UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Tesis doctoral

Arquitectura de comunicaciones de datos inalámbricas para sistemas C4ISR

Autor: Luis Ernesto Hernández Blanco

Director: Dr. D. Manuel Esteve Domingo

Octubre 2015

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Debo agradecer a muchas personas su ayuda, apoyo y colaboración a lo largo de los años que ha durado la realización de este trabajo de tesis.

En primer lugar, me gustaría agradecer de corazón al catedrático Manuel Esteve su paciencia, confianza, dedicación, motivación y apoyo en la dirección y supervisión de esta tesis doctoral, así como sus siempre acertados consejos que han hecho fácil lo difícil. Sinceramente, ha sido un privilegio el trabajar junto a él.

Quiero agradecer, a continuación, al resto de compañeros del grupo de investigación de Sistemas de Tiempo Real Distribuido, su inestimable colaboración y ayuda durante todos estos años me empujaron en la aventura de esta tesis doctoral. Muy especialmente a Israel Perez, Javier Martinez, Benjamín Molina, Fede Carvajal, el profesor Carlos Palau, Alfonso Climente, Ximo Mares y Flavio Pileggi han contribuido enormemente al desarrollo del presente trabajo y, sin su aportación, éste no se hubiera llevado a cabo.

También quiero agradecer a todas las personas con las que he tenido el privilegio de trabajar a lo largo del desarrollo de la presente tesis en los diversos proyectos y demostraciones realizados.

A mi padre por su apoyo e impulso constante para finalizar la tesis y en especial a mi madre que aunque no está hoy entre nosotros siempre me brindo su apoyo y amor constante para impulsarme por este arduo camino y desde el cielo comparte mi alegría por el objetivo conseguido, a mis hermanas por su apoyo y ayuda en todo momento y a mi familia en general, por todo lo que me han enseñado y dado.

Y finalmente a Rossana y Alejandro. Sin ellos, sin su apoyo, cariño y amor incondicional, esta tesis no hubiese sido posible, y nada tendría sentido.

En fin, son muchas personas que me han apoyado y ayudado a conseguir esta meta. Muchas gracias a todos.

Resumen - Los actuales sistemas de mando y control se basan en tecnologías inalámbricas como TETRAPOL, TETRA, HF, VHF, enlaces satelitales, etc., que a pesar de dar un amplio alcance, disponen de un ancho de banda muy limitado. Debido a estas limitaciones sólo se puede disponer de comunicaciones vocales y de transmisión de datos a velocidades bajas que no reproducen por completo el COP (Common Operacional Picture) de la situación de conflicto o emergencia.

Las comunicaciones en el campo de batalla son principalmente inalámbricas, sólo en algunos enlaces troncales se utilizan redes cableadas. Las redes de datos inalámbricas son considerablemente menos robustas, ya que generalmente sólo tienen una fracción de la capacidad de transmisión de sus homólogas cableadas, y también sufren problemas debido a la interferencia y propagación del entorno radio efecto que en las redes cableadas no suceden. Para combatir estos efectos, los protocolos inalámbricos suelen enviar información adicional para la corrección de errores, y pueden incluir algún tipo de transmisión redundante. En el ámbito militar el ancho de banda es realmente bajo y ciertas tecnologías no permiten la transmisión de información de vídeo. Los equipos radio HF y VHF utilizados ampliamente en los ejércitos de todo el mundo son un claro ejemplo.

Por lo tanto se hace latente la necesidad de disponer de un sistema de mando y control que permita proveer información desde y hacia las tropas de forma rápida y fiable. La presente tesis doctoral se enmarca en el desarrollo y evolución práctica de una arquitectura de comunicaciones de redes inalámbricas para sistemas C4ISR (Command Control, Computers and Communications Information Surveillance and Reconaissance), en particular los relativos a pequeñas unidades. Por pequeña unidad se entiende aquella que es de orden jerárquico menor o igual al de batallón en el ámbito militar o a una unidad autónoma de intervención en el ámbito de las emergencias.

En la tesis doctoral se describe la arquitectura de comunicaciones de SIMACOP (SIstema de MAndo y COntrol de Pequeñas unidades), el cual es un sistema C4ISR basado en tecnología COTS con capacidades de distribución de contenidos multimedia y fusión sensorial.

Las principales contribuciones tecnológicas en este marco son las siguientes: la arquitectura de comunicaciones cross-layer y cognitiva propuesta, la introducción de streaming de video y audio de alta calidad en la arquitectura de comunicaciones del sistema C4ISR, la detección de elementos a través de GPS, la fusión de datos recogida mediante distintos sensores desplegados en la zona de operaciones y la integración de diversos sistemas de comunicaciones inalámbricas con diversos anchos de banda. Por ejemplo, VHF, HF, comunicaciones satelitales, IEEE 802.11 y WiMAX (IEEE 802.16d), las cuales conforman la red a distintos niveles de mando que serán descritas en el presente trabajo. Los objetivos principales son estudiar e identificar las necesidades existentes en mando y control a nivel de comunicaciones tácticas, tanto en la vertiente civil como en la militar, y plantear una arquitectura de comunicaciones global para sistemas C4ISR que permita establecer comunicaciones multimedia a través redes móviles tácticas de nueva generación basadas en IP, incluyendo streaming de video para mejorar la conciencia situacional (SA) en cada nivel de la cadena de mando con un esquema de representación multi resolución. Esta mejora de la SA se probará tanto en el ámbito civil como en el militar.

Abstract - The current command and control systems are based on wireless technologies such as TETRAPOL, TETRA, HF, VHF, satellite links, etc., despite providing a wide scope, usually have a very limited bandwidth. Because of these limitations they can only provide voice communications and data transmission at low speeds which could not completely reproduce the COP (Common Operational Picture) of a conflict or emergency.

Communications on the battlefield are mainly wireless, only on a few trunks wired networks are used. Wireless data networks are considerably less robust, since generally they only provide a fraction of the transmission capacity of the wired counterparts, and also suffer problems due to interference and radio environment propagation effect which do not happen in wired networks. To combat these effects, wireless protocols typically send additional information for error correction, and may include some redundant transmission. In the military field, bandwidth it is really low and certain technologies do not allow the transmission of video information. The VHF and HF radio equipment widely used in armies around the world are a clear example.

Therefore becomes latent the need to have a command and control system that allows information flows to and from troops in a quickly and reliable way. This thesis is framed in the development and practical evolution of a communications architecture for wireless networks C4ISR systems (Command, Control, Communications, Computers, Information Surveillance and Reconnaissance), particularly for small units. Being a small unit one located at battalion hierarchical level or lower in the military, or an autonomous unit of intervention in the field of emergencies.

In this thesis, it is described a communications architecture for SIMACOP (Which is a Spanish acronym for: SIstema de MAndo y Control de Pequeña Unidad), which is a C4ISR system based on COTS technology with capabilities for multimedia content distribution and sensor fusion.

Major technological contributions in this context are: the cognitive cross-layer communications architecture proposed, the introduction of high quality video and audio streaming included in the communications architecture of the C4ISR system, detecting elements through GPS, merging data collected by various sensors deployed in the area of operations and integration of several wireless communication systems with different bandwidths. For example, VHF, HF, satellite communications, IEEE 802.11 and WiMAX (IEEE 802.16d), which builds the network at different levels of command that will be described in this thesis. The main objectives are to study and identify the needs in command and control at the level of tactical communications in both the civil and the military side, and raise a global communications architecture for C4ISR systems to establish multimedia communications over next generation IP-based mobile tactical networks, including video streaming to improve situational awareness (SA) at each level of the chain of command with a scheme of multi-resolution representation. This improvement of the SA will be tested in both civil and military fields.

Resum - Els actuals sistemes de comandament i control es basen en tecnologies sense fils com TETRAPOL, TETRA, HF, VHF, enllaços satelitales, etc., que tot i donar un ampli abast, disposen d'un ample de banda molt limitat. A causa d'aquestes limitacions només es pot disposar de comunicacions vocals i de transmissió de dades a velocitats baixes que no reprodueixen per complet el COP (Common Operacional Picture) de la situació de conflicte o emergència.

Les comunicacions en el camp de batalla són principalment sense fils, només en alguns enllaços troncals s'utilitzen xarxes cablejades. Les xarxes de dades sense fils són considerablement menys robustes, ja que generalment només tenen una fracció de la capacitat de transmissió de les seves homòlogues cablejades, i també pateixen problemes a causa de la interferència i propagació de l'entorn ràdio efecte que a les xarxes cablejades no succeeixen. Per combatre aquests efectes, els protocols sense fils solen enviar informació addicional per a la correcció d'errors, i poden incloure algun tipus de transmissió redundant. En l'àmbit militar l'ample de banda és realment baix i certes tecnologies no permeten la transmissió d'informació de vídeo. Els equips ràdio HF i VHF utilitzats àmpliament en els exèrcits de tot el món són un clar exemple.

Per tant es fa latent la necessitat de disposar d'un sistema de comandament i control que permeti proveir informació des de i cap a les tropes de forma ràpida i fiable. La present tesi doctoral s'emmarca en el desenvolupament i evolució pràctica d'una arquitectura de comunicacions de xarxes sense fils per a sistemes C4ISR (Command Control, Computers and Communications Information Surveillance and Reconaissance), en particular els relatius a petites unitats. Per petita unitat s'entén aquella que és d'ordre jeràrquic menor o igual al de batalló en l'àmbit militar oa una unitat autònoma d'intervenció en l'àmbit de les emergències.

En la tesi doctoral es descriu l'arquitectura de comunicacions de SIMACOP (sistema de comandament i control de Petites unitats), el qual és un sistema C4ISR basat en tecnologia COTS amb capacitats de distribució de continguts multimèdia i fusió sensorial.

Les principals contribucions tecnològiques en aquest marc són les següents: l'arquitectura de comunicacions cross-layer i cognitiva proposta, la introducció de streaming de vídeo i àudio d'alta qualitat en l'arquitectura de comunicacions del sistema C4ISR, la detecció d'elements a través de GPS, la fusió de dades recollida mitjançant diferents sensors desplegats a la zona d'operacions i la integració de diversos sistemes de comunicacions sense fils amb diversos amples de banda. Per exemple, VHF, HF, comunicacions satelitales, IEEE 802.11 i WiMAX (IEEE 802.16d), les quals conformen la xarxa a diferents nivells de comandament que seran descrites en el present treball. Els objectius principals són estudiar i identificar les necessitats existents en comandament i control a nivell de comunicacions tàctiques, tant en el vessant civil com en la militar, i plantejar una arquitectura de comunicacions global per a sistemes C4ISR que permeti establir comunicacions multimèdia a través xarxes mòbils tàctiques de nova generació basades en IP, incloent streaming de vídeo per millorar la consciència situacional (SA) en cada nivell de la cadena de comandament amb un esquema de representació multi resolució. Aquesta millora de la SA es provarà tant en l'àmbit civil com en el militar.

1 Introducción y objetivos

1.1 Introducción.

La evolución de las redes y comunicaciones inalámbricas tácticas han seguido un camino diferente al de las redes y comunicaciones inalámbricas comerciales. Un hito importante en el desarrollo de la redes inalámbricas tácticas ocurrió en la década de 1970, con el cambio de las radios tipos push-to-talk, hacia las primeras radios que implementaban técnicas de spread sprectrum y salto de frecuencia (frequency hopping) lo cual permitía implementar capacidades anti-jamming. Desde la Segunda Guerra mundial, comandantes y soldados en el campo se han comunicado de manera efectiva con radios que forman subredes de voz en broadcast. Estas subredes, con una pequeña área de cobertura, funcionaban de manera independiente al núcleo de la red. Con el paso del tiempo, esto evolucionó a una arquitectura donde el núcleo de la red se utilizaba para enlazar nodos de mando táctico con nodos de mando y control (C2, de las siglas en inglés de Command-and-Control) y de allí hacia el puesto de mando superior (Headquarters). Los mandos en el campo utilizaban radios push-to-talk para comunicarse con sus soldados y se apoyaban en vehículos de transmisión para enlazar con sus superiores a través de redes de conmutación de circuitos por enlaces de microondas o enlaces satélites. Aunque aún existen hoy en día versiones mejoradas de esta arquitectura, podríamos considerarla como una arquitectura desfasada.

Los sistemas C4ISR (Command Control, Computers and Communications Information Surveillance and Reconaissance) engloban un amplio número de arquitecturas y sistemas informáticos y de comunicaciones. Su principal finalidad, tanto en aplicaciones civiles como militares, es la obtener información sobre el estado del teatro de operaciones para entregársela, convenientemente formateada, a las personas al mando de una operación de forma que se construyan una adecuada visión del mismo que les permita tomar las decisiones correctas. Por otra parte, deben servir de plataforma de comunicaciones para transmitir dichas órdenes y cualquier otra información que se estime oportuna.

Podemos señalar múltiples aplicaciones y arquitecturas de mando y control, tanto en un ámbito civil como militar, destacando áreas como operaciones militares, gestión de tráfico aéreo, gestión de operaciones espaciales, sistemas de detección y actuación ante catástrofes naturales, operaciones ante emergencias como incendios, accidentes de tráfico, salvamentos, inundaciones, e inclusive la aplicación de arquitecturas y conceptos relacionados en el mundo de la empresa y la estructura de organizaciones.

Todos ellos tienen varios denominadores comunes: se requiere construir una imagen veraz y precisa de lo que está ocurriendo en una determinada zona y en tiempo real o, mejor dicho, en tiempo útil respecto a la escala temporal de los eventos que se están produciendo. Este es uno de los elementos fundamentales del mando y control, el permitir a las personas al mando hacerse una visión certera de la situación, de lo que está ocurriendo en el teatro de operaciones, para ayudarles en la toma de decisiones.

La presente tesis doctoral se enmarca en el desarrollo y evolución práctica de una arquitectura de comunicaciones de redes inalámbricas para sistemas C4ISR, en particular los relativos a pequeñas unidades. Por pequeña unidad se entiende aquella que es de orden jerárquico menor o igual al de batallón en el ámbito militar o a una unidad autónoma de intervención en el ámbito de las emergencias.

El tipo de operaciones a desarrollar hoy en día, tanto en un ámbito civil como en uno militar, como por ejemplo operaciones con fuerzas asimétricas, operaciones en entornos urbanos, operaciones de mantenimiento de paz, intervenciones en catástrofes naturales, operaciones antiterroristas, etcétera, constituyen intervenciones novedosas respecto a las clásicas, con otros tipos de agentes,

ritmos de intervención y resultados esperados que condicionan nuevos enfoques y soluciones a nivel de topología de red y arquitecturas de comunicaciones para ejercer el mando y control.

Ante este nuevo escenario, en los últimos años, ha habido un replanteamiento de los procedimientos y tecnologías asociadas al mando y control, lo que se ha llegado a denominar como *'Revolution in the military affairs'* que ha conducido a una nueva corriente de trabajos teóricos y aplicados auspiciados por el Command and Control Research Programme del Departamento de Defensa Estadounidense, entre otros. Entre estos cambios se encuentra la propuesta de cambiar de aplicaciones basadas en plataformas a aplicaciones basadas en red las cuales permiten el intercambio de información entre un gran número de nodos interconectados. En el ámbito militar ha tenido mucho auge el enfoque de aplicaciones basadas en la red y se comienza a implantar la tecnología de redes a las operaciones tácticas para conseguir el Network Centric Warfare (NCW) [Alb99]. El concepto de NCW se refiere a la doctrina que intenta trasladar la superioridad en información en superioridad de combate vía la interconexión robusta y reconfigurable de fuerzas propias muy bien informadas y potencialmente dispersas en un marco geográfico [Alb99] [Alb00].

El concepto de NCW requiere que las aplicaciones basadas en red y la infraestructura de red inalámbrica se integren en una arquitectura de comunicaciones corporativa a nivel táctico. Una arquitectura corporativa, se define como "la organización fundamental de un sistema, definido en base a sus componentes, sus relaciones entre sí y con el medio ambiente y los principios que rigen su diseño y evolución" [Min08]. Esta definición de arquitectura corporativa indica que el diseño del sistema debe tener en cuenta las aplicaciones, el contenido y la infraestructura que soporta los flujos de información. Para que una red sea capaz de convertirse en un sistema corporativo, debe ser capaz de interconectar componentes heterogéneos. Este no es el caso cuando se utilizan medios de comunicación propietarios.

Una segunda consideración de los cambios más recientes ocurridos en el campo de las comunicaciones es que ahora es común que los sistemas de comunicación corporativa incluyan aplicaciones que se ejecutan desde teléfonos inteligentes móviles. La creciente popularidad de los dispositivos móviles inteligentes se debe en gran medida a la búsqueda continua de los consumidores de información valiosa en estas redes ya que el contenido, fiabilidad y conectividad se mezclan en un solo dispositivo. Los dispositivos móviles modernos se encuentran en el centro de una ola de innovaciones en la industria comercial que proporcionan a los consumidores un acceso continuo a la información y potencian la inteligencia corporativa [Tray09]. Un ejemplo de una aplicación militar de esta tecnología es la comunicación entre el jefe de la patrulla y el centro de operaciones tácticas en la identificación de un sospechoso. En el pasado, esto podría tardar varios minutos ya que el jefe de la patrulla debía describir al sujeto a través de comunicaciones por voz, mientras que hoy la transmisión de una fotografía digital podría tardar unos segundos [Dix10]. Esto genera varias preguntas, ¿sería posible que los militares empleasen una red de banda ancha móvil, inalámbrica a nivel táctico?, ¿Generaría el mismo valor para el soldado como lo hace claramente para las personas en la sociedad actual? ¿Cómo puede gestionarse esta infraestructura de red táctica con el fin de maximizar el valor y crear oportunidades para los líderes de pequeñas unidades y permitirles acceder a compartir información? Por último, ¿puede una arquitectura de comunicaciones asegurar la disponibilidad de la red, y aportar los mismos de disponibilidad como otras infraestructuras en que los consumidores están acostumbrados?

