trabajando tradicionalmente bajo diferentes arquitecturas, plataformas, estándares, procedimientos, metodologías, redes de comunicaciones, etcétera, lo que ha provocado numerosas deficiencias como dificultades de integración y coordinación, multiplicidad de esfuerzos, multiplicación de costes de los recursos, etcétera, avocado al Ministerio finalmente a establecer una política tendente a la optimización y mejora de los recursos

El exponente de mayor relevancia en esta nueva política, y que más se acerca a la visión que se expone a lo largo de este trabajo, es el *Plan Director de Sistemas de Información y Telecomunicaciones (PD CIS)*, que surge en 1999 y se aprueba en 2002, y para cuya elaboración el secretario de Estado constituyó el Grupo de Trabajo de Tecnologías de la Información y Comunicaciones. El objeto de este Plan, según se recoge en su resumen ejecutivo, es establecer la política del Ministerio de Defensa respecto de las TIC determinando las necesidades y definiendo y priorizando las acciones precisas para el cumplimiento de dicha política. Comprende, por tanto, aspectos de carácter técnico como son los sistemas e información, la plataforma informática, las telecomunicaciones y la seguridad correspondiente a los mismos, así como aspectos relativos a la estructura orgánica,

los recursos humanos y económicos, la concienciación, etcétera. Incorpora *50 objetivos* desglosados a su vez en *242 acciones* que se agrupan y subdividen a su vez el PD CIS en tres planes:

a) El Plan de Gestión, que trata aspectos relacionados con la estructura orgánica CIS del Ministerio, la adecuación presupuestaria, los recursos humanos, la concienciación y divulgación del Plan.

b) Plan de Arquitectura y Plataforma Tecnológica, que se centra en la Red Global de Telecomunicaciones del Ministerio (Sistema de Telecomunicaciones Militares, Red Privada Virtual para Voz y Red de Datos), en la Plataforma Informática que debe soportar a los sistemas de información, y en la seguridad correspondiente a ambos campos.

c) Plan de Obtención y Modernización de los Sistemas de Información, donde se establecen los sistemas que necesita el Departamento, se determina el proceso a seguir y se fijan sus prioridades.

La fecha de inicio para la ejecución de las acciones del Plan General fue el día 1 de enero de 2002, siendo su duración total cuatro años, desglosada en tres fases:

a) La primera fase, que abarca todo el año 2002, tiene como objetivo crear las bases del modelo.

b) La segunda fase, (año 2003), aborda la implantación de los modelos de plataforma y telecomunicaciones y algunos sistemas importantes.

c) En la tercera fase, (años 2004 y 2005), consolidadas las plataformas informática y la Red Global de Telecomunicaciones, se completan los sistemas de información definidos en el Mapa de Sistemas.

En resumen, podemos decir que las principales líneas estratégicas de la política CIS y que pone de manifiesto en el PD CIS se centran en los componentes que se muestran en la figura 4.

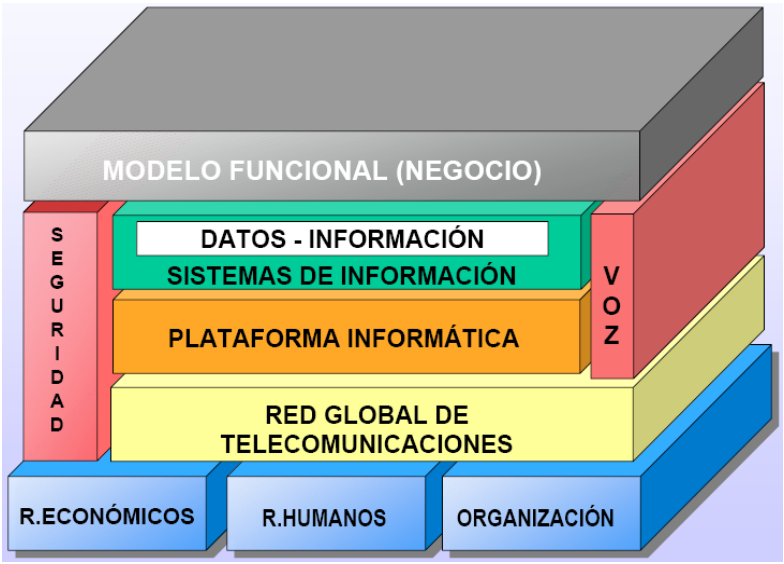


Figura4. *Modelo de Referencia CIS*.

Fuente: (Royo, 2005)

Hacia un modelo de gobierno y gestión de las TIC en Defensa

Con el objeto de abordar el estudio sobre la implementación de un modelo de gestión y en su extensión de gobierno de las TIC en Defensa, se abordaron dos frentes. Por un lado se realizó una revisión del PD CIS que se entendió era el que más se podía acercar a un planteamiento de este tipo con el objeto de valorar si incluía aspectos de gestión o de gobierno de las TIC, o en su defecto sentaba las bases correctas para que pudiese abordarse a posteriori y como una extensión del plan un modelo de gestión y gobierno adecuado. Por otro lado se realizo una encuesta detallada que abordaba desde aspectos genéricos de las TIC a aspectos referentes a la gestión de las TIC e ITIL, y que fue dirigida a los principales órganos de Defensa que se consideró podían aportar información relevante, con el objeto de detectar si se realizaban procesos de gestión de las TIC, se utilizaban marcos de actuación, estándares u otros, y el conocimiento e inquietud que de estos temas se tenia. Exponemos los resultados a continuación.

Respecto a la revisión del PD CIS, se observa que este se centra principalmente en lo que denominábamos “gestión de la infraestructura en el apartado «El gobierno y la

gestión de las TIC", P. 00 de este capítulo y que se reflejaba en la figura 1 P. 00. Si bien esto sitúa las TIC en Defensa en un estadio anterior a la gestión, en el que supuestamente están debatiéndose en la actualidad las organizaciones, hay que decir que dada la situación inicial de partida reflejada con anterioridad se considera que el PD CIS opta por la opción correcta, abordando y poniendo en orden la gestión de la infraestructura antes de abordar fases posteriores como modelos de gestión o gobierno de las TIC. Este planteamiento es consistente desde el punto de vista del ITGI (2003) que en su revisión y segunda edición del *Board Briefing on IT Governance*, un referente en la literatura sobre gobierno de las TIC, incorpora la gestión de los recursos como pieza clave para dirigir el resto de aspectos principales: el alineamiento de las TIC con los objetivos del negocio, la gestión del riesgo, la generación de valor, y la medición de resultados.

Por lo que respecta a la encuesta y entrevistas realizadas, se desprende que no se llevan a cabo implantaciones de modelos de gestión o gobierno de las TIC de manera específica, si bien se pone de manifiesto por un lado que los distintos responsables detectan la necesidad de aplicar este tipo de marcos de actuación, y por otro que marcos como ITIL son conocidos y se acogería con agrado la adopción del mismo.

En resumen podemos decir que tras la finalización del PD CIS, se estaría en disposición de abordar con éxito una siguiente etapa focalizada a la gestión y gobierno de las TIC, si bien se hecha en falta el dicho plan una mención o propuesta de extensión y de futuro en esta línea de manera explícita. Esto situaría a Defensa en el camino correcto, que con la implementación de otro plan de dos a tres años focalizado en estos aspectos podría situarle como referente en la Administración Pública española.

Abordar un plan de este tipo tiene riesgos importantes si no se realiza de la forma correcta. Esbozamos a continuación algunos aspectos a tener en cuenta para el diseño del plan. Dado el grado de externalización observado, es de vital importancia la selección de los socios tecnológicos prestadores de estos servicios. Nos encontramos ante un contexto puramente dominado por un proceso, el de la gestión de la seguridad, que debería desde un inicio extenderse al concepto de gestión del riesgo, lo cual hace muy particular la forma de abordar un modelo de gestión de las

TIC. Enfoques estandarizados centrados en la aplicación inicial de procesos de soporte como la gestión de incidencias y problemas no serían apropiados en este caso. Por otro lado, debe prestarse especial atención a las herramientas de soporte para implantar los procesos, en el sentido en que se debe prescindir completamente de ellas en las etapas de definición y diseño del plan, y no deben constituir más que un mecanismo que permita implementar los procesos que a corto, medio y largo plazo se decida implantar. Este es el principal error cometido por la mayoría de las organizaciones que basan sus decisiones en la herramienta y acaban amoldando el modelo a estas, cuando existen numerosas herramientas de gran calidad en el mercado (HP OpenView, Computer Associates, Remedy, Tivoli, etc.) que se adaptarán al modelo que se defina por lo que no debe preocupar a los gestores del plan. Otro aspecto de vital importancia es la formación interna. La selección desde el inicio de un conjunto de personas motivadas que realicen una formación adecuada en la materia, por ejemplo certificándose en ITIL, será uno de los factores claves para el éxito del plan. Respecto a marcos concretos a utilizar, se recomienda el diseño de un plan de gobierno de las TIC general aunque sea en su forma más sencilla, y que incluya el plan de gestión. Siguiendo un modelo como el que se representa en la figura 5 que aborda los cuatro dominios principales del gobierno TIC es posible abordar y extraer el subconjunto que formaría el modelo de gestión, y en la base de este, representado en la figura como el dominio de los mecanismos seleccionar los adecuados para la implementación.

Figura 5 *Dominios del Gobierno TIC*

Conclusiones

Parece irrenunciable y resulta obligatorio caminar hacia arriba en la escala de madurez en la gestión de las TIC, para alcanzar el mas alto grado de eficiencia en el gobierno de las TIC.

El camino hacia la meta nos lo señalan la empresas más vanguardistas y que han detectado la importancia de las TIC en los resultados de su negocio y han buscado y obtenido unos mejores resultados a través de una mejor administración de los recursos TIC.

Por lo que respecta a Defensa, al igual que otras organizaciones públicas, su objetivo no es la presentación de un balance de pérdidas y ganancias muy favorable, ni obtener una mejor cotización en Bolsa y así acreditar un incremento en el valor de la misma. La Administración Pública es juzgada por la eficiencia en el gasto del dinero público puesto en sus manos para que lo transforme en servicios al ciudadano. Precisamente en apoyo de este objetivo el buen gobierno de las TIC puede potenciar las capacidades humanas y materiales disponibles.

ITIL, por las razones que se expusieron en páginas anteriores se presenta como la metodología óptima en este momento para facilitar el buen gobierno de las TIC. Ahora bien, ITIL debe adaptarse y adecuarse a cada organización. Defensa es un compleja organización, donde convive el aspecto puramente administrativo similar al de otro Ministerio, y por lo tanto perfectamente mensurable y comparable su eficiencia con la de otros Ministerios de tamaño similar, con un aspecto específico y singular que es llamado mando y control donde a nuestro juicio el esfuerzo de adaptación es mayor pero que a su vez puede reportar mayores beneficios

¿Cómo abordar esta tarea? No se puede pasar de cero al infinito en un plazo corto y de salto. Se debe alcanzar primero una eficacia en la gestión de los servicios en grado bueno: planificación, provisión de servicios, disponibilidad y seguridad, para desde ahí pasar a un estadio superior como es el buen gobierno.

Consideramos como suficientemente aceptable el grado de eficacia actual en la gestión de las TIC alcanzado, por lo que estaríamos en el momento de iniciar la formación en ITIL de un equipo de personas, que desde dentro del órgano de

planeamiento de la política CIS (inspección CIS) pilotaran la implantación de ITIL dentro de la organización de Defensa. Implantación que debe hacerse despacio, paso a paso, ya que requiere una personalización del modelo ITIL a cada caso concreto, incorporando a todas las células CIS de los diferentes cuarteles generales y organismos dependientes del Ministerio.

BIBLIOGRAFÍA

Avison D., Jones J., Powell P., Wilson D. (2004): Using and Validating the Strategic Alignment Model. *Journal of Strategic Information Systems,* 13, 3, 2004 pp. 223-246.

Carr, N. (2003): *IT doesn't Matter*. Harvard Business Review, May.

Duffy, J. (2002). *IT*/Business alignment: Is it an option or is it mandatory? *IDC document*, 26831.

Guldentops, E. (2004). Governing Information Technology through CobiT. In *W. Van Grembergen (Ed.), Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.

Henserson, J.C., & Venkatraman, N. (1993). Strategic alignment: Leveraging Information Technology for transforming organizations. *IBM Systems Journal*, 32(1).

ITGI (2001). *Board briefing on IT Governance*. www.itgi.org.

ITGI (2005a). *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*. www.itgi.org.

ITGI (2005b). *CobiT 4.0*. www.itgi.org.

Luftman, J. (2002). Assessing Business-IT alignment maturity. In *Van Grembergen, Wim (Eds.), Strategies for Information Technology Governance*. Hershey, PA, USA, Idea Group Inc., p 99-128.

Peterson, R. (2003*). Integration strategies and tactics for Information Technology governance*. *In W. Van Grembergen (Ed.), Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing. pp. 37-80

Royo, C. (2005): *Plan Director de Sistemas de Información y Telecomunicaciones*. Seminario Administración electrónica en Defensa y Seguridad, Sociedad de la Información. Accesible al público en http://www.socinfo.info/.

Van Grembergen, W., De Haes S. and Guldentops E., (2004): Structures, processes and relational mechanisms for information technology governance: theories and practices, in *Strategies for Information Technology Governance*, book ed. by Van Grembergen, Idea Group Publ.

Weill P. and Ross J. (2004c): *IT Governance*. Harvard Business School Press.

CAPÍTULO TERCERO

OPERACIONES M ILITARES

Y ENTORNOS DE REALIDAD VIRTUAL

OPERACIONES MILITARES Y ENTORNOS DE REALIDAD VIRTUAL

Por José Miguel Castillo Chamorro

y Luis Pastor Pérez

Resumen

Los entornos de realidad virtual son una herramienta muy potente en todos los campos de aplicación. El núcleo base de estos entornos está formado por la simulación. Se trata de una ciencia interdisciplinar que podemos aplicar en muchas ramas del conocimiento. Uno de los campos en los que la simulación adquiere una especial significación es en el campo del entrenamiento, en el que se busca alcanzar una destreza por parte del usuario antes de llegar al sistema real. También puede ser utilizada para conseguir una mejora en la eficacia en el uso del sistema real mediante el estudio pormenorizado de la interactuación del usuario con el mismo.

Sólo se podrá conseguir una verdadera eficiencia de los sistemas de simulación cuando la elaboración del modelo que simula el sistema real se haya realizado con la suficiente precisión, admitiendo en su caso un margen de error aceptable que no produzca vicio en el entrenamiento. El plantear el desarrollo de un sistema de simulación no es por lo tanto un problema trivial, será necesario aplicar una metodología para generarlo. El uso de un procedimiento contrastado y científico nos permitirá construir un simulador con el objetivo de alcanzar un grado de entrenamiento eficiente que nos permita una mejora en las destrezas en el uso o ejecución del sistema real. Este trabajo presenta algunas clasificaciones de los simuladores y realiza un análisis de la metodología que puede aplicarse para el desarrollo de proyectos de simulación. Se describen las tecnologías usadas en los entornos de realidad virtual y finalmente se analizan las necesidades futuras dentro del mundo de la simulación aplicada.

Introducción

El papel de la simulación ha crecido significativamente en los últimos años y, prácticamente, en todos los países sin excepción. Sin duda se han producido

innovaciones tecnológicas importantes que han influido en el proceso, pero la causa fundamental de este aumento ha sido el convencimiento de que la simulación y la realidad virtual pueden aportar soluciones en diversos campos, desde la enseñanza y entrenamiento hasta la evaluación, la planificación y la toma de decisiones.

Gracias a las tecnologías actuales se puede conseguir aumentar el grado de entrenamiento y adiestramiento utilizando medios de simulación, que sin pretender sustituir el uso del sistema real permiten economizar el número de ellos y poderlos utilizar con un mayor grado de eficacia. Para la implantación de estas nuevas tecnologías se articulan los programas Investigación, Desarrollo e innovación (I+D+i) tanto en los organismos dependientes de la administración como en las empresas privadas. Estos programas intentan desarrollar un producto prototipo. Posteriormente los programas de adquisiciones permitirán, suministrar réplicas de los sistemas de simulación generados en un Programa I+D+i.

El enfoque que se expone a continuación surge como consecuencia del estudio de la utilización de sistemas de simulación en la última década, desde el convencimiento de que la unificación de criterios en la especificación de requisitos, permitirá obtener un mayor control del diseño y construcción del sistema, así como un mejor uso y mantenimiento de los mismos. Asimismo, el uso de una metodología facilitará el marco adecuado para generar la documentación entregable que evite que estos proyectos se conviertan en un sistema cerrado y con un ciclo de vida corto o de mantenibilidad inviable.

El presente estudio, no sólo plantea la problemática surgida de la implantación de forma paralela de nuevas tecnologías, sino que también intenta proponer soluciones atendiendo a la aplicación de estándares.

La simulación. Consideraciones generales

Pasado y presente

Podemos señalar tres aspectos clave en el actual desarrollo alcanzado por los simuladores, con respecto a un pasado aún próximo:

1. La capacidad de cálculo de los ordenadores.

2. La conectividad.

3. Los visuales.

Las *capacidades de cálculo* alcanzadas por los ordenadores actuales, junto con la disponibilidad de multiprocesadores que pueden ejecutar cálculos complejos en tiempo real, son el factor básico y primigenio que soporta, al menos en parte, a los otros dos. Sin este avance, que multiplica las posibilidades de todo tipo de los modernos simuladores, sería imposible concebir el actual estado del arte.

Respecto al segundo, la *conectividad* con otros sistemas, podemos asegurar que ya estamos en condiciones de crear escenarios de simulación complejos y distribuidos. La Arquitectura de Alto Nivel (HLA), que nos permite interconectar simuladores y sistemas reales instrumentados admitiendo la actuación humana e independientemente de su situación geográfica, es una realidad a nuestro alcance.

En cuanto al tercero, la creciente sofisticación de los *visuales*, quizá sea el aspecto que capta más la atención. La posibilidad del cambio del punto de vista y de la animación del mundo 3D, creado sintéticamente en tiempo real, nos ha introducido en un nuevo y auténtico mundo virtual de enormes posibilidades y horizontes ilimitados.

Otra consideración de interés en cuanto al pasado y presente de la simulación es que se ha producido una "*convergencia*" de esfuerzos con el campo de la experimentación que, hasta ahora, eran divergentes en cierto sentido.

ETAPAS TECNOLÓGICAS

De hecho, esta revolución de lo visual no ha sido, ni es, cosa de un día. Se han debido cubrir diversas etapas tecnológicas hasta llegar a formar una masa crítica suficiente para hacer bascular el campo de lo visual desde aquella otra era en que poco tenían que ver las imágenes generadas entonces con las de hoy en día.

Así, podemos destacar: *La aparición de técnicas de síntesis y de tratamiento algorítmico de la imagen*. Por una parte la imagen es calculable por ordenador con una calidad cada vez mayor que ha llegado a ser equivalente a la fotográfica; por otra parte no sólo el origen de las imágenes puede ser numérico, sino que

posteriormente su manipulación, tratamiento, almacenamiento, transmisión a distancia y aprovechamiento se puede realizar bajo ese formatos estándar.

La *posibilidad de interactuar en tiempo real con el escenario*. Esta técnica, banalizada por los juegos electrónicos, se ha generalizado en muchísimas aplicaciones y alcanza su máxima expresión en los simuladores de propósito específico. La capacidad de cálculo es suficiente para interactuar con el escenario en el momento mismo que se manifiesta la voluntad humana de modificarlo.

El sentimiento de inmersión dentro de la imagen, posible gracias a la disponibilidad de sofisticados sistemas de detección de acciones del operador y de generación de estímulos sensoriales (principalmente vista, oído y tacto). Entre ellos, hay que destacar las técnicas de *visualización estereoscópicas*. Estas no se deben considerar un mero truco, sino como auténticas técnicas con múltiples variantes que tienen la propiedad de cambiar de forma radical nuestra actuación en relación al escenario. Con ellas, ya no nos situamos meramente delante de la imagen, sino dentro de la misma imagen.

El desarrollo de técnicas que combinan *imágenes sintéticas y telecomunicaciones* ha dado lugar a nuevas formas de comunicación y de trabajo mediante la manipulación, a distancia, de escenarios virtuales incluyendo la posibilidad de operar de forma remota sistemas y dispositivos, permitiendo al operador recibir una información similar a la que tendría si estuviese realmente presente dentro del sistema.

Todo ello, en conjunto, nos permite, ya hoy en día, sumergimos en nuevos mundos virtuales. Unos mundos virtuales que son, en cierto modo, cada vez más y más reales.

Esta tecnología de lo visual ha tenido su impacto dentro del campo de la defensa y, en particular, en las diferentes etapas del ciclo de vida de los sistemas de armas.

La simulación en la ingeniería de sistemas

Las técnicas de simulación junto con las de visualización de modelos están permitiendo crear mundos virtuales sobre los cuales experimentar y en consecuencia *conocer* y *decidir* sobre su diseño, operación, formación, etc. para alcanzar un objetivo.

Es posible hacer una clasificación de las aplicaciones de las tecnologías de simulación en el mundo de los sistemas de armas a partir de las diversas fases por las que pasa durante su ciclo de vida:

- Análisis de alternativas.
- Prototipado e Innovaciones.
- Instrucción y adiestramiento.
- Formación.
- Operación de los sistemas (preparación y conducción de operaciones, optimización de doctrinas de empleo, monitorización de operaciones, etc.).

ANÁLISIS DE ALTERNATIVAS

El análisis de alternativas es una tarea típica durante la fase de definición de cualquier programa. Se trata de estudiar las diferentes alternativas que se presentan comparando, normalmente, prestaciones, tiempos y costes. Del resultado de dicho análisis dependerán decisiones cruciales, que tendrán un gran impacto en las fases posteriores del programa. Aunque los aspectos de tiempos y costes suelen ser tratados en forma numérica, en el apartado de prestaciones interviene cada vez más el aspecto visual.

PROTOTIPADO E INNOVACIONES

Entendemos por tal, el proceso en el que se genera, analiza y evalúa un diseño de ingeniería antes de ser construido. Los sistemas complejos requieren extensas simulaciones que generan una enorme cantidad de datos numéricos. Para comprenderlos se hace necesario el empleo de potentes estaciones gráficas que permiten visualizar e interpretar los resultados (visualización de datos). Los datos de la simulación son presentados en forma de imágenes o secuencias animadas con las que los diseñadores pueden buscar características o fenómenos relevantes en el diseño tales como la ergonomía, detección de fallos, etc.

Su ventaja se mide en términos de menor tiempo en el diseño, menor tiempo de aprendizaje, mejor comprensión de los sistemas complejos y una reducción del coste al ser menor el número de prototipos físicos a construir.

INSTRUCCIÓN Y ADIESTRAMIENTO

Una de las "lecciones aprendidas" en los últimos conflictos bélicos ha sido el escaso tiempo de reacción ante la amenaza de los sistemas de armas enemigos. En consecuencia, algunas de las "acciones de configuración" que conforman el futuro deseado deben ser tomadas cuantos antes y se concretan en:

- Necesidad de medios de alerta con mayor alcance y con mayor precisión.
- Necesidad de Sistemas de Mando y Control que decidan la mejor defensa en el menor tiempo posible.
- Necesidad de medios de comunicación rápidos y fiables.
- Necesidad de una instrucción y adiestramiento tal que haga casi *instintiva* cualquier respuesta.

Esta última acción se deberá concretar en un realismo adecuado de las simulaciones y en una *inmersión* de los alumnos en ellas con continuas evaluaciones y reciclajes, hasta alcanzar una gran destreza en el manejo de los sistemas.