Para realizar el estudio de estas preguntas antes es necesaria una definición operativa de *valor*. En el ámbito corporativo generalmente se piensa en valor como la capacidad de generar beneficios. Las organizaciones modernas tratan de mejorar su capacidad de adaptación a las circunstancias cambiantes del medio ambiente mediante el uso de sistemas de información para tomar mejores decisiones más rápidamente. Esta capacidad de procesamiento de información mejorada permite a estas organizaciones lograr mejores resultados y obtener una ventaja competitiva. El objetivo de la aplicación de sistemas de información a las operaciones militares debe ser el mismo que las organizaciones comerciales, es decir, maximizar la relación de valor añadido frente a coste [Hay05].

Una medida del valor añadido a las operaciones militares podría ser cómo la información contribuye al cumplimiento de la misión. El piloto de la Fuerza Aérea John Boyd es famoso por introducir el ciclo de procesamiento de la información y toma de decisiones denominado, Observar-Orientar-Decidir-Actuar (OODA) [Cor02]. Las organizaciones que operan este bucle más rápido que sus competidores tienen una ventaja. Por lo tanto, un procesamiento superior de la información contribuye a "tener una comprensión exacta de lo que está sucediendo a su alrededor y lo que es probable que ocurra en el futuro cercano", este concepto se verá con más detalle en puntos posteriores y se denomina en la literatura “situational awareness” o conciencia situacional. La conciencia situacional conduce a una ventaja competitiva, ya que permite por un lado la oportunidad de controlar el ritmo operativo. En este contexto, el valor de la información no es simplemente el resultado de los datos brutos recogidos, sino la capacidad de procesar estos datos y transmitir sólo la información pertinente y oportuna en un tiempo útil a los nodos correctos que necesitan esta información para lograr la conciencia situacional. Con esta ventaja, los nodos (por ejemplo, los comandantes tácticos) son capaces de planear y ser proactivos en lugar de simplemente responder a las cosas que están sucediendo alrededor de ellos.

Basados en los conceptos del bucle OODA y la conciencia situacional, podemos definir el concepto red cognitiva, la cual se define como: una red con un proceso cognitivo que puede percibir las condiciones actuales de la red, y luego planificar, decidir y actuar sobre tales condiciones. La red puede aprender de estas adaptaciones y usarlas para tomar decisiones futuras, al mismo tiempo que tiene en cuenta los objetivos de extremo a extremo [Tho05].

Cabe destacar que los nuevos escenarios de operaciones, ya sean civiles o militares, precisan de dos elementos anteriormente no considerados en la teoría y en la praxis de mando y control. Por un lado se precisa información de niveles inferiores (de batallón para abajo) a los que tradicionalmente se ha requerido. Además, dicha información proveniente de niveles inferiores, debe ser obtenida en tiempo real, o al menos en “tiempo útil” (antes del deadline que invalide dicha información). Por otro lado se precisan otros tipos de información adicionales (multimedia y datos fusionados, entre otros) a los que tradicionalmente se han utilizado. Existen los medios tecnológicos para que las personas al mando de una operación, ya sea civil o militar, puedan acceder en tiempo útil a flujos multimedia (video, audio, etcétera) que les permita ‘ver con sus propios ojos’ lo que está ocurriendo en el teatro de operaciones.

En definitiva, la arquitectura de comunicaciones sobre la cual se deben basar las redes tácticas debe ser capaz de mantener una infraestructura de red heterogénea que permita la convergencia de contenidos y conectividad al mismo nivel disponible en las redes comerciales. El desarrollo de tal arquitectura maximizará el *valor* de la red. Esta infraestructura debe soportar medios de comunicación heterogéneos tales como radios VHF, HF, satélites comerciales y militares, redes 802.11, WiMAX o cualquier tecnología radio futura. Esto requiere una arquitectura capaz de mantener la infraestructura en las condiciones más difíciles y extremas que la unidad táctica pueda encontrar.

Las unidades tácticas pueden operar bajo una alta dispersión geográfica o confinados dentro de una zona urbana, o bajo condiciones adversas tanto ambientales como inducidas por el enemigo, donde el acceso a la infraestructura fija no está disponible. Estas unidades deben ser capaces de desplegar rápidamente la infraestructura necesaria para establecer comunicaciones con el puesto de mando superior que puede estar fuera de la línea de vista (NLOS, Non Line Of Sight), y transmitir la información recogida por las unidades desplegadas así como los sensores asociada ellas en la zona de operaciones.

Proporcionar una red completamente integrada en los bordes a nivel táctico (*tactical edge*) implica proveer los medios y mecanismos para mantener interconectado escuadrones de unidades pequeñas con el puesto de mando superior a través de redes inalámbricas que puedan compartir información e incrementar su conciencia situacional en tiempo útil, con información relevante para sus operaciones. El campo de desarrollo está totalmente abierto en este sentido siendo uno de los

más prometedores en el ámbito de los sistemas de comunicaciones tácticas tanto en el ámbito civil como en el militar.

1.2 Objetivos

La presente tesis doctoral se centra en identificar las necesidades existentes en mando y control a nivel de comunicaciones tácticas, tanto en la vertiente civil como en la militar, y plantear una arquitectura de comunicaciones global para sistemas C4ISR que permita diseñar, desarrollar e implementar una solución cognitiva y cross-layer para sistemas de mando y control de pequeñas unidades (nivel de batallón e inferiores) que permita establecer comunicaciones multimedia a través redes móviles tácticas de nueva generación basadas en IP, integrando diferentes medios de transmisión que se comunican de forma transparente entre sí, donde cada nodo de la red puede obtener y aprender de su información de la situación.

Para conseguir este objetivo global se deberán alcanzar los siguientes objetivos parciales:

- Realizar un exhaustivo y profundo análisis del estado del arte acerca de las arquitecturas de comunicaciones y medios de transmisión utilizado en los sistemas de mando y control, desde sus comienzos hasta las últimas propuestas. Esto nos conducirá a investigar, estudiar y evaluar las distintas arquitecturas y aproximaciones existentes en el área de sistemas C4ISR de pequeña unidad, área a la que se circunscribe la presente tesis. Por otra parte, al ser los sistemas C4ISR complejos elementos que integran múltiples módulos tecnológicos, se deberá llevar a cabo un profundo y extenso estado del arte de los componentes tecnológicos de las arquitecturas de comunicaciones de sistemas C4ISR. Estos incluyen arquitectura y frameworks de sistemas C4ISR, sistemas de comunicaciones tácticos, arquitecturas cross-layer, redes cognitivas, enrutamiento en redes tácticas, modelos de Calidad de Servicio (QoS) y sistemas de gestión, entre otros.
- Proponer una arquitectura de comunicaciones para sistemas de mando y control de pequeñas unidades. Dicha arquitectura se debe descomponer en una arquitectura de red, una arquitectura software y una arquitectura de gestión cross-layer como módulos constituyentes fundamentales.
- Diseñar y desarrollar implementaciones prototipo de la arquitectura de comunicaciones propuesta. Dicho arquitectura, al ser orientada a un entorno táctico, deberá probarse en entornos reales con medios transmisión tácticos, de forma que estén claramente integrados en los entornos de uso.
- Validar la arquitectura de comunicaciones sobre sistemas de mando y control de pequeñas unidades. Para ello, se considera que la mejor manera posible es desarrollando e implementando sistemas y probándolos en las condiciones de uso más reales que se puedan dar, esto es en entornos y escenarios de uso de los potenciales usuarios finales de un sistema de mando y control. Además, se considera que dicha validación debería llevarse a cabo por organismos e instituciones que certifiquen la validez de los sistemas desarrollados y la arquitectura propuesta que implementan, tanto nacionales como internacionales.

2 Estado del Arte

2.1 Sistema de Información C4ISR.

Los sistemas C4ISR (Command Control, Computers and Communications, Information, Surveillance and Reconaissance) engloban un amplio número de arquitecturas y sistemas informáticos y de comunicaciones. Su principal finalidad, tanto en aplicaciones civiles como militares, es la obtener información sobre el estado del teatro de operaciones para entregársela, convenientemente formateada, a las personas al mando de una operación de forma que se construyan una adecuada visión del mismo que les permita tomar las decisiones correctas. Por otra parte, deben servir de plataforma de comunicaciones para transmitir dichas órdenes y cualquier otra información que se estime oportuna.

Podemos señalar múltiples aplicaciones y arquitecturas de mando y control, tanto en un ámbito civil como militar, destacando áreas como operaciones militares, gestión de tráfico aéreo, gestión de operaciones espaciales, sistemas de detección y actuación ante catástrofes naturales, operaciones ante emergencias como incendios, accidentes de tráfico, salvamentos, inundaciones, e inclusive la aplicación de arquitecturas y conceptos relacionados en el mundo de la empresa y la estructura de organizaciones.

Todos ellos tienen varios denominadores comunes: se requiere construir una imagen veraz y precisa de lo que está ocurriendo en una determinada zona y en tiempo real o, mejor dicho, en tiempo útil respecto a la escala temporal de los eventos que se están produciendo. Este es uno de los elementos fundamentales del mando y control, el permitir a las personas al mando hacerse una visión certera de la situación, de lo que está ocurriendo en el teatro de operaciones. Este concepto se verá con más detalle en puntos posteriores y se denomina en la literatura "situational awareness". Del mismo modo, el sistema debe permitir que las personas a cargo de los puestos de mando y control, puedan enviar sus órdenes a los subordinados y operativos, también en tiempo útil. Además, las situaciones a tratar son críticas pues un fallo del sistema puede acarrear pérdida de vidas humanas. En el caso de sistemas C4ISR aplicados a las organizaciones las pérdidas se cifrarían en cantidades económicas y puestos de trabajo.

A nivel técnico se pueden esquematizar los sistemas C4ISR como un conjunto de N sensores de distinta naturaleza, ubicación espacial y requerimientos de procesamiento de sus señales generadas, M actuadores, en principio humanos aunque en muchas arquitecturas se pueden encontrar servosistemas y sistemas robotizados y/o puestos de mando y control, jerárquicamente organizados (hay que señalar que las nuevas tendencias en mando y control apuntan en una línea de mando distribuido) que procesan la información del entorno y toman decisiones en consecuencia. Interconectándolos a todos, y como elemento fundamental, se encuentra una arquitectura de red.

2.1.1 Arquitecturas y frameworks de sistemas C4ISR

Debido a ser sistemas tan genéricos (C4ISR como arquitectura de arquitecturas, tal y como se la define en el framework del departamento de defensa de los Estados Unidos(DoD)[C4197]) engloban gran número de áreas dentro de la informática y las comunicaciones: sistemas de tiempo real, middleware, agentes software, técnicas de calidad de servicio, multimedia, sistemas y protocolos de comunicaciones, redes de sensores, sistemas embebidos, sistemas operativos, fusión sensorial, inteligencia artificial y un amplio etcétera.

Según las versiones originales del Modelo de Referencia del framework del DoD, la arquitectura de sistemas C4ISR estará compuesta por 3 planos: 1) operativo: descripción de las tareas y actividades de los elementos operativos del sistema, así como del flujo de información entre los mismos (OV: Operational View), 2) sistemas: descripción de los sistemas físicos y lógicos, así como de sus interconexiones (SV: Systems View), 3) tecnológico: componentes y estándares involucrados en la implementación del sistema (TV: Technical Standards Views).

La definición de una arquitectura consiste en generar una serie de productos para cada plano que lo describen inequívocamente. Además existen una serie de matrices para cada plano que permiten llevar a cabo un seguimiento de la interrelación de los distintos productos. Actualmente el DoD exige el seguimiento de su aproximación a los productos que se pretenden adquirir.
En las nuevas versiones de la arquitectura [C4107] se ha añadido una vista extra denominada all view (AV) que facilita productos y herramientas para una descripción global de la arquitectura que se está desarrollando.

La OTAN tiene estandarizado un framework sobre arquitecturas C3 que desarrolló a partir del norteamericano. En concreto, es la denominada Arquitectura Técnica de Mando y Control OTAN, NATO C3 Technical Architecture (NC3TA), que se corresponde al STANAG 5524 [STA5524]. En este trabajo se inspiran la mayor parte de las arquitecturas técnicas de los países miembros de la organización.

En otros países existen aproximaciones similares como es el caso de Francia con la arquitectura AGATE(Atelier de Gestion de l'ArchiTEcture des systémes d'information et de communication)) [AGA05] desarrollada por la Delegación general para el Armamento (DGA), MODAF [MODa] promovida por el ministerio de defensa del Reino Unido o España donde el ministerio de defensa dentro de la inspección General CIS (IGECIS) ha sacado adelante la denominada Arquitectura Técnica Unificada (ATU) [ATU] sí bien esta es una aproximación mucho más simplificadora que se limita a dar normas y recomendaciones en los estándares y productos a utilizar en las vistas técnica y de sistemas.

Es de destacar que el framework C4ISR del DoD ha sido aplicado también al ámbito civil, en concreto la arquitectura se ha aplicado a determinadas agencias del departamento del tesoro de los estados unidos, como se puede ver en [Tho00].

El framework C4ISR del DoD está basado en el concepto de Network Centric Warfare (NCW), el cual es bastante reciente y tiene sus primeras acepciones en el trabajo del Almirante W.Owens [Owe96] quien considera que se debe producir una revolución en las arquitecturas militares para conducir al concepto de "sistema de sistemas" que englobe una arquitectura global y distribuida de sensores, puestos de mando y control, sistemas de armamento o actuadores. Esta arquitectura global debe, gracias a la superioridad de información, conducir a una mayor efectividad. En el documento "Joint vision 2010" [JOV] también se destaca la necesidad de la superioridad de la información gracias a una interconexión eficiente de todos los sistemas militares para alcanzar la superioridad de efectividad en las misiones.

Los sistemas y arquitecturas militares previos (actualmente aún siguen siendo la mayoría) seguían una aproximación denominada platform-centric y caracterizada por las comunicaciones analógicas y punto a punto, sin transparencia de la ubicación y los medios en gran parte de los casos.

Así, el concepto de Network Centric Warfare (NCW) y su otra acepción de Network Centric Operations (NCO) (en el Reino Unido se denomina Network Enabled Capability (NEC)) se corresponden a la doctrina militar en boga inicialmente planteada por Alberts et al [A1b99] [Alb00] que intenta trasladar la superioridad en información en superioridad de combate vía la interconexión robusta y reconfigurable de fuerzas propias muy bien informadas y potencialmente dispersas en un marco geográfico. El trabajo inicial ha sido continuado en [A1b03] y [A1b06], entre otros.

El modelo NCW tiene muy presente la adecuación de la parte técnica a un cambio global también en procedimientos, organización y doctrinas para generar nuevas formas de comportamientos organizativos. Se puede enunciar con la siguiente línea de pensamiento:

- Una fuerza con un modelo de interconexión y unas redes de comunicaciones robustas mejora el intercambio y la compartición de información entre sus elementos constituyentes.
- La compartición de información mejora la calidad de la misma y la conciencia situacional compartida.
- Una conciencia situacional compartida permite la colaboración y la auto sincronización, mejorando la sostenibilidad y la velocidad del mando.
- Todo esto, finalmente, mejora ostensiblemente la efectividad en el desarrollo de la misión.

Según se destaca en [A1b06] [Est06], Network Centric Warfare es:

- Elevada conectividad de red y elevado grado de digitalización (*Infostructure*)
- No mover personas o medios, mover información
- Una nueva forma de pensar, de comportamiento individual y de organización

Y sin embargo no es:

- Sólo red o medios tecnológicos.
- El cambio definitivo en el arte de la guerra

Respecto a este punto, en [FOT05] se destaca que los principios de NCW no van a reemplazar los principios de la guerra clásica probados durante siglos: masa, objetivo, ofensiva, seguridad, economía de fuerzas, maniobra, unidad de mando, sorpresa, simplicidad, entrenamiento y valor individual. NCW provee una nueva manera de hacer las cosas, complementaria en muchos casos con lo anteriormente existente.

Según se enuncia en [Alb06] NCW posibilita una serie de ventajas a las fuerzas que apliquen dicha aproximación respecto a enfoques previos:

- Compartir la información: que constituiría la ventaja trivial de esta aproximación
- Mejorar la percepción individual de la realidad
- Compartir la percepción de la realidad: En este caso ya no se está hablando de compartir la información sino un nivel superior de la misma, la percepción como información elaborada.
- Permitir la colaboración y sincronización
- En el caso extremo, permitir la auto sincronización
- Aumentar el ritmo de las operaciones
- Mejorar de forma notable la efectividad

Es muy importante destacar que NCW no es sólo red. De hecho se requiere un cambio sustancial en doctrinas, procedimientos y formación para poder llevarlo a cabo. Así, uno de los objetivos fundamentales de NCW es transformar una ventaja de información en una ventaja operativa en efectividad respecto al adversario. Esa ventaja operativa en efectividad no sólo explota la ventaja en información sino que debe apoyarse en procedimientos y doctrinas adecuadas a las nuevas formas de trabajar determinadas por NCW para provocar el cambio en comportamiento.

Dentro de los programas del DoD existen otros que tienen una relación estrecha con el NCW. En concreto, según las directivas del DoD, el programa Global Information Grid (GIG) debería ser el framework tecnológico principal sobre el que se sustentará el NCW. Según está directiva, todos los sistemas de sensores, armamentísticos y de mando y control deberían estar interconectados mediante GIG, en un concepto que han denominado 'sistema de sistemas'. Sin embargo GIG se ha revelado como un muy ambicioso proyecto que no acaba nunca por concretarse, mientras que el

concepto NCW sí que está siendo implementado, un poco como sucedió con la aproximación de la ITU para el correo electrónico (X.400) respecto a la del IETF.

Diversos programas y sistemas del ejército estadounidense ya en despliegue han sido desarrollados con la filosofía NCW, cabe destacar el programa Cooperative Engagement Capability (CEC) [CEC] de la armada para el seguimiento de blancos y el proyecto Future Combat Systems (FCS) [FCS] que interconectará redes de sensores, Unmanned Aerial Vehicle (UAV), Unmanned Ground Vehicle (UGV), sistemas a nivel de desmontado y sistemas de mando y control de nivel de batallón e inferiores.

La calidad del mando y control está determinada por la interrelación de las calidades de las etapas asociadas. Así la calidad del mismo viene determinada por la calidad del mando, la calidad del control, la calidad de la comprensión de la situación (SA) y la calidad de la ejecución. El elemento del que dependen todas ellas es el de la calidad de la información para la consecución del objetivo final de todo sistema C2, la efectividad en el desempeño de una misión. Esto se puede ver en la Figura 1 [Alb06] [Est06]:

El factor determinante o elemento sin el cual todo falla es el de la calidad de la información. La calidad de la información se puede descomponer en sus partes constituyentes: calidad ISR (Intelligence, Surveillance and Reconaissance), calidad en el transporte y calidad en los servicios de información. En el primer caso, factores como la calidad de los sensores, los rangos de cobertura de los mismos y las tasas de actualización serán determinantes. En el caso de la calidad del transporte, la calidad de servicio, la conectividad y la interoperabilidad serán básicos. Respecto a la calidad en los servicios de información, la posibilidad de descubrimiento de servicios, la colaboración, la seguridad y la visualización serán los elementos clave.

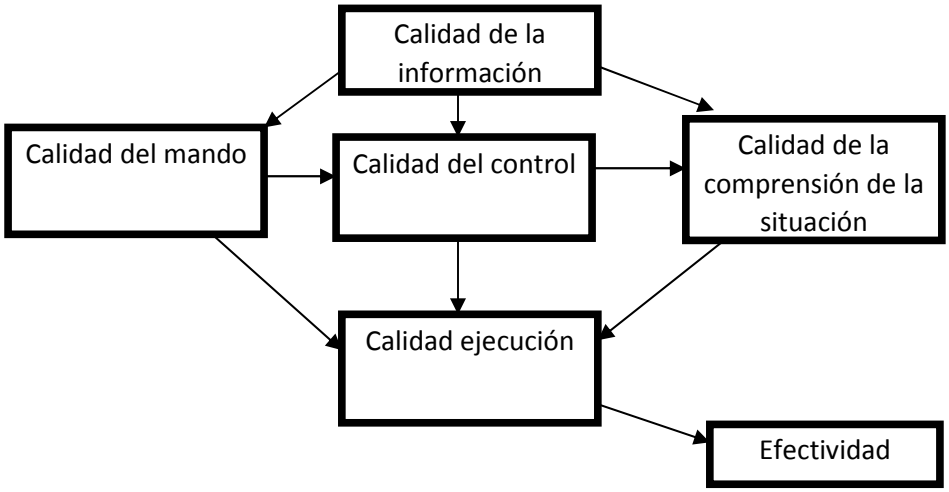

Figura 1. Calidad del Mando y control

En [Alb06] [Alb03] se definen toda una serie de primitivas y dominios para articular su teoría de mando y control. En concreto se señalan cuatro dominios básicos entendidos como las partes en las que se divide la arquitectura conceptual CIS: dominio físico, dominio de la información, dominio cognitivo y dominio social. En la Figura 2**,** se pueden ver los distintos dominios con sus efectos asociados.

- El dominio físico es el relativo al entorno real del teatro de operaciones donde se producen los eventos
- El dominio de la información es el relativo a los datos obtenidos por los sensores y transportados por los dispositivos de red

- El dominio cognitivo es el relativo a la información elaborada (conocimiento) que manejan los comandantes a partir de los datos del dominio de la información.
- El dominio social es aquel en el que se llegan a establecer acciones conjuntas entre comandantes

El paradigma define tres dimensiones en el dominio de la información: riqueza o calidad de la información, alcance o calidad de distribución y calidad de interacción.

Las tres dimensiones se optimizan en un paradigma 'post and smart pull'' que es el que se preconiza en la literatura: entregar la información que se obtiene del entorno y tomar del sistema la que nos es necesaria. Para ello, como se indica en [Alb03], es necesario utilizar las arquitecturas y herramientas adecuadas que faciliten dicha aproximación: Service Oriented Architecture (SOA), arquitecturas y tecnologías ricas en metadatos y protocolos de descubrimiento de servicios y recursos, entre otros. No sólo la parte técnica de los sistemas debe experimentar ese cambio para favorecer la transformación, velocidad, acceso. También los usuarios deben modificar sus usos y procedimientos para explotar las ventajas del paradigma.

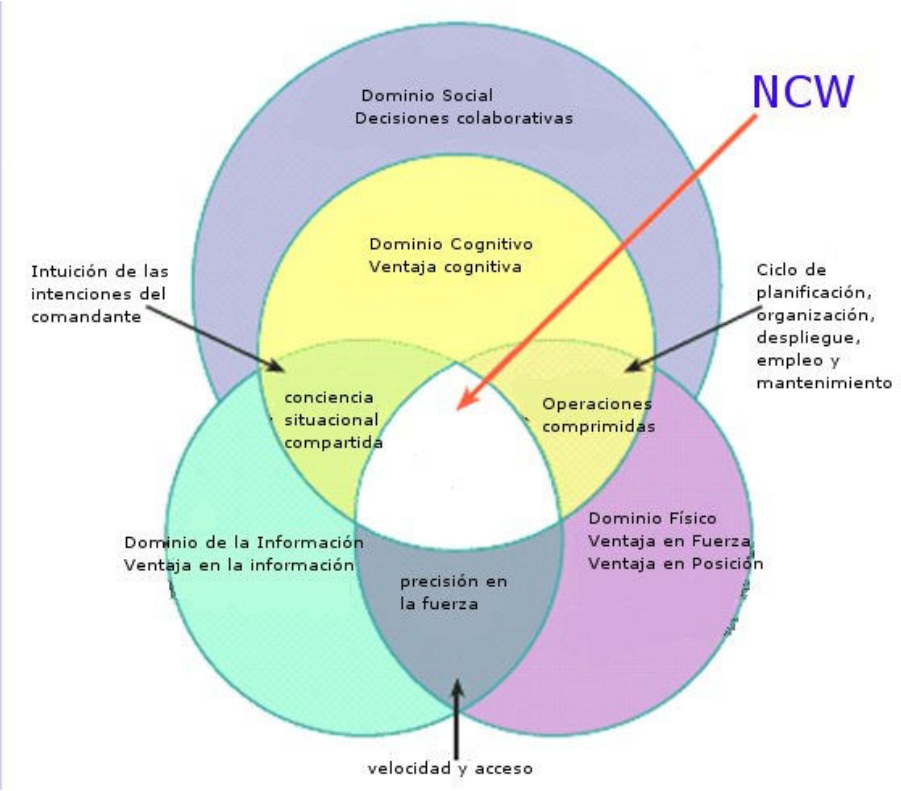

Figura 2. Dominios de NCW y su interrelación

Existen estudios que critican abiertamente a NCW, principalmente por los siguientes factores: complejidad, poca base formal subyacente, plantear haber descubierto un cambio radical en el mando y control y demostrarlo a partir de concepciones y premisas no demostradas suficientemente.

Así, algunos estudios [GA008] destacan los desafíos técnicos existentes a la hora de implementar arquitecturas que soporten plenamente muchas de las características de NCW. Así, se destaca como principal dificultad la escalabilidad de una red tan vasta como la propuesta en GIG, aunque eso no es una demanda estricta de NCW. Otro problema que se destaca es la complejidad y

estancamiento que está experimentando el programa Joint Tactical Radio System (JTRS) y el asociado Software Defined Radio (SDR), como vehículos para hacer transparentes los medios radios subyacentes. En cualquier caso, existen soluciones para interconectar distintos medios radios tácticos de manera transparente sin tener que pasar por JTRS o SDR. Por otra parte, otro punto que se destaca en estos estudios es el hecho de que existen diversos dominios de seguridad en las redes militares y que, si bien existen diversas soluciones para transportar información entre dominios con diferente nivel de seguridad, ésta no es una cuestión del todo resuelta. Otro problema que se destaca es el de asignación de frecuencias en el campo de batalla, aunque en cualquier caso ésta es una cuestión inherente a las radiocomunicaciones y no a una implementación de NCW. Otro problema que se señala por resolver, es el de la geolocalización de unidades, pues la excesiva dependencia de GPS se destaca como problemática. Finalmente, el último punto que se destaca por resolver, es el de la interoperabilidad entre sistemas a todos los niveles, de forma que se posibilite plenamente la interconexión de los mismos en el concepto NCW.

Otros estudios, como por ejemplo el llevado a cabo por CSR para el congreso estadounidense en 2007 [Wil07] dudan del paradigma NCW por considerarlo algo muy vasto, muy complejo, que no está fuertemente probado ni respaldado por procedimientos formales y estrictos y que siendo una tendencia muy en boga, mucha gente está siguiendo ciegamente como la nueva panacea. De todas formas, como se destaca en este mismo estudio, se valora positivamente y se considera como la aproximación a seguir en los próximos años, pese a todos los problemas señalados.

2.1.2 Clasificación de sistemas C4ISR

Los sistemas de mando y control se pueden clasificar en dos grandes niveles:

- Sistemas de mando y control de Gran Unidad (GU), que abarca desde nivel de batallón o superior.
- Sistema de mando y control de Pequeña Unidad (PU), que abarca desde nivel de batallón hacia abajo. Dentro de este nivel, encontramos tres subcategorías: Battlefield Management Systems (BMS), sistemas de seguimiento de fuerzas propias o Friendly Force Tracking (FFT) y sistemas de seguimiento del desembarcado o soldado individual.

El objeto de estudio de la presente tesis son los sistemas de mando y control de pequeña unidad. Es de anotar, que no existe una clasificación clara y no ambigua que defina inequívocamente las distintas subcategorías. Sin embargo, habitualmente se considera a los sistemas tipo seguimiento del desembarcado como sistemas intra-pelotón para la gestión únicamente de soldados individuales dentro de un pelotón, generalmente con medios para propagar toda esa información hacia niveles jerárquicos de red superiores y a su vez poder recibir órdenes y otro tipo de información. En dichos sistemas se suelen dota al desembarcado de equipación extra como: sistemas de cómputo con la filosofía weareable computer, sensores, etc., la cual acompañada del despliegue de una red radio, permiten al jefe de pelotón ejercer el mando y control sobre su unidad. Opcionalmente, se le permite al soldado individual acceder a una parte de la visión del teatro de operaciones, siempre evitando la sobrecarga de información y la interferencia con el desempeño de sus tareas. Dichos sistemas suelen integrarse en los sistemas de nivel superior FFT y BMS.

En un nivel jerárquico superior se encuentran los sistemas Friendly Force Tracking (FFT) que abarcan desde el vehículo de pelotón, o incluso del desembarcado, hasta el nivel de batallón y que consisten básicamente en uno o varios medios de transmisión tácticos, un sistema de posicionamiento y un dispositivo computacional donde se ejecuta la aplicación de seguimiento de fuerzas propias que permite a los comandantes tener una visión de la ubicación de sus fuerzas veraz. Estos sistemas permiten a los comandantes hacerse una visión muy rápida y actualizada de lo que está sucediendo en el teatro de operaciones, en tiempo casi real, dependiendo de las

limitaciones de propagación de los medios radio utilizados, constituyendo sistemas de mando y control muy ágiles y sencillos, adecuados a un entorno operativo táctico donde la situación puede cambiar radicalmente en cuestión de minutos. Estos sistemas han cobrado mucho auge en los últimos tiempos, debido a la transformación experimentada en las características de los escenarios, enemigos y tipos de operaciones, así como su elevada funcionalidad en la evitación del fuego fratricida.

En el mismo ámbito jerárquico que los sistemas FFT se encuentran los sistemas BMS. Éstos últimos tienen características similares a los FFT puesto que permiten a los comandantes hacerse una visión del teatro de operaciones, pero poseen toda una serie de funcionalidades extra que los hacen más complejos y con más posibilidades operativas. Cabe destacar que dichos sistemas permiten una gestión completa de una operación, no sólo el seguimiento de fuerzas propias. Para ello facilitan herramientas para la designación de líneas tácticas, la generación automática de órdenes (FRAGO), la preparación de misiones, utilización de superponibles, inclusión de elementos de logística, herramientas colaborativas y mensajería pre formateada, entre otras.

A pesar de las diferencias entre sistemas FFT y BMS, conforme evolucionan los primeros se denota la existencia de una clara convergencia entre ambos sistemas, reflejada principalmente en el posicionamiento automático de unidades acompañados de herramientas de mando y control, por ejemplo: gestión de amenazas y alarmas, compartición de información sobre objetos en el campo de batalla, configuración y reconfiguración de unidades durante la misión, mensajería y planificación [Cap03]. En definitiva, ambos sistemas (FFT y BMS) proveen información vital a los comandantes en el área de operaciones, ayudándoles a tomar mejores decisiones.

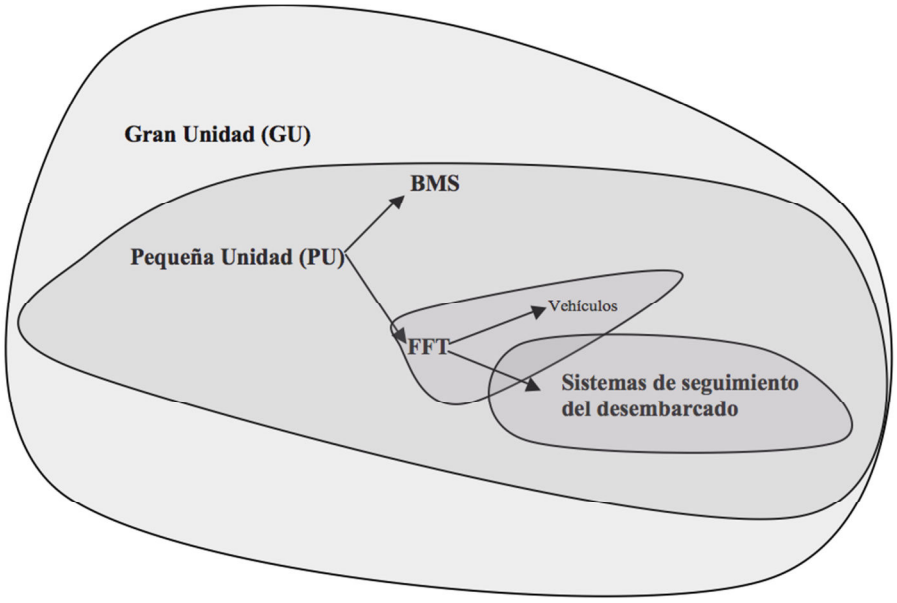

Figura 3. Clasificación de sistemas C4IS

2.1.2.1 Sistemas de seguimiento del desembarcado

Entre los sistemas de seguimiento del desembarcado se destaca el proyecto del ejército de Estados Unidos denominado Objective Force Warrior [OFW], sucesor del proyecto Land Warrior. En el mismo, las comunicaciones contemplan canales de bajo ancho de banda, por lo que no hay video de calidad en tiempo real y el puesto de mando y control hace un seguimiento por GPS de los operativos. Una versión a más largo plazo de este mismo proyecto es el denominado Future Force Warrior [FFW]. Un proyecto similar es el del ejército del Reino Unido Future Integrated Soldier [FIS] llevado a cabo por Thales UK, entre otros. Es bastante similar al estadounidense,

adoleciendo de video e incorporando mecanismos para la adquisición y seguimientos de blancos. Además incorpora la arquitectura de comunicaciones Bowman, que cubre un amplio rango de comunicaciones HF, VHF y UHF. En la misma línea de la adquisición y seguimiento de blancos está el proyecto del ejército francés FELIN [FEL] incorporando GPS en cada operativo, el sistema alemán IDZ [IDZ] y el del ejército australiano Project Lan 125 [LAN], el más limitado de todos. El sistema IDZ, desarrollado por EADS Alemania y Rheinmetall-Detec, incluye además en la arquitectura global UAVs, en concreto los sistemas de video Aladin y MIKADO cuyos streams de video se podrán reproducir en las PDA de los soldados. En España, el proyecto Combatiente del Futuro (COMFUT), incorpora sistemas de ayuda al seguimiento de blancos, visión nocturna, módulo NBQ, geolocalización del desmontado y de unidades contactadas visualmente así como visualización de la situación en el casco del desmontado.