Una mención especial en este campo debe dedicarse al papel que juegan las tecnologías de *realidad virtual***.** La posibilidad de definir interactivamente una articulación, grados de libertad de cada objeto, su interacción con otros dentro de la escena, la integración con el *hardware-software* de sonido cuadrafónico y con el *hardware-software* táctil está permitiendo aproximarse a escenarios que son un fiel reflejo de la realidad.

FORMACIÓN

En el campo de la formación es necesario mencionar los sistemas multimedia, es decir, sistemas que son capaces de manejar sonido, imagen, texto, vídeo y gráficos de una manera coherente e integrada. En la definición de multimedia encontramos

algunas de las tecnologías que se aplican en el campo de la realidad virtual: sonido, imagen, etc.

La posibilidad de crear animaciones, en tiempo no real, grabarlos en *CD-ROM* y el posterior acceso a través de un equipo informático de manera selectiva pueden tener una gran aplicación no sólo en la formación, sino también el proceso de mantenimiento y apoyo logístico de los sistemas de armas.

OPERACIÓN DE LOS SISTEMAS

Los estados mayores de los ejércitos modernos emplean herramientas de modelización y simulación sofisticadas en las que constantemente ejecutan misiones en un ordenador para determinar el mejor curso del ataque.

Un ejemplo de simulación visual lo encontramos en la *Planificación asistida por ordenador* de despliegues de artillería antiaérea (0). Con ella se puede determinar la ruta más peligrosa de aproximación a un punto vital de modo que se minimice la función riesgo ya sea por estar fuera del alcance de las armas o de los elementos de detección propios. Además, la posibilidad de visualizar en una animación el aspecto con que se vería el escenario de confrontación, es una ayuda inestimable en la preparación de la operación, figura 1.

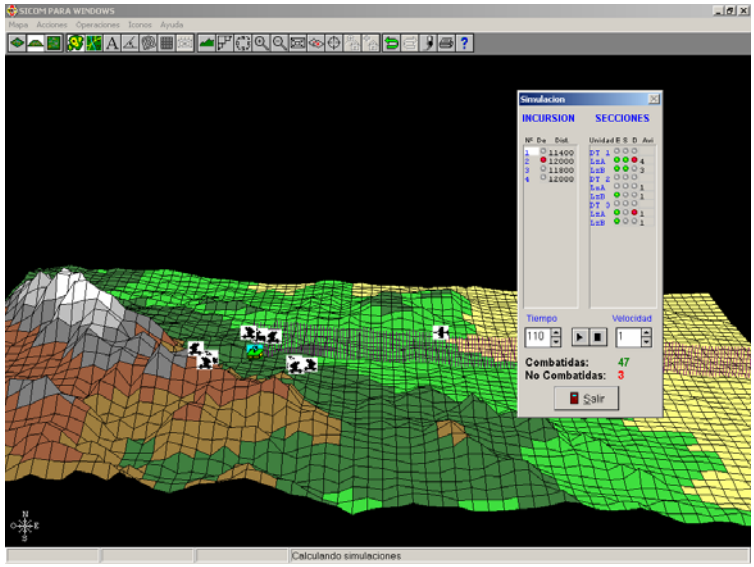


Figura 1.

Conceptos

Antes de intentar clasificar los diversos simuladores es necesario destacar algunos conceptos, que dentro del marco de este trabajo son importantes:

- *Entrenamiento*: aquellos aspectos de la enseñanza que requieren del aprendizaje y repetición de destrezas básicas.

- *Adiestramiento*: aquellos aspectos de la enseñanza que además de permitir destrezas básicas permite inferir reacciones del usuario y su interactuación con el sistema.

- *Simulación*: conjunto de acciones, actividades y medios, que tienen por objetivo facilitar y perfeccionar la enseñanza y posibilitar las evaluaciones del personal, mediante la representación fiel del sistema real y de las situaciones derivadas de su funcionamiento y empleo.

Desde el punto de vista de la enseñanza, el entrenamiento, y el adiestramiento, se entiende por simulación la representación de un sistema real y su utilización para la adquisición de conocimientos, destrezas, y experiencias, así como su evaluación.

Clasificaciones

Algunas de las clasificaciones actuales se exponen a continuación (0). Ninguna de ellas es excluyente por lo que un simulador en concreto podrá incluirse en cualquiera de ellas dependiendo de la taxonomía utilizada.

Atendiendo al tipo de representación que proporciona:

- *Simulación virtual*: proporciona imágenes de apariencia real de medios, terreno y situaciones, mediante el uso de la informática.

- *Simulación en vivo*: permite la interactuación con los sistemas reales mediante la sensorización de parte de los mismos. Se simula el ambiente restante mediante técnicas similares a las usadas en simulación virtual.

- *Simulación constructiva*: permite el entrenamiento de equipos y va encaminada a facilitar la toma de decisiones, bien en un equipo aislado o con otros simuladores de igual o menor nivel interconectados.

Según el ámbito de aplicación de la simulación, se definen tres niveles:

- *Nivel 1*: individual.
- *Nivel 2*: equipo. Conjunto de individuos que realizan tareas comunes o complementarias.
- *Nivel 3*: sistema. Conjunto de equipos que interaccionan bajo un objetivo común.

Atendiendo a su finalidad, se pueden clasificar en:

- *Entrenadores*: equipos que, por sí mismos o asociados, reproducen características de un elemento y exigen la ejecución de las tareas necesarias en el orden adecuado para el correcto funcionamiento del aspecto que se quiere instruir. El entrenador está diseñado para sistematizar la práctica de operaciones rutinarias; no se aplica con finalidad de toma de decisiones ni interactúa con el operador en ese ámbito.
- *Simuladores:* son la representación física de un elemento que reproduce las características fundamentales del mismo, incluidos sus efectos, de forma virtual o real. Suelen incluir medios informáticos que, al ejecutar los correspondientes programas, actúan como lo haría el equipo simulado al ser empleado. El simulador interactúa con el operador de forma que transmite a éste en tiempo real el resultado de sus acciones.
- *Simuladores de adiestramiento para la toma de decisiones*: se utilizan para el adiestramiento de equipos mediante el uso de herramientas informáticas que establecen un escenario virtual. Pueden usarse en tiempo real o en una escala temporal adaptada a las necesidades del usuario, permitiendo, incluso, detener la acción. Contemplan los efectos de las decisiones, así como la influencia de factores diversos que pueden ir modificándose durante el transcurso del ejercicio simulado.

Atendiendo a la necesidad de respuesta:

- *Simuladores con respuesta en tiempo real o tiempo útil*: son los más extendidos dentro del campo del entrenamiento. Es necesario ajustar la respuesta del

simulador y en especial sus interfaces hombre-máquina al objeto de obtener resultados o interacciones en tiempo útil en los mismos intervalos en los que los proporcionaría el sistema real.

Por contraposición, podemos clasificar el resto de los simuladores como aquellos que no requieren producir una respuesta dentro de un margen determinado, por lo que no necesitarán del uso de sofisticados mecanismos de tiempo real.

Clasificación según tecnologías empleadas

Las clasificaciones expuestas en el apartado anterior están íntimamente relacionadas con la funcionalidad que desarrollan, sin embargo y con la intención de analizar en detalle las tecnologías que se aplican dentro de los diferentes simuladores se propone la siguiente taxonomía de los elementos que intervienen en la simulación:

- *Elementos de simulación analítica*: comprenden todos aquellos módulos de cálculo o algorítmicos que son el verdadero motor de la simulación. Entre ellos se encuentran las subrutinas que generan datos, fusión de datos, movimiento de móviles y sus intersecciones con el terreno, etc.

- *Elementos de simulación virtual*: engloban todos aquellos procedimientos que permiten la representación realista del escenario donde se desenvuelve la acción. Dentro de este grupo se encuentran los modelos tridimensionales tanto del terreno como móviles que interaccionan o están sujetos a éste, módulos de generación del terreno tridimensional, sonidos cuadrafónicos, elementos sinápticos, etc.

- *Elementos de simulación inteligente*: entre estos elementos se encuentran aquellas subrutinas especiales que intentan introducir una lógica en el simulador que emule el conocimiento aprendido por el elemento humano, tales como lógica inteligente de móviles, evaluación inteligente de acciones, interfaces inteligentes para la elección del nivel de uso del simulador, reconocimiento de voz, reconocimiento de imagen, etc.

- *Elementos de simulación de equipos operativos*: en este apartado se encuadra todo dispositivo físico que emule un equipo o material orgánico, tales como plataformas, asientos de conducción, volantes, elementos de transmisión radio, prismáticos, brújulas, y equipo en general, etc.

Beneficios iniciales

La inversión inicial en la implantación de sistemas de Simulación se promueve por las enormes ventajas que se aportan. Entre las que se encuentran las siguientes:

- *De índole económico*: se produce un considerable ahorro, debido a que la simulación no consume elementos caros como combustibles, sin gasto del sistema real o consumo de los elementos simulados, etc.

- *De instrucción y adiestramiento*: la simulación permite adquirir buena experiencia a un número elevado de sujetos quienes, ante el elevado coste de los ejercicios reales, apenas podrían realizar una pequeña porción de ellos. Por otra parte, el entrenamiento exige la realización de ejercicios bajo diversas condiciones, incluso las de uso en condiciones extremas que no se dan de una manera habitual. La simulación puede provocar estas situaciones con la verosimilitud necesaria, con las variantes que se requieran, y pudiendo ser repetidas el número de veces que se necesite, añadiéndole los efectos que simulen su realización con condiciones adversas de todo tipo, durante el día o la noche, ajustando la velocidad del ejercicio a juicio del instructor, deteniendo, repitiendo o modificando el ejercicio y registrando todos los detalles y actuaciones para su análisis posterior.

- *De seguridad*: el uso del sistema real puede en algunos casos constituir un riesgo para las personas, instalaciones y equipos, no sólo los directamente implicados en los ejercicios, sino también para los de un entorno no muy precisable. La sustitución de una parte de los ejercicios por simulación, no sólo reducirá el riesgo, sino que además permitirá que los ejercicios u operaciones reales sean más eficaces, puesto que se llegará a ellos con un entrenamiento previo de una muy alta calidad.

- *De aspecto ecológico*: otro problema relacionado con el uso de los sistemas reales especialmente en el campo militar es el ecológico, que a su vez puede

desencadenar otros de tipo político. También este problema se atenúa o se suprime por análogas razones a las de seguridad, mediante el uso de sistemas de simulación.

El arte del modelado

Es necesario definir más concretamente lo que entendemos por modelo, pues es un concepto muy usado dentro del campo de la simulación y de otras ciencias (0, 2 y 11). Un modelo es una simple descripción o representación parcial de la realidad. Debido a la dificultad de alcanzar una réplica exacta en cuanto al funcionamiento de la realidad exterior, la ciencia selecciona los aspectos o magnitudes que le interesa tener en cuenta y que constituyen las variables del modelo. En el caso de un modelo físico, se tratará de reproducir estos parámetros con la mayor precisión, intentando hacer una copia exacta de la realidad. En el caso de un modelo formal o matemático, la ciencia tratará de elaborar leyes generales expresables matemáticamente, que relacionen estas magnitudes y que permitan que algunas variables puedan ser consideradas como parámetros de entrada, o datos del problema. Las restantes ostentarán el carácter de variables de salida, o solución del problema.

De una forma genérica podríamos clasificar los modelos como:

- *Modelos materiales*: son modelos que intentan de una forma física reproducir con exactitud la realidad. Son objetos físicos palpables, por ejemplo puentes a escala reducida, que permitan comprobar su resistencia sometiéndolos a esfuerzos a escala, etc.

- *Modelos formales*: son modelos que pretenden ajustarse al comportamiento de la realidad mediante un desarrollo matemático, son denominados modelos conceptuales.

Desde un punto de vista científico podremos encontrar otros tipos diferentes de modelos:

- *Modelos estáticos o dinámicos*: según que el tiempo se considere explícitamente o no como una variable del modelo.

- *Modelos de tiempo continuo o discreto*: en función de que la variable tiempo, considerada por ambos, cambie de forma continua o a saltos.

- *Modelo determinista o estocástico* (aleatorio): en los primeros no se considera el azar o la probabilidad, mientras que en los segundos esta característica tiene suma importancia.

- *Modelos cualitativos o cuantitativos*: cuando las variables que se consideran, toman un valor entre un número finito de valores o entre un número infinito.

El proceso mediante el cual se deduce el modelo del sistema que se está estudiando puede describirse como un *arte* intuitivo. Cualquier conjunto de reglas para desarrollar modelos tiene una utilidad limitada y solamente puede servir como una estructura o planteamiento sugerido. Al intentar hacer explícito el proceso de modelado, tratamos de sistematizar la intuición y experiencia de nuestros predecesores. Lamentablemente, toda la investigación científica se divulga o comunica en forma de una reconstrucción lógica de eventos, la cual trata de justificar los contenidos producidos. Esta reconstrucción lógica suele tener muy poca relación con la forma en que se realizó la investigación.

El planteamiento para la construcción de modelos tiene como base la elaboración y el enriquecimiento continuo. Se comienza con un modelo muy simple, para intentar continuar con modelos más elaborados que reflejen la situación compleja con más claridad. La analogía o asociación con estructuras previamente desarrolladas parece tener una función importante en la determinación del punto inicial para este proceso de elaboración y la mejora del modelo. El proceso de elaboración y enriquecimiento implica una interacción constante y un proceso de retroalimentación entre la situación del mundo real y el modelo. Existe una influencia recíproca entre la modificación del modelo y una confrontación con los datos generales. Conforme se prueba y se intenta validar cada versión del modelo, se produce una nueva versión que conduce a realizar otras pruebas y a la revalidación.

Siempre y cuando el modelo sea computacionalmente manejable, el analista puede aspirar a un nuevo enriquecimiento o complicación de las suposiciones. Cuando éste se vuelve intratable o no puede resolverse, se recurre a la simplificación y a la abstracción. Por tanto, el arte de modelado consiste en la habilidad para analizar un

problema, resumir sus características esenciales, seleccionar y modificar las suposiciones básicas que caracterizan al sistema, para posteriormente enriquecer y elaborar el modelo hasta obtener una aproximación útil.

La naturaleza evolutiva de la construcción de modelos es inevitable y deseable; por tanto, no deberíamos pensar en un proyecto como el diseño de un único gran modelo. Conforme se logran los objetivos y se resuelven los problemas, se identifican nuevos problemas o se desea mayor realismo, lo cual conduce a las revisiones del modelo y a mejores soluciones. Este proceso de empezar con un modelo simple y luego hacerlo más elaborado y enriquecerlo también tiene aplicaciones positivas para el proceso de implementación. La velocidad y la dirección de la evolución dependen de dos factores principales: el primero es la flexibilidad inherente del modelo y el segundo la relación del constructor del modelo con el usuario del modelo. Al trabajar conjuntamente durante el proceso de evolución, el constructor del modelo y el usuario de éste pueden crear un ambiente de mutua confianza y entendimiento que les ayudará a asegurar que el resultado final cumpla con los objetivos, las metas y los criterios importantes.

El arte de modelar pueden dominarlo quienes poseen la habilidad necesaria de ingenio, organización y perspicacia, así como un amplio conocimiento y análisis de los sistemas y fenómenos que tratan de modelar. No existe un procedimiento rígido acerca de cómo se aborda. No hay fórmulas mágicas para decidir qué debería incluirse en el modelo en forma de variables y parámetros, relaciones descriptivas y restricciones, y el criterio para el juicio de la efectividad. Es importante señalar, que nadie resuelve el problema, sino que se resuelve el modelo del problema que se ha construido. Este concepto ayuda a conservar el modelo y el arte del modelado en una perspectiva adecuada.

El aprendizaje humano. Un sistema adaptativo

Al usar la simulación como herramienta de aprendizaje, es necesario tener en cuenta quién es el sujeto pasivo sobre el que se van a aplicar estos sistemas. Es por tanto importante analizar el proceso de aprendizaje del ser humano, al objeto de definir con qué precisión ha de generarse el modelo que se asemeje al sistema real.

El motor del proceso de aprendizaje radica en el cerebro humano y se alimenta de las señales que recibe de sus órganos sensoriales (0 y 0).

Si nos hacemos una pregunta genérica en la que nos planteemos cómo de preciso ha de ser un modelo de entrenamiento para que no se produzcan vicios en el proceso de aprendizaje, la respuesta será que dependerá del sistema real que pretendemos emular. Valga para comprender este punto un par de ejemplos sencillos. Supongamos que construimos un simulador de conducción de un vehículo y la palanca de cambios la situamos dos centímetros a la derecha de la posición de la palanca original. Si nos preguntamos si este error puede producir vicio en el entrenamiento, podríamos concluir que en un porcentaje muy elevado de los casos la naturaleza adaptativa del cerebro humano permite salvar este error, permitiendo aplicar en el sistema real las mismas habilidades aprendidas en la fase de entrenamiento en el sistema de simulación. No ocurriría así si hubiéramos cometido el error de colocar la mencionada palanca en el lado contrario (mano izquierda), pues este cambio afectaría a la lateralidad y sería difícil reproducir los movimientos aprendidos con la mano derecha.

Nos podríamos plantear igualmente cuál ha de ser la precisión y latencia admisible en un visual que represente un escenario virtual. Nuevamente la respuesta dependerá del sistema real que pretendamos simular. En un simulador de una aeronave en el que el piloto debe reaccionar en fracciones de segundo, no pueden permitirse latencias que interaccionen con el proceso de reacción del piloto. Sin embargo, estas mismas latencias podrían admitirse en simuladores para reconocimiento de objetivos o para corrección del tiro. En este caso la naturaleza adaptativa del cerebro humano permitiría al individuo, en su interacción con el sistema real, desarrollar las habilidades aprendidas en el sistema de simulación, sin modificación alguna en su conducta.

La realidad virtual. Tecnologías de aplicación

Conceptos básicos

El término de Realidad Virtual (RV) resulta algo contradictorio, ya que proviene de la unión de dos términos opuestos: *real* y *virtual*. Podríamos definirlo como la rama de la tecnología que estudia la creación de estímulos sensoriales sintéticos, como

imágenes, sonido y sensaciones táctiles, que puedan ser percibidos de forma realista por el hombre. A diferencia de las imágenes y sonidos comúnmente generados por ordenador, la realidad virtual trata de generar sensaciones *interactivas*, es decir, que respondan ante las acciones del observador e *inmersivas*, que ocupan todo el entorno visual y sensorial de una persona, facilitando así el sentimiento de integración en el mundo virtual que la rodea.

Se puede discutir si la realidad virtual es realmente una nueva tecnología, ya que aprovecha muchas de las ideas que se han utilizado en las últimas décadas para el diseño de simuladores avanzados. Sin embargo, existen razones para considerarlo así, ya que existe una gama de equipos y software relativamente amplia que permite emplear una misma metodología y entorno de trabajo para la resolución de problemas de índole muy diversa. Sus orígenes se puede considerar que se remontan a la década de los años sesenta, en la que Ivan Sutherland planteó muchas de las ideas y soluciones que se utilizan actualmente, y a la aparición en la década de los años setenta de los simuladores de vuelo, que alcanzaron rápidamente una amplia difusión.

Como se ha mencionado previamente, hay tres aspectos que resultan característicos en lo que se ha dado en llamar realidad virtual: la interacción, la inmersión y el realismo. La interacción, porque para que estos sistemas sean útiles habitualmente resulta imprescindible permitir que el usuario actúe y modifique el entorno ficticio que le rodea. La inmersión, porque evita que el operador perciba cualquier sensación externa al entorno virtual, con lo que se aumenta la credibilidad de las situaciones generadas en el sistema. Por último, el realismo, porque cuando se logra un adecuado nivel, se consigue que el sistema entero resulte creíble.

Para conseguir niveles óptimos de inmersión y realismo hace falta primeramente ser capaz de captar al máximo la atención del usuario, ya que siempre será difícil aislarle completamente de los estímulos externos; si se es capaz de conseguir este propósito se puede permitir incluso un menor nivel de realismo, lo que puede resultar en grandes economías (hay que señalar que para conseguir mejoras relativamente pequeñas en realismo suele ser necesario realizar inversiones prohibitivas). Para mejorar la inmersión resulta útil cuidar la sensación “propioceptiva” que recibe el usuario, sensación íntimamente ligada a las consecuencias que sus propios

movimientos o acciones generan, y que debe percibir una relación directa entre sus actos y los resultados que capta a través de sus sentidos.

En general, se suele distinguir entre realidad virtual no inmersiva e inmersiva. En el primer caso, se suministra al usuario información textual, auditiva, gráfica (incluso gráfica tridimensional), etc., pero el grado de aislamiento del entorno real que rodea al usuario es escaso. En el segundo caso, se sumerge verdaderamente al operador dentro de los estímulos generados por el sistema, a partir de un grado de aislamiento mucho mayor de él respecto al entorno real.

Realidad virtual y realidad aumentada

Otro concepto que es interesante mencionar es el de *Realidad Aumentada* (RA). Si bien la RV persigue introducir al usuario en un mundo ficticio a base de reemplazar lo que percibe, la realidad aumentada persigue introducirle en un mundo (también ficticio), pero en el que conviven elementos reales y virtuales. Entre los primeros y más relevantes ejemplos de mezcla de imágenes reales con datos sintéticos están los sistemas denominados como HUD *(Head Up Display*), en los que se proyecta información que se superpone a la que ve el observador a través de una pantalla que permite el paso de la luz (y por tanto, la visión del operador más allá de la pantalla).

En general, en estas aplicaciones el usuario puede interaccionar con los objetos que percibe, de los cuales una parte son reales y otros sintéticos. En el diseño de estos sistemas sigue siendo importante fomentar la sensación de inmersión y captar la atención del operador, así como cuidar la sensación propioceptiva mencionada anteriormente, que en este caso incluirá objetos reales con los que el usuario podrá interaccionar como en cualquier actividad habitual, y objetos virtuales, que deben ser modificados de acuerdo con las acciones y movimientos llevados a cabo por el operador.

Para esto hace falta una etapa relativamente compleja, en la que se deben alinear cada uno de los objetos ficticios con los que pueblan el mundo real. La complejidad de esta última labor radica en la necesidad de disponer de información precisa sobre el entorno tridimensional en el que se halla el usuario y sobre su posición, teniendo en cuenta que el entorno real puede sufrir variaciones debidos tanto a la acción del

propio usuario (aunque sea solamente debido a su desplazamiento dentro de la escena), como a las de otras personas o entidades que puedan actuar sobre el medio. La utilidad de los sistemas de realidad aumentada radica en la posibilidad de añadir información útil para un operador que debe realizar una labor concreta, así como la posibilidad de incorporar elementos reales cuyo modelado puede ser difícil o imposible.

Componentes básicos para los sistemas de realidad virtual y aumentada

Para el diseño y puesta a punto de sistemas de realidad virtual y aumentada necesitamos dedicar especial atención tanto a la generación de estímulos como a la interfaz hombre-máquina. Para lo primero será necesario disponer de los adecuados modelos del comportamiento de los elementos involucrados, con el fin de poder simular el comportamiento de todo el sistema. Para lo segundo, necesitaremos dispositivos de entrada y salida que puedan cubrir las tareas a desempeñar en el funcionamiento de todo el conjunto, incluyendo tanto las sensaciones que debe percibir el operador como las acciones que éste pueda realizar para modificar su entorno. En los siguientes apartados se describen todos ellos.

MODELIZACIÓN DEL COMPORTAMIENTO

En el apartado «La simulación. Consideraciones generales», P. 00 se ha tratado ya este tema, por lo que no se va a entrar en profundidad. Solamente es preciso reseñar que, además de la necesidad de disponer de modelos matemáticos que puedan describir la dinámica del sistema o subsistemas que integran el mundo virtual, es necesario realizar algunas tareas adicionales, como pueden ser las siguientes:

- Detección de colisiones e interferencias entre los diferentes objetos que intervienen en la simulación, con el objeto de calcular los efectos que cada uno de ellos genera en los demás. Esta etapa es esencial, ya que la ocurrencia de interpenetraciones entre objetos en movimiento penaliza fuertemente el nivel de realismo de cualquier simulación. Como comentario adicional, la detección de colisiones en tiempo real entre objetos deformables o que puedan estar sujetos a modificaciones importantes de su geometría (cortes, roturas, etc.) no es un problema trivial.

- Síntesis de reacciones a la interacción entre elementos. Las colisiones e interferencias entre objetos producen reacciones que hay que calcular y representar, generando todos los estímulos visuales, auditivos, táctiles, etc. asociados a estos procesos.

En general, tan importante como la precisión de los algoritmos utilizados es que la latencia global del sistema (medida como el tiempo que transcurre desde que el usuario toma una acción hasta que esa acción es representada) no introduzca distorsiones importantes en el proceso de simulación. Por lo tanto, un aspecto destacable es la implementación de los algoritmos a fin de trabajar en tiempo real (como se señaló anteriormente, la latencia admisible y por tanto la noción de *tiempo real* depende de la naturaleza del sistema y la utilidad que se le quiera dar)

DISPOSITIVOS DE ENTRADA

El tipo de aplicación condiciona habitualmente la naturaleza y número de los dispositivos de entrada, ya que se tienen que adaptar a los requisitos específicos de las tareas a realizar por el operador. Atendiendo a su funcionalidad, es posible clasificar a los dispositivos de entrada dentro de las siguientes categorías:

- *Rastreadores (dispositivos de seguimiento* o trackers). Su función es permitir la que quizás es más básica de las acciones encaminadas a fomentar las sensaciones propioceptivas del operador: el cambio de perspectiva asociado a los cambios de posición que se producen cuando él mismo se mueve dentro del área de trabajo. La ubicación de algún elemento de rastreo en algún punto cercano a los ojos del usuario permite que a partir de los datos de posición y orientación que éste envíe al sistema, se calculen las transformaciones geométricas asociadas al nuevo punto de vista del operador. Estas transformaciones se utilizarán posteriormente para conocer cómo y en qué posición se deben representar cada uno de los objetos que conforman el universo virtual. Las principales características de los rastreadores que pueden resultar relevantes para una aplicación determinada son su precisión, resolución, repetitividad y área de trabajo. Hay varios tipos de rastreadores disponibles comercialmente. Entre las tecnologías disponibles se pueden mencionar las siguientes:

1. Rastreadores mecánicos. Suelen basarse en una cadena cinemática movida por el operador. El conocimiento de la posición de cada junta permite determinar la posición del operador. Son rápidos e inmunes a las interferencias, pero son engorrosos.

2. Rastreadores electromagnéticos: se basan en la medida del campo generado por un emisor, detectado mediante un conjunto de receptores. Son pequeños y ligeros. No se ven afectados por oclusiones, aunque precisan calibración y se ven afectados por la presencia de materiales ferromagnéticos o campos electromagnéticos.

3. Rastreadores ópticos: pueden tener espacios de trabajo grandes, aunque se ven afectados por oclusiones. Son inmunes a interferencias.

4. Rastreadores ultrasónicos: se basan en la medida del tiempo de recepción de una señal que recorre diferentes caminos. Sensibles a oclusiones, figura 2.

Figura 2.

– *Dispositivos de navegación*. Existe una relativamente amplia variedad de elementos que han sido diseñados para permitir la navegación del usuario en

entornos tridimensionales. Estos periféricos, que de alguna manera pueden verse como una generalización de dispositivos 2D como el ratón, pueden ser de muy diversos tipos (como el *microscribe* de immersion). Pueden incluso estar basados en rastreadores como los descritos previamente, ya que estos equipos nos devuelven la posición espacial de cualquier objeto unido al mismo.

- *Dispositivos gestuales*. Igualmente, existen también una gran variedad de dispositivos que permiten capturar los gestos o movimientos que realiza el operador. Dependiendo del tipo de aplicación, se pueden utilizar desde los guantes dirigidos a la adquisición de movimientos de la mano, hasta los trajes utilizados en captura de movimiento para animación. Respecto a los guantes, posiblemente los más utilizados en entornos de realidad virtual, se pueden mencionar sistemas como el *Pinch Glove* de Fakespace o el *CyberGlove* de Immersion. Es frecuente que se requiera una calibración para adaptarse a cada usuario, especialmente cuando se necesita un cierto grado de precisión en la medida de la posición de los dedos figura 3.

Figura 3.Guante para captura de gestos

Dispositivos de salida

Al igual que en cualquier sistema que genera información para nuestros sentidos, la importancia de los dispositivos de salida en las aplicaciones de realidad virtual es

enorme: aunque los algoritmos de modelado, detección de colisiones, síntesis de gráficos, realimentación háptica o de esfuerzos, etc., sean precisos, realistas y eficientes, una mala calidad del sistema que genere los estímulos sensoriales afectará negativamente a la opinión final que del sistema obtengan sus usuarios. Por otra parte, como en la mayoría de los campos en ingeniería, pequeños aumentos en las prestaciones llevan aparejados aumentos mucho mayores en los precios. Por tanto, a la hora de diseñar una aplicación de este tipo es muy importante buscar una adecuada relación precio-prestaciones. En consecuencia, se han desarrollado un gran número de equipos que se quieren adaptar a todas las necesidades y presupuestos; en los siguientes apartados se dará una breve relación de las principales opciones que existen en la actualidad. Para ello, se agruparán según los sentidos hacia los que se dirigen, fundamentalmente los de visión y tacto-fuerza.

Dispositivos de visualización. Al hablar de dispositivos de visualización hay que tener en cuenta dos aspectos: la generación de la salida gráfica y la proyección de las imágenes generadas. Respecto al primer punto, los últimos años han visto un aumento espectacular del volumen de ventas de videojuegos, lo que ha espoleado el progreso técnico y la reducción de precio de este tipo de sistemas. Posiblemente el hecho más característico es que en una década se ha conseguido pasar de sistemas gráficos basados en estaciones y servidores de altas prestaciones y muy elevado precio a equipos basados prácticamente en hardware de consumo, de prestaciones comparables y precio mucho más reducido. Si a esta reducción de coste se le suma el progreso producido previamente en los algoritmos de síntesis de gráficos 3D con calidad fotorrealista junto con la posibilidad actual de integrarlos en procesadores específicos de bajo coste y altas prestaciones, se puede concluir que la invasión paulatina que estamos experimentando de la informática gráfica en todos los aspectos de nuestra vida no ha hecho más que comenzar.

En cuanto a la proyección de las imágenes sintetizadas, los últimos años han visto también un aumento significativo en la calidad, variedad y precio de estos equipos. Los más relevantes son:

1. Equipos personales no inmersitos.

2. Sistemas de visualización inmersiva personales.

3. Sistemas de visualización inmersiva para grupos.

Respecto a los equipos personales no inmersivos, podemos encontrarnos con sistemas de muy diferentes tipos. Al monitor gráfico habitual de los ordenadores actuales se le pueden realizar desde hace tiempo modificaciones para convertirlo en estereoscópico, por ejemplo mediante la utilización de *gafas activas* que bloquean la visión de cada ojo de forma alternativa en sincronismo con la pantalla. De esta forma, si refrescamos la imagen con una frecuencia de 100 Hz, 50 imágenes pueden ser destinadas al ojo izquierdo, y otras 50 al derecho (y la disponibilidad de imágenes diferentes para cada ojo es la base para la consecución de la visión estereoscópica). El desarrollo y comercialización de monitores *autoestereoscópicos* está en sus inicios, pero es de suponer que el impacto que tendrán en el mercado de alto consumo permitirá su rápido abaratamiento y difusión.

También se pueden considerar como equipos personales no inmersivos, aunque puedan ser compartidos por dos o tres usuarios simultáneamente, a otros sistemas como las *ventanas virtuales* o los *pupitres de trabajo*. En las primeras, la incorporación de rastreadores y mandos de navegación a una pantalla LCD (*Liquid Crystal Display*) permite que el usuario pueda “asomarse” al mundo virtual, cambiando de perspectiva según mueva la pantalla y actúe sobre los mandos.

En los segundos, se presenta al usuario una imagen 3D proyectada sobre un pupitre o mesa de trabajo, sobre la que puede trabajar en cualquier tipo de aplicación.

Figura 4.

Dentro de los equipos de visualización inmersiva personales hay que destacar los típicos *cascos* o *HMDs*, dispositivos de visualización que se montan sobre la cabeza del operador. Sus principales inconvenientes son los derivados de la incomodidad que representa llevar montado un equipo grande, pesado y unido mediante cables al ordenador. Sin embargo, representan una solución económica y han sido bastante utilizados. La posibilidad de añadirles cámaras de video que capten la imagen del escenario situado delante del observador para mezclarlo con imágenes de objetos sintéticos les permite ser adaptables a las necesidades de los sistemas de realidad aumentada.

Por último, dentro de los dispositivos para visualización inmersiva para grupos, se pueden mencionar las *cuevas y anfiteatros de realidad virtual*, que son de los dispositivos más completos disponibles en la actualidad. Una *cueva* consiste en una sala cuyas paredes y suelo son pantallas donde se proyectan imágenes estereoscópicas generadas por ordenador. Dentro de dicha sala, los observadores se encuentran rodeados de imágenes que pueden representar cualquier escena que el computador desee mostrarle, pudiendo incluso caminar dentro de la escena. Gracias al uso de la tecnología de visión estereoscópica, el sistema puede incluso mostrar objetos que parecen estar en el interior de la cueva o más allá de sus paredes. El sistema se completa con un rastreador para actualizar el punto de vista del observador en la escena y un equipo de sonido envolvente.

Los anfiteatros utilizan pantallas curvas para situar a un grupo de observadores sentados en un patio de butacas dentro de una proyección envolvente, de forma similar a como lo hacen los cines 3D o los planetarios. Frente a las cuevas, presentan como ventaja la posibilidad de ser utilizados simultáneamente por un mayor número de espectadores, si bien las posibilidades de interacción de estos resultan fuertemente disminuidas.

Dispositivos hápticos para la realimentación de esfuerzos y tacto. Para la generación de sensaciones táctiles se emplea una gran variedad de dispositivos, denominados hápticos (del griego *hapthai*, tacto). Después de los de visualización, los dispositivos que generan sensaciones táctiles o de esfuerzos son los más empleados en las aplicaciones actuales de RV. Su principal problema reside en que para crear este tipo de sensaciones se precisan determinados elementos (electromecánicos,

hidráulicos, etc.) que son caros, voluminosos y pesados. Sin embargo, el grado de inmersión que proporcionan estos dispositivos a veces resulta sorprendente. Entre los más utilizados se pueden mencionar los guantes y los brazos articulados, figura 5.

Figura 5. Guantes para realimentación de tacto y fuerza

Un *guante de realidad virtual* consiste en un dispositivo al que se han acoplado una serie de sensores de flexión sobre cada una de las articulaciones de la mano, lo cual le permite al ordenador conocer la postura de la misma. Adicionalmente, se le pueden añadir elementos que produzcan fuerzas o vibraciones, de forma que den al operador la sensación de tocar objetos virtuales. La utilización de *exoesqueletos*, o conjuntos de articulaciones externas, permite aplicar la fuerza en la articulación deseada, figura 6.

Respecto a los brazos articulados, el más conocido es el *phantom* de Sensable. Consiste en una cadena cinemática que puede ser movida por el usuario libremente en el espacio que queda ante él. La existencia de motores eléctricos y codificadores en cada articulación permite que, según el objeto virtual con el que estamos trabajando, el brazo oponga una resistencia que depende del punto en el que coloquemos el extremo del brazo. Gracias a él, podremos seleccionar y arrastrar objetos dentro de una escena tridimensional, tocar objetos o simular la interacción de un útil dentro de un escenario virtual formado por varios objetos. Con él podemos saber también si un objeto es suave o rugoso, duro o blando, y si está pegado al suelo o se puede empujar.

Existen también otros planteamientos para la generación de estímulos táctiles y de esfuerzos, como pueden ser los basados en la utilización de sedales que se mantienen en tensión mediante la acción de poleas controladas por motores eléctricos y codificadores angulares. En ellos, la posición del punto de aplicación de la fuerza junto con las características del escenario simulado definen las acciones que deben tomar el conjunto de motores y poleas para actuar sobre el operador, que percibe una sensación táctil en correspondencia a la simulación que se está llevando a cabo, figura 7.

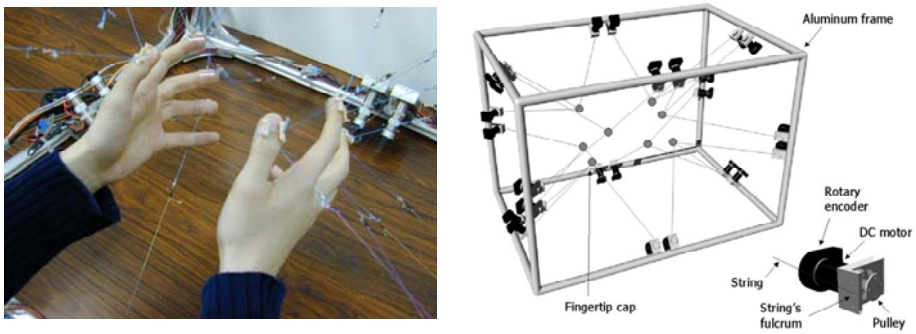


Figura 7. Dispositivo basado en poleas y sedales (*spider 8)*

La generación de estímulos olfativos y de gusto se encuentran en un punto menos avanzado que el resto de sensaciones. La generación de sensaciones olfativas generalmente se ha resuelto mediante una serie de pulverizadores controlados por ordenador, cargados con diversas esencias. Presenta dos grandes problemas: sólo puede aportar los olores cargados en el pulverizador, y no es sencillo hacer desaparecer un olor una vez aplicado. Los problemas son similares para el sentido del gusto, añadiendo la incomodidad del sistema de aportación de estímulos dentro de la boca.

Respecto al sonido, no se ha entrado en detalle en este capítulo dado que los equipos para generación de sonido en entornos de realidad virtual no presentan diferencias físicas importantes con los empleados en otras aplicaciones. Las diferencias pueden radicar más bien en su control dentro de la simulación, incluyendo los retrasos relativos que se puedan añadir a la generación de sonidos en cada altavoz, dado que persiguen el objetivo de mejorar la sensación de inmersión del operador dentro del entorno virtual.

Resumiendo, el uso de técnicas y dispositivos de realidad virtual permite crear interfaces entre el hombre y la máquina muy adecuados para realizar tareas de entrenamiento y simulación. Primero porque permite recrear de forma realista situaciones de cierto riesgo reduciendo la posibilidad de accidentes, por ejemplo mediante los ya clásicos simuladores de vuelo. Además, la comunicación entre el hombre y la máquina se realiza por medios mas intuitivos, al permitir la transmisión de sensaciones táctiles, por ejemplo, y poder el ordenador encargado de realizar la simulación recoger la respuesta refleja ante dichas sensaciones.

Metodología para la generación de proyectos de simulación

Una metodología puede definirse, en un sentido amplio, como un conjunto de métodos o técnicas que ayudan en el desarrollo de un producto *software*, tal como señala Rumbaugh (0).

> “Una metodología es un proceso para la producción organizada, empleando una colección de técnicas predefinidas y convenciones en las notaciones. Una metodología se presenta normalmente como una serie de pasos, con técnicas

y notaciones asociadas a cada paso. Los pasos se organizan normalmente en un ciclo de vida consistente en varias fases de desarrollo.”

Para desarrollar un sistema de simulación, aplicable a nuestro entorno, debemos recurrir a un procedimiento, que basado en el método científico (0), permita asegurarnos la consecución de los objetivos. La experiencia sugiere que la planificación de proyectos de simulación requiera un procedimiento que conste de los pasos o etapas siguientes:

- Formulación del problema:
    - Definición de los objetivos que pretendemos resolver.
- Definición del sistema.
    - Determinación de los límites o fronteras, restricciones y medidas de efectividad que se usarán para definir el sistema que se estudiará.
- Preparación de datos:
    - Identificación de los datos que el modelo requiere y reducción de éstos a una forma adecuada.
- Formulación del modelo:
    - Reducción o abstracción del sistema real a un diagrama de flujo lógico.
- Estimación de parámetros:
- Detección y determinación de los parámetros que intervienen en el modelo.
    - Traducción del modelo. Descripción del modelo en un lenguaje aceptable tanto para el ordenador como para el fin que se requiera.
    - Evaluación. Encontrar un nivel aceptable de confianza de modo que la inferencia obtenida del modelo respecto al sistema real sea correcta.
    - Experimentación. Ejecución del programa de simulación para generar los datos deseados y efectuar el análisis de sensibilidad.

- Implantación-documentación:

- Registro de las actividades del proyecto y los resultados así como de la documentación del modelo y su uso.

Con los pasos anteriores se supone que el problema de la simulación se resuelve de una forma adecuada. Puede que no sea la forma más efectiva ya que la simulación es un planteamiento aproximado o un último recurso para resolver problemas. En realidad, es cierto que cuando un problema puede reducirse a un modelo simple y resolverse analíticamente, la simulación no es necesaria. Deben investigarse todas las herramientas disponibles para manejar cada problema y optimizar entre los resultados y el costo.

Debido a que es necesario y conveniente ajustar el procedimiento al problema y no al contrario, las decisiones referentes a qué herramienta o método usar deben seguir la formulación del problema. La decisión de usar la simulación no debe considerarse como irrevocable. Conforme se obtienen más datos y se entiende más el problema, la validez del uso de la simulación debe revaluarse. Ya que es necesario el uso de ordenadores y de complicados procedimientos dentro de los proyectos de simulación, el coste asociado es casi siempre alto comparado con la resolución de un pequeño problema analítico.

El coste probable y el tiempo de realización de un proyecto de simulación siempre deberán compararse con el valor del resultado que probablemente producirán. Si la simulación en ordenadores es capaz de producir soluciones significativas y relativamente fáciles de interpretar para un problema dado, a un coste aceptable comparado con cualquier otro procedimiento, entonces debemos utilizarla como procedimiento de resolución del problema. Si estas condiciones no se satisfacen, debemos cuestionarnos si existe otra alternativa más provechosa.

La decisión de emplear o no la simulación como técnica para resolver un problema en particular, no constituye en sí una tarea sencilla. Más aún, en el análisis final tal decisión se apoya en tres grandes consideraciones: la aplicabilidad, el coste y la simplicidad. Los pasos de una simulación y sus relaciones se muestran en el diagrama de flujo de la figura 8.

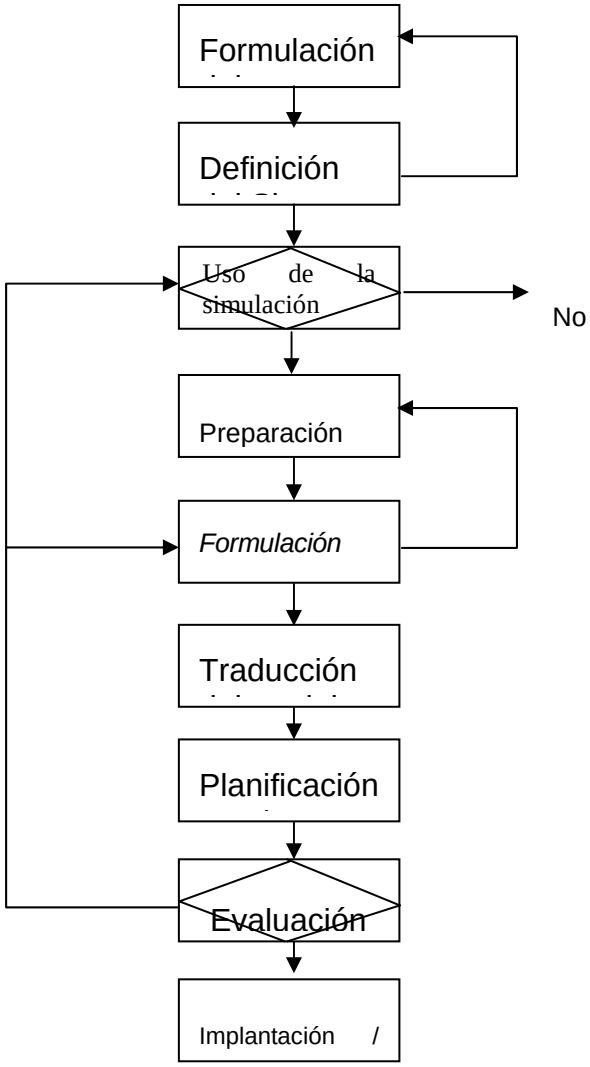


Figura 8. Esquema de la metodología

Formulación del problema

Para encontrar una solución óptima o aceptable para un problema, primero se tiene que saber cuál es el problema. Inicialmente y en muchos casos, no se pueden identificar los propios problemas correctamente. Se sabe que hay un problema, pero no se puede identificar el problema real. Por lo tanto, un proyecto de análisis de sistemas usualmente empieza mediante la realización de un estudio del sistema bajo el control de quien toma las decisiones. El equipo de investigación debe entender y articular un conjunto de objetivos y metas aplicables.

La experiencia indica que la formulación de un problema es un proceso continuo a lo largo del estudio. Continuamente, la investigación genera nueva información referente a restricciones, objetivos y alternativas. Dicha información debe usarse periódicamente para actualizar la formulación y la definición del problema. Es necesario, y en primer lugar, definir claramente los objetivos de nuestro proyecto, antes de hacer cualquier intento encaminado a plantear la realización del mismo. Con toda seguridad, encontraremos que la exposición original del problema varía considerablemente de su versión final, ya que la formulación del problema es un proceso secuencial que generalmente requiere una reformulación continua y progresiva y un refinamiento de los objetivos del experimento durante su realización.

Definición del sistema

Una parte importante de la formulación de problemas es la definición del sistema a estudiar. Todos los sistemas son, en sí, subsistemas de otros sistemas más grandes. Por tanto, debemos especificar el propósito y las restricciones bajo las cuales creamos nuestra abstracción o modelo formal.

El primer paso para definir el sistema que deseamos estudiar es efectuar un análisis de las necesidades del entorno. Después de haber especificado las metas y objetivos del estudio y definido los límites del sistema, procedemos a reducir el sistema real a un diagrama de flujo lógico o a un modelo estático. Deseamos construir un modelo del sistema real que no simplifique demasiado el sistema al punto donde el modelo se vuelva trivial (o peor aún, engañoso) y que no contenga demasiados detalles de manera que se convierta en algo mal hecho o sumamente costoso.

Por consiguiente, deben tomarse dos decisiones importantes antes de comenzar a trabajar con cualquier proyecto de simulación. En primer término, hay que decidir los objetivos del proyecto y en segundo lugar, es necesario decidir el conjunto de criterios para evaluar el grado de satisfacción al que deba sujetarse el experimento a fin de que cumpla nuestros objetivos.

Preparación de datos

Cada estudio implica recopilar datos. La recolección de datos, por lo general se interpreta como recogida de números. El analista de sistemas debe preocuparse por los datos referentes a las entradas y salidas del sistema que estudia así como de la información acerca de los componentes del sistema y de las interconexiones o relaciones entre ellos (0).

Existen tres posibles fuentes para generar información:

a) Datos Históricos o series de tiempo.

b) Opiniones de expertos.

c) Estudios de Campo.