El proyecto del ejército Sueco MARKUS [MAR] es, probablemente, el más completo y ambicioso de todos incluyendo multimedia mediante HDTV e infrarrojos, GPS así como la integración de redes de sensores. De todas formas, está todavía en una fase inicial y se prevé su completa implantación a largo plazo, asociado al proyecto ROLF 2010.

Todos estos proyectos adolecen en su mayoría de no incorporar información multimedia y si lo hacen de no atender a las señales biomédicas de los operativos, centrándose más en áreas de la facilitación del seguimiento de blancos y similares. Por otra parte, los sistemas de comunicaciones son, en su mayoría, muy tácticos (radios de VHF y HF) con lo que, lógicamente, proveen escaso ancho de banda, no permitiendo la transferencia de dicha información multimedia.
Otro proyecto es el desarrollado por Ericsson Microwave Systems y el Royal Institute of Technology de Suecia denominado GALDER [Bry05], sistema de mando y control a nivel táctico que, aunque carece de vídeo, incorpora técnicas de predicción del comportamiento del enemigo, mediante particle filtering.

En el área civil, y dentro del mismo campo de sistemas de seguimiento del desmontado, se encuentran varios proyectos. En la universidad sueca de Lulea se ha desarrollado un sistema [Hal04] orientado a la difusión de eventos deportivos con información enriquecida mediante sensores (GPS, biomédicos) ubicados en los participantes, se utiliza Bluetooth y GPRS como los dos niveles de red para distribuir dicha información y transmitir a los que visualizan el evento (que actúan como puestos de mando y control pero sin capacidades de mando) esos datos para aumentar su Situational Awareness de lo que está ocurriendo. Otro proyecto muy similar, orientado a la difusión y control de eventos deportivos es Arena Project [ARE] donde los jugadores de un equipo de hockey van equipados con cámara, sensores y micrófono.

Existen otros proyectos orientados al mando y control a nivel de desmontados en equipos de bomberos. En concreto, el proyecto danés IP Firefighter [Sys03] de la empresa Systematik es muy ambicioso pero que no contempla información multimedia y por otra parte no resuelve la cuestión del posicionamiento indoor. Está ya en su fase de implantación y contempla una PDA por operativo con comunicaciones comerciales, posicionamiento y COP sobre un GIS e información biomédica así como logística de la operación (número de botellas de oxígeno disponibles, etc.)
El proyecto Info-Firefighter [Wir00], llevado a cabo por la Swedish Rescue Services Agency (SRSA) es un proyecto de mando y control aplicado a operaciones de bomberos, donde cada operativo sensoriza información que es transportada, mediante MANETs y redes civiles, a los puestos de mando y control.

2.1.2.2 Sistemas Friendly Force Tracking

Los sistemas de Friendly Force Tracking (FFT) o Blue Force Tracking (BFT), como anteriormente se denominaban, deben ser sistemas de mando y control de una elevada agilidad y una respuesta temporal muy rápida, próxima al tiempo real, para el eficaz seguimiento de las fuerzas propias y sus movimientos y la evitación del fuego fratricida. Deben integrarse en los sistemas de comunicaciones existentes de la manera más transparente posible, mantener un elevado grado de

disponibilidad y adaptabilidad frente a perturbaciones, implementar estándares OTAN de interconexión entre sistemas de diversas naciones/agencias (fundamentalmente NFFI (NATO Friendly Force Information) [STA5527]), y poderse integrar en los sistemas de mando y control previamente existentes.

El sistema FFT de referencia es el que actualmente tiene en uso el ejército estadounidense denominado Force XXI Battle Command Brigade and Below (FBCB2) [FBC] que es un sistema muy completo con comunicaciones HF, VHF y satélite integradas. Hay que destacar que se integra plenamente con los sistemas existentes, posee funcionalidades de IFF (Identification Friendly or Foe) así como mecanismos de señalización de objetivos y enemigos, soporte para el control de logística y utilización del estándar VMF (Variable Message Format) [VMF] para el intercambio de información FFT.

También existe un sistema más experimental en estados unidos denominado ABWS (ARSTRAT BFT Web Services) [ARS] que da soporte NFFI a los sistemas de mando de nivel superior como Global CCIS – Joint (GCCS-J) y JADOCS (Joint Automated Deep Operations Coordination System).

El sistema alemán German Army CCIS [GCC] es un sistema de mando y control de brigada que incorpora interoperabilidad a nivel estratégico (MIP: Multilateral Interoperability Programme) y a nivel táctico (NFFI), niveles IP1 e IP2. Tiene la capacidad de actuar como hub NFFI.

El sistema italiano BFT [CWI] es una herramienta de nivel táctico que facilita Situational Awareness con un enfoque hacia herramientas geográficas extendidas. Soporta los niveles NFFI IP1, IP2 y SIP3, así como la capacidad de actuar como hub LTIS. Existe otro sistema FFT italiano, denominado IT-BFSA (Blue Force Tracking Situational Awareness) [BFS], desarrollado por la empresa SELEX, que tiene menor capacidad en cuanto a herramientas SIG y soporta únicamente los niveles NFFI IP1, IP2 y SIP3 como cliente.

El sistema noruego NORCCIS II (Norwegian Command and Control Information System) es un sistema de mando y control de nivel de brigada que incorpora funcionalidades de FFT. En concreto posee una de las implementaciones más completas de NFFI con todos los niveles indicados en el estándar, incluido Land Tracking Information Service (LTIS), y pasarela NFFI a MIP.

El sistema de la OTAN JCOP (Joint Common Operacional Picture) [JCO] es un sistema de nivel superior, mando conjunto, para la representación de la COP de distintas organizaciones. Si bien su ámbito es mucho más elevado que el nivel táctico, se ha utilizado como consumidor directo de la información NFFI en diversos ejercicios, vía la capacidad web service y SOA del perfil SIP3 del estándar NFFI. Por otra parte, la agencia OTAN responsable del estándar de comunicación NFFI para los sistemas FFT, la Nato Command and Control Consultation Agency (NC3A), tiene desarrollado su propio sistema FFT, el denominado NATO Blue Force Situational Awareness (NATO BFSA), con, lógicamente una implementación muy completa del estándar NFFI y de sistemas de concentración y redistribución de la información, hub NFFI y LTIS.

En zona de operaciones, la OTAN utiliza un sistema FFT desarrollado por una iniciativa liderada por la empresa EMSSATCOM. Es de destacar que bastantes naciones implicadas en ISAF (Internacional Security Assistance Force), o no tienen un sistema FFT o lo tienen en estado experimental, de forma que utilizan por vía del alquiler este mismo sistema.

En Francia destacan dos sistemas principales: el desarrollado por EADS y el desarrollado por Thales. El primero, denominado IMPACT [IMP] es una solución completa basada en el uso de diversos sistemas de comunicaciones tácticos, PDA militarizada y soporte de los perfiles NFFI, aunque el perfil SOA con un soporte muy básico.

El sistema desarrollado por Thales, TBMS (Thales Battle Field Management System), está optimizado para sistemas de comunicaciones tácticas desarrollados por esa compañía, con una

implementación bastante completa de los perfiles NFFI, y con funcionalidades de sistema Battlefield Management System (BMS). Esta empresa tiene otros sistemas adicionales que hacen uso de las funcionalidades FFT, utilizados en pruebas conjuntas de la OTAN, denominados SICF (Battle Command Information System) MAESTRO (Land Tactical System) y SIR (Army Regiment Information System).

El sistema rumano SICIB [SIC] desarrollado por la empresa Interactive, es un sistema de mando y control de nivel de brigada/batallón muy completo con funcionalidades para MIP en la interoperabilidad de nivel estratégico y NFFI para niveles tácticos. La implementación de NFFI es una de las más completas existentes.

Suecia tiene el sistema IS-SWERAP en una fase muy experimental, estado en el que también está el sistema danés BMD-Flex, de la empresa Systematik.

2.1.2.3 Sistemas Battlefield Management System (BMS)

Los sistemas BMS, como se ha comentado previamente, se ubican en el mismo rango jerárquico que los sistemas FFT pero se les presupone algunas características extra. Es de destacar que la tendencia en los últimos tiempos es a ir incorporando determinadas características de los sistemas BMS en los FFT de forma muchos sistemas FFT están incorporando funcionalidades anteriormente aceptadas para los sistemas BMS contribuyendo a hacer más ambigua la frontera.

Para la gestión de toda la información en dicha info-esfera se ha desarrollado el denominado Battlefield Management Lenguage (BML) [Car01a] [Bla05] [Pul07] una variante de XML para la diseminación de órdenes y reportes de manera automatizada entre nodos así como para formatear estandarizadamente la información y peticiones de la misma que fluyen entre los mismos. Las ordenes siguen el formato define por el STANAG 2014[STA2014] para la especificación de las mismas. El lenguaje es bastante simple con tan sólo una serie de primitivas básicas (ordenes, reportes e información de sensores) y se ha diseñado para que refleje la mayor parte de elementos existentes en el modelo de datos Joint Command Control Communications Information Exchange Data Model (JC3IEDM) [STA5255] que es bastante extenso y complejo de forma que se puedan llevar a cabo mapeos de una manera inmediata. El modelo de interacción entre agentes es petición-respuesta

Una extensión del mismo es Geospatial Battlefield Management Lenguage (GBML) [Kle07] que intenta aumentar el mismo incorporando el elemento geográfico. Es de destacar que el mayor uso práctico que se le ha dado a ambos lenguajes es en el dominio de las simulaciones y el entrenamiento como se puede ver en [Kru07].

A continuación se detallan toda una serie de soluciones existentes y en uso actualmente.

El sistema TBMS de Thales, ya comentado en el punto anterior por sus funcionalidades de FFT, es uno de los más completos con extenso soporte de BMS, generación de planes y órdenes, reportes automáticos, superponibles, soporte para un buen número de medios radio, IFF, etc.

El sistema Maria BMS [Bre03] de la empresa noruega Teleplan tiene soporte para FFT (vía NFFI), GIS con superponibles, intercambio de ordenes e información operacional así como mensajería táctica.

El sistema BattleHawk [BAT], de la empresa Chelton Defence Communications que tiene funcionalidades de seguimiento de fuerzas propias, enemigos y objetivos, así como de generación de reportes preformateados. El sistema permite la conexión de diversos tipos de sensores, incluyendo radar y sísmicos para el control perimetral.

Elbit Systems, de Israel, ha desarrollado un BMS denominado WIN BMS [ELB] que actualmente está en uso en Holanda, con un interfaz muy simple e intuitivo y orientado al seguimiento de objetivos, soporte para fuego indirecto, incorporación de información de inteligencia y logística.

La empresa de Singapur ST Electronics ha desarrollado el sistema BMS incluido en su plataforma de sistemas de mando y control y apoyo a la toma de decisiones BionixII [BIO]. Una de las características más destacadas es la facilidad para la generación de planes y la diseminación de los mismos.

El ejército Pakistaní dispone del sistema Integrated Battlefield Management System (IBMS) [PAK] con funcionalidades de FFT y seguimiento de enemigos, así como soporte para BML. El sistema utiliza las principales radios tácticas en HF y VHF y está diseñado de forma que cada vehículo pueda actuar como replay de los otros.
S-TEMAS [ITT] de la empresa norteamericana ITT utiliza como elemento básico de interconexión la radio SANGRAS desarrollada por la misma empresa. Posee funcionalidades de seguimiento de fuerzas propias y enemigas, generación de reportes y envío de órdenes siguiendo formatos estándar MIL así como alertas y mensajería.

TROP Battle Field Management System [TRO] es un BMS desarrollado por WB Electronics, con funcionalidades de IA para la ayuda a la toma de decisiones, superponibles, preparación de misiones, alertas y mensajería, soporte para diversos medios de comunicación tácticos, IFF y geolocalizadores láser.

2.2 Arquitectura de comunicaciones para sistemas de información de mando y control

Las complejas misiones militares actuales en las que participan las fuerzas de la coalición, unidades robóticas de apoyo, redes de sensores remotos y vehículos autónomos no tripulados (UAV, UGV) requieren de infraestructuras de comunicación subyacentes que sean flexibles, eficientes y robustas con el fin de operar con éxito en el combate. La capacidad de generar, procesar y compartir información de manera eficiente entre los nodos del mismo nivel horizontal en el campo de batalla es de suma importancia en entornos tácticos. De esta forma se consigue el concepto de guerra centralizada en la información (NCW) que ha sido promovida por los programas combatiente del futuro de distintos países.

Los programas combatiente del futuro de los distintos ejércitos prevén un sistema de sistemas, conectado un número de unidades operativas ligeras a través de una infraestructura de comunicaciones tácticas. El objetivo es capacitar a las fuerzas de combate con información y equipamiento ágil, al contrario de tanques de combate que son relativamente lentos y costosos de transportar y operar. La reducción de la pesada armadura y en su lugar, la agilidad y la flexibilidad se verá compensado por una inteligencia superior y el conocimiento de la información directamente a disposición de los soldados y vehículos en el campo.

En este nuevo entorno, la red de comunicaciones es el punto central de conexión para todas las unidades, convirtiéndose en uno de los elementos más importantes y críticos en el sistema. La infraestructura de comunicaciones debe ser lo suficientemente flexible como para soportar enlaces de datos de alta capacidad entre las unidades operativas, así como ambientes altamente dinámicos ad-hoc en el borde de la red.

En esta sección se presenta una comparación entre las redes inalámbricas comerciales y las tácticas (utilizadas en sistemas de información de mando y control), resaltando sus diferentes requerimientos, necesidades y restricciones. Primero se analiza el modelo comercial de redes inalámbricas y luego se analiza desde un punto de vista teórico las redes inalámbricas tácticas, para ayudar a establecer una comparación significativa entre los dos. En la segunda parte de la

sección se verán distintos enfoques en las arquitecturas de comunicaciones y se analizaran escenarios de uso fuera del mundo militar.

2.2.1 Características y consideraciones de diseño

Las redes inalámbricas comerciales (específicamente 3G y 4G), están basadas en las recomendaciones de organismos de estandarización como el 3GPP, que definen su arquitectura general y las interfaces de comunicación entre los distintos módulos. Un proveedor de servicio comercial típico tiene usuarios finales móviles y torres de red fijas con estaciones base (BSS). Múltiples BSs se puede conectar a un controlador de BS (BSC), y los BSCs están conectados a una red central a través de una puerta de enlace.

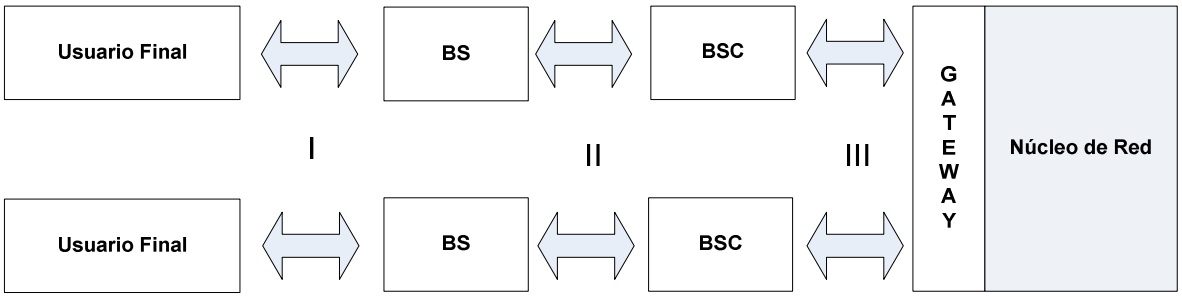

Figura 4. Arquitectura de comunicaciones de redes inalámbricas comerciales

Un aspecto importante de esta tecnología es la definición de documentos de interfaces de control estándar abiertas (ICDs). Consideremos un flujo de mensajes típico (de usuario final a usuario final), donde los paquetes van del usuario final a una BS, de ahí a un BSC, a continuación, al núcleo de red, y de allí se envía a un BSC que a través de una BS lo envía al otro usuario final. La Figura 4, muestra las cuatro entidades principales de este flujo, con tres ICDs principales necesarias para definir las interfaces. La ICD I define la interfaz aérea del usuario final a BS, ICD II define la interfaz BS a BSC, mientras que ICD III define la interfaz del BSC al núcleo de la red. Ha de tenerse en cuenta que hay ICDs más detalladas, como aquellas que definen el handover del usuario final entre dos BSS diferentes.