Las series históricas o de tiempo, que han sido previamente limpiadas de irrelevancias, son datos útiles y de rápido procesamiento para convertirlos en información. La desventaja es que su grado de detalle puede estar limitado y, por lo tanto su utilidad, es solamente parcial. La opinión de expertos es generalmente información subjetiva, a veces carente de detalle, pero es una manera efectiva y rápida de obtener cierto tipo de información complementaria.

Los estudios de campo son el método más eficiente, aunque más costoso y largo en su elaboración. Esta estrategia requiere el operar con el sistema real al objeto de obtener los mencionados datos en estados diversos y cambiantes.

Formulación del modelo

La formulación de los modelos lógicos o matemáticos consiste en tres pasos:

1. Especificación de los componentes.

2. Especificación de las variables y los parámetros.

3. Especificación de las relaciones funcionales.

La formulación del modelo matemático de cualquier sistema es más un arte que una ciencia (0). El proceso de observar algún sistema en la realidad, formular una o más hipótesis relativas a su funcionamiento y reducir éstas a un nivel de abstracción que permita la formulación de un modelo matemático que describa su comportamiento, no constituye un proceso directo. Aunque tener un conocimiento completo del sistema que se va a analizar, al igual que cierta habilidad y pericia en las operaciones matemáticas, se consideran condiciones necesarias para la construcción de modelos matemáticos validos, en ningún caso es una condición suficiente, toda vez que la construcción de modelos matemáticos acertados depende en gran parte de:

- La *experiencia* del analista.

- Los procedimientos de *prueba y error*.

- Una considerable *intuición*.

Parece apropiado enumerar ciertas dificultades potenciales que el constructor de modelos afrontará en sus esfuerzos por describir el comportamiento de los sistemas, mediante la técnica de modelos matemáticos:

1. Quizá sea imposible cuantificar o medir ciertos tipos de variables que afectan el comportamiento del sistema.

2. El número de variables a considerar al describir un sistema dado, posiblemente exceda de nuestra capacidad de control del problema.

3. Podemos desconocer algunas de las variables exógenas significativas que afectan la salida del sistema.

4. Es factible que desconozcamos alguna de las relaciones entre las variables exógenas y las endógenas de nuestro sistema y sea, además, imposible obtenerlas.

5. Las relaciones entre las variables que afectan el comportamiento del sistema son en muchos casos tan complejas que no pueden expresarse como una o más ecuaciones matemáticas.

Una vez definido el modelo será preceptivo el traducirlo a un lenguaje de programación adecuado. Hoy en día los lenguajes más usados son los denominados de carácter genérico, los cuales permiten la programación de interfaces gráficas adecuadas y son adecuados para la interconexión a través de redes.

Evaluación

La evaluación es un proceso de carácter iterativo, que permite llevar al modelo a un nivel aceptable de confianza que permita asumir que el proceso de simulación ha sido correcto. Es imposible probar que cualquier simulador es un modelo que refleja exactamente al sistema real. En su lugar lo que realizamos es un proceso de validación de los resultados obtenidos de la simulación. Por tal motivo, es más importante la utilidad operativa del modelo que la semejanza en su estructura con el sistema real.

Interconexión del sistemas de simulación

Un nuevo objetivo planteado en los últimos años es el de conseguir un adiestramiento conjunto de equipos de trabajo a través de la simulación. Para ello es necesario tener como base los simuladores que aportan un adiestramiento individual, y posteriormente que esos simuladores tengan capacidad de interconexión y transmisión de sucesos que permitan interactuar en el mismo entorno. Para satisfacer la necesidad de interconexión de simuladores se ha diseñado por la comunidad científica la HLA de alto nivel, que establece la filosofía de transmisión de eventos entre simuladores.

La versión conceptual de esta arquitectura de interconexión se recoge en el IEEE 1516, así como el *Stanag* 4574. Por otro lado, el desarrollo técnico de las plantillas a las que hace referencia el mencionado acuerdo está en continua evolución pues son el elemento que define los atributos, cualidades e interacciones de los objetos que intervienen en la simulación, así como el formato en el que van a ser transmitidos. Estas plantillas aunque normalizadas en versiones, van ampliándose con la inclusión

de las necesidades de una extensa gama de simuladores que con el paso del tiempo se incorporan a la comunidad internacional de medios de simulación.

Un primer error en la generación de simuladores en la que nos encontramos ha sido el pensar que la HLA era poco menos que una arquitectura *plug and play*, y que era suficiente con dotar de esta capacidad individual a los simuladores que se generen, para posteriormente poder montar el complejo puzle del adiestramiento conjunto de unidades. Aquel que llevado por un impulso de innovación tecnológica pueda pensar que con plasmar en los requisitos de un simulador, la necesidad de interconexión con otros simuladores mediante la HLA, sin más especificación, conseguirá que éste se conecte en un futuro con otros simuladores, se equivoca rotundamente. Es por tanto necesario establecer en los requisitos previos de construcción de cualquier simulador, la definición del conjunto de simuladores con los que se pretende interactuar. De esta manera estaremos definiendo la federación de simuladores con los que se trabajará en ejercicios de adiestramiento conjunto.

Por otro lado, y a tenor de la evolución de las plantillas que desarrollan la mencionada arquitectura habrá que fijar cuál es la versión de las mencionadas plantillas sobre la que se va a generar el complejo entramado de objetos y atributos a compartir, pues el trabajar con versiones diferentes muy probablemente impida o dificulte la correcta interactuación.

Por último, habrá que definir la operativa de funcionamiento conjunto en cuanto al sentido táctico de los ejercicios, es decir, habrá que diseñar la naturaleza de esos ejercicios, al igual que se definen los de entrenamiento individual. Será necesario designar el simulador sobre el que recae la responsabilidad de apertura y cierre del ejercicio así como de su evaluación conjunta.

Otra interpretación, no equivocada desde el punto de vista técnico pero no por ello exenta de dificultades, ha sido la de plantear la interconexión entre simuladores de distinto nivel. El incluir en una misma federación simuladores que trabajen en entornos de tiempo diferentes es técnicamente posible, pero implicaría una doble problemática. Por un lado, los simuladores de nivel superior actúan en entornos discretos de tiempo, de manera que simplifican o engloban las acciones de niveles inferiores, permitiendo la realización de ejercicios en plazos de tiempo aceptables,

sin dilatarse en esperas de ejecución. Por otro lado, el manejo de datos y resultados a alto nivel es de magnitud diferente al de los simuladores individuales.

Por ejemplo, para un simulador de carro, las fases o estados en la simulación de un combate de encuentro son básicas para el entrenamiento, mientras que para un simulador de entidad superior como por ejemplo batallón, la información que debe manejar es de entidad muy diferente y posiblemente sólo necesite conocer el resultado final del enfrentamiento. Para poder compaginar los objetivos de ambos simuladores será necesario insertar un *software* de abstracción de datos que permita traducir la información a la magnitud que trabaja el simulador de nivel superior. Es evidente que la inserción de ese módulo complicará alguno de los dos simuladores, pero deberá hacerse sin perder ninguna de las prestaciones para las que cada simulador en su individualidad ha sido diseñado.

Por otra parte, si ambos simuladores trabajan conjuntamente en una federación deberán adecuar la base de tiempos en la que trabajan; es decir, tendrán que sincronizar los entornos discretos de tiempo o trabajar ambos en tiempo continuo, lo que implicará tiempos de espera e inactividad en el simulador de nivel superior.

El futuro de los entornos de realidad virtual

para entrenamiento en Defensa

Hacia una estandarización en el desarrollo de simuladores

La unificación de criterios en el uso de una metodología para el desarrollo de proyectos de simulación permitirá reducir costes de desarrollo y simplificar los costes asociados al mantenimiento de los simuladores. Por otro lado, al objeto de evitar duplicidad en productos de simulación desarrollados con funcionalidad similar en diferentes simuladores y atendiendo a la clasificación tecnológica expuesta anteriormente, es preciso unificar esfuerzos garantizando la reusabilidad de esos elementos.

En resumen, los aspectos más destacables que hoy en día merecen ser punto de reflexión, se centran en la aplicación de una metodología de desarrollo de simuladores, la reutilización de componentes y la interconexión de simuladores.

Reusabilidad de componentes

Es evidente que después de una fase inicial de implantación de tecnologías de simulación en la que se hayan seguido desarrollos paralelos de diversa índole, se hayan producido duplicidades en la obtención de módulos de naturaleza similar y en ocasiones idéntica, por no existir un estándar común de uso.

Con vistas a crear una nueva generación de simuladores dentro del sector de defensa, es necesario mejorar el aspecto de aprovechamiento de recursos por parte de los programas que comiencen, reutilizando aquellos elementos con los que ya se cuenta y aplicando estándares que se han generado o seguido en proyectos anteriores. Indudablemente esta medida tendrá repercusión directa en el abaratamiento de los costes del desarrollo.

La experiencia actual en el diseño de simuladores permite identificar aquellos elementos con capacidad de poder ser reutilizados en otros desarrollos, así como aquellos que han propuesto un estándar y que sería provechoso el mantenimiento del mismo.

Dentro de los recursos reutilizables son de destacar tres elementos base:

1. Módulos de carácter analítico.

2. Terreno en 2D Sistema de Información Geográfica (GIS).

3. Modelado tridimensional: terreno, modelos de objetos.

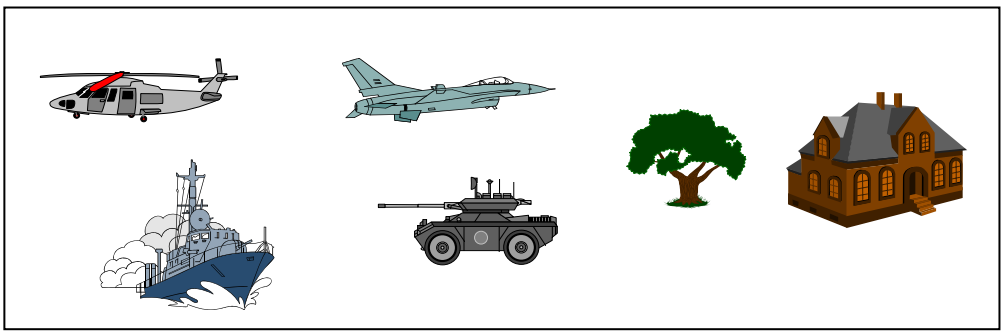
Son múltiples y variados los *módulos de carácter analítico* que se han generado en el desarrollo de simuladores y que estando bien documentados bajo una metodología de generación de *software*, permitirán su adaptación e inclusión en nuevos simuladores. Es evidente que los costes de adaptación son generalmente menores que los de un desarrollo nuevo, ya que la algoritmia que sirve de solución lógica del problema ya se ha concebido, comprobado e implementado.

Dentro de la amplia gama de módulos reusables directamente o tras un proceso de adaptación se encuentran en la actualidad, módulos de movimiento de móviles para la generación de trayectorias, ajuste de curvas para la generalización de datos tales

como tablas de comportamiento ante eventos, módulos de cálculo en meteorología, etc.

La *representación del terreno en dos dimensiones* apoyándose en un GIS con la intención de confeccionar un ejercicio dentro de un simulador es una práctica común en casi todos los simuladores. Es por tanto el GIS un elemento común estandarizable y reusable, que basándose en datos obtenidos por organismos de las administración permite la representación en dos dimensiones del terreno, sin textura real y a la escala que el sistema informático permita.

Cada vez está más extendida la necesidad de generación de *modelos tridimensionales*, que dentro de un escenario virtual conforman la escena en la que se desarrolla un ejercicio de simulación. Analizando la problemática del modelado tridimensional, podemos observar que se han abordado simultáneamente el modelado de una gran variedad de objetos 3D y que seguramente se han repetido por lo que probablemente su coste se haya duplicado o en ocasiones incluso triplicado, figura 9.



En lo concerniente al terreno en tres dimensiones, es necesario precisar que éste se ha generado atendiendo a las necesidades inherentes a cada simulador por lo que en general, pierden su característica de reusabilidad. No obstante, los elementos que se han utilizado para la confección de este modelo tridimensional son perfectamente utilizables en otros desarrollos. Entre estos datos se encuentran los modelos digitales de terreno, con diversos pasos de malla, y las fotografías tomadas desde satélite y en vuelo a baja cota que permiten obtener la textura geoespecífica con la que vestir el modelo. Una estandarización en el uso y procedimiento de datos

para la generación de entornos tridimensionales abarataría los costes de desarrollo y mantenimiento en las próximas generaciones de simuladores, figura 10.

Imagen virtual de terreno

Explotación de simuladores

Una cuestión importante en el desarrollo de los simuladores es la de su ubicación. Hoy en día los simuladores que se desarrollan incorporan de manera inherente la necesidad de un espacio y de una infraestructura que en la mayoría de los casos y debido a necesidades de funcionalidad y de buen funcionamiento de los equipos informáticos implicará una adaptación de locales o una nueva construcción. Los costes que acarrean cualquiera de las dos soluciones no están contemplados en el desarrollo del simulador; circunstancias por las cuales será necesario generar la solicitud de apoyo logístico necesario, con la suficiente antelación que permita disfrutar del simulador sin retrasos y procurando evitar instalaciones provisionales que podrían encarecer el coste del producto. Como puede observarse, esta contingencia no se contempla en ninguna metodología de desarrollo.

Antes de que el simulador esté preparado para su explotación y uso, se deberá haber diseñado el esquema de mantenimiento del mismo. A los sistemas de simulación se les puede aplicar los mismos niveles de mantenimiento que a los sistemas informáticos con hardware y software asociados. Un primer y segundo nivel de mantenimiento encargado de realizar las tareas propias de cualquier sistema informático en lo referente a tareas técnicas de funcionamiento diario, actualización de datos, copias de seguridad, y apoyo al correcto uso y obtención de las máximas prestaciones del simulador. De esta relación de tareas se deduce la necesidad de tener personal a pie de obra, dedicado al simulador o simuladores integrados en un centro de simulación. La contratación externa de este servicio aumenta considerablemente los costes de mantenimiento, que hay que tener en cuenta a la hora de hacer un análisis coste-beneficio de un proyecto de simulación.

Las dos cuestiones planteadas, infraestructura y personal de mantenimiento, aunque no directamente relacionadas con el desarrollo de cualquier simulador son de una importancia básica para la consecución de los objetivos para los que fue diseñado; pues podría darse el caso de finalizar un excelente desarrollo y no poder ponerlo en funcionamiento por falta de infraestructura o personal para su explotación.

Una vez instalados los sistemas de simulación, y bajo la supervisión del personal adecuado, es necesario planificar su uso de forma eficiente por la entidad receptora. De esta manera podrá rentabilizarse la inversión efectuada.

Necesidades futuras

Muchas son las expectativas de mejora en los simuladores que se desarrollen a corto y medio plazo. Partiendo del principio de que a consecuencia de la aparición del problema se suceden las múltiples soluciones tecnológicas, se puede resumir que a raíz de los problemas encontrados a la hora de materializar ciertas soluciones es preciso avanzar en el uso de nuevas tecnologías.

A continuación se enumeran alguna de las expectativas de mejora dentro de los entornos de realidad virtual.

Los *visuales* generados en plataformas de realidad virtual, aunque con una velocidad de refresco de escena suficiente, carecen de una resolución que permita

simular con precisión a las de la observación real. Por ejemplo, un observador experimentado puede identificar un móvil a una distancia comprendida entre 1.500 y 2.000 metros. Con la resolución de los visuales actuales, en los que se emplean apenas una decena de pixeles para representar un móvil a esa distancia, es imposible que ese observador experimentado sea capaz de identificar el mismo objetivo que reconoce en un escenario real. Cabe esperar a corto plazo, una mejora en la resolución visual que solvente el problema enunciado.

Imagen virtual generada en el simulador SIMACA

Para conseguir que el simulador capte los datos con los que se genera una determinada acción, se diseñan *interfaces* con el sistema que a veces no son todo lo naturales que deberían y pueden producir un vicio en la instrucción sobre el sistema real. Un ejemplo claro en la mayoría de los simuladores actuales es el de facilitar la entrada de datos al simulador colocando una interfaz materializada en un ordenador con un formulario de datos, cuando en el sistema real el usuario transmite el resultado de su acción vía radio o teléfono mediante el lenguaje natural. Es de esperar por tanto, una mejora e implantación de sistemas de reconocimiento de voz que eliminen o hagan más naturales las interfaces hombre máquina que se implementan en nuestros simuladores, figura 12.

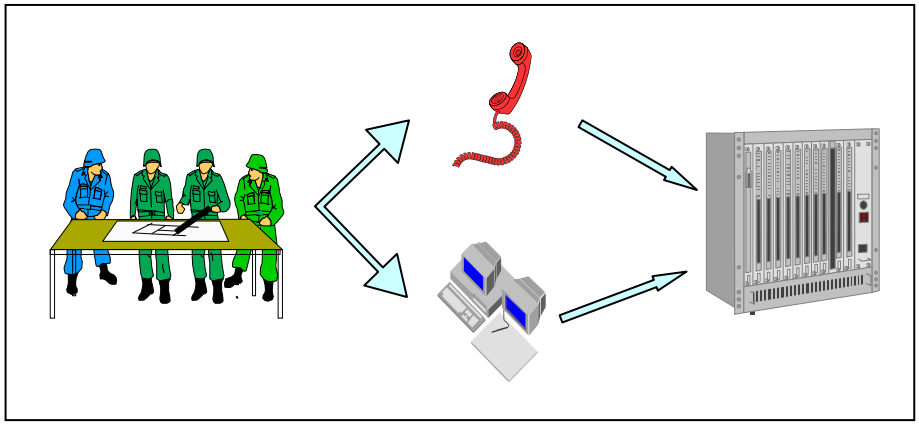


Figura 12. Mejora de los interfaces hombre-máquina

El *comportamiento* de algunos *objetos* dentro de la escena simulada se realiza de manera guiada e interactiva durante la ejecución del ejercicio, o bajo parámetros preestablecidos e inamovibles a la hora de generarlo. Se podría obtener un entrenamiento más real si el objeto tuviera reacciones no dependientes de la acción del instructor, sino que reaccionase de forma autónoma con la lógica generada por el conocimiento de expertos en este tipo de eventos. Sería pues el propio simulador el que produciría las reacciones basándose en una lógica extraída de un sistema experto.

Ante la necesidad de no incrementar las plantillas en los centros que dispongan de sistemas de simulación con el cometido de facilitar su *uso y mantenimiento*, es necesario que el propio sistema de simulación incorpore procedimientos de autoarranque en virtud de las capacidades y deseos del usuario que intente mejorar su entrenamiento o adiestramiento. Será pues necesario hacer sencilla la utilización del cualquier simulador, aplicando sistemas inteligentes de ayuda al usuario. Igualmente, es necesario mejorar la automatización de chequeos y detección de averías que simplifiquen el mantenimiento del sistema de simulación.

Por último, un aspecto que es común a cualquier simulador es el de la evaluación del ejercicio que realiza el usuario, según unos parámetros preestablecidos. La evaluación que hasta ahora se incorpora en la mayoría de los simuladores es una

evaluación de tipo objetivo, en el que se valora una respuesta por comparación con los datos inicialmente cargados en el simulador y teóricamente correctos. Este tipo de evaluación es adecuada en simuladores de nivel bajo, pero en aquellos simuladores que desarrollan complejos ejercicios en los que intervengan varios puestos, el instructor necesita una ayuda mayor basada en una evaluación subjetiva que proporcione más datos sobre cómo mejorar el adiestramiento en su conjunto. El instructor necesita una valoración sobre la naturaleza del fallo, incluso si es debido a un error humano inferir las causas del mismo (falta de instrucción elemental de un puesto, desconocimiento del procedimiento técnico, cansancio del usuario, desconocimiento del manejo del interfaz hombre-máquina, etc.). Este *procedimiento inteligente de evaluación* debe aportar ayudas o soluciones que permitan, una vez detectada la causa, mejorar el adiestramiento de la unidad en su conjunto.

Conclusiones

Es importante sacar consecuencias del empleo de la simulación en esta última década, al objeto de mejorar el diseño de la siguiente generación de simuladores. Para impulsar estas mejoras, se debe manejar una *metodología* de desarrollo común que permita unificar criterios y facilite el seguimiento de proyectos. Es importante analizar los criterios que han impulsado a nivel técnico a decidir por la utilización de unos *estándares de modelado*, los cuales pueden ser aprovechados por otros simuladores y que facilitarán el mantenimiento e interconectividad de los medios de simulación.

La *interconexión de simuladores* es un objetivo fundamental para la realización de ejercicios conjuntos, pero es necesario conocer sus particularidades para definir bien los requisitos que satisfagan las necesidades de realización de los mismos. El futuro de los nuevos sistemas está fundamentalmente basado en técnicas de *simulación inteligente*, mediante las cuales se podrá facilitar la relación del hombre con la máquina usando interfaces capaces de procesar el lenguaje natural, interaccionar con sistemas expertos y realizar inferencias sobre la evaluación de los ejercicios realizados, aportando soluciones para conseguir un mejor grado de adiestramiento.

Una buena planificación en la implantación de nuevas tecnologías en materia de simulación, junto con la correcta articulación de programas de investigación y

desarrollo conseguirán incentivar a la Universidad, la Administración y a la Industria para la implantación de nuevas tecnologías en los futuros entornos de realidad virtual en apoyo a las operaciones militares.

BIBLIOGRAFÍA

R. E. Shannon, “Simulación de Sistemas”, Ed. Trillas. Méjico, 1.988.

M. Law, W. D. Kelton, “Simulation, Modeling and Analysis”, Ed. Mc. Graw Hill, New York, 1.982.

J. T. Morgan, “Elements of Simulation”, Ed. Chapman & Hall, London 1.984.

Naylor, Balintfy, Burdick, “Técnicas de simulación en computadoras”, Ed. Limusa

M. Bunge. “La ciencia su método y su filosofía”. Ed. Siglo XX. Buenos Aires 1.971

Interservice/Industry Training, Simulation and Education Conference, “Proceedings”, Orlando (Florida) Nov. 1.998. www.iitsec.org

Rumbaugh, J., Jacobson, I. y Booch, G. The Unified Modelling Language Reference Manual, Addison-Wesley, 1999.

Koch, Christof, y Joel L. Davis, “Large-sacale Neuronal Theories of the Brain, MIT Press, Cambridge (Massachusetts), 1994

Mountcastle, Vernon B., Perceptual Neuroscience: The Cerebral Cortex; Hardvard University Press Cambridge (Massachusetts), 1998

Castillo, J.M., El Analizador de Despliegues Aspide. Memorial de Artillería. 1996

Rios Insua, D.; Rios Insua, S.; Martin, J. Técnicas de simulación. RA-MA, 1997.

CAPÍTULO CUARTO

LAS REDES *AD HOC* Y SU USO EN COMUNICACIONES MILITARES

LAS REDES *AD HOC* Y SU USO

EN COMUNICACIONES MILITARES

Por Javier Ramos López

y Carlos Alberich Landáburu

Resumen

En este capítulo, se revisan los últimos desarrollos en redes *ad hoc* desde una perspectiva eminentemente tecnológica, evaluando las ventajas e inconvenientes de su uso para comunicaciones militares.

Definición y clasificación de redes *ad- hoc*

En este apartado introducimos el concepto de red *ad hoc*, analizando las diferencias con el otro gran grupo de redes inalámbricas, las redes celulares. También se menciona y aclara el concepto de red *mesh* y su relación con el concepto de red *ad hoc*. En el segundo apartado se mencionan los principales retos que debe abordar esta tecnología y las ventajas que representa. Se mencionan también las aplicaciones más destacadas de forma breve, ya que más adelante se desarrollarán aquellas que tienen un ámbito militar. En el apartado siguiente se describen los distintos tipos de redes ad-hoc o redes mesh existentes, atendiendo a diversos criterios. Por último, se describen algunos de estos tipos de redes, con redes propuestas como alternativas para las comunicaciones militares.