Las redes inalámbricas tácticas son extremadamente complejas. A diferencia de las redes inalámbricas comerciales, no existe una infraestructura fija. No se puede utilizar una ubicación fija para una BS. Además, no existe un equivalente a la noción de la infraestructura comercial de un núcleo de red estático.

Al contrario de las redes inalámbricas comerciales, los nodos de redes inalámbricas tácticas pueden ser todos los móviles, no hay infraestructura fija, y los nodos de usuario final son parte de la infraestructura. Los nodos que sirven de puerta de enlace (con radios de varios canales, formas de onda múltiple o distintas tecnologías de acceso radio) no son un punto único de fallo dado que una subred puede tener varios nodos que pueden transmitir el tráfico entre las capas jerárquicas para crear la conectividad total en cualquier lugar en el teatro de operaciones.

Las redes tácticas se forman instantáneamente de una manera no planificada a medida que los usuarios se congregan en un área. La red comienza a formarse cuando dos o más nodos entran en el rango de cobertura entre ellos. A medida que los demás llegan a la escena, se unen a la red de forma automática e inmediata. A medida que la red crece, más enlaces se forman y se hace más resistente desde el punto de vista de la redundancia. También se adapta conforme los usuarios se mueven y otros llegan al lugar o salen de la zona. Cuando alguno de los usuarios adquiere el acceso a una red de infraestructura fija o a otra red con tecnología de acceso radio (RAT: Radio Access Technology) distinta, otros usuarios pueden acceder a la infraestructura/RAT a través de

ese usuario que funciona como Gateway. Un usuario puede así pasar a través de varios nodos (varios saltos) para llegar al usuario de destino, si el usuario no está conectado directamente y. por lo tanto requiere el establecimiento de rutas.

En general, puede haber tres componentes principales en el establecimiento de enrutamiento dinámico en una red táctica:

- Un mecanismo de descubrimiento de nodos,
- Una metodología de actualización de la topología y
- Un mecanismo de enrutamiento, que pueden emplear diferentes criterios para la selección de rutas, tales como minimizar el número de saltos, maximizar el ancho de banda de extremo a extremo, minimizar el retraso total de la ruta o reducir al mínimo el consumo de energía, etc.

Los principales desafíos en el diseño e implementación de protocolos de enrutamiento incluyen lograr: una carga baja en tráfico de control, bajo retardo, actualizaciones rápidas de la tabla de enrutamiento (convergencia), la escalabilidad y fiabilidad. Además, el uso de multicast juega un papel clave en una red táctica para la utilización eficiente del ancho de banda y de esta manera dar cabida a grandes volúmenes de tráfico multimedia. Tales aplicaciones de banda ancha multimedia, incluyen aplicaciones de: vídeo, conciencia situacional, acceso a Internet y transferencia de imágenes, entre otros.

La calidad de servicio (QoS) es un factor importante en la comunicación de red y es un tema particularmente difícil en las redes inalámbricas en comparación con las redes cableadas. Las conexiones inalámbricas de extremo a extremo sufren varias limitaciones, como banda de frecuencias licenciadas, ancho de banda de canal asignado a cada usuario, interferencia y fading en el canal debido a las características de RF. El proveedor de servicios puede asegurar más ancho de banda a un cliente a un costo mayor, pero aun así limitado respecto al ancho de banda total del canal y al número de usuarios simultáneos. La interferencia entre canales inalámbricos es otro problema que se traduce en más retardo o incluso la pérdida de datos. La calidad de servicio, es aún más necesaria en aplicaciones sensibles al retardo como voz sobre IP (VoIP) y videoconferencia, especialmente cuando se transfiere a través de medios inalámbricos. Las principales limitaciones a la calidad de servicio en las redes inalámbricas se indican a continuación:

- *Ancho de banda limitado:* la fuente de información transmite datos a una velocidad de datos específicos en un canal inalámbrico que tiene un tamaño limitado de ancho de banda. Si la tasa de transmisión de datos es alta, entonces es necesario un mayor ancho de banda para transmitir todos los paquetes hacia su destino. Por otra parte, los datos sensibles al tiempo no debe tener ningún retraso significativo antes de llegar a su destino. Por lo tanto, los protocolos de comunicación en redes inalámbricas tácticas deben tener en cuenta que el ancho de banda es limitado y los paquetes de datos se pueden perder o se deterioran en la trayectoria de origen al destino.
- *Latencia o retardo:* La latencia se define como el tiempo que tarda un paquete en ir de un punto a otro en una red. Hay varias razones que pueden causar la latencia, tales como retraso debido al tiempo de propagación, las características del medio de transmisión, los dispositivos de red tales como routers y switches que un paquete se encuentra en la ruta hacia su destino, y el número de usuarios que comparten el ancho de banda en un momento dado [Hos04]. En una red congestionada con recursos limitados, los paquetes de datos sufren un mayor retraso, ya que tienen que esperar por más tiempo en la cola antes de ser entregados. El retraso puede ser tolerable para algunas aplicaciones como la transferencia de archivos a través de FTP, o incluso streaming de vídeo, pero se convierte en un serio problema con aplicaciones en tiempo real como VoIP o videoconferencia. En estas aplicaciones, el retraso es una cuestión crítica y puede degradar significativamente la calidad de los datos recibidos.

- *Interferencia:* en las redes inalámbricas, los datos enviados en canales inalámbricos pueden estar separados por frecuencia en cuyo caso utilizan canales distintos para transmitir y recibir, o bien pueden estar separados por tiempo, en este caso los procesos de transmisión y recepción utilizan el mismo canal de frecuencia. La interferencia co-canal o entre canales adyacentes causa ruido en el canal lo que da lugar a la distorsión de paquetes de datos e incluso a la pérdida de paquetes. El parámetro de relación señal a ruido (SNR) se utiliza para estudiar las características de un canal, por lo que este valor debe mantenerse lo más alto posible en las comunicaciones inalámbricas con el fin de evitar interferencias.
- *Fading y pérdida en el trayecto:* el fading se refiere a la distorsión que experimenta una portadora modulada sobre ciertos medios de propagación. En la comunicación móvil, se distinguen dos tipos de fading que pueden afectar a la señal [Skl97]: el fading a pequeña escala que se refiere a la distorsión dramática de la señal como resultado de pequeños cambios en la posición entre el receptor y el transmisor, y fading a gran escala que representa la atenuación de potencia de la señal o la pérdida en la trayectoria debido al movimiento en áreas de gran escala. El fenómeno de pérdida en la trayectoria se ve afectado por los obstáculos que la señal puede encontrar, como colinas, árboles, edificios, etc.

Otro punto importante en las redes tácticas es la seguridad. Las redes tácticas se enfrentan a retos graves para la seguridad, incluyendo espionaje inalámbrico, denegación de servicio y ataques de enrutamiento. Hay cinco servicios de seguridad para redes tácticas [Yu05]. La *autenticación* significa que la identidad correcta de un nodo es conocida por el extremo de la comunicación, la *confidencialidad* significa que la información del mensaje se mantiene a salvo de las partes no autorizadas, la *integridad* significa que el mensaje no se altera durante la transmisión, *no repudio*: significa que el origen de un mensaje no puede negar haberlo enviado, la *disponibilidad* significa que se mantiene normal la prestación de servicios frente a todo tipo de ataques. Entre todos los servicios de seguridad, la autenticación es probablemente el tema más complejo e importante en redes tácticas ya que es el punto de arranque de todo el sistema de seguridad. Sin saber exactamente con quién se está hablando, no vale de nada proteger los datos de ser leídos o alterados.

Un nodo móvil de la red táctica debe ser capaz de detectar otros nodos y de establecer un contexto de seguridad entre ellos. La autenticación dinámica entre los nodos de la malla se debe lograr sin un servidor central de autenticación dado que la malla móvil puede no tener acceso o puede estar desconectada de cualquier infraestructura de red fija. Las arquitecturas centralizadas de seguridad de red, no son viables en este escenario porque la conectividad entre un nodo y la autoridad central no puede ser garantizada.

En aplicaciones críticas, tal como una aplicación militar en un ambiente hostil, hay requisitos de seguridad más estrictos que en redes inalámbricas con fines comerciales o de usos personales. De haber un nodo comprometido, este debe ser detectado y negarse la comunicación con otros nodos lo más pronto posible para proteger la red, en otras palabras, en las redes tácticas debemos considerar tanto ataques externos como internos, en donde los ataques internos son más difíciles de tratar. Mantener la privacidad y la integridad de los datos en la red táctica requiere un alto nivel de cifrado en cada salto.

En caso de ser necesario, la seguridad de extremo a extremo en la ruta debe estar disponible. Cada vez que una ruta atraviese elementos externos (por ejemplos redes de operadores civiles) que no sean parte de la red segura, puede ser necesaria una conexión de red privada virtual (VPN) para llegar de forma segura al nodo final. La privacidad de los datos a nivel de aplicación se puede asegurar mediante el cifrado a nivel de aplicación de extremo a extremo.

Los nodos de una red táctica pueden desplazarse dentro y fuera del área de cobertura y entre distintas redes, ya sea entre redes homogéneas (misma tecnología de acceso radio) o

heterogéneas (distinta tecnología de acceso radio). Es altamente deseable que los dispositivos móviles sean capaces de unirse y salir de una red táctica y/o conectarse a una infraestructura fija pública o privada, en tiempo real sin perder conectividad con aplicaciones críticas. Este roaming en tiempo real, por lo general implica handoffs transparentes tanto en la capa de acceso al medio como en la capa IP.

Cuando el roaming se hace dentro de una red homogénea, es posible que implique reasociación y reautenticación del nodo. Cuando el roaming se hace entre medios físicos no homogéneos, puede implicar la llamada a diferentes mecanismos de autenticación y asociación. Dependiendo de cómo se administren las direcciones IP, el roaming podrá exigir que un nodo adquiera una nueva dirección IP que luego tendrá que ser comunicada a los nodos externos correspondientes para preservar la sesión en curso. En estos pasos del proceso de handoff, en las dos capas (capas 2 y 3), se puede acumular una latencia considerable, a veces lo suficiente larga como para interrumpir la sesión o hacer que se pierda la información.

Una red táctica debe prestar un servicio de transporte de datos fiable entre origen y destino. Sin embargo, las tecnologías convencionales de redes se basan en protocolos de transporte orientados a la conexión con tiempos de espera restrictivos no están diseñados para redes tácticas inalámbricas. Por ejemplo, es bien sabido que el protocolo TCP (Transmission Control Protocol), ampliamente utilizado, presenta importantes problemas en los enlaces inalámbricos. TCP interpreta la pérdida temporal de la calidad de un enlace inalámbrico como congestión e invoca a los procedimientos de retransmisión, los cuales podrían terminar la conexión TCP, lo que conduce a la pérdida de una sesión que no se restablece automáticamente cuando el enlace vuelve a estar disponible.

Varios mecanismos se sugieren en la literatura para mejorar la respuesta de TCP o para imitar los intercambios TCP con el fin de evitar la finalización de conexión TCP en enlaces inalámbricos. Las principales alternativas existentes son:

- TCP Tahoe, incorpora los mecanismos de control de congestión y de estimación de RTT. El primero de los mecanismos que fue introducido fue el de Inicio Lento, y el segundo el de la estimación de RTT basado, además de la media, en medidas de la varianza. Otro mecanismo incorporado fue el de Prevención de la Congestión. Por último, se introdujo el mecanismo de Retransmisión Rápida. TCP Tahoe tiene por tanto los mecanismos básicos de congestión y recuperación de pérdidas, y es el más común en las implementaciones actuales. No obstante, el principal inconveniente que presenta es el del Inicio Lento, concretamente en enlaces de retardo elevado, provocando el bajo rendimiento del protocolo.
- TCP Reno, incorpora todas las características de TCP Tahoe y añade el algoritmo de Recuperación Rápida que actúa conjuntamente con el de Retransmisión Rápida. De esta forma, tras la retransmisión no se invoca el algoritmo de Inicio lento, sino el de Prevención de la Congestión, permitiendo una recuperación más rápida tras la retransmisión. El inconveniente más destacado es que, en caso de tener múltiples pérdidas por ventana, el protocolo de retransmisión rápida no puede recuperar de forma rápida más que la primera pérdida.
- TCP New-Reno, propone una modificación al algoritmo de Recuperación Rápida de forma que en caso de que existan varias pérdidas por ventana se soluciona el problema de TCP Reno.
- TCP Vegas, se modifican algunos aspectos de los algoritmos de Retransmisión y Recuperación Rápida, así y como del de Inicio Lento. Como aspecto más relevante, no obstante, es la propuesta a actuar contra la congestión antes de que ésta se detecte por la expiración del temporizador de retransmisión. TCP Vegas introduce un algoritmo para la predicción de la cantidad de datos que el enlace puede cursar sin congestión, e inyecta en el enlace dicha cantidad. Esta predicción se basa en medidas de throughput. Mejora las prestaciones entre un 40 y un 70% según diferentes publicaciones.

- TCP SACK (Selective ACK), es una extensión de TCP Reno intentando mejorar los problemas de este y su versión new-Reno relativos a la detección de múltiples paquetes perdidos y la retransmisión de más de un paquete perdido por RTT. TCP SACK mantiene el arranque lento y la retransmisión rápida, así como la gestión de temporizadores introducida por TCP Tahoe

Existen otras versiones de TCP pero las cinco anteriores son las más extendidas y las que más se emplean en sistemas operativos Linux y Microsoft. En el caso de las comunicaciones radio sería recomendable un sistema de retransmisión selectiva como el proporcionado por TCP SACK y la gestión de ancho de banda y control de la congestión que proporciona TCP Vegas en función del throughput, en el caso de que no dispusiéramos de un sistema de control y gestión de errores a nivel de enlace de datos. En el caso de que si dispusiéramos de él podríamos prescindir de la retransmisión selectiva y utilizar únicamente las prestaciones que nos proporciona TCP Vegas a efectos de eficiencia en la utilización del ancho de banda.

Asegurar la fiabilidad de los datos, en el entorno de red móvil y autónomo de una red táctica, es un problema más difícil ya que una ruta de extremo a extremo puede tener múltiples saltos con niveles de calidad y latencia diferentes y variables en el tiempo. Los protocolos basados en UDP (User Datagram Protocol), combinado con estrategias de reconocimiento (ACK), son una vía interesante para el desarrollo de aplicaciones C4ISR que sean tolerantes ante la conectividad intermitente y son más apropiados para manejar tráfico multimedia en tiempo real.

Las aplicaciones que funcionan sobre redes tácticas inalámbricas se enfrentan a varias limitaciones en comparación con las aplicaciones pensadas para redes fijas, como el comportamiento impredecible de la red inalámbrica subyacente debido a las condiciones de propagación, la movilidad, el cambio de los niveles de congestión, la interferencia radio, la gran variedad de dispositivos móviles con diferentes capacidades para crear y mostrar contenido, consumo de potencia limitado y almacenamiento local limitado. Además, las aplicaciones tienen que ser ágiles y adaptables para responder dinámicamente a las condiciones cambiantes de la red. También es importante adaptar las interfaces de usuario para facilitar su uso en consonancia con las limitaciones del dispositivo. Algunos ejemplos de aplicaciones de banda ancha inalámbrica móvil son:

- *Video en tiempo real:* dependiendo de los casos de uso, puede ser necesario tanto video en alta definición como video de baja calidad, junto con la adaptación de vídeo en origen, según corresponda. Para satisfacer la demanda de ancho de banda de video de alta calidad, la red táctica puede hacer uso de protocolos multicast.
- *Voz sobre IP:* las soluciones de voz sobre IP, están bien establecidas tanto en Internet fijo como en redes WLAN. Los principales problemas relativos a voz en tiempo real, son el retardo de extremo a extremo y la variación del retardo (jitter). En una red táctica móvil de varios saltos, el jitter puede variar significativamente y por tanto requiere de almacenamiento en búfer y mecanismos de reproducción adecuados.
- *Mensajería multimedia instantánea:* una aplicación distribuida de mensajería instantánea para sesiones peer-to-peer o peer-to-grupo, es fundamental en una red táctica móvil dado que la información de presencia está disponible tan pronto como un nodo se une a la red. Por lo tanto, no es necesario tener un servidor central para la indicación de presencia o la autenticación. Además de los mensajes instantáneos basados en texto, los usuarios pueden tener la capacidad de compartir archivos en una variedad de formatos, incluyendo documentos, hojas de cálculo, diagramas, fotografías digitales y fotogramas seleccionados de un vídeo.
- *Seguimiento de recursos:* la información de presencia, junto con los datos de localización mediante GPS, se pueden utilizar para el seguimiento de recursos usando mapas estándar que indica donde están los nodos en cualquier momento. Se pueden utilizar herramientas de imágenes y clips de vídeo sobre los mapas, para la planificación interactiva.

- *Comunicaciones entre grupos afines:* los grupos con intereses comunes pueden utilizar aplicaciones colaborativas distribuidas, como las conferencias multimedia en tiempo real y pueden incluir a otros miembros a través de Internet u otra red privada si cualquiera de los nodos en la red tiene la capacidad para conectarse a la infraestructura.

La Tabla 1, resume las diferencias entre las redes inalámbricas convencionales y las redes inalámbricas tácticas para sistemas C4ISR.

Red Inalámbrica Táctica	Red Inalámbrica Convencional
Red móvil autónoma	Estática y pre-planificada
Una red de usuarios	Una red de puntos de acceso
Independiente de la tecnología de acceso radio, o bien, capacidad de migración fácil a otras frecuencias	Hardware de frecuencias especificas
Autenticación distribuida	Autenticación centralizada
Enrutamiento multi-salto diseñado para facilitar la movilidad	Enrutamiento entre nodos fijos
Necesita soportar la QoS de las aplicaciones	La QoS de las aplicaciones la manejan los proveedores de servicio
Necesita soportar aplicaciones distribuidas sin servidor en mallas aisladas	No hay aplicaciones - actúa como transporte

Tabla 1. Diferencias entre redes inalámbricas tácticas y comerciales

Vista las características de estas redes (autonomía, movilidad, aplicaciones distribuidas, etc.) y las consideraciones de diseño, el tipo de redes que más se ajusta a este perfil son las redes ad-hoc móviles (MANET: Mobile Ad-hoc Network). Una red ad-hoc móvil generalmente se define como un sistema autónomo de nodos conectados por enlaces inalámbricos que se comunican a través de múltiples saltos. Los beneficios de la redes ad-hoc son muchos, pero el más importante es su facilidad de implementación, sin necesidad de una administración centralizada o infraestructura fija, por lo tanto es una tecnología ideal para el despliegue de redes tácticas.

Si tomamos como referencia el modelo norteamericano de redes inalámbricas tácticas, el cual está basado en JTRS (Joint Tactical Radio System), su arquitectura de comunicaciones está compuesta por niveles de subredes (en realidad son islas de MANET). Estas subredes se construyen con formas de onda (una forma de onda es una tecnología de radio frecuencia inalámbrica de acceso múltiple). La Figura 5, muestra una vista teórica de tales capas (jerárquica) de islas (subredes) MANET.

Hay una forma de onda de radio a nivel de soldado (SRW: Soldier Radio Waveform) [SLI03], que puede tener dos subniveles, uno para las comunicaciones de soldado a soldado y una para la red de sensores. Por encima de esta, está el nivel WNW (Wideband Networking Waveform) [WNW03], que también tiene dos subniveles; uno forma las subredes locales para las comunicaciones vehículo a vehículo, y la otra es para la conectividad global, para generar un subconjunto único en todo el teatro. Es de anotar, que en cada nivel, puede haber varias subredes con diferentes frecuencias (a excepción de la subred global), formando islas de MANETs.

Algunos nodos seleccionados pueden tener capacidad multicanal para acceder a diferentes subredes y hacer de puertas de enlace entre las subredes. Por encima de estas capas de escalones inferiores, viene la capa de escalón superior con otro núcleo de red inalámbrica móvil (por ejemplo, WIN-T (Warfighter Information Network-Tactical) [WINT]), que en si misma puede tener una mezcla de nodos fijos y nodos tácticos móviles de mando. Esta red táctica principal puede utilizar formas de onda, como la HNW (High-band Networking Waveform) [HNW] o la NCW (Network-Centric Waveform) [Wis07], que ofrecen comunicaciones por satélite en movimiento (OTM), además, el núcleo de la red táctica utiliza enlaces de microondas para redes de nodos estacionarios o nomadicos.

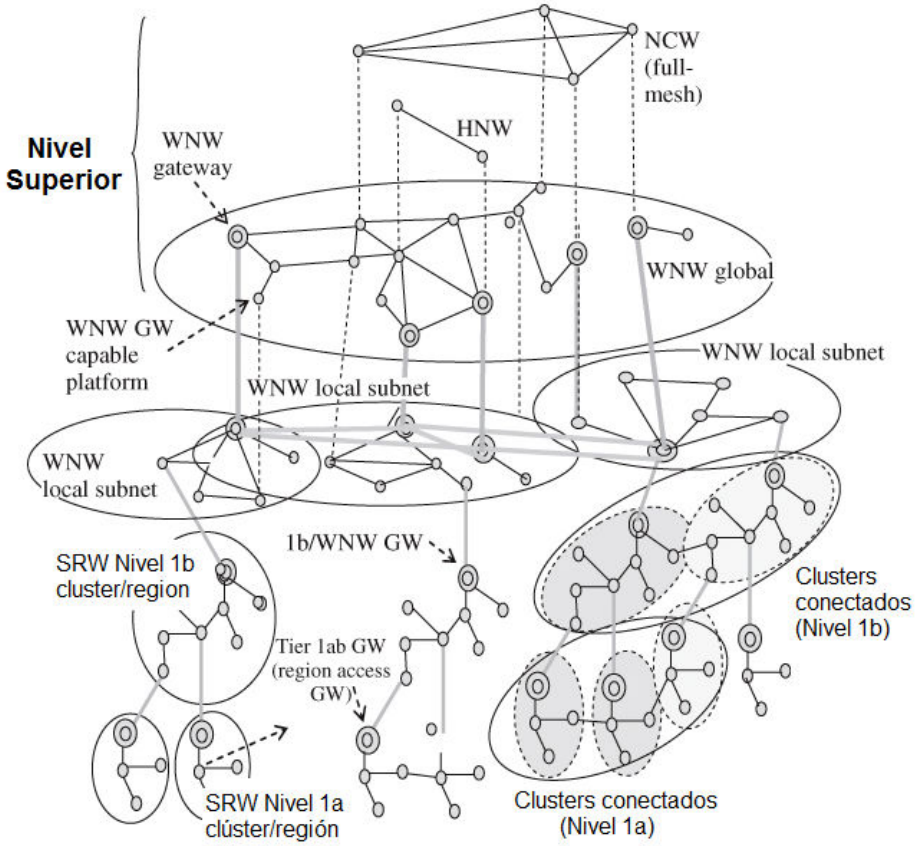

Figura 5. Vista de las redes inalámbricas tácticas con islas jerárquicas de subredes

2.2.2 Escenarios de uso

Los escenarios de uso de las redes inalámbricas tácticas, o las redes ad-hoc móviles en un sentido más amplio, y la arquitectura de comunicación C4ISR asociada, no se limitan solo al mundo militar los usos son variados y los retos en el diseño de sistemas para tales casos de uso, aunque algunos de ellos son comunes, pueden necesitar adaptaciones específicas. Algunos de los escenarios de usos potenciales se describen a continuación.

El elemento más invalidante en las operaciones de socorro tras las secuelas de un desastre de gran magnitud es la pérdida de la infraestructura de comunicaciones fijas de todo tipo, como sucedió durante el huracán Katrina en 2005 en Louisiana y Mississippi en los Estados Unidos [FCC06], los Tsunami al sur de Asia o los terremotos en Pakistán, India y Afganistán. Durante estos desastres naturales prácticamente todos los teléfonos fijos, celulares y sistemas de radio móvil terrestre desaparecieron o quedaron inutilizados ya sea debido a los vientos huracanados y las lluvias o las inundaciones posteriores. Los sistemas que se lograron reunir de forma apresurada carecían de interoperabilidad y por lo tanto no fueron capaces de comunicarse directamente entre sí. También quedó claro que en caso de catástrofes de tal magnitud como los huracanes y los terremotos, las comunicaciones de voz por sí solas no son adecuadas para la evaluación de los daños y determinación de la localización de heridos y áreas de desastre, son necesarias herramientas que mejoren la conciencia situacional a través de vídeo, imágenes e información de posicionamiento.

De acuerdo con un debate que tuvo lugar en el taller regional sobre comunicaciones durante desastres del ITU/ESCAP [ITU06] el 50% de las muertes ocurren en durante las dos horas

posteriores al desastre, por lo tanto, la disponibilidad y accesibilidad a una red de comunicaciones es necesaria para apoyar la respuesta al desastre y las actividades de recuperación. Refiriéndose a los últimos eventos de desastres una serie de organizaciones, entre ellas la UIT, PNUD, UNESCO, UNICEF, OTAN, etc., están trabajando de forma independiente (conjunta en algunos casos) para definir un marco de actuación para establecer una infraestructura de comunicaciones ante situaciones de emergencia.

En muchos países europeos, la solución convencional para la comunicación en las operaciones de socorro ante desastres, se basa principalmente en Terrestrial Trunked Radio (TETRA), diseñada para comunicaciones vocales y mensajería de estado, alcanzando velocidades de entre 2.4 y 7.2 kbps [Gra07]. Estos límites de velocidad de datos son insuficientes para dar acceso a los socorristas a los detalles de la construcción de un edificio o para el transporte de imágenes de vídeo. Otra desventaja de TETRA, es la falta de cobertura dentro de edificios. Esto es especialmente desfavorable para los bomberos y equipos de rescate, ya que con frecuencia tienen que entrar en los edificios para luchar contra los incendios o rescatar heridos de los escombros, la perdida de comunicación es inaceptable en estas situaciones. Aunque estas limitaciones se solucionan en parte con la llegada de TETRA-II, sigue siendo un problema grave que TETRA sea una infraestructura de red fija de estaciones base, y por lo tanto es susceptible ante desastres de gran envergadura.

Los servicios de seguridad pública necesitan redes móviles de banda ancha, instantáneas, sin infraestructura, auto organizables, para responder de forma efectiva y segura a la gestión del incidente o emergencia. Además de las aplicaciones tradicionales basadas en voz, servicios de banda ancha tales como video, aplicaciones de conciencia situacional (SA), acceso a Web y bases de datos y transferencias de imágenes de alta resolución son necesarias para la respuesta efectiva del incidente. En la mayoría de situaciones los socorristas (first-reponders) no tienen acceso a una infraestructura de red de banda ancha y en la mayoría de los casos tales infraestructuras no son viables. Las redes ad-hoc móviles aportan una forma de establecer rápidamente comunicaciones stand-alone instantáneas con la habilidad de conectarse a infraestructura cuando sea necesario.

La necesidad de comunicaciones multimedia ha sido ampliamente reconocida por los first-responders para tener una situational awareness efectiva y realizar mejor la gestión del incidente además las soluciones basada en IP resolverían varios problemas críticos de interoperatividad.

Varias organizaciones han contribuido a la comprensión y documentación de los requerimientos técnicos y operativos de los servicios de seguridad pública, incluyendo el proyecto SAFECOM [SAFECOM], proyecto MESA (Mobility for Emergency and Safety Applications) [MESA], el NPSTC (National Public Safety Telecommunications Council) de USA, entre otros. Varias de estas organizaciones han identificado la necesidad de redes ad-hoc móviles de banda ancha para suplir las necesidades de los socorristas en los incidentes.

En los últimos años se han realizado varios proyectos de investigación sobre gestión de crisis y redes móviles de emergencia, tales como: IST SHARE [SHARE], un proyecto europeo, destinado a ofrecer un sistema de información y comunicación para apoyar a los equipos de emergencia durante operaciones de rescate a gran escala. El proyecto ICIS (Interactive Collaborative Information Systems) [ICIS], cuyo objetivo era desarrollar mejores técnicas para hacer sistemas de información complejos más inteligentes y que sirvan de apoyo en situaciones de toma de decisiones.

El proyecto GeoBIPS [GeoBIPS] y su sucesor ADAMO [ADAMO] han definido y probado una arquitectura que permite la comunicación local entre los miembros de un equipo de rescate mediante una red mesh inalámbrica basada en IEEE 802.11, la arquitectura utiliza voz sobre IP (VoIP), para la comunicación entre los socorristas. Mientras GeoBIPS está centrado únicamente en los aspectos de comunicación en el lugar del incidente, ADAMO se centró en la comunicación de extremo a extremo y los flujos de información entre un centro de crisis y el lugar del incidente.

Algunas aproximaciones proponen soluciones hibridas entre un nivel de red ad-hoc móvil y un nivel de red con infraestructura en la zona del incidente. Por ejemplo, en [Jan09] se propone p2pnet que utiliza ordenadores portátiles para la construcción de un sistema de información y comunicación de emergencia basado en MANET. Una red inalámbrica híbrida, que combina las redes ad hoc y una red celular, se describe en [Fuj05] para mantener la conectividad entre una estación base y los nodos de un desastre. En [Ber07] se presentó el proyecto WISECOM que tiene como objetivo desarrollar una solución completa de telecomunicaciones que puede ser rápidamente desplegada, inmediatamente después del desastre y sustituir así el uso tradicional de los teléfonos por satélite o los dispositivos pesados y engorrosos. WISECOM restaura OSM locales o 30 infraestructuras, lo que permite que los teléfonos móviles normales puedan ser utilizados, y además permite el acceso inalámbrico de datos estándar (por ejemplo, WiFi o WiMAX).

En [Bai10] se propone IECS (Integrated Emergency Communication System), un sistema de comunicación que se compone de redes inalámbricas heterogéneas: MANET, redes de sensores (WSN), la red de telefonía móvil celular y redes de satélite móvil. El sistema propuesto permite la comunicación entre los usuarios finales (las víctimas, los equipos de salvamento o cualquier otro tipo de persona involucrada), situados dentro o fuera de la zona de desastre con diferentes tipos de dispositivos de comunicación. Además, se propone IESS (Integrated Emergency Service System) que opera conjuntamente con IECS para proporcionar una variedad de servicios de gestión de emergencias a las personas que participan en la misión de socorro.

En la arquitectura de comunicaciones de IECS, la red de sensores (WSN) se utiliza para obtener y monitorizar la información local. MANET es la red de transmisión para las comunicaciones locales en el sitio del desastre, y funciona como la red de tránsito para las comunicaciones remotas hacia las zonas seguras fuera del área del desastre. MANET conecta con la red de satélite a través de puerta de enlace por satélite (S-OW) y se conecta con la red de telefonía móvil celular a través de puerta de enlace (COW). La red de satélite se conecta con otras redes, tales como PSTN (Public Switched Telephone. Network) o Internet a través de puertas de enlace terrestre. En concreto se conecta vía satélite con la red celular a través de una puerta de entrada terrestre.

El sistema de comunicación MITOC [Yar09] (Man-portable, Interoperable, Tactical Operations Center) que fue financiado por el Departamento de Seguridad Nacional de EE.UU. El objetivó principal de la investigación MITOC ha sido el diseño, implementación, prueba, y evaluación de herramientas móviles, interoperables y accesibles de comunicación de voz, datos y vídeo para los comandantes y socorristas en el lugar del incidente. Un objetivo secundario del proyecto ha sido generar tácticas, técnicas y procedimientos (TTP) para el uso eficaz y evaluación de sistemas de comunicación y la tecnología de información avanzada, para mejorar el rendimiento de los comandantes de incidente, los organismos de apoyo, y personal de socorro.

MITOC propone una arquitectura de comunicaciones, formada por una burbuja inalámbrica, a partir de un sistema mesh inalámbrico con equipamiento de Rajant Breadcrumb®, para la comunicación entre los miembros del equipo de rescate y el centro móvil de operaciones de emergencia y el uso de terminales satelitales portables BGAN (Broadband Global Area Network) de Hughes, para la comunicación con el centro de coordinación, Internet u otras organizaciones fuera del alcance del incidente.

El grupo de investigación HFN (Hastly Formed Networks) del NPS (Naval Postgraduate School) de California, propone en [Don05] un kit de comunicaciones fly-away (FLAC: Fly-away Communications), este concepto denota a un sistema de comunicación rápidamente desplegable durante una catástrofe, el sistema está compuesto por una red inalámbrica ad-hoc móvil para la comunicación entre socorristas, una red WiMAX para la comunicación entre distintos centros de coordinación y conexión satelital BGAN/VSAT para acceso a Internet. El sistema ha sido probado tras el Tsunami que azoto a Asia en 2004, tras el huracán Katrina en 2005 [Kat05] y más recientemente tras el terremoto en Haití [Hai10].

La arquitectura de comunicaciones de sistemas de mando y control también tienen aplicación en Telemedicina. El proyecto Med-on-@ix [Pro09] tiene como objetivo apoyar al personal de servicios de emergencia médica (EMS) en el lugar del incidente desde un Centro de Competencia remoto (CompC). Se puede conseguir una mayor eficiencia de costes y en la calidad del tratamiento mediante la transferencia de datos de información táctica y los datos médicos pertinentes, tales como los signos vitales, auscultación y material de video desde el sitio de emergencia al CompC por medio del sistema de apoyo telemático.

En la arquitectura de comunicaciones definida, la ambulancia cuenta con una unidad de comunicaciones. La unidad de comunicación es un equipo integrado que alberga el middleware, las lógicas de red y las interfaces de hardware de red. A la unidad de comunicación se conectan: sensores (auriculares, estetoscopio, etc.) a través de Bluetooth, una red 802.11 para conectar las tablet PC de los operarios y otros sensores (ej.: ECG) y por medio de GSM / TETRA y GPRS, UMTS se conecta la ambulancia con el CompC y/o a Internet.
Las redes ad-hoc móviles también tienen aplicaciones en los sistemas ITS (Intelligent Transportation System) son ejemplo de ello los proyectos europeos CVIS [CVIS] y SAFESPOT [SAFESPOT] e iniciativas como car-2-car [C2C-CC], en aplicaciones de video vigilancia y en logística.