Definición y caracterización

En las redes de comunicaciones tradicionales los usuarios se comunican dos a dos a través de una infraestructura común. En el caso de las comunicaciones inalámbricas, cada usuario, que representa un nodo de la red, se comunica únicamente con una estación base cercana. El resto de la red, denominada troncal, suele no ser inalámbrica, y es la que realiza la mayor parte del trabajo. Este tipo de

redes se denominan redes celulares, y el esquema típico de su topología se representa en la Figura 1.

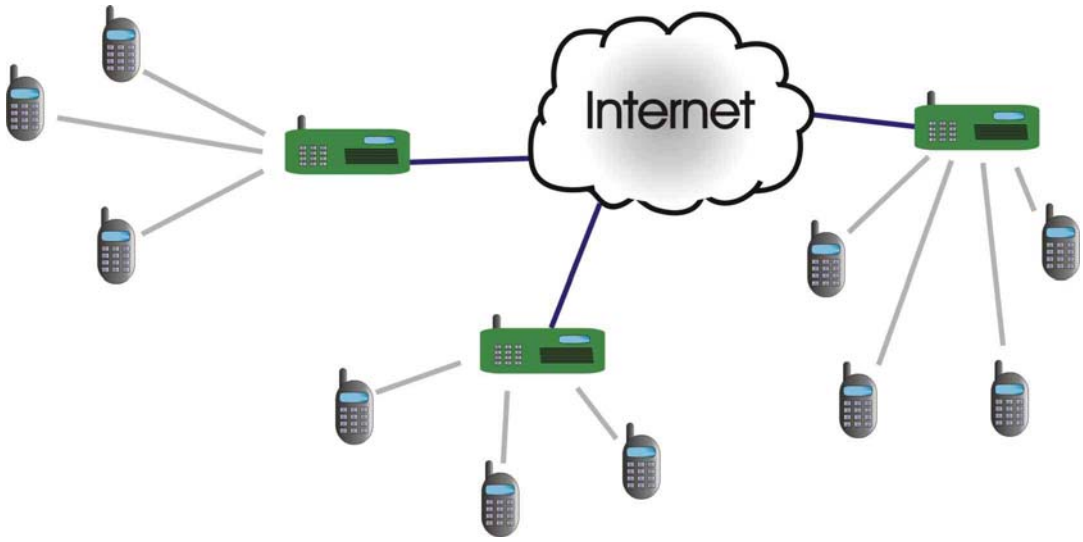


Figura 1. Topología de red tradicional con infraestructura.

Las redes *ad hoc* se definen en contraposición a estas redes celulares como aquellas en las que los usuarios pueden interconectarse entre ellos sin necesidad de la existencia de una estación base u otra infraestructura. En realidad, el término *ad hoc* se refiere en este caso al concepto “creado a partir de lo disponible de forma inmediata, improvisado”, es decir, a una red generada de forma espontánea a partir de los usuarios que eventualmente se incorporan a la misma, y que no cuenta con una infraestructura previamente diseñada, jerarquizada y establecida. Una forma clásica de una red *ad hoc* se puede observar en la **¡Error! No se encuentra el origen de la referencia.** (1, 2, 3 y 4).

Muchos autores también denominan a estas redes como redes *mesh*. El término *mesh* se traduce literalmente por malla, y por tanto este tipo de redes se denominan redes malladas. En efecto, la definición de redes mesh es un concepto íntimamente ligado a la topología de la red, que en el caso puro es aquella en la que los nodos están comunicados directamente todos con todos. En la Figura 2 se representa un ejemplo típico de esta topología.

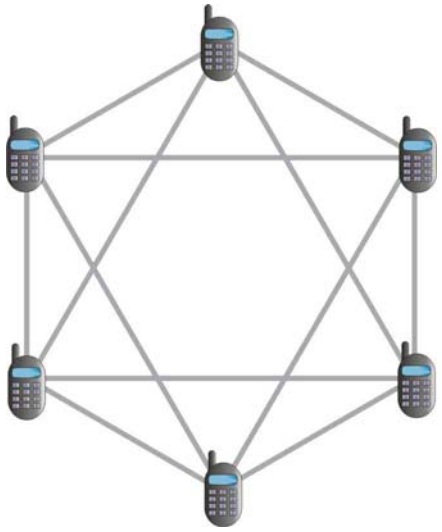


Figura 2. Topología de red *mesh*.

Como se puede observar, ambos conceptos, redes *ad hoc* y redes *mesh*, parecen no ser idénticos, y sin embargo, ambos se usan a menuda de forma indistinta. Esto es debido a que ambos conceptos, aparte de ser similares, se suelen dar de manera simultánea. El hecho de que todos los nodos estén interconectados entre sí sin el uso de infraestructura, como en las redes *ad hoc*, lleva a una topología en la que o bien todos los nodos están en el radio de cobertura de todos los demás, o bien se utilizan otros nodos similares (no jerarquizados) para realizar la conexión, por lo que ambos conceptos tienen mucho en común. En este documento utilizaremos indistintamente ambos términos.

Retos y ventajas

El uso de redes inalámbricas *ad hoc* es un reto tecnológico importante. Existen dificultades intrínsecas a la propia definición de estas redes (1).

El hecho de que no exista una infraestructura común, implica que todos los procesos que la red debe llevar a cabo (enrutamiento, control de tráfico, seguridad) tienen que ser realizados de forma distribuida, lo cual genera una complejidad alta en los diseños de procesos y algoritmos.

Por otra parte, cada nodo debe realizar un descubrimiento de la red cuando entra en ella, pues esta tampoco es una información que se encuentre centralizada. Además los nodos deben ser reconfigurables pues es inherente a las redes *ad hoc* una gran variabilidad de sus componentes. De esta manera las redes deben ser autoconfigurables, lo cual produce que la implantación sea automática y sencilla, pues basta con desplegar los nodos por la zona de cobertura deseada.

Al ser la red inalámbrica, y no existir un control centralizado de los nodos que existen o pueden entrar en la red, la seguridad frente a nodos no deseados o frente a interferencias externas es otro de los grandes retos de estas redes.

Por último, es necesario que estas redes den soporte a los servicios de última generación para que su desarrollo sea factible y tenga utilidad (8). Algunos de estos servicios son tráfico de datos de alta velocidad, aplicaciones en tiempo real o comunicaciones de vídeo y voz, que a su vez necesitan de un sistema que controle la calidad de servicio y el caudal disponible.

A pesar de todos los retos que se le plantean a estas redes existen importantes ventajas que han promovido un fuerte desarrollo de la investigación en este campo (1 y 2).

En primer lugar es obvio que la primera ventaja es la no necesidad de una infraestructura previa. Esto tiene múltiples efectos positivos, entre los que destacan el abaratamiento de la red, la velocidad y facilidad de implantación o la disponibilidad para situaciones adversas, como conflictos bélicos o desastres naturales. Allí donde es inconcebible o extremadamente cara la implantación de una infraestructura, una red cuyos nodos finales establezcan de forma automática y autónoma una malla entre ellos que permita la comunicación de todos se convierte en una alternativa clara y potente.

En segundo lugar, la no existencia de una jerarquía entre los nodos hace que ningún nodo sea imprescindible. Por ello estas redes son denominadas también redes robustas frente a fallos, ya que la eliminación de un nodo no supone en ningún caso la caída de la red, o de una parte de la red.

Estas dos ventajas conforman las dos características más importantes de las redes *ad hoc*: la flexibilidad y facilidad de implantación y la robustez. Finalmente, otra ventaja importante es la capacidad teórica de usar más eficientemente los recursos disponibles (ancho de banda, principalmente).

Aplicaciones

Algunas de las aplicaciones típicas donde el uso de estas redes se hace más aconsejable son las que se enumeran a continuación (2):

- Comunicaciones militares: donde la rapidez de la implantación y la robustez sean más críticos.
- Operaciones de búsqueda y rescate, por las mismas razones.
- Comunicaciones en edificios históricos, donde instalar cables no es posible.
- Redes inalámbricas en conferencias, o allí donde el número de nodos sea elevado.
- Comunicaciones entre vehículos.
- Comunicaciones entre satélites.

Clasificación de las redes ad hoc

A la hora de clasificar las redes *ad hoc* podemos hacerlo en función de varios criterios, de los que destacamos: la topología, el ancho de banda y la tecnología de los nodos.

En cuanto a la topología, en apartados anteriores denominábamos redes *ad hoc* o *mesh* puras a aquellas cuya topología consta de nodos sin jerarquizar conectados todos con todos. Sin embargo, desde un punto de vista más amplio, es conveniente

mencionar aquí topologías híbridas o jerarquizadas, ya que algunas de las redes *ad hoc* desarrolladas hasta hoy cuentan con estas características. Mencionamos también un tipo de red especial, denominada redes celulares de rápido despliegue, por tener objetivos comunes con el tipo de red tratado en este documento, así como interés en algunos tipos de comunicaciones militares. Centrándonos únicamente en enumerar y diferenciar las distintas categorías, sin entrar en más detalle, la clasificación de redes *ad hoc* según su topología sería la siguiente (7):

- Redes malladas puras. Son las descritas hasta el momento en este documento. En ellas todos los nodos tienen la misma categoría, y sirven tanto de punto final como de repetidor. Son muy robustas y su despliegue es sencillo. La complejidad tecnológica es elevada.

- Redes malladas con posibilidad de infraestructura. La mayoría de las redes mesh de la actualidad son aquellas que conforman Redes Inalámbricas de Ordenadores de Área Local (WLAN, de sus siglas en inglés), que disponen también de la posibilidad de añadir un modo infraestructura, en el que algunos nodos realizan funciones de red tales como enrutado, sirviendo así de punto de acceso a los demás nodos. Estos nodos principales se conectarán entre sí con la misma filosofía que una red mallada pura, sin ninguna jerarquía. Se trata por tanto de una situación híbrida.

- Redes jerárquicas autoorganizadas. Recoge el tipo de redes en el que sí existe una jerarquía, si bien esta no es rígida y se genera de una forma autónoma (autoorganización). Algunos nodos, semejantes a los demás, son elegidos de alguna manera como cabezas de un *cluster*. Todos los nodos pertenecientes a ese *cluster* les utilizarán para que realicen funciones de enrutado y de comunicaciones troncales. Este modo no nos permite ahorrar complejidad *hardware* debido a que cualquier nodo se puede convertir en algún momento en cabeza de *cluster*, pero sí simplifica enormemente las tareas de encaminamiento.

- Redes celulares de rápido despliegue. Se caracterizan por el uso de telefonía celular con estaciones base portátiles que se organizan entre ellas de manera rápida y flexible, tal y como lo harían los nodos principales en una red mallada con infraestructura. Existen numerosos inconvenientes en el uso de este tipo de

redes, que se analizarán más adelante. Otra posible clasificación que podemos realizar es la que se refiere al ancho de banda o velocidad de la red. Según este parámetro las redes *ad hoc* se pueden clasificar en redes de banda ancha y de banda estrecha.

- Redes *ad hoc* de banda ancha. Cuando la aplicación requiere la transmisión de datos de alta velocidad y con latencia reducida es necesario que la red pueda soportar una velocidad de transmisión alta. La complejidad es alta en estas redes, ya que deben soportar diferentes servicios, cada uno de ellos con sus requerimientos de calidad de servicio.

- Redes *ad hoc* de banda estrecha. A veces la principal función de la red no es el transporte masivo de una gran cantidad de datos, sino la transmisión rápida de pequeñas cantidades de información. El caso más típico de estas redes son las Redes Inalámbricas de Sensores WSN (*Wireless Sensor Networks*). Están formados por nodos cuya función, aparte de la propia de comunicaciones, es la de sensar el medio que le rodea. Cuando un evento se produce el nodo lo detecta y desea enviar esa información a un punto concreto de la red. Este tipo de redes han despertado un enorme interés por su amplia gama de aplicaciones, entre ellas militares, y serán descritas con más profundidad en apartados posteriores. Otra clasificación de las redes *ad hoc* que resulta interesante es la que divide a las redes según la tecnología utilizada como infraestructura para los nodos o los repetidores (7). Sin entrar en detalles, podemos destacar:

  - Redes inalámbricas terrestres. Los nodos son iguales y están situados a nivel de tierra.

  - Redes con estaciones base móviles. Algunos nodos son más complejos, y en el despliegue se elije su posición de forma estratégica, como en el caso de las estaciones base portátiles.

  - Redes con repetidor en una aeronave. Los nodos son terrestres pero se apoyan en una red troncal aérea, formada por aeronaves.

Por último mencionamos otras dos clasificaciones interesantes. La primera de ellas se refiere a la movilidad de los nodos. Las redes pueden ser móviles o no. Si bien

las redes inalámbricas están preparadas para que los nodos puedan desplazarse libremente por la zona de cobertura, la movilidad y el tipo de movilidad (esporádica, continuada, rápida y lenta) afecta al diseño de la red, sin olvidar que algunas redes inalámbricas muy comunes, como las redes de ordenadores, no son inherentemente móviles, sino que los terminales permanecen fijos la mayor parte del tiempo. La última clasificación que mencionamos es aquella que divide a las redes por su cobertura. Dentro de las redes *ad hoc* es común encontrar redes de área personal, con unos pocos metros de cobertura (PWAN) y redes de área local, con unos cientos de metros de cobertura (WLAN). Asimismo, también podemos señalar redes más extensas, que cubren una zona de decenas de kilómetros, denominadas Redes de Área Metropolitana (WMAN). Finalmente, uno de los objetivos de las redes *ad hoc*, en especial en las comunicaciones militares, es proporcionar una infraestructura robusta, flexible y heterogénea que dote a la red de una cobertura global.

Descripción de algunos tipos de redes ad hoc

REDES CELULARES DE RÁPIDO DESPLIEGUE

Existe un interés considerable por parte de los militares estadounidenses en el uso de telefonía celular con estaciones base modificadas que sean transportables. Ericson desarrolló un sistema de estas características en el año 1997. Operaciones en zonas catastróficas también se podrían beneficiar de estos sistemas.

Sin embargo, existen muchos inconvenientes a tener en cuenta en el uso de este tipo de redes para comunicaciones tácticas. En primer lugar, las estaciones bases deben ser cuidadosamente colocadas, según una planificación previa, para que den una cobertura global y sin agujeros, y para que las interferencias entre células sean pequeñas. Esta planificación necesita un tiempo para llevarse a cabo, y además es necesario la colaboración de personal muy especializado. Además, se necesita una planificación de frecuencias para que células adyacentes no reutilicen la misma. Por otra parte, la red troncal que une y coordina las antenas en las situaciones en las que una única antena no de suficiente cobertura es compleja y debe instalarse en cable o con enlaces de muy alta velocidad.

Por último, otro problema de las redes GSM es que en cada país utilizan diferentes frecuencias, por lo que sería necesario equipos especiales que pudieran adaptarse a

esta situación. Si unimos esto al hecho de que una vez puestas las antenas es complicado cambiarlas, y a que toda la instalación se debe hacer con rapidez y celeridad observamos que el uso en comunicaciones tácticas en zonas en conflicto es poco recomendable.

En realidad, únicamente se contempla la posibilidad de uso de estas tecnologías en centros de operaciones, áreas de retaguardia, o zonas urbanas en las que se realizan misiones de paz, donde las circunstancias permiten la instalación mas detenida del sistema, que puede sustituir a las comunicaciones telefónicas con cable.

REDES MÓVILES CON TOPOLOGÍA MALLADA

Las redes móviles con topología mallada son las que hemos denominado redes mesh puras, y sus características se han explicado ya. Aquí analizamos las ventajas más importantes para las comunicaciones militares.

Mientras que en áreas de retaguardia las comunicaciones pueden ser sostenidas mediante redes celulares de despliegue rápido u otras alternativas híbridas que necesiten infraestructura, en el frente, o en acciones ofensivas de avance rápido, las condiciones del campo de batalla son aparentemente y en ocasiones realmente caóticas. Unidades ligeras de alta movilidad, como vehículos de combate ligeros, abandonan rápidamente agrupamientos tácticos para unirse y dar respaldo a otros. Entre estos agrupamientos, con toda esta movilidad, la tecnología de red que de soporte a las comunicaciones debe ser inmediatamente reconfigurable, completamente descentralizada y debe ofrecer redundancia en los enlaces para dar robustez. Todas estas características son las propias de una red móvil con topología mallada. Un grupo de aeronaves y barcos en una operación naval también pueden formar una red *mesh*. En operaciones anfibias este grupo también puede comunicarse con unidades móviles de tierra.

A pesar de que se puede concebir una red *mesh* con diferentes tipos de nodos, que no tengan la misma potencia de transmisión, el mismo número de antenas ni la misma capacidad de almacenamiento o procesado, el diseño de la red sería realmente muy complicado si se intenta utilizar las ventajas de cada característica especial de cada nodo. Sin embargo, debido a la “maldición” de la herencia histórica

de equipos, éstos serán, inevitablemente, diferentes, y las redes *mesh* militares deberán aprovechar esta diversidad en su diseño.

Todos estos argumentos nos llevan a pensar que la elección de redes móviles puramente malladas es una alternativa adecuada para soluciones en situaciones críticas. Sin embargo, es importante destacar las dificultades que esta opción conlleva y que se explican a continuación.

El principal inconveniente de las redes móviles malladas puras es la complejidad extra que cada nodo debe tener para poder almacenar el estado de la red, participar en el encaminamiento de la información o almacenar paquetes de otros nodos para su reenvío. De hecho, el coste de una red mesh puede ser más alto que el de una red jerarquizada con una zona de red troncal móvil, porque en el caso de la red *mesh* todos los nodos deben poder realizar las funciones que en el caso de la rede jerarquizada sólo realizan los nodos troncales.

Para situaciones donde el coste del equipo de comunicaciones sea bajo en relación con el de la plataforma que lo soporta, como por ejemplo una red naval, el concepto de red móvil mallada parece apropiado en términos económicos.

Si nos fijamos ahora en otro aspecto, el tamaño y portabilidad de los componentes, hay que plantearse si un equipo con múltiples receptores, capacidad de enrutamiento y almacenamiento y otros servicios necesarios es transportable por un soldado. Esta discusión es, sin embargo, una cuestión de tiempo, ya que durante esta década los equipos que se desarrollen pueden llegar a ser realmente minúsculos.

Por otro lado, las comunicaciones inalámbricas que un solo salto conectan al terminal móvil con una infraestructura fija son apropiadas para muchas situaciones, tanto civiles como militares, y son tecnologías conocidas y probadas. En el mundo civil, y en bases militares o en zonas de retaguardia, los usuarios siempre operan en las cercanías de una red cableada.

En este punto de la discusión aparece una nueva problemática de las redes mesh utilizadas en comunicaciones tácticas: la necesidad de alcanzar una buena cobertura y conectividad. Para conseguirla es necesario que todos los equipos estén

continuamente transmitiendo. Aparte del problema de duración de baterías, en el que existe una intensa investigación, otro problema aparece, ya que el soldado se ve amenazado por el hecho de que al tener una radio con él que está todo el tiempo transmitiendo, puede estar delatando su posición al enemigo. Este nuevo reto tecnológico deberá ser tenido en cuenta en el diseño de estas redes.

Todo lo dicho parece indicar que las redes con tecnología mallada pura son solamente apropiadas para zonas conflictivas, en el frente, o en operaciones en zonas catastróficas donde no existe ninguna infraestructura, y aún así existen problemas asociados que hace falta resolver.

REDES MÓVILES JERÁRQUICAS TERRESTRES

Una alternativa a las redes *mesh* puras y sus inconvenientes asociados son las redes totalmente móviles jerárquicas terrestres. Si bien son menos ambiciosas en términos de diseño de protocolos y complejidad *hardware*, el esquema jerárquico puede ofrecer una funcionalidad comparable con las redes *mesh*.

En una red móvil jerárquica la mayoría de los nodos son relativamente simples, pues tienen un procesado sencillo y una capacidad de almacenamiento mínima. Únicamente un conjunto pequeño de los nodos tendrían el *hardware* necesario para realizar funciones de enrutado, conmutación, almacenamiento, etc. Estos nodos son también móviles, y se denominan estaciones base móviles.

Hace pocos años las Fuerzas Armadas de los Estados Unidos desarrollaron un punto de acceso radio que en muchos aspectos es similar al concepto de estaciones base móviles. Estos puntos unían equipos de transmisión y conmutación de datos para dar servicios de voz, datos y vídeo para comunicaciones tácticas. Soportaba movilidad y conectaba a los usuarios a una red troncal ATM. Este tipo de solución no cubre, sin embargo, situaciones de operaciones de unidades infiltradas en el territorio enemigo o de pequeñas unidades aisladas.

En la arquitectura analizada en este apartado, una estación base móvil, como una fija de telefonía convencional, proporcional conectividad a los usuarios que están próximos a ella. Además estas estaciones base deberán estar conectadas de alguna manera. El sistema de comunicaciones terrestres y espaciales que el Centro de

Comunicaciones ha desarrollado pretende dar capacidad de uno a cien megabits por segundo con coberturas de hasta 40 kilómetros, y sirve de ejemplo de la infraestructura que sería necesaria para unir las estaciones base móviles.

Existen casos en los que la conectividad es más compleja. En terrenos montañosos resulta inviable el establecimiento de enlaces en los que sea necesaria la línea de visión directa, en especial porque las estaciones base móviles están a nivel de tierra. En estas zonas, o en zonas controladas por el enemigo o cercadas por este una salida a la conectividad de la zona es necesaria. Para ello existen dos alternativas, las comunicaciones por satélite y las comunicaciones con una aeronave, que se explica en el siguiente apartado.

REDES CON REPETIDOR EN UNA AERONAVE

Una solución al problema de la conectividad de las redes móviles jerárquicas terrestres es poner alguna o todas las estaciones base en plataformas aéreas. Previamente a desarrollar el concepto, presentamos el JTIDS (*Joint Tactical Information Distribution System*), que nos proporciona un importante punto de referencia.

El JTIDS es una red *mesh* pura, desarrollada para comunicaciones aire-aire o aire-tierra. Está basada en redes de radio. Cada 30 redes usan un patrón distinto para la modulación *frequency hopping*. Dentro de cada red, todos los nodos se comunican por todos transmitiendo en difusión. El punto más interesante de esta arquitectura es que no existen nodos críticos, con lo que la pérdida de un nodo no implica la pérdida de conectividad.

La mayor ineficiencia de una red de este tipo viene dada porque la reutilización de frecuencias no existe y porque no se puede realizar correcciones de frecuencia y fase en el transmisor, ya que los receptores son muchos y un mismo transmisor observa diversos canales hasta los receptores. Además, en un Sistema TDMA como el JTIDS los tiempos de guarda deben ser grandes, para evitar que dos estaciones lejanas empiecen a transmitir a la vez. En resumen, la distancia variable y la diversidad de receptores para una misma transmisión implican dificultades que no permiten utilizar algunas técnicas típicas de comunicaciones inalámbricas que mejorar el rendimiento del sistema.

Si usamos un repetidor en una aeronave los tiempos de guarda pueden ser pequeños y conocidos, y se puede realizar una corrección de tiempo y frecuencia tanto en el transmisor como en el receptor porque cada nodo transmite únicamente hacia un nodo, el repetidor, y por tanto el canal es único y se pueden usar diversas técnicas de estimación de canal, control de potencia o estimación del tiempo de guarda.

La primera opción posible es colocar el repetidor en un avión pilotado, de manera que no se necesitan nuevas plataformas, sino sólo modificar las existentes. Hay, sin embargo, un inconveniente muy importante: en el caso de terrenos montañosos será necesario que los aviones sobrevuelen la zona de conflicto, con lo que pondríamos en peligro el avión pilotado.

Si colocamos el repetidor en un Avión No Pilotado UAV (*Unmanned Air Vehicle*) solventamos este problema. Además se pueden aprovechar los protocolos existentes para comunicaciones por satélite. Además el UAV puede transmitir su posición por un canal seguro de manera que los transmisores puedan corregir el efecto doppler y el sincronismo. Según la banda utilizada, se pueden alcanzar anchos de banda de 500 MHz (*X-band*). Para solventar la vulnerabilidad del sistema sería necesario tener repetidores dispersos o un modo de respaldo para comunicaciones directas sin repetidor.

Aunque esta arquitectura simplifica enormemente el diseño de protocolos y la complejidad hardware, tiene aún limitaciones que sugieren alguna mejora a la idea básica.

La primera mejora es un sistema de doble banda que añada al sistema la posibilidad de establecer enlaces directos que no pasen por el repetidor para nodos cercanos entre sí. Esta opción le quita tráfico al repetidor, que queda sólo para comunicaciones de más largo alcance, y permite a los nodos ahorra energía. Otra mejora es el uso de un anillo de UAV en el cielo que permita cubrir un área grande y además no tener que realizar enlaces excesivamente largos. Los UAV estarían comunicados entre ellos, aumentando su complejidad, pero disminuyendo la de los nodos. Estas dos mejoras se pueden combinar para dar un sistema altamente flexible y robusto.

REDES INALÁMBRICAS DE SENSORES

Las investigaciones iniciales en el campo de las WSN surgieron para aplicaciones militares, con la agencia DARPA (*Defense Advanced Research Projects Agency*), que ha financiado proyectos importantes de investigación (como *Smart Dust* o NEST). Las líneas de investigación comunes han derivado en una definición *de facto* de las redes de sensores como un conjunto de muchos nodos con capacidad de sensar el medio (miles, cubriendo zonas geográficas amplias), inalámbricos, con topología *ad hoc*, encaminamiento multisalto. Los nodos son pequeños, prácticamente inmóviles después de su colocación, todos homogéneos y esparcidos de forma aleatoria por la zona de cobertura (9 y 30).

Estas redes tienen dos objetivos, sensar el medio y transportar de forma eficaz y eficiente la información a algún punto determinado. Además de las ventajas en cuanto a cobertura, flexibilidad y robustez, las redes de sensores mejoran el sensado en sí ya que permiten una gran redundancia en la información que puede utilizarse para depurarla convenientemente.

Por todos estos motivos en la actualidad las redes de sensores inalámbricas copan gran parte del interés de los investigadores, en especial dentro del campo de las redes *ad hoc*.

De forma más reciente se han considerado otras aplicaciones civiles, como monitorización de especies, agricultura, producción industrial o cuidado de la salud. Estudios y proyectos concretos en todas estas áreas y también en las propias aplicaciones militares demuestran que la definición dada *de facto* inicialmente no cubre todas las características necesarias. Actualmente el debate sobre lo que son o dejan de ser las redes de sensores sigue abierto, y por ello a continuación describimos brevemente algunas dimensiones del espacio de diseño de estas redes, que permiten hacernos una idea de la utilidad de las mismas y del rango de aplicaciones tan heterogéneas que pueden cubrir.

Según la manera en que estas redes son desplegadas en el medio físico podemos encontrar distintos tipos. Los nodos pueden ser desplegados de forma aleatoria (definición clásica) o instalados de forma deliberada en ciertos puntos estratégicos. El despliegue puede ser de una vez, en la instalación de la red, o bien un proceso

continuo en el tiempo de uso de la red para, por ejemplo, relevar a los nodos con baterías agotadas. El tipo de despliegue afecta a muchas propiedades de la red, como la densidad de nodos esperada, la localización de los mismos o la evolución en el tiempo de la conectividad.

También se puede dar la posibilidad de que los nodos cambien de posición después del despliegue inicial. Esta movilidad puede ser accidental (viento, mareas, etc.) o bien porque los nodos estén en infraestructuras móviles (un vehículo, un ser humano) o porque los propios nodos tengan movilidad. La movilidad puede afectar a todos los nodos o a algunos, y ser esporádica o continua. Todo ello tiene un impacto importante sobre el tipo de dinámica que tendrá la red o el tiempo que un nodo está conectado con otro nodo.

Otros factores importantes son el coste, el tamaño y la energía. Respecto al coste, es significativo diferenciar aquellas redes con pocos nodos todos ellos importantes (estaciones meteorológicas, por ejemplo) en el que la complejidad de cada nodo puede ser alta, o aquellas redes con muchos nodos que deben ser sencillos y barato (como los *Smart Dust* para las aplicaciones militares). También el tamaño se puede analizar en los mismos términos. Existirán redes con nodos muy pequeños (los mismos *Smart Dust*) y otras en los que el tamaño no sea tan crítico (un sensor en un avión).

La energía también es un factor importante en estas redes. Gran parte de la investigación realizada sobre ellas se centra en conseguir protocolos, *software* y *hardware* que maximicen el tiempo de vida de las baterías. En algunos casos es posible que las baterías puedan recargarse (con paneles solares, porque están enchufadas a la red) y en otros ser irreemplazables, con lo que el nodo muere cuando la batería se acaba.

Por último la homogeneidad o heterogeneidad de los nodos, como ya se ha discutido anteriormente en las redes *ad hoc* genéricas es un elemento muy importante que puede cambiar totalmente la topología y la arquitectura de la red.

Como se puede observar, el ámbito de aplicación y la flexibilidad de estas redes es amplio. En concreto, dentro de las aplicaciones militares las más destacadas son monitorización de campo de batalla, vigilancia, reconocimiento, adquisición de

objetivos, vigilancia de ataques Nucleares, Biológicos o Químicos (NBQ), detección de intrusos, detección de francotiradores, radares o sónares distribuidos y otras muchas.

Estado del arte en redes *Ad Hoc*

Tecnologías implicadas

ULTRA WIDE BAND (UWB)

Las comunicaciones UWB se caracterizan por la transmisión de pulsos electromagnético de muy corta duración (1 nanosegundo o menos) y por no usar frecuencias portadora. El ancho de banda ocupado por esos pulsos es inversamente proporcional a su duración, y por tanto ocupan desde bajas frecuencias a frecuencias del orden de gigahercios. Es por tanto una señal en banda base con un espectro muy amplio, y poca densidad espectral de potencia (poca potencia en una banda de frecuencias determinada), (10).

Sus propiedades más importantes es que debido a lo ancho del espectro es extremadamente difícil de detectar por usuarios externos, por lo que representa una gran oportunidad para comunicaciones seguras. La baja probabilidad de intercepción LPD (*Low Probability of Detection*) es una demanda clave de todas aquellas aplicaciones con requerimientos de seguridad, como lo son todas las militares.

Además al tener poca potencia en cada banda de frecuencias no interfiere con otros sistemas, ya que frente a ellos aparece como ruido de baja potencia. Otra característica es que puede operar en situaciones de línea de visión directa o en situaciones en las que no la hay, ya que atraviesa muros y puertas con facilidad. La inmunidad a la dispersión multitrayecto es una ventaja también muy importante de estos sistemas.

Otras ventajas son su bajo coste, el bajo consumo, que es plenamente digital y que los equipos pueden estar integrados en un solo chip.

De entre las aplicaciones más importantes se pueden destacar las que tienen que ver con posicionamiento, las de comunicaciones y las de imagen (en realidad detección de objetivos).

Respecto a las primeras, UWB permite detectar tanto la posición como la distancia y permite seguimiento y navegación en tiempo real tanto en interior como en exterior. Como ejemplo, con un sistema de pruebas de 400 MHz de ancho de banda y 2,5 nanosegundos de pulso, se consiguen precisiones en localización de 30 cm en interiores y 10 cm en exteriores.

En cuanto a las aplicaciones en comunicaciones se investiga en utilizar estos sistemas para comunicaciones personales de corto alcance, redes inalámbricas de ámbito local, comunicaciones entre vehículos y comunicaciones móviles con alta capacidad de envío de datos.

Para aplicaciones radar se puede utilizar para detección de objetos subterráneos (minas antipersonales), localización de personas escondidas, localización de canalizaciones metálicas en muros o seguridad en la automoción con detección de colisiones.

Resulta evidente que todas estas aplicaciones son realmente útiles en el ámbito militar, tanto para comunicaciones tácticas como estratégicas y operacionales, pues ofrecen un alto nivel de seguridad y son difícilmente interceptables, a lo que hay que sumar el alto ancho de banda que ofrecen para, por ejemplo, vídeo en tiempo real. La detección de objetos y personas detrás de muros o la capacidad de localización precisa son también claros ejemplos de utilidad en el ámbito militar.

Por tanto, los sistemas UWB permiten comunicaciones inalámbricas de gran ancho de banda. El precio que hay que pagar es, sin duda, el corto alcance de los equipos. Esto conduce a los diseñadores de UWB a buscar una alianza tecnológica con un tipo de redes que permita la coexistencia de muchos nodos y la aproveche para disminuir el alcance necesario de los enlaces: las redes *mesh*. Las redes *mesh* en general acortan la distancia de enlace ya que implican que los nodos existentes puedan comunicarse entre ellos en lugar de comunicarse con una estación base que puede estar lejos. Por ello, ambas tecnologías se complementan muy bien y la industria está apostando claramente por esta unión, que aporta gran ancho de banda y alcances más altos.

El reto está, evidentemente, en que la red *mesh* pueda hacer uso de ese potencial ancho de banda que puede llegar al medio gigabit por segundo en la actualidad.

Para ello la retransmisión de los datos en cada nodo, las funciones de encaminamiento, el control de tráfico y la calidad de servicio se deben realizar de una manera muy optimizada, lo cual supone un reto tecnológico claro para este tipo de redes.

Por último, cabe destacar que debido al corto alcance que esta tecnología permite, al menos en el ámbito de las comunicaciones, queda claro que una topología de red diseñada correctamente es necesaria para su implantación. Evidentemente, para un gran número de nodos, situados a poca distancia, una configuración *ad hoc* podría permitir explotar las ventajas de esta tecnología que en estos años comienza a explotar y que en breve se convertirá en la más potente de las tecnologías inalámbricas.

WIFI (WIRELESS FIDELITY)

El término WiFi hace referencia al estándar del IEEE 802.11, en sus modalidades *a*, *b* y *g*. El estándar define los niveles de enlace y físico para la interconexión inalámbrica de estaciones (11).

Las versiones más usadas son la *b* y la *g*. La velocidad de transmisión máxima que soporta la versión 802.11*b* es de 11 Mbps, si bien la velocidad se adapta a las condiciones del canal y puede ser también de 1, 2 o 5 Mbps. La versión *g* posibilita los 54 Mbps como máximo.

Las distancias típicas de cobertura son de pocos centenares de metros como máximo, aunque depende del tipo de antes que se utilicen. En cualquier caso para las distancias largas es necesario hacer modificaciones sobre el estándar.

El estándar define dos tipos de arquitectura. La primera es el habitual modo infraestructura, en el que los nodos se conectan a la red a través de un punto de acceso. Los distintos puntos de acceso se conectan entre sí y con el resto de la red por medio de una red cableada. La segunda arquitectura se corresponde con el modo *ad hoc*, en el que los nodos se pueden interconectar entre ellos sin necesidad de punto de acceso, creando así entre todos una red *mesh*.

La importancia de esta tecnología viene dada por su amplia difusión en el mercado, tanto empresarial como doméstico. Las enormes economías de escala basadas en

la popularidad de estas redes han permitido un abaratamiento de los productos muy importante. La mayor parte de las redes son redes de ordenadores, en las que los habituales cables ethernet se sustituyen por conexiones inalámbricas.

Las ventajas más importantes de esta tecnología son su amplio uso, el conocimiento extenso que existe sobre ella y que además está estandarizada. Las desventajas son su corto alcance, que se puede solucionar contando con una red mesh, y la falta de seguridad que tiene.

Desde el comienzo de la existencia de WiFi ha existido un interés militar por esta tecnología, y algunas empresas como Texel han modificado las tarjetas para cumplir con los requisitos de seguridad militares en Estados Unidos.

El uso de esta tecnología en su formato *ad hoc* tiene aplicaciones de comunicaciones de media distancia básicamente, y para la interconexión en bases militares y puestos de retaguardia.

WORDWIDE INTEROPERABILITY FOR MICROWAVE ACCESS (WIMAX)

WiMAX es el nombre de una tecnología radio de acceso muy reciente, que corresponde a un nuevo estándar del IEEE, el 802.16x, y que es una especificación para redes metropolitanas promovida por algunas de las empresas más destacadas del sector (como Intel y Nokia) (13).

WiMAX no es aún una tecnología de consumo, y eso de momento ha permitido que el estándar se desarrolle conforme a un ciclo bien establecido, lo cual garantizará con el tiempo la estabilidad e interoperabilidad de los componentes.

Esta tecnología está pensada para dar coberturas mucho mayores que WiFi y con velocidades de transmisión que lleguen hasta los 100 Mbps. Podrían situarse como tecnología paraguas que permita a los proveedores de internet dará acceso inalámbrico en la última milla, ya que puede coexistir con WiFi. En la figura 4 se muestra el alcance pretendido de esta tecnología y su situación respecto a WiFi.

En marzo de 2003, se ratificó una nueva versión del estándar, el 802.16a, y fue entonces cuando WiMAX, como una tecnología de banda ancha inalámbrica, empezó a cobrar relevancia. También se pensó para enlaces fijos, pero llega a

extender el rango alcanzado desde 40 a 70 kilómetros, operando en la banda de 2 a 11 GHz, parte del cual es de uso común y no requiere licencia para su operación. Es válido para topologías punto a multipunto y, opcionalmente, para redes en malla, y no requiere línea de visión directa. Emplea las bandas de 3,5 GHz y 10,5 GHZ, válidas internacionalmente, que requieren licencia (2,5-2,7 en Estados Unidos), y las de 2,4 GHz y 5,725-5,825 GHz que son de uso común y no requieren disponer de licencia alguna.

El estándar 802.16 puede alcanzar una velocidad de comunicación de más de 100 Mbit/s en un canal con un ancho de banda de 28 MHz (en la banda de 10 a 66 GHz), mientras que el 802.16a puede llegar a los 70 Mbit/s, operando en un rango de frecuencias más bajo (<11 GHz).

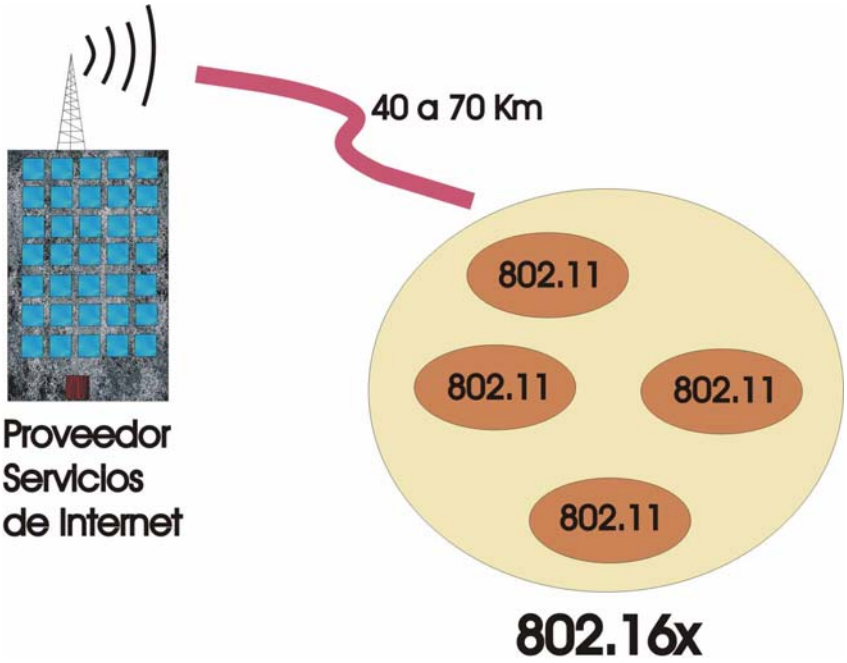


Figura 4. WiMAX. Alcance y compatibilidad con WiFi.

En el cuadro 1 se muestra una comparativa entre algunas tecnologías de acceso de última generación. Se muestran las velocidades, coberturas, ventajas e inconvenientes, así como la necesidad de licencias.

	WiMAX 802.16	Wi-Fi 802.11	Mobile-Fi 802.20	UMTS y cdma2000
Velocidad	124 Mbit/s	11-54 Mbit/s	16 Mbit/s	2 Mbit/s
Cobertura	40-70 km	300 m	20 km	10 km
Licencia	Si/No	No	Si	Si
Ventajas	Velocidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Movilidad
Desventajas	Interferencias?	Bajo alcance	Precio alto	Lento y caro

Tabla 1. Comparativa entre tecnologías inalámbricas.

WiMAX Soporta varios cientos de usuarios por canal, con un gran ancho de banda y es adecuada tanto para tráfico continuo como a ráfagas, siendo independiente de protocolo; así, transporta IP (*Internet Protocol*), Ethernet, ATM, etc. y soporta múltiples servicios simultáneamente ofreciendo Calidad de Servicio (QoS) en 802.16*e*, por lo cual resulta adecuado para voz sobre IP (VoIP), datos y vídeo. Por ejemplo, la voz y el vídeo requieren baja latencia pero soportan bien la pérdida de algún bit, mientras que las aplicaciones de datos deben estar libres de errores, pero toleran bien el retardo.

Otra característica de WiMAX es que soporta las llamadas antenas inteligentes (*smart antenas*), propias de las redes celulares de 3G, lo cual mejora la eficiencia espectral, llegando a conseguir 5 bps/Hz, el doble que 802.11*a*. Estas antenas inteligentes emiten un haz muy estrecho que se puede ir moviendo,

electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.

Una de las principales limitaciones en los enlaces a larga distancia vía radio es la limitación de potencia, para prever interferencias con otros sistemas, y el alto consumo de batería que se requiere. Sin embargo, los más recientes avances en los procesadores digitales de señal hacen que señales muy débiles (llegan con poca potencia al receptor) puedan ser interpretadas sin errores, un hecho del que se aprovecha WiMAX. Con los avances que se logren en el diseño de baterías podrá haber terminales móviles WiMAX, compitiendo con los tradicionales de GSM, GPRS y de UMTS.

Finalmente, es importante destacar que el estándar contempla la posibilidad de formar redes malladas (*mesh networks*) para que los distintos usuarios se puedan comunicar entres sí, sin necesidad de tener visión directa entre ellos. Ello permite, por ejemplo, la comunicación entre una comunidad de usuarios dispersos a un coste muy bajo y con una gran seguridad al disponerse de rutas alternativas entre ellos. En cuanto a seguridad, incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES 128 bits) y RSA (1.024 bits).

El Ejército de los Estados Unidos está probando el estándar WiMax implementado por la empresa Telos Corp. en bases como el fuerte Carson, Colorado, para enlaces punto a punto y punto a multipunto. La idea es extender la red cableada a zonas de difícil acceso (14). En el fuerte Dix, New Jersey, se está extendiendo el acceso de banda ancha a Internet a las zonas de entrenamiento. El resultado es un despliegue rápido que abarata enormemente los costes de la red (a menos de la mitad). Por ello, el desarrollo actual de las redes WiMAX en usos militares se dirigen a la posibilidad de implantar redes troncales de banda ancha con rapidez, flexibilidad y de forma económica. Si a estas características les añadimos la posibilidad de formar redes mesh, queda claro que el siguiente paso será el de proporcionar comunicaciones móviles a un conjunto de nodos dispersos, siendo estas comunicaciones de alta velocidad.

ZigBee

La alianza de empresas ZigBee presentó el pasado diciembre la especificación v1.0 del protocolo radio para transmisión de datos a baja velocidad para aplicaciones de automatización de viviendas y edificios, fábricas y otras aplicaciones de monitorización en diferentes sectores (15).

ZigBee es una nueva tecnología inalámbrica de corto alcance y bajo consumo que tiene su origen en la antigua alianza HomeRF. A esta iniciativa de la conocía con nombres como: PURLnet, RF-Lite, Firefly, y HomeRF Lite, finalmente se escogió el término ZigBee.

ZigBee pretende ser la base sobre la que crear productos y sistemas para diversidad de sectores como la domótica (automatización en viviendas), la inmótica (automatización en edificios), la automatización en fábricas y en otros sectores con necesidad de usar diversidad de sensores repartidos en un área acotada.

De la diversidad de miembros que forman parte de esta alianza, destacan empresas como Invensys, Mitsubishi, Philips y Motorola que trabajan para crear dispositivos de domótica, automatización de edificios (inmótica), control industrial, periféricos de PC y sensores médicos.

Las empresas que han desarrollado el ZigBee han formado el “ZigBee Working Group” (16) el cual también participa en el grupo de trabajo 4 del comité de estandarización IEEE 802.15. Este grupo está enfocado en el desarrollo de especificaciones de para productos WPAN (*Wireless Personal Area Network*) en las bandas de frecuencia de uso sin licencia. De esta manera, el ZigBee está ratificado como estándar el IEEE, al igual que por ejemplo la tecnología Bluetooth (IEEE 802.15.1).

El estándar IEEE 802.15.4 tiene como objetivo especificar los niveles físicos y de acceso al medio (MAC) de redes inalámbricas con dispositivos de muy bajo consumo y baja velocidad. Colaboran con el ZigBee Working Group con el objetivo de publicar un único estándar. La tecnología ZigBee será la responsable de implementar las funciones de la aplicación del dispositivo en cuestión, de la gestión de la red y la seguridad.

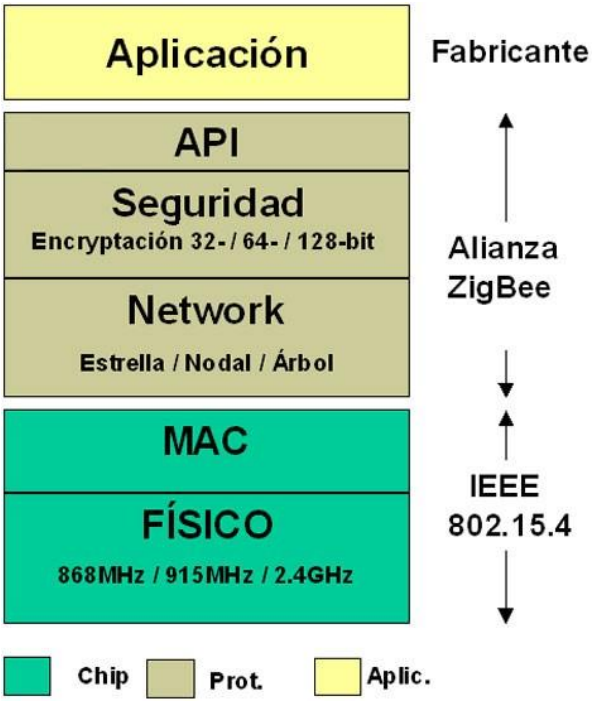


Figura 3. Torre de protocolos asociada a Zigbee.

En la figura 5 se recoge la torre de protocolos de ZigBee. Se observa la flexibilidad del nivel físico y una capa especial dedicada a seguridad.

Con velocidades comprendidas entre 20 kB/s y 250 kB/s y rangos de 10 m a 75 m, ZigBee puede funcionar en las bandas de 2,4 GHz, 868 MHz y 915 MHz, aunque la mayoría de fabricantes optarán por la primera ya que puede ser usada en todo el mundo, mientras que las dos últimas sólo se pueden usar en Europa y Estados Unidos, respectivamente.