En el marco de CVIS se define CALM (Communication Access for Land Mobile), la cual es una arquitectura que abarca un conjunto de normas bajo la especificación técnica ISO en el Comité del Grupo de Trabajo 16 204 (TC204 WG16). El ámbito de aplicación de CALM es proporcionar una arquitectura de comunicaciones que presten un conjunto estandarizado de protocolos de interfaz de aire y los parámetros de mediano y largo plazo, la comunicación de alta velocidad ITS usando uno o más medios de comunicación y varios protocolos de red que ofrecen una conectividad transparente a través de cualquier medio posible.

La plataforma CVIS incorpora y se valida con tres tecnologías de acceso inalámbrico, radio de corto alcance en 5,9 GHz M5 CALM (ISO 21215), CALM IR (ISO 21214) y CALM 2G/3G (ISO 21212-21213). Para las comunicaciones internas de la estación se utiliza Ethernet por cable.

2.2.3 Arquitecturas Cross-layer

En la pila de protocolos de distribución de contenido multimedia sobre redes inalámbricas ad-hoc móviles, cada capa tiene uno o varios parámetros clave que afecta significativamente el rendimiento general del sistema. Si tomamos como ejemplo la distribución de video sobre redes tácticas, en la capa de aplicación, el compromiso entre la velocidad y la distorsión es una característica inherente de todos los esquemas de compresión para la codificación de fuentes de vídeo. El modo de predicción y el tamaño del paso de cuantificación son dos parámetros fundamentales para alcanzar un buen compromiso. En la capa de red, los algoritmos y protocolos de enrutamiento son importantes para encontrar la mejor ruta a través de la red inalámbrica ad-hoc móvil. Antes de hacer el enrutamiento, se deben determinar unas métricas de enrutamiento adecuadas. En la capa física, la selección de la modulación y la codificación de canal establecen un compromiso entre la tasa de transmisión y la tasa de pérdida de paquetes. Por otra parte, el rendimiento de extremo a extremo no está determinado en su totalidad por los parámetros de una capa individual, sino por la combinación de parámetros de todas las capas.

Por ejemplo, el retardo de extremo a extremo está dado por el retardo de propagación (determinado por el número de saltos de la ruta seleccionada), el retardo de transmisión (determinado por las condiciones del canal, la modulación y codificación de canal, el número máximo de retransmisiones y la tasa de la fuente) y el retardo de las colas de tráfico (determinado por la tasa de transmisión, y la ruta seleccionada). Por otra parte, debido a la naturaleza variable en el tiempo de los canales inalámbricos, cada nodo de la red tiene que ajustar estos parámetros con rapidez para mantener un buen rendimiento.

Todo esto nos indica claramente, que el diseño por medio de capas separadas no puede garantizar un rendimiento óptimo de extremo a extremo en la distribución de contenido multimedia sobre redes inalámbricas ad-hoc móviles. Por lo tanto, en los últimos años las arquitecturas cross-layer se han considerado como la forma más eficaz y eficiente para proporcionar calidad de servicio en redes tácticas móviles [Car06]. La idea básica del diseño cross-layer es aprovechar al máximo las interacciones entre las variables de diseño (parámetros del sistema) que residen en diferentes entidades funcionales de la red (capas de red) para mejorar el rendimiento global en el diseño de redes inalámbricas. Un ejemplo sencillo de un sistema de cross-layer es aquel donde la velocidad de datos de la capa PHY se puede cambiar dinámicamente basándose en la tasa de pérdida de paquetes en la capa MAC.

Basado en la literatura de investigación publicada, se han propuesto cuatro formas básicas de arquitecturas de diseño cross-layer [Sri05]: la creación de nuevas interfaces, la fusión de las capas adyacentes; acoplamiento de diseño sin necesidad de nuevas interfaces; calibración vertical a través de las capas. Además de las cuatro propuestas de diseño cross-layer, en la literatura, también se han hecho propuestas iniciales sobre cómo se pueden implementar las interacciones cross-layer. Estas pueden clasificarse en tres categorías: la comunicación directa entre capas, una base de datos compartida a través de las capas; abstracciones completamente nuevas.

Como ejemplo de proyectos que hayan aplicado una arquitectura de comunicaciones cross-layer tenemos: en [Maj07] se propone un framework para las comunicaciones posteriores a un desastre natural y en [Kid10] se propone una arquitectura para la administración de redes tácticas basado en un enfoque cross-layer.

La mayoría de los esquemas cross-layer actuales se basan en la adaptación a corto plazo en intervalos de tiempo de microsegundos o milisegundos, esto quiere decir que el objetivo fundamental de estas estrategias de cross-layer es vigilar y detectar cambios a corto plazo en el canal para notificar a las capas superiores sobre las nuevas condiciones de QoS. En este modelo, se espera que las aplicaciones modifiquen sus tasas de transmisión, cuando se les notifique por medio de una capa vecina que las condiciones actuales de servicio ya no están disponibles.

Como se ilustra en [Gol02], la adaptación propiamente dicha y la comunicación entre las capas se hace generalmente después que las adaptaciones locales a la capa ya no son posibles (o rentables). Por ejemplo, los cambios en la relación señal a ruido (SNIR) sobre vínculos ad hoc tienden a variar a una tasa mucho más rápida (en el orden de microsegundos) que los cambios en la topología, que por lo general son del orden de segundos. Las escalas de tiempo diferentes en cada capa por lo general implican que la adaptación local dentro de cada capa, por lo general, se produce en primer lugar (y con mayor frecuencia) que la adaptación entre capas.

Por lo tanto, los regímenes de cross-layer basado en la adaptación a corto plazo son eficaces para mejorar el rendimiento QoS de red de capas inferiores, como las capas MAC y PHY, pero son apenas útiles cuando se aplica a las capas superiores de la red, tales como enrutamiento, el transporte, y las capas de aplicación. Por lo tanto, es necesario desarrollar una arquitectura multi-escala para coordinar la entidad funcional cross-layer que reside en cada capa de red para maximizar la ganancia del diseño cross-layer en redes complejas de gran escala en sistemas dinámicos, como las redes móviles.

La arquitectura cross-layer propuesta en esta tesis, se diferencia de los enfoques tradicionales de cross-layer, en que se centra en los requisitos a nivel de aplicación y en la interfaz entre las aplicaciones y la red y las capas MAC, a diferencia de las estrategias tradicionales de cross-layer que se basan en las interacciones entre capas de protocolo vecinas.

2.2.4 Redes cognitivas

La red ad-hoc cognitiva es una red cognitiva distribuida. La red cognitiva se define en [Tho05] como: una red con un proceso cognitivo que puede percibir las condiciones actuales de la red, y luego planificar, decidir y actuar sobre tales condiciones. La red puede aprender de estas adaptaciones y usarlas para tomar decisiones futuras, al mismo tiempo que tiene en cuenta los objetivos de extremo a extremo. El diseño de la red está basado en el ciclo OODA (Observe, Orient, Decide, Act) [Tho05], el cual se muestra en la Figura 6 [Boy76].

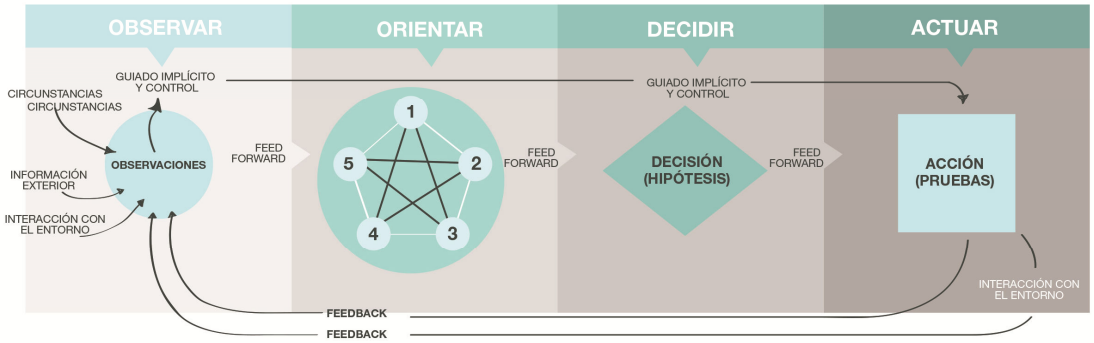

Figura 6. Bucle OODA completo

Cuando hablamos en términos cognitivos, los términos Software Defined Radio (SDR) y Radio Cognitiva son a menudo confundidos. SDR es simplemente la capa radio la cual transmite las radio frecuencias (RF) y frecuencias intermedias (IF). La radio cognitiva es la capa por encima de la capa SDR y es inteligente. La capa de radio cognitiva controla al SDR y determina su modo de operación.

El diseño de redes cognitivas es un área de tremendo interés. Las redes inalámbricas han sido estudiadas como entornos complejos, heterogéneos y dinámicos y su nivel cognitivo esta aún bajo investigación [Mah06]. Las redes cognitivas pueden ser usadas para mejorar la administración de recursos [Ron06], [Zha07], la calidad de servicio [Tsa08], la seguridad y el control de acceso [Ras08], [Sim07], [Cla08]. Varios investigadores han propuesto construir redes cognitivas usando agentes cognitivos [Huh98], lo cuales estarían integrados en la arquitectura para aportar inteligencia a la red.

En esta tesis, se define una arquitectura cognitiva cross-layer para permitir comunicaciones multimedia a través redes móviles tácticas de nueva generación basadas en IP, donde cada nodo de la red puede obtener y aprender de su información de la situación. A continuación, el nodo responderá a los cambios del entorno mediante la adaptación de parámetros del sistema y servicios de red, basados en los resultados aprendidos, a través de un controlador cross-layer distribuido que reside en cada nodo móvil. Este controlador proporciona Calidad de Servicio (QoS) a los servicios multimedia y utiliza plenamente los recursos de red.

3 Componentes tecnológicos de la arquitectura de comunicaciones para un C4IS

La arquitectura de comunicaciones de un sistema C4ISR se desarrolla e implementa utilizando una serie de componentes tecnológicos. Éstos cubren un amplio espectro de las ingenierías, aunque fundamentalmente en el área de la informática y las comunicaciones, e incluyen las tecnologías de comunicaciones, mecanismos de QoS para los distintos medios de transmisión utilizados, mecanismos de adaptación al medio de transmisión, sistemas de tiempo real, protocolos de enrutamiento en escenarios distribuidos y, particularmente, en entornos tácticos y sistemas de gestión, operación y mantenimiento.

En el presente capítulo se verá un estado del arte en las tecnologías relacionadas y necesarias para la definición de una arquitectura para sistemas C4ISR, paso previo para evaluar en qué estado se encontraba la técnica en las diversas áreas implicadas y que sirvió de punto de partida para el posterior desarrollo e implementación de las soluciones propuestas en el presente trabajo. Por otra parte también se estudian las diversas aproximaciones y soluciones existentes a la hora de integrar dichos componentes tecnológicos en un sistema de mando y control.

3.1 Sistemas de tiempo real.

Un sistema de tiempo real es aquel en el que la corrección de los resultados no depende únicamente de la corrección lógica de las computaciones sino también del tiempo en que estas se producen [Sta88], [But97]. Si los requerimientos temporales del sistema no se cumplen, esto es, no se lleva a cabo la tarea antes del cumplimiento de un tiempo máximo o deadline, se determina que el sistema falla.

Esto conduce a la característica fundamental de los sistemas de tiempo real: éstos deben ser deterministas y predecibles en su comportamiento. Deben garantizar la corrección del comportamiento temporal tanto para el caso peor como el mejor, independientemente de la carga. No se trata de ser rápido o eficiente sino de poder dar una respuesta determinista, acotada en el tiempo. Es más, se precisa que los sistemas de tiempo real puedan demostrar su corrección temporal a priori mediante técnicas de validación.

Se pueden considerar dos tipos de sistemas de tiempo real, según sean sus requerimientos: sistemas de tiempo real crítico (Hard real time en la terminología inglesa) y sistemas de tiempo real no crítico (Soft real time). En el caso de los sistemas de tiempo real crítico los deadlines son absolutamente estrictos mientras que en el caso de los sistemas de tiempo real no crítico se puede permitir perder deadlines exhibiendo un funcionamiento degradado siempre y cuando la distribución estadística de los tiempos de respuesta sea aceptable. Como se destaca en [Est04], en los sistemas de tiempo real crítico, "el no cumplimiento de las restricciones temporales puede acarrear consecuencias irreparables para el propio sistema y sus usuarios". En el caso de los sistemas de tiempo real no crítico, y según el mismo trabajo, "el no cumplimiento de las restricciones temporales sólo supone una pérdida de prestaciones o funcionalidades del sistema, aunque en ningún caso es deseable."

Sin embargo, otras aproximaciones han detectado las limitaciones existentes en esa taxonomía definiéndose los sistemas con otra aproximación el concepto de tiempo útil [Gou77], [C1a90], [Rav05]. Básicamente, la aproximación de tiempo útil trata de paliar la limitación semántica del concepto de deadline entendido como un punto en una dimensión, introduciendo el concepto de las funciones de tiempo-utilidad y beneficio. Así la restricción temporal no solo viene limitada por el deadline sino por una función asociada a la ejecución de una tarea y que tiene un punto de inflexión en dicho deadline.

El problema fundamental en los sistemas de tiempo real consiste en la asignación de un número limitado de recursos (CPU, red, etc.) a una serie de procesos para llevar a cabo unas tareas con unas condiciones/restricciones de satisfacción (SAT) muy estrictas. Para poder implementar sistemas de tiempo real existen dos aproximaciones fundamentales en las arquitecturas software [Liu73]

- Arquitectura síncrona (ejecución secuencial): Las tareas a realizar se ejecutan en un orden preestablecido conforme a plan de ejecución fijo. El sistema operativo (en cuanto a planificación) se sustituye por un ejecutivo cíclico. Esta aproximación se caracteriza por su simplicidad, por ejemplo, no hacen falta mecanismos para garantizar la exclusión mutua ni hacen falta técnicas de análisis, la validación del sistema se lleva por construcción. Sin embargo esta aproximación se caracteriza por su rigidez: si una tarea modifica su comportamiento temporal es posible que haya que rediseñar todo el aplicativo y el manejo de tareas aperiódicas es complicado. Por otra parte, el diseño del plan es un problema NP-Completo
- Arquitectura asíncrona (ejecución concurrente): Las tareas compiten por el procesador en tiempo de ejecución. En cada momento se ejecuta la tarea que tenga una mayor prioridad asociada. Esta aproximación engloba a una amplia familia de soluciones que se caracterizan por una mayor complejidad y como contraprestación una mayor flexibilidad respecto a las arquitecturas síncronas. Se precisan técnicas de análisis específicas para comprobar si los requisitos temporales están garantizados

Dentro de los planificadores de tiempo real podemos encontramos dos tipos: planificadores estáticos, en el que la asignación de tareas — recurso se lleva a cabo antes de la ejecución; y planificadores dinámicos, donde dicha asignación se lleva a cabo en tiempo de ejecución. La planificación siempre se lleva a cabo respecto a un parámetro de relevancia correlado con el deadline, este parámetro suele ser la prioridad de la tarea a llevar a cabo. Así los planificadores suele dividirse en planificadores con prioridades fijas y planificadores con prioridades dinámicas

La carga crítica es conocida de antemano y las prioridades se asignan antes de ejecutar. Existen varios algoritmos para la planificación de tareas por prioridades fijas, destacando Rate Monotonic [Leh89] en el que se asigna mayor prioridad a la tarea más frecuente y Deadline Monotonic [Aud90] en el que se asigna mayor prioridad a la tarea con deadline más próximo. Una característica importante de los algoritmos Rate Monotonic y Deadline Monotonic es que son óptimos, si un sistema/problema es planificable entonces lo será por Rate Monotonic/ Deadline Monotonic. En particular se observa que RM es un caso particular de DM en el que los plazos de terminación son iguales a los periodos.

En el caso de la planificación de tareas con prioridades dinámicas la carga crítica total no está necesariamente acotada y las prioridades se asignan durante la ejecución. En cada activación de una tarea se recalculan y se reasignan las prioridades. Destacan los algoritmos de Earliest Deadline First (EDF) [But93] donde se asigna la mayor prioridad a la tarea cuyo deadline está más próximo y Least Laxity First (LLF) [Yan98] donde se asigna la mayor prioridad a la tarea con menor laxitud.

Otro problema relacionado con los planificadores es la gestión de tareas aperiódicas, que son aquellas que tienen un carácter asíncrono e impredecible. Para poder tratarlas, se las debe caracterizar como críticas y no críticas. Para tratar a las primeras, se las considera como una tarea descrita por el caso peor de su deadline y del tiempo mínimo entre llegadas. Para el caso de las tareas no críticas, el objetivo es ofrecer un buen tiempo de respuesta mediante un servicio aperiódico, el cual se puede implementar mediante: servidor de polling [Wel05], servidor esporádico [Gon91], aislamiento y desacoplo entre procesos mediante el paradigma de constant bandwidth server [Abe98], e incluso aproximaciones con monitorización de estado y realimentación [Kat07], etcétera

La asignación de recursos en planificadores suele ser una actividad con coste computacional intratable en muchos casos de aplicación al mundo real. Es por ello que también existen muchas aproximaciones heurísticas al problema de la asignación de prioridades y/o recursos siempre, lógicamente, para aplicaciones de tiempo real no crítico: Ejemplos de esto se pueden ver en [Mai95] y [Sco06] [Mou08]

3.2 Comunicaciones en entornos tácticos.

El campo de las comunicaciones de datos inalámbricas para entornos tácticos es muy amplio y ha experimentado una variación muy significativa en los últimos años. En este punto nos centraremos principalmente en el estado del arte de las tecnologías utilizadas como medio de transmisión en el presente trabajo.