Una red ZigBee puede estar formada por 65.000 nodos, agrupados en subredes de hasta 255 nodos, los cuales tienen la mayor parte del tiempo el transceptor ZigBee dormido con objeto de reducir el consumo al mínimo. El objetivo es que un sensor equipado con tecnología ZigBee pueda ser alimentado con dos pilas AA durante al menos seis meses y hasta dos años, aunque en la práctica se ha verificado que se

podrán conseguir más de cinco años de duración de batería en aplicaciones de domótica y seguridad.

Hay tres topologías: estrella, árbol y en red mallada (*mesh network*). Siempre hay un nodo de red que asume el papel de coordinador central encargado de centralizar la adquisición y las rutas de comunicación entre dispositivos. Además, si se aplica el concepto de *mesh network*, pueden existir coordinadores o *routers*, alimentados permanentemente en espera de recibir/repetir las tramas de los dispositivos o sensores. Ambos dispositivos son del tipo FFD (*Full Functionality Device*), debido a que exigen empotrar la mayoría de primitivas definidas por el *stack* ZigBee.

Sin lugar a dudas, una de las mayores aportaciones del ZigBee y el que mayor interés está despertando a las empresas desarrolladoras de productos, es el concepto de red nodal o *mesh network* por el que cualquier dispositivo ZigBee puede conectarse con otro dispositivo usando a varios de sus compañeros como repetidores. De esta manera cualquier nodo ZigBee puede hacer llegar los datos a cualquier parte de la red inalámbrica siempre y cuando todos los dispositivos tengan un vecino dentro de su rango de cobertura.

La aplicación del concepto de *mesh networks*, hará viable muchas aplicaciones, de distintas áreas, como domótica vía radio en viviendas construidas, o aplicaciones industriales o militares, allí donde las tecnologías radio de generaciones anteriores estaban limitadas en cuanto a la cobertura o alcance entre dispositivos. Gracias a esto la instalación y puesta en marcha de dispositivos en cualquier situación será una tarea muy sencilla e independiente de la tipología y tamaño de la red.

Las dos limitaciones clave de esta tecnología son la distancia máxima entre nodos (unos 75 m) y la velocidad. Por ello, su uso en aplicaciones militares puede centrarse en dos vías. La primera de ellas las comunicaciones entre dispositivos de seguridad, por ejemplo, en bases militares. La otra, actuando como redes de sensores, con sus múltiples aplicaciones, incluso en el campo de batalla. El tamaño de los elementos es muy reducido y su larga vida y bajo coste permitirían un despliegue rápido de una red de sensores por el área requerida.

Enrutado dinámico y robusto

En las redes de comunicaciones de datos raramente el transmisor y el receptor de la información se encuentran directamente enlazados. Normalmente necesitan nodos intermedios para realizar la comunicación. En una red normal, será preciso que el transmisor conozca la ruta por la que sus paquetes de datos puedan alcanzar el receptor. Este es el cometido de los protocolos de enrutado.

En las redes *ad hoc* no existe un nodo central que gestione las rutas, y el enrutado debe realizarse de forma eficiente para evitar que el mismo protocolo añade un tráfico a la red desmesurado. Además, el número de nodos suele ser grande, y a esto se le puede añadir la componente de la movilidad de nodos. En resumen, la tarea de enrutar paquetes en una red ad-hoc es realmente compleja, y existen numerosas líneas de investigación que tratan de solventar los problemas asociados (17, 18 y 19).

Aún quedan más dificultades por añadir en el momento en que consideramos el escenario de las comunicaciones militares. Un enrutado dinámico que soporte cambios en la topología, que sea flexible según las circunstancias es imprescindible. También es fundamental que sea robusto, y no se produzca la pérdida de rutas al desaparecer nodos.

En general, se puede hablar de dos tipos de enrutado básicos. Los protocolos proactivos y los reactivos. En los primeros, la ruta se descubre en cuanto la red se despliega, y se va modificando cada vez que sea necesaria una actualización. Se añade una cantidad de tráfico de control a la red bastante grande, pero una vez que tenemos las rutas diseñadas, cada vez que un nodo tenga que transmitir un paquete lo hará de forma inmediata, por lo que son protocolos de baja latencia. Los protocolos reactivos, sin embargo, no realizan el descubrimiento de la ruta hasta que tienen un paquete que transmitir. Conocerán solamente, por tanto, las rutas que necesiten. Se malgastan muchos menos recursos, ya que el tráfico de control asociado es mucho menor, pero la latencia es mucho mayor porque cada vez que llega un paquete debemos redescubrir la ruta antes de mandarlo. Existen protocolos híbridos intermedios que intentan recoger lo mejor de ambas aproximaciones.

Otras aproximaciones, como el enrutado geográfico, implican conocer la posición, al menos aproximada, del nodo receptor. Siendo así, múltiples protocolos explotan ese conocimiento para optimizar el enrutado.

En redes *ad hoc*, múltiples investigadores tratan de realizar protocolos de enrutado robusto. Algunos de ellos presentan modificaciones robustas de protocolos conocidos, como Robust AODV, que es un protocolo reactivo que utiliza actualizaciones locales para dar robustez a las rutas, ya que las rutas son capaces de adaptarse rápidamente a los cambios de la topología. Otros protocolos están diseñados para redes móviles.

En los cuadros 2 y 3 se muestran listas resumidas de los protocolos actuales más destacados. Se añaden solamente para mostrar la gran variedad de protocolos existentes, y la complejidad de este campo. En los protocolos proactivos, se observa que muchos no tienen nodos críticos, lo que evidentemente les proporciona robustez.

Basic characteristics of proactive routing protocols

Protocol	RS	Number of tables	Frequency of updates	HM	Critical nodes	Characteristic feature
DSDV	F	2	Periodic and as required	Yes	No	Loop free
WRP	F	4	Periodic	Yes	No	Loop freedom using predecessor info
GSR	F	3 and a list[a]	Periodic and local[b]	No	No	Localised updates
FSR	F	Same as GSR	Periodic and local[b]	No	No	Controlled frequency of updates
STAR	H	1 and a 5 lists	Conditional[c]	No	No	Employes LORA and/or ORA. Minimize CO
DREAM	F	1	Mobility based	No	No	Controlled rate of updates by mobility and distance
MMWN	H	Maintains a database	Conditional	No	Yes, LM	LORA and minimized CO
CGSR	H	2	Periodic	No	Yes, Clusterhead	Clusterheads exchange routing information
HSR	H	2 (link-state table and location management)[d]	Periodic, within each subnet	No	Yes, Clusterhead	Low CO and Hierarchical structure
OLSR	F	3 (Routing, neighbour and topology table)	Periodic	Yes	No	Reduces CO using MPR
TBRPF	F	1 Table, 4 lists	Periodic and differential	Yes	Yes, Parent node	Broadcasting topology updates over a spanning tree

R = routing structure; HM = hello message; H = hierarchical; F = flat; CO = control overhead; LORA = least overhead routing approach; ORA = optimum routing approach; LM = location manager.

[a] GSR also has a list of all available neighbours.

[b] In GSR and FSR link-state is periodically exchanged with neighbouring nodes.

[c] In conditional update methods, the updates occur if a particular event occurs.

[d] Number of link-state tables may vary according to the number of logical levels.

Figura 4. Tabla resumen protocolos proactivos.

Basic characteristics of reactive routing protocols

Protocol	RS	Multiple routes	Beacons	Route metric method	Route maintained in	Route reconfiguration strategy
AODV	F	No	Yes, hello messages	Freshest & SP	RT	Erase route then SN or local route repair
DSR	F	Yes	No	SP, or next available in RC	RC	Erase route the SN
ROAM	F	Yes	No	SP	RT	Erase route &[a]
LMR	F	Yes	No	SP, or next available	RT	Link reversal & Route repair
TORA	F	Yes	No	SP, or next available	RT	Link reversal & Route repair
ABR	F	No	Yes	Strongest Associativity & SP &[b]	RT	LBQ
SSA	F	No	Yes	Strongest signal strength & stability	RT	Erase route then SN
RDMAR	F	No	No	Shortest relative distance or SP	RT	Erase route then SN
LAR	F	Yes	No	SP	RC	Erase route then SN
ARA	F	Yes	No	SP	RT	Use alternate route or back track until a route is found
FORP	F	No	No	RET & stability	RT	A Flow_HANDOFF used to use alternate route
CBRP	H	No	No	First available route (first fit)	RT at cluster head	Erase route then SN & local route repair

RS = routing structure; H = hierarchical; F = flat; RT = route table; RC = route cache; RET = route expiration time; SP = shortest path; SN = source notification; LBQ = localised broadcast query.

[a] Start a diffusing search if a successor is available, else send a query with infinite metric.

[b] Route relaying load and cumulative forwarding delay.

Figura 5. Tabla resumen protocolos reactivos.

Existen pocos protocolos de enrutado comerciales especializados en redes mesh. Un caso interesante es el protocolo de *mesh networks*. Una vez analizadas las necesidades especiales de las redes mesh han desarrollado un protocolo dinámico, que permite autoconfiguración de los nodos, y que está a caballo entre los

protocolos reactivos y proactivos. Además permite configuraciones mesh y con jerarquía. Implementa también un sistema para aumentar la vida de los nodos, teniendo en cuenta el nivel de batería de cada uno a la hora de establecer las rutas. Sirva este protocolo de ejemplo práctico, aún con muchas limitaciones, de las posibilidades que las redes ad-hoc pueden tener si la tecnología es capaz de resolver las dificultades asociadas a esta topología.

Sensores

Dentro de las redes *ad hoc*, destacan, como se ha comentado ya, las redes inalámbricas de sensores. Hemos analizado sus características más destacables, en todo lo que a su dimensión de red de comunicaciones se refiere. Aquí nos referimos a los sensores en sí mismos.

Algunos tipos de sensores son: los sensores de movimiento, sensores de presión, de temperatura, de humedad, de detección de gases, de detección de componentes bioquímicos, sensores magnéticos, sensores de radiación, sensores de movimiento, sensores de aceleración, etc.

Destacan los sensores de infrarrojos que se emplean para localizar y seguir objetivos, para la guía de misiles y para recopilar información. Las imágenes infrarrojas se utilizan también para detectar minas escondidas y para desarrollar sistemas de alarma preventivos.

Las aplicaciones típicas de todos estos sensores son la vigilancia, establecimiento de perímetros de seguridad, detección de personas, localización, seguimiento de objetivos, detección de ataques NBQ.

Tanto en la localización y seguimiento como en la recopilación de información, así como en la detección de ataques químicos o biológicos resulta especialmente conveniente el despliegue de los sensores como una red inalámbrica, que permita la distribución de la información y la mejora del procesamiento de la misma.

Todas estas tecnologías están enormemente avanzadas, y comercialmente se encuentran multitud de opciones tecnológicas diferentes para la misma aplicación (20).

Confidencialidad

El rápido crecimiento de los sistemas de comunicaciones inalámbricos ha puesto de manifiesto un problema común a todos ellos: la seguridad. Muchos de estos sistemas nacieron sin la preocupación primordial de proporcionar seguridad a los usuarios. Según pasan los años el uso de este tipo de comunicaciones está más extendido en las comunicaciones entre empresas, particulares o el ejército. A la vez, diferentes y tipos de ataques amenazan la seguridad de los sistemas creados. Hoy en día, los investigadores están muy ocupados desarrollando nuevas tecnologías seguridad y tapando los agujeros de las ya creadas (21).

De forma clásica, las comunicaciones por cable también han necesitado protegerse de ataques. Sin embargo, las características propias de los sistemas inalámbricos ofrecen un mayor reto a los diseñadores de sistemas de seguridad. En las comunicaciones por cable, para acceder a una red, es necesario en primer lugar tener una conexión física con esa red. En las conexiones inalámbricas esta conexión física es mucho más vulnerable, ya que cualquier persona dentro de la zona de cobertura de la red está conectado físicamente. Ello supone una diferencia básica tanto en el tipo de ataques como en la filosofía a aplicar para los diseños de sistemas de seguridad.

Analizamos brevemente los tipos de amenazas que una red inalámbrica puede tener. La taxonomía de las amenazas ha sido analizada en diversos documentos científicos, pero se puede resumir en algunas líneas generales.

En primer lugar, diferenciamos entre amenazas desde fuera (*outsiders*) o desde el interior de la red (*insiders*). Los outsiders tienen acceso a la red inalámbrica y el *software* y *hardware* que utilizan no es interno a la red, sino comercial. Los insiders son usuarios legales de la red cuyo objetivo es obtener datos de la red a los cuales no tienen acceso de forma legítima. Utiliza por tanto *software* y *hardware* propio de la red, totalmente válido (22).

En general, existen tres tipos de ataques genéricos. El primero es un ataque de disponibilidad. Se trata de impedir la conexión física en la red (el equivalente a cortar un cable) normalmente introduciendo interferencias potentes en la red, para que ningún receptor pueda detectar información útil. El segundo de los tipos genéricos es

el ataque contra la confidencialidad y el tercero son ataques que violan la integridad de los datos.

De forma más concreta diferenciamos siete tipos de ataques. Tres de ellos únicamente violan la confidencialidad o privacidad de la sesión y son: análisis del tráfico, escucha pasiva y escucha activa. Otros tres violan la integridad y otro se sitúa a caballo entre estas dos situaciones. Los siete casos son:

1. Análisis de tráfico: el atacante únicamente es capaz de leer la cantidad de paquetes y el tipo de paquetes que se están enviando, pero no es capaz de leer la información que los paquetes contienen. Puede hacerlo con cualquier antena situada dentro de la red y una tarjeta que incluya el nivel físico y el nivel de enlace la red espiada. Le permite tres cosas: detectar que existe actividad (detectar la red), detectar la posición de los puntos de acceso, routers, nodos, y así poder detectar zonas más vulnerables; y el tipo de protocolo que la red utiliza, basándose en el tipo, tamaño y número de paquetes que detecta.

2. Escucha pasiva: el atacante escucha de forma pasiva los paquetes y los datos contenidos en los paquetes. Si los datos están encriptados debe desencriptarlos para leer contenido. El peligro no es sólo que el atacante lee la información, y por tanto rompe la privacidad, sino que se puede hacer con datos que luego le faciliten un ataque mucho más peligroso.

3. Escucha activa: el atacante escucha la transmisión de paquetes, es capaz de leer su carga, y además puede incluir paquetes de datos en la transmisión con el propósito de facilitar la escucha. Por tanto, no modifica los datos, pero sí se asegura mediante pequeñas transmisiones que tendrá todas las claves necesarias para la escucha.

4. Atacante en el medio: el atacante rompe una sesión establecida entre un nodo y un punto de acceso, y cuando el nodo intenta volverse a conectar, el atacante suplanta al punto de acceso, consigue información, y se conecta también al punto de acceso, con lo que el nodo cree estar conectado como siempre, pero en realidad sus datos pasan por el atacante. Cuando sólo existe encriptación a nivel de red o nivel tres (en una red privada virtual, por ejemplo) este ataque permite

obtener y modificar la información a nivel dos. Es un ataque que viola la confidencialidad y tiene potencial para violar la integridad de los datos.

5. Acceso no autorizado: un atacante externo intenta acceder a la red en su conjunto, consiguiendo identificarse de alguna manera en un punto de acceso. Una vez conseguido puede lanzar otros ataques.

6. Suplantación de sesión: el atacante corta una sesión y suplanta al nodo que se ha identificado correctamente, obteniendo así privilegios y permisos para hacer lo que quiera dentro de la red.

7. Ataque por réplica: el atacante saca información de una sesión actual para más tarde poder identificarse y entrar en la red, replicando las claves y mecanismos de acceso que el objetivo utilizó.

¿Cómo actuar frente a estos ataques? Depende de la aplicación y de las posibles consecuencias del ataque. En general, las técnicas para proporcionar seguridad utilizan la modulación, codificación, encriptación, *interleaving* (entrelazado de datos) y autenticación. Un esquema lógico de estas técnicas es el representado en la figura 6 (23).

El encriptado es una capa que modifica los datos enviados con algún algoritmo. Los más complejos sólo se pueden decodificar con una inspección continuada y analítica de los datos, y mediante procesado intensivo. Las agencias de seguridad de Estados Unidos utilizan un código de encriptado con una clave de 64 bits, lo que haría necesario 1.27×10^{89} operaciones matemáticas para poder decodificar los datos “por la fuerza bruta”.

El *interleaving* consiste en desordenar de forma pseudoaleatoria los datos. Unida a la codificación del encriptado, resulta complejo su intercepción, ya que los datos aparecen como ruido en el receptor que no conoce el algoritmo.

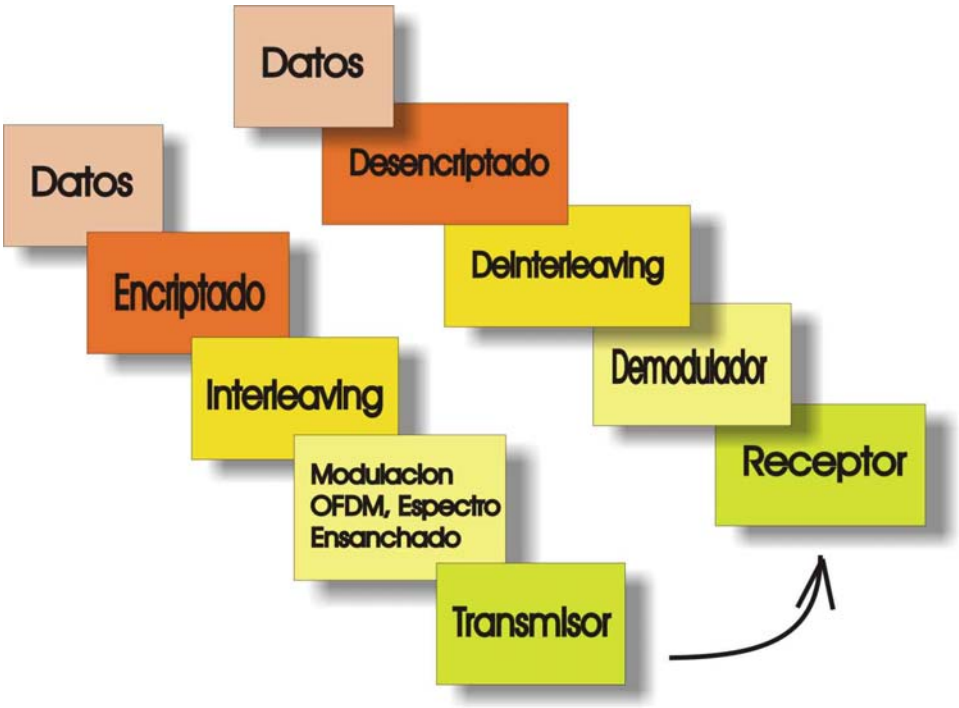


Figura 6. Esquema lógico técnicas de seguridad.

La modulación también puede ser una parte muy importante del sistema para proporcionar seguridad. En general, las técnicas de espectro ensanchado permiten enviar la información abarcando un espectro muy amplio pero sin enviar mucha potencia en cada banda de frecuencia, lo que las hace difícilmente detectables. Por otra parte, la codificación con la que se ensancha el espectro CDMA (*Frequency Hopping*) tienen siempre un carácter de aleatoriedad que genera robustez frente a aquellos intrusos que no conocen el código. Cambiar la frecuencia central de emisión cada cierto tiempo es también una técnica muy utilizada para dar mayor seguridad a las transmisiones FH (*Frequency Hopping*). Cabe destacar en este punto las redes de baja probabilidad de intercepción LPD. Se trata simplemente de utilizar las características mencionadas del espectro ensanchado llevándolas al extremo, de forma que se transmita una potencia tan baja que la señal quede por debajo de la potencia de ruido. Para cualquier receptor de banda estrecha o que no tenga el código de ensanchado la señal se recibe como ruido indetectable.

Equipos disponibles en el mercado

A estas alturas existen numerosos productos en el mercado relacionados con las redes *ad hoc.* En general, podemos encontrar empresas que ofrecen soluciones basadas en ZigBee, WiFi, UWB o en menor medida, WiMAX. Señalamos aquí las más destacadas, que ofrecen soluciones *ad hoc* o mesh independientemente de la tecnología de enlace que utilicen. En el cuadro 4 se resume la información más relevante de cada compañía y sus productos, señalando una pequeña descripción de cada uno.

Compañia	**Producto**	**Descripción / Comentarios.**
Ascentry	Instantly Deployable Interoperable Communications.	Una plataforma ad-hoc de propósito general que proporciona conectividad. Aplicaciones: seguridad, defensa, redes instantáneas, …
BTNode	BTNode	Plataforma hardware y software basada en tecnología Bluetooth como demostración de redes ad-hoc móviles.
Colligo	Conexión ad-hoc	Software para gestionar redes ad-hoc entre ordenadores personales y portátiles.
Dust Networks	Dust Networks' SmartMesh™	Proporciona una red mesh para sensores y sistemas de control de forma totalmente inalámbrica.
Firetide	HotPort™ High Performance Mesh Network	Proporciona redes mesh que funcionan a 4.0 GHz para situaciones de emergencia.
BelAir Networks	BelAir Mesh	Ofrecen redes mesh de gran cobertura que soportan movilidad.
Kiyon Inc	Kiyon Autonomic Networks	Redes ad-hoc que no necesitan gestión externa y que soportan cualquier aplicación con cualquier calidad de servicio.
LocustWorld	LocustWorld MeshAP	Diseñan redes mesh con funcionalidades extras y ofrecen el núcleo del software de su diseño en su web.
Strix Systems	Access/One Network	Desarrollan redes mesh empleando sistemas multi-radio y multi-canal para ofrecer soluciones escalables y flexibles basadas en redes mesh.
MeshDynamics	Hybrid Mesh™ Networks for Public	Desarrollan redes mesh híbridas para uso militar.

	Safety Network and the Battlefield	
AutoNet	AutoNet	Una red ad-hoc punto a punto para redes de tráfico.
Millenial Net	MeshScape™	Redes mesh para comunicaciones en grandes edificios de negocios y entornos difíciles.
NovaRoam	Tactical, Practical Meshed Networks™	Redes robustas y de largo alcance para situaciones de alta movilidad.
OrderOne	OrderOne Network	Redes para miles de nodos, con alta movilidad, auto-configurables.
AeroComm	MeshRF™ Protocol	Redes mesh de corto alcance a 900 MHz.
Sarnoff Corp.		Redes inalámbricas ad-hoc para acceso a Internet y en general, comunicaciones corporativas.
MobileRoute	Wireless Ad-hoc Routing Protocol	Protocolo de enrutamiento para redes ad-hoc.
Tropos Networks	MetroMesh	Tecnologías de acceso con redes mesh para comunicaciones empresariales o urbanas en general.
MeshNetworks (ahora Motorola)	Varios	Gran distribuidor y pionero de redes mesh y protocolos asociados. Ahora comprada por Motorola.

Tabla 4. Productos *ad hoc* en el mercado.

Temas abiertos de investigación

BATERÍAS/CONSUMO/VIDA ÚTIL

El concepto de redes *ad hoc* o redes mesh es relativamente amplio. Se pueden incluir aquí desde redes de una decena de ordenadores personales conectados sin punto acceso hasta redes de decenas de miles de pequeños sensores distribuidos aleatoriamente por un campo de cultivo con el objetivo de tener medidas de humedad precisas en todos los puntos.

Sin embargo, prácticamente en todos los casos el concepto de red *mesh* va unido al concepto de autonomía. Autonomía para que la red se configure automáticamente, autonomía para que no se produzcan fallos, o para que se recalculen las rutas si un nodo cae. Pero, evidentemente, también autonomía energética. En algunos la

energía será un bien escaso a cuidar (PC portátil) y en otros un recurso limitado que no se puede reponer (nodo en medio del campo, una vez que se queda sin batería, muere).

Por ello un porcentaje altísimo de la investigación en redes *ad hoc* se ha desarrollado entorno al concepto de eficiencia energética. Recortar el gasto de batería en cada una de las tareas que realiza un nodo permite alargar la vida del nodo en la mayoría de los casos, o bien simplemente darle más autonomía, que en ocasiones puede ser vital para que una red tenga utilidad práctica. Será necesario, por lo tanto, analizar donde se produce el gasto energético y cuál es la mejor manera de limitarlo. En este tipo de redes, el problema energético tiene a veces una dimensión peculiar, ya que muchas veces no se trata de minimizar el consumo en un nodo, sino de maximizar la vida de la red, ya que la existencia o no de un nodo concreto no es importante para muchas aplicaciones.

Mirando la literatura existente se pueden encontrar cientos de artículos que tratan el tema desde aproximaciones muy diversas (24). Desde el punto de vista del nodo, diferentes trabajos desarrollan arquitecturas hardware de bajo coste, computación limitada por la energía del nodo, software eficiente energéticamente y radios que realizan gestión de potencia. También se han tenido usado modelos no ideales de baterías, que tienen en cuenta las características no lineales de las baterías reales.

Desde el punto de vista de la red, las aproximaciones más importantes son el enrutado eficiente y el protocolo de acceso al medio eficiente. Al hablar de enrutado eficiente energéticamente, cambiamos la perspectiva habitual del enrutado, que es lograr el transporte de los datos en el menor tiempo posible, y migramos a una orientación distinta, que es encontrar las rutas actuales y futuras que maximicen el tiempo de vida de la red. En los protocolos de acceso al medio, encontramos numerosos artículos que intentan discernir qué método de acceso es óptimo, analizando sistemas CDMA, TDMA, etc., y viendo la mejor manera de no incrementar el tráfico con las gestiones propias de estos protocolos.

SEGURIDAD

Como hemos mencionado antes el tema de seguridad es crítico en comunicaciones inalámbricas, tanto militares como civiles. Hasta la fecha se han desarrollado

multitud de de algoritmos en todos los niveles que pretenden proporcionar un nivel de seguridad determinado a una red concreta.

El desarrollo más conocido es el relacionado con redes inalámbricas 802.11. En este estándar se incluye el protocolo WEP (*Wire Equivalent Protocol*) como intento de simular la seguridad de redes cableadas, utilizando claves cifradas para cada usuario registrado.

Un aspecto muy importante y que aún representa un reto es la habilidad de autentificar las fuentes de información de una manera fiable. En entornos militares, o en aplicaciones de transacciones comerciales es una cuestión crítico. Hay diversas maneras de llevar a cabo, todas ellos englobadas bajo el acrónimo PKI (*Public Key Infrastucture*), y son actualmente uno de los puntos calientes en la investigación.

Otro aspecto en desarrollo actualmente es el proporcionar seguridad en las redes inalámbricas mediante la conexión a través de redes privadas virtuales. El gran problema que esto representa es que es una seguridad a nivel tres o superiores, y necesita ser acompañada por otros mecanismos de niveles inferiores.

En esta misma línea, el uso de Firewalls especializados en comunicaciones inalámbricas es otra línea de investigación importante en estos momentos para aplicaciones como WAP, (21).

La criptografía utilizada en el 802.11 es conocida y presenta ya dificultades, por lo que nuevos algoritmos son necesarios. Hasta ahora, otros protocolos utilizaban técnicas que incluían el uso de certificados y técnicas de gestión de claves simétricas. En cualquier caso, todos estos tipos de técnicas asumen el conocimiento previo de algún tipo de semilla con el que generar la clave. En una red *ad hoc* las dificultades que esto implica son grandes, debido a la gran movilidad de los nodos y la variabilidad de la topología (25).

La autenticación de los nodos es otro problema en el que sigue habiendo muchos puntos oscuros. En WiFi se utiliza un protocolo basado en claves encriptadas compartidas, que utilizan la dirección de la tarjeta MAC. Si un atacante escucha la conversación y es capaz de leer la dirección de la tarjeta la seguridad de la red estará comprometida.

Frente a todos estos problemas una serie de nuevos estándares están siendo desarrollados. De ellos destacamos PIC (*Pre-IKE Credential*), en el que existe un servidor de licencias donde cada usuario debe solicitar una clave que luego utilizará en sus otras comunicaciones. También en desarrollo está OMAP, un protocolo de Texas Instruments que implementa una librería de software que se usará en terminales y nodos inalámbricos utilizados para transacciones comerciales. MeT es un consorcio de grandes productores de teléfonos móviles para afrontar estos temas de seguridad. Por último la utilización técnicas biométricas conforma el estado del arte de las tecnologías de seguridad inalámbrica.

Análisis de prestaciones y limitaciones en campo militar

de las redes ad hoc

Seguridad

Una vez analizadas las técnicas generales de seguridad para redes inalámbricas, analizamos los requerimientos típicos de las comunicaciones militares (26, 27 y 28). En este escenario, surge el concepto de seguridad multinivel. En este concepto las entidades no son simplemente seguras o inseguras, sino que tienen diversos grados de sensibilidad (como difusión limitada, confidencial, reservado o secreto) que origina la coexistencia simultáneamente de distintas redes en el teatro de operaciones o zona de crisis. Los esquemas deben, por tanto, proporcionar comunicaciones que puedan soportar estas clasificaciones. Evidentemente, en redes *ad hoc*, esto debe ser conseguido por protocolos de enrutado complejos.

Para ello, se deben asegurar los siguientes requerimientos:

- Todos los nodos participantes en un protocolo deben tener un determinado nivel de privilegio de lectura y transmisión. Cada entidad leerá o transmitirá sólo aquellos mensajes que tiene permitido por ese nivel.
- Todos los mensajes intercambiados por el canal deben tener un nivel en la clasificación anterior.
- Todos los nodos deben ser autenticados correctamente antes de poder participar en la comunicación.

- El origen de los datos puede ser cualquier participante, siempre y cuando transmita mensajes que estén dentro de sus limitaciones de seguridad.

- Los nodos de mayor nivel pueden leer todos los mensajes y tomar todas las decisiones, y pueden transmitir en cualquier nivel.

- Es necesario disponer de mecanismos para echar a un miembro del grupo.

- Los datos deben ser totalmente secretos de cara a agentes externos a la red.

- Es necesario que la identidad de los miembros legítimos del grupo permanezca también en secreto, para evitar intrusos suplantadores.

Dentro del genérico mundo de las redes *ad hoc* móviles existen protocolos que tratan de ofrecer seguridad en sus transmisiones, dando solución al problema que conlleva la seguridad multinivel en un escenario de difusión multisalto. Algunos de ellos son:

- ARAN (*Authenticated Routing for Ad hoc Networks*). Es un protocolo de enrutado reactivo, que usa certificados encriptados para asegurar la seguridad en el enrutado. El problema que tiene es que usa criptografía asimétrica, que no es adecuada para una red ad-hoc en la que todos los nodos son parecidos en complejidad.

- Ariadne: basado en MAC (*Messae Authentication Code*) y TESLA, un protocolo de gestión de claves. Necesita que el transmisor sea consciente de la topología de la red y no permite que el receptor autentifique un paquete inmediatamente a su llegada. Además no proporciona confidencialidad en los mensajes.

- LHAP (*Lightwight Hop-by-hop Authentication Protocol*). Está diseñado para una red genérica. Requiere un gran número de operaciones por nodo para asegurar la seguridad.

- SAR (*Security-aware Ad hoc Routing*). Asigna distintos niveles de seguridad a cada nodo y los paquetes sólo pueden enrutados por nodos de igual nivel de seguridad. Esta restricción en el camino que puede tomar el paquete es excesiva para una red *ad hoc*.

Finalmente, algunos trabajos tratan de cubrir todos los requerimientos, como el de (M. Choudhary), que integran todas las características permitiendo diferenciar cada individuo o paquete según distintos niveles de seguridad.

En resumen, observamos como el tema de seguridad en comunicaciones inalámbricas, especialmente militares donde los requerimientos son más estrictos, es un tema abierto tanto en investigación, como en desarrollo, como a nivel de mercado. Existen soluciones probadas y robustas pero que no ofrecen toda seguridad requerida. Los protocolos más avanzados están todavía en sus primeras fases de desarrollo. Representa por tanto un aspecto clave de este tipo de comunicaciones, en especial en las basadas en redes *ad hoc*.

Robustez

Al describir los distintos tipos de redes *ad hoc* utilizables en entornos militares hemos hecho mención a los problemas y ventajas de robustez que las redes *ad hoc* representan. En este apartado, se resumen los aspectos más importantes teniendo en cuenta las distintas opciones (7).

En primer lugar, cabe destacar que el uso de las redes *ad hoc* se considera apropiado para aplicaciones militares por dos motivos fundamentales: rapidez de despliegue y flexibilidad y por la robustez de esta solución. Como ya hemos mencionado, la gran ventaja de una topología mallada pura es que ningún nodo es imprescindible, y por tanto, si el diseño de la red está bien realizado, y se dan las condiciones de conectividad necesarias, no existe ninguna otra configuración más segura frente a pérdidas de nodos o ataques externos.

Sin embargo, este primer análisis debe puntualizarse brevemente. En primer lugar porque las condiciones de conectividad necesarias implican que cada nodo tenga en su rango de cobertura a varios nodos, cuantos más mejor, y que la red no se disgregue en ningún momento en pequeñas redes, es decir, es decir, que exista una continuidad en la malla formada por los nodos. Esto no siempre será posible, en especial en situaciones conflictivas o en zonas controladas o cercadas por el enemigo, o en zonas montañosas.

Existen además casos especiales como unidades aisladas o soldados en campo enemigo que no deberían o no querrían delatar su posición con una transmisión continua necesaria para actuar como repetidores en una red *mesh*.

Por tanto para asegurar la conectividad y por tanto la robustez es necesario, bien de asegurar la existencia de una densidad de nodos suficiente, bien dotar a la red de puntos de acceso visibles por todos los nodos, a modo de eje troncal, con algunas de las soluciones indicadas en el primer apartado.

Por supuesto, estas soluciones por sí mismas son menos robustas que una red mallada pura, a no ser que se disponga de una redundancia suficiente de nodos troncales. Uniendo ambas aproximaciones, la red mallada pura y la red, se obtendría, desde el punto de vista de la estructura de la red y la conectividad, un sistema robusto resistente a fallos y ataques.

Queda sin embargo el análisis de robustez en capas superiores, íntimamente ligado al de la seguridad. El uso de sistemas de espectro ensanchado, por ejemplo, proporciona robustez en el nivel físico, ya que hace más difícil producir una interferencia malintencionada. Otros sistemas, como los de encriptación y autenticación proporcionan robustez en las comunicaciones a niveles superiores.

Por todo lo dicho, se puede concluir que aunque la robustez en las redes *ad hoc* es aún tema abierto, con mucho camino de investigación por delante, con el diseño adecuado y conjuntamente con soluciones híbridas, las redes *mesh* representan una opción que mejora la robustez de los sistemas en comunicaciones tácticas, que es donde su uso es más indicado.

Utilización en comunicaciones de nivel estratégico

y nivel operacional

A lo largo de los primeros apartados hemos analizado los tipos de redes *mesh* y sus características, así como el estado del arte de las tecnologías implicadas y los productos existentes. Este apartado recoge las ideas desarrolladas para concluir con la viabilidad del uso de las redes ah-hoc en comunicaciones de nivel estratégico y operacional. El siguiente apartado lo hará con las comunicaciones tácticas.

De entre las características exigibles en una red de este tipo destacan la fiabilidad y robustez de la red, una facilidad relativa de despliegue, un alcance amplio, y una seguridad de muy alto nivel.

Si bien todas estas características se pueden alcanzar con una red ad-hoc con tipología mallada pura, no existe en la práctica ninguna necesidad de recurrir a estos sistemas novedosos que añaden tanta complejidad a los nodos.

Como se ha explicado anteriormente, la fiabilidad y robustez de la red se pueden alcanzar con redes híbridas, o redes celulares de rápido despliegue, que utilicen un único salto inalámbrico y luego encaminen los datos por canales más robustos. El despliegue, que no tiene que ser tan ágil como en el campo de batalla, se adapta perfectamente a las características de las redes híbridas o a las soluciones basadas en telefonía celular de rápido despliegue. La seguridad, incluso, mejora si optamos por redes con menos saltos inalámbricos.

Por tanto, en comunicaciones de nivel estratégico y nivel operacional resulta conveniente el uso de redes *ad hoc* que utilicen algún tipo de jerarquía, o soluciones híbridas en los que la zona mallada o *ad hoc* sea sólo el salto final hacia el posible usuario móvil. Estos tipos de redes se han descrito en el primer apartado, y representan las alternativas más claras para las comunicaciones mencionadas, como así los atestiguan los numerosos casos prácticos llevados a cabo.

Utilización en comunicaciones de nivel táctico

Las comunicaciones de nivel táctico deben ser robustas, seguras, y permitir rapidez en el despliegue. Además, el número de nodos a comunicar puede ser elevado, y la topología muy cambiante.

Para la realización práctica de una red de estas características resulta conveniente el tipo de red *ad hoc* mallada pura. Una estructura mesh permite, siempre y cuando la densidad de nodos sea suficiente, un red de comunicaciones muy robusta y de despliegue inmediato.

Reforzar estas redes con enlaces de reserva que usen nodos troncales, es una buena táctica que asegura la comunicación en situaciones especiales en las que la densidad de nodos no es suficiente o las circunstancias así lo aconsejan.

Para ello, cada soldado, vehículo móvil, elemento de artillería, etc, puede representar un candidato ideal para soportar un nodo. Un despliegue masivo de centenares o incluso miles de nodos pequeños y difícilmente detectables asegura una conectividad total, y es otra de las alternativas en investigación en la actualidad.

De todo lo dicho se desprende que las redes mesh puras representan potencialmente el núcleo futuro de las comunicaciones de nivel táctico, siempre y cuando los retos tecnológicos a los que se enfrentan estas complejas redes sean soluciones, y siempre y cuando los diseños se vean reforzados por otras redes clásicas para situaciones especiales.

Aplicaciones avanzadas de redes *ad hoc*

Existen muchas aplicaciones específicas de este tipo de redes en el entorno militar. En primer lugar están las de comunicaciones que se han comentado ya. También existen muchas basadas en redes de sensores. Describimos las líneas generales de los grandes grupos de aplicaciones, algunas de ellas en desarrollo (2 y 29).

Comunicaciones

Como se han comentado hasta ahora una aplicación importante de las redes *ad hoc* en campo militar es su capacidad para proporcionar redes de comunicación de rápido despliegue, flexible, móviles y robustas frente a ataques, en especial para comunicaciones tácticas.

Monitorización de fuerzas amigas, equipamiento y munición

En una situación de conflicto el equipo de mando puede monitorizar constantemente el estado de sus tropas, las condiciones y disponibilidad del equipamiento y la munición en el campo de batalla. Cada tropa, vehículo, equipamiento y munición crítica puede llevar un nodo que informe sobre su estado. La información se envía a nodos con capacidad de transmisión de gran ancho de banda que lo reenvían al centro de mando.

Vigilancia en campo de batalla

Terrenos críticos, rutas de acceso y caminos importantes pueden ser objeto de un despliegue de redes de sensores que permitan monitorizarlas. De esta manera, en todo momento se puede recopilar información sobre la actividad en esos puntos.

Reconocimiento de las fuerzas enemigas y los terrenos ocupados

Pequeños nodos, casi indetectables, pueden ser dispuestos en el terreno enemigo para obtener información valiosa y detallada sobre su posición y otros parámetros importantes.

Información sobre daños

Antes y después de un ataque se pueden desplegar redes de sensores que cuantifiquen los daños y realicen un informe de la situación.

Detección precoz de ataques nucleares, biológicos y químicos

La detección precoz de un ataque de estos tipos es muy importante, pero muy complicada sin poner en peligro a seres humanos. Desplegar una red por toda la zona de interés permite avisar de ataques nucleares, biológicos o químicos, y además determinar la naturaleza del ataque.

Localización

Las redes mesh tienen la capacidad de ofrecer un sistema de posicionamiento 3D de alta precisión. También permiten realizar el seguimiento del objetivo y todo ello sin la necesidad de usar satélites. Extraer información de localización mediante el Sistema de Posicionamiento Global (GPS) siempre es más complicado que cuadrar la posición de un objetivo con nodos situados a escasos cientos de metros entre sí. Los sistemas actuales basados en esta tecnología (*mesh netoworks position system*) permiten precisiones de menos de diez metros a velocidades mayores de 250 Km/h.

Seguimiento de vehículos militares

Cada vehículo militar amigo puede llevar incorporado un nodo que le permita dar su posición a los nodos más cercanos, que, formando una red *ad hoc* envían la información al centro de mando.

Despliegue de minas inteligentes

Las minas anti-tanque son equipadas con equipos de comunicaciones y sensado que aseguran que una determinada zona está cubierta. Si se detecta el fallo de una mina en una zona se envía el mensaje para que sea sustituida.

Localización de francotiradores

Detectar y localizar de forma precisa francotiradores es una tarea complicada para la que no existe hasta ahora una solución fiable. Existen múltiples aproximaciones a este problema, algunas de ellas basadas en redes *ad hoc*. La más actual y más potente consiste en una red *ad hoc* compuesta de sensores inalámbricos de bajo coste. Después del despliegue los sensores sincronizan sus relojes, se auto-organizan y esperan eventos acústicos. Los sensores pueden compartir la información que detectan y conseguir así detectar un sonido de bala, calcular su velocidad y su dirección, de manera que pueden estimar la posición donde se generó el disparo.

BIBLIOGRAFÍA

[1] R. Ramanathan, J. Redi. “A brief overview of ad hoc networks: Challenges and directions”. IEEE Commun. Mag., vol 40, no 5, pp 20-22, May 2002.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramanian, E. Cacyirci, “Wireless sensor networks: a survey”, Computer Networks (Elsevier) Journal, vol. 38, no 4, pp 393-422, Mar. 2002.

[3] I. F. Akyildiz, X. Wang, W. Wang, “Wireless mesh networks: a survey”, to appear, Computer Networks Journal (Elsevier).

[4] MeshNetworks, “Mesh Networks Technologies”, Now Wireless Limited, http://mesh.nowwireless.com/technology.htm

[5] M. A. Buckner, S. Batsell, “Mobile Ad Hoc Networking”, Sensors Magazine Online, Enero 2001. http://www.sensorsmag.com

[6] R. Poor, “Wireless Mesh Networks”, Sensors Magazine Online, Intelligent Systems, Febr. 2003, . http://www.sensorsmag.com

[7] P. M. Feldman, “Emerging Commercial Mobile Technology and Standars: Suitable for the Army?”, RAND Documents, ref. MR-960-A, pags xvii-80. RAND Corporation, 1998.

[8] J. Nilsson, A. Hansson, U. Sterner, “The ability to provide services in military radio networks – A feasibility study”, IEEE, 2000.

[9] C. Y. Chong, S. P. Kumar, “Sensor Networks: Evolution, Opportunities and Challenges”, Proc. Of the IEEE, Invited Paper, agosto 2003.

[10] R. Kolic, “An introduction to Ultra Wideband (UWB) wireless”. Technology@Intel Magazine. http://www.intel.com/technology/magazine/. Intel Corp. 2004.

[11] Breeze Wireless Communications Ltd. “IEEE 802.11 Technical Tutorial” Wireless Communication. http://www.breezecom.com

[12] IEEE Standard, “802.11. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”. 1997

[13] J. M. Huidrobo, “WiMAX. ¿El sustituto de WiFi?”. http://www.monografías.com

[14] J. Hawk, “WiMAX Paln Aims To Cut Army Costs”. Signal AFCEA’s International Journal. Septiembre, 2005.

[15] D. Vazquez. “Homeplug y Zigbee”, http://www.casadomo.es, Mayo 2005.

[16] Zigbee Alliance, “Zigbee Specification”, http://www.zigbee.org/

[17] C. Jones, K. M. Sivalingam, P. Agrawal, J. C. Chen, “A survey of Energy Efficient Networks Protocols for Wireless Networks”, Wireless Networks, n 7, pp 343-358, Kluwer Academic Publishers, 2001.

[18] J. N. Al-Karaki, A. E. Kamal, “Routing techniques in wireless sensor networks: a survey”, Wireless Sensor Networks, IEEE 2004.

[19] Q. Jiang, D. Manivannan, “Routing protocols for Sensor Networks”, IEEE, 2004.

[20] Sensors Magazine Online, http://www.sensorsmag.com

[21] S. K. Miller, “Facing the challenge of wireless security”. Technology News. Computer Mag. Julio, 2001.

[22] D. Welch, S. Lathrop, “Wireless Security Threat Taxonomy”, Proc. Of the 2003 IEEE Workshop on Information Assurance. West Point, USA, Junio 2003.

[23] W. W. Manges, G. O. Allgood, “How Secure Is Secure?” Sensors Magazine Online, Intelligent Systems, Febr. 2002, . http://www.sensorsmag.com

[24] V. Raghunathan, C. Schurgers, S. Park, M. B. Srivastava. “Energy-aware wireless microsensor networks”, IEE Signal Processing Magazine, IEEE, Marzo 2002.

[25] V. Balakrishnan, Vijay Varadharajan, “Designing Secure Wireless Mobile Ad hoc Networks”, Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05), IEEE, 2005.

[26] J. J. Harrington, D. A. Pritchard, “Concepts and Applications of Wireless Security Systems for Tactical, Portable, and Fixed Sites”, IEEE, 1997.

[27] M. Choudhary, P. Sharma, D. Shangi, “Secure Multicast model for ad-hoc military networks”. IEEE, 2004.

[28] Niranjan, A. Ganz, “Adaptative Link Layer Security for wireless networks, (ALL-SEC)”, 2004 IEEE Military Communications Conference. IEEE. 2004.

[29] Miklos Maroti, Gyula Simon, Akos Ledeczi, and Janos Sztipanovit, Shooter Localization in Urban Terrain, Computer Magazine, Agosto 2004.

[30] K. Römer, F. Mattern, “The design space of wireless sensor networks”, IEEE Wireless Comm. Magazine. IEEE. Dic. 2004.

COMPOSICION DEL GRUPO DE INVESTIGACION

- David Ríos Insua. Catedrático de Estadística e Investigación Operativa y Vicerrector de Nuevas Tecnologías de la Universidad Rey Juan Carlos. Numerario (electo) de la Real Academia de Ciencias Exactas, Físicas y Naturales.
- Coronel José Antonio Valdivieso Dumont, Diplomado de Estado Mayor , Profesor del CESEDEN
- TCol. Carlos Alberich Landáburu, Jefe de Redes y Servicios de Red del CCEA del Ministerio de Defensa.
- Francisco Javier Ramos López, Director de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Universidad Rey Juan Carlos
- TCol. José Miguel Castillo Chamorro, Secretario de Estudios de la Escuela de Informática del Ejército
- Luis Pastor Pérez. Catedrático de Arquitectura y Tecnología de Computadores y Director del Departamento de Arquitectura y Tecnología de Computadores y Ciencia de la Computación e Inteligencia Artificial de la Universidad Rey Juan Carlos
- Eugenio Fernández Vicente, Profesor Titular EU y Director Académico del Servicio de Informática de la Universidad Rey Juan Carlos.
- Coronel Isaías Peral Puebla, Coronel de Transmisiones, Jefe de Comunicaciones e Informática de la Casa de S.M. el Rey.