3.2.1 Comunicaciones tácticas

Las comunicaciones tácticas se caracterizan por llevarse a cabo en medios generalmente bastante adversos con: un muy bajo ancho de banda (600 bps a 19200 kbps), elevadas tasas de errores, sistemas de comunicaciones con débil implementación IP, así como sistemas cerrados y propietarios donde el desarrollador tiene pocas posibilidades de modificar diseños o conocer tan siquiera parámetros de funcionamiento. Ante estas dificultades es preciso adaptar cualquier diseño que se vaya a llevar a cabo a tan particular entorno.

Dentro de estas comunicaciones cabe destacar tres dominios en función de las frecuencias de funcionamiento: HF, VHF y UHF. Hay otro domino extra en la banda de las microondas que se corresponde a las comunicaciones vía satélite.

3.2.1.1 Comunicaciones HF

High Frequency (HF) se refiere a las transmisiones radio en el rango desde 3 a 30 MHz. Debido a que la ionosfera refleja las ondas de HF (fenómeno conocido como propagación skywave), HF es ampliamente utilizado para comunicaciones radio de medio y largo alcance (incluso rangos intercontinentales). Sin embargo, la estabilidad del canal que se puede establecer es muy variable y en función de una combinación compleja de factores como pueden ser: actividad solar, época del año, nivel de luz solar en la ubicación tanto del transmisor como del receptor, proximidad al terminador, auroras boreales, etc. El ruido electromagnético proveniente de dispositivos eléctricos afecta considerablemente a las transmisiones HF

Sin embargo, el desarrollo de la denominada Automatic Link Establishment (ALE) basada en los estándares MIL-STD-188-141A [Bak89] y MIL-STD-188-141B [MIL-STD-188-141B] así como el STANAG 4538 [STA4538] permite la conectividad entre estaciones y la selección del canal de manera automática y relativamente transparente para el usuario. El desarrollo de módems de alta velocidad conformes al estándar MILSTD-188-110B [MIL-STD-188-11013] y su versión OTAN STANAG 4285 [STA4285] y 4539 [STA4539] con tasas binarias de hasta 9600 bps han permitido la interconexión de redes de datos mediante HF. Otros estándares como el STANAG 5066 [STA5066] permiten el transporte confiable de datos mediante el uso de protocolos ARQ y constituyen casi una pila completa TCP/IP denominada High Frequency Internet Protocol (HFIP / HF- IP).

Es de destacar que existe un estándar extra, MIL-STD-187-721C [MIL-STD-187-721C] que define una arquitectura de red con capacidades de routing, monitorización de la calidad del enlace, etc. para poder establecer LANs de HF e interconexión de dichas LANs.

3.2.1.2 Comunicaciones VHF

Very High Frequency (VHF) se refiere a las transmisiones radio en el rango desde 30 MHz a 300 MHz. Las características de la propagación VHF permiten rangos de algo más allá de LOS (Line of sight). En concreto, una aproximación de la fórmula de la distancia de propagación sería:

$$D_{propagación} = \sqrt{(17 * \text{Altura antena en metros})}, \text{ medida en kilómetros.}$$

Las transmisiones VHF no se ven reflejadas en capas de la atmósfera (como pasa con HF e ionosfera) con lo cual el rango queda limitado a islas de cobertura un poco más allá de la línea de vista y como contraprestación no se interfiere en transmisiones VHF más allá de esa isla LOS. Por otra parte, VHF se ve menos interferido por el ruido atmosférico y/o dispositivos eléctricos como puede pasar en frecuencias inferiores. VHF, al ser de longitud de onda mayor, se ve más interferido por objetos grandes (como pueden ser elementos orográficos) que frecuencias más bajas pero menos interferido por objetos menores como edificios que en frecuencias UHF.

Las Combat Net Radio (CNR) en VHF permiten conectividad con valores limitados a 64 Kbps (teóricos) en frequency-hopping y valores reales probados en el rango de 9600 a 4800 Kbps. Estas velocidades y características se prevé que permanezcan estables entorno a estos valores durante bastante tiempo, pues las radios de última tecnología, como la Pr4G v3 F@stnet de Thales o las radios Sincgars de ITT se mueven entorno a esos valores

Otro tipo de radios VHF muy utilizadas en entornos tácticos son las punto a punto de enlace de datos. No permiten la movilidad y el uso en primera línea de las CNR pero a cambio dan enlaces punto a punto de 500 Kbps en distancias de 7 a 10 Km., usadas por ejemplo, para enlazar clústeres de radios VHF. Ejemplos de ellas son las radios Mercury de ITT o EPLRS de Raytheon.

También existen soluciones de ad-hoc networking y mesh-networking en estos ámbitos de VHF y UHF. Cabe destacar las radios Spearnet de ITT, la solución de General Dynamics y la PNR-500 de Tadiran. En todos los casos permiten el relay de información entre nodos utilizando soluciones similares a [MES] con protocolos de enrutamiento [RFC3626] [RFC3561], la reconfiguración dinámica de la topología de red y distancias de en torno a 1 Km. entre nodos.

La seguridad en este tipo de radios es fundamental, tanto a nivel de COMSEC (físico) como de INFOSEC (datos). Las PR4G encriptan la información, aplican frecuency hopping y tienen una amplia gama de contra medidas electrónicas, como se puede ver en [Lag92].

Software Defined Radio (SDR) se refiere a los dispositivos radio en los que gran parte del hardware típico de radio (mezcladores, filtros, amplificadores, moduladores/demoduladores, detectores, etc.) viene reemplazado por software, DSPs y conversores A/D y D/A de forma que modificar un dispositivo de un tipo de radio y rango de frecuencias a otro sea lo más rápido y transparente posible. Esta aproximación introduce gran número de desafíos tecnológicos. Estas soluciones han despertado mucho interés en el DoD estadounidense que ha llevado a cabo proyectos como los SpeakEasy I y II [Vid97] y el programa Joint Tactical Radio System (JTRS). Éste último tiene como objetivo producir radios SDR fácilmente intercambiables e interoperables por medio de la denominada Software Communications Architecture (SCA) [SCA] basada en CORBA y en sistemas operativos que cumplan POSIX [POSX]. Harris y Thales tienen ya productos en uso como las radios AN/PRC-152.

3.2.1.3 Comunicaciones UHF

Las comunicaciones UHF tienen cierta aplicación en el ámbito táctico, aunque mucho menos que las VHF o HF. Uno de los motivos es que esta banda ocupa el rango de frecuencias de 300 MHz a 3 GHz y en ella se encuentran asignadas frecuencias para muchas tecnologías civiles (Televisión, GSM, wifi, Bluetooth, radar, RFID, etc.). Lógicamente las tasas binarias que se permiten son

mayores que las habituales al disponerse de mayores rangos de frecuencia aunque las características de propagación y rangos son mucho menores debido al aumento de frecuencia.

Las tasas binarias que permiten los sistemas tácticos existentes están entorno a los 30 Kbps como por ejemplo en las soluciones PNR-500 de Tadiran, SRR330 de Saab o la radio de Marconi Mobile H4855. Sin embargo, en el programa LandWarrior del ejército USA se ha seleccionado la radio EPLRSLight (Enhanced Position Location Reporting System) que promete tasas binarias de 486 Kbps. Otros dispositivos, como las Spearnet de ITT o las ST@RMILLE de Thales también permiten anchos de banda muy superiores (en torno a 1 Mbps) a los habituales en entornos tácticos. De momento, sin embargo, el principal uso que se está dando a este tipo de dispositivos es el de comunicaciones vocales.

3.2.1.4 Comunicaciones vía satélite

Las comunicaciones vía ssatélite, en entornos tácticos tanto civiles como militares, permiten una serie de beneficios:

- cobertura ubicua
- infraestructura instantánea cuando han caído todo tipo de redes o bien, directamente, éstas no existen.
- son una solución temporal perfecta
- enlace entre nodos muy distantes
- despliegue y funcionamiento muy rápido
- telefonía/datos
- punto a punto o punto a multipunto con acceso a Internet.

Como contraprestaciones cabe destacar:

- la necesidad de disponer de una red de satélites propia o alquilada o bien comprar ancho de banda a operadores comerciales.
- la seguridad
- la disponibilidad relativa por temas de coberturas por zonas u orientación de satélites

Las frecuencias de microondas que utilizan los satélites vienen determinadas en una serie de bandas. En concreto nos encontramos con:

- ***Banda L:*** en el rango de frecuencias de 1 a 2Ghz. Utilizada en servicios satélite con movilidad, ofrece unas buenas en condiciones climáticas adversas o de vegetación densa.
- ***Banda C:*** en el rango de 3.7 a 6.2 Ghz. Las transmisiones se ven poco afectadas por las condiciones atmosféricas. Sin embargo, debido a la potencia asociada, los equipos terrestres suelen ser de tamaño considerable. Su principal utilidad es para enlaces satélite punto a punto en redes públicas e Internet.
- ***Banda X:*** el rango de frecuencias va de 8.0 a 12.0 Ghz. Esta banda permite transmisiones con considerable potencia usando terminales de tamaño pequeño. Suelen utilizarse en manpacks, comunicaciones de emergencia y móviles así como en aviones y buques. Otra ventaja de esta banda es que es poco vulnerable a la lluvia así como a la interferencia de otras fuentes de ondas radio.
- ***Banda Ku:*** frecuencias de 11.7 a 14.5 GHz. Sensible a interferencias y condiciones climáticas, tiene aplicación en ámbitos multimedia.
- ***Banda Ka:*** frecuencias en el rango de 17.7 a 21.2 GHz. Considerable potencia, usos en Internet de alta velocidad y videoconferencia. Bastante sensible a interferencias.

Hay que destacar que las bandas más utilizadas en ámbitos tácticos son la L y la X, ofreciendo un buen compromiso entre robustez y ancho de banda. Éstos suelen ir de 64 Kbps hasta 2 Mbps con retardos típicos de comunicaciones satélite alrededor de 0.5 a 2 segundos.

3.2.2 Comunicaciones civiles

En las comunicaciones civiles las restricciones son mucho más relajadas que en el ámbito táctico encontrándonos con medios con: elevado ancho de banda (del orden de decenas de Mbps), sistemas abiertos con los que los ciclos de desarrollo son mucho más cortos, menores costes, etc.

3.2.2.1 Wireless Lan 802.11

El protocolo IEEE 802.11 o Wi-Fi es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN (Wireless LAN), El primer estándar IEEE 802.11 se publicó en 1997. Desde el estándar original, se han publicado muchas enmiendas y correcciones, y varias versiones del estándar han sido adoptadas como estándares por la ISO.

3.2.2.1.1 Arquitectura de protocolos IEEE 802.11

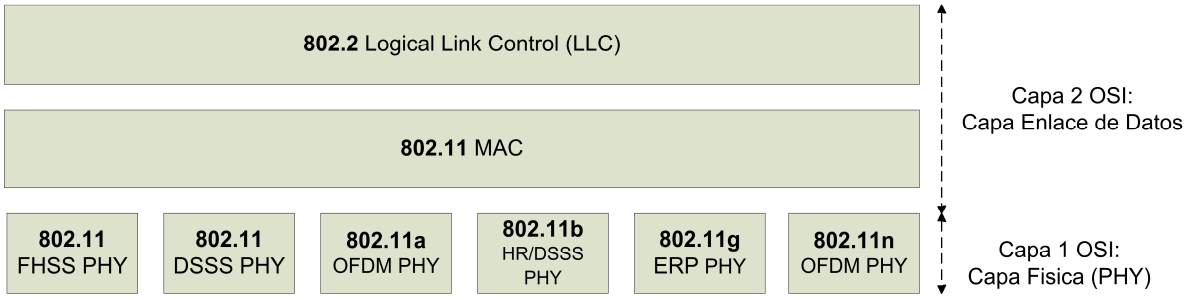

Figura 7. Capa de protocolos del estándar 802.11

La Figura 7 muestra la capa de protocolos del estándar IEEE 802.11. La capa LLC en el protocolo modelo IEEE 802.11 aísla a los distintos protocolos LAN y WLAN de las capas de red como IP. Esto permite la ejecución de aplicaciones, protocolos de capas superiores y mecanismos de administración sobre 802.11. La capa LLC 802.2 hace al protocolo IEEE 802.11 indistinguible de otros protocolos IEEE 802.

La especificación original 802.11 incluye la capa MAC 802.11 y dos capas físicas: una capa física FHSS (Frequency Hopping Spread-Spectrum) y capa de enlace DSSS (Direct-Sequence Spread-Spectrum). Revisiones posteriores añadieron capas físicas al 802.11, 802.11b especifica una capa HR/DSSS (High Rate Direct-Sequence); los productos basados en 802.11b llegaron al mercado en 1999, con velocidades de 5 hasta 11 Mbps, trabajando en la frecuencia de 2,4 GHz.

802.11a describe una capa física basada en OFDM (Orthogonal Frequency Division Mutiplexing) sobre una frecuencia de 5 Ghz que alcanza los 54 Mbps, tiene la ventaja de utilizar frecuencias poco concurridas por lo que la probabilidad de interferencias baja considerablemente. Sin embargo, al doblarse la frecuencia, disminuye considerablemente la capacidad de penetración así como el rango. Posteriormente se incorporó un estándar a esa velocidad y compatible con el h que recibe el nombre de 802.11g este estándar está basado en el uso de OFDM.

802.11 permite el acceso móvil a redes, para cumplir este objetivo, un conjunto de características adicionales se incorporaron en la capa MAC. Como resultado, la MAC de 802.11 puede parecer bastante compleja comparada con otras especificaciones MAC IEEE 802.

El uso de ondas radio como medio físico también requiere una capa PHY relativamente compleja. 802.11 divide la capa PHY en dos componentes genéricos: el PLCP (Physical Layer Convergente Procedure), para mapear las tramas MAC en el medio y un sistema PDM (Physical Medium Dependent) para transmitir esta tramas. El PLCP se extiende a ambos lados de los límites de las capas PHY y MAC, tal como se muestra en la Figura 8. En 802.11, el PLCP añade una serie de campos a la trama y la transmite "en el aire".

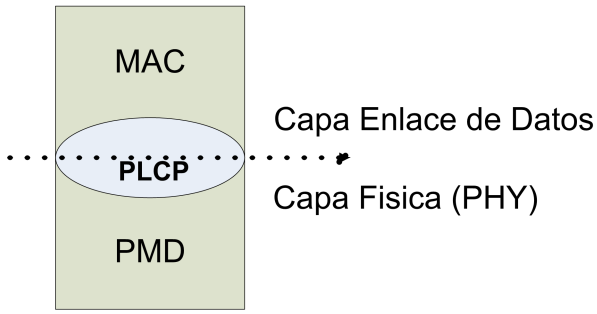

Figura 8. Capa de protocolos del estándar 802.11

La Tabla 2 muestra el desarrollo de las especificaciones de la capa física para WLANs 802.11, incluyendo la banda en la que operan, los métodos de codificación utilizados y la tasa de transmisión de datos.

Año	Estándar / Revisión	Banda	Encoding	Ancho de banda del canal (MHz)	Tasa Tx (Mbps)
1997	802.11	IR (Infra-rojos)	PPM	20	1,2
1997	802.11	2.4 GHz	FHSS	20	1,2
1997	802.11	2.4 GHz	DSSS	20	1,2
1999	802.11b	2.4 GHz	DSSS /CCK	20	1, 2,5.5, 11
1999	802.11b	2.4 GHz	DSSS /PBCC	20	1, 2, 5.5, 11
1999	802.11a	5 GHz	OFDM	20	6, 9, 12, 18, 24, 36, 48, 54
2003	802.11g	2.4 GHz	DSSS /CCK	20	1, 2, 5.5, 11
2003	802.11g	2.4 GHz	OFDM	20	6, 9, 12, 18, 24, 36, 48, 54
2003	802.11g	2.4 GHz	DSSS /OFDM	20	6, 9, 12, 18, 24, 36, 48, 54
2003	802.11g	2.4 GHz	PBCC	20	22, 33
2009	802.11n	2.4 / 5 GHz	OFDM	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2
				40	15, 30, 45, 60, 90, 120, 135, 150

Tabla 2. Estándares, banda, codificación y tasas de transmisión.

3.2.2.1.2 Arquitectura IEEE 802.11

Esta sección examina la arquitectura común a la familia 802.11 y su evolución. IEEE 802.11 ha definido una arquitectura lógica que no incluye solamente dispositivos también incluye entidades lógicas para crear una arquitectura robusta aunque flexible. La arquitectura es distribuida e incluye funcionalidades claves como ahorro de energía como parte de la .arquitectura. La arquitectura es flexible para permitir redes ad hoc y puede soportar redes permanentes en el hogar o en el trabajo.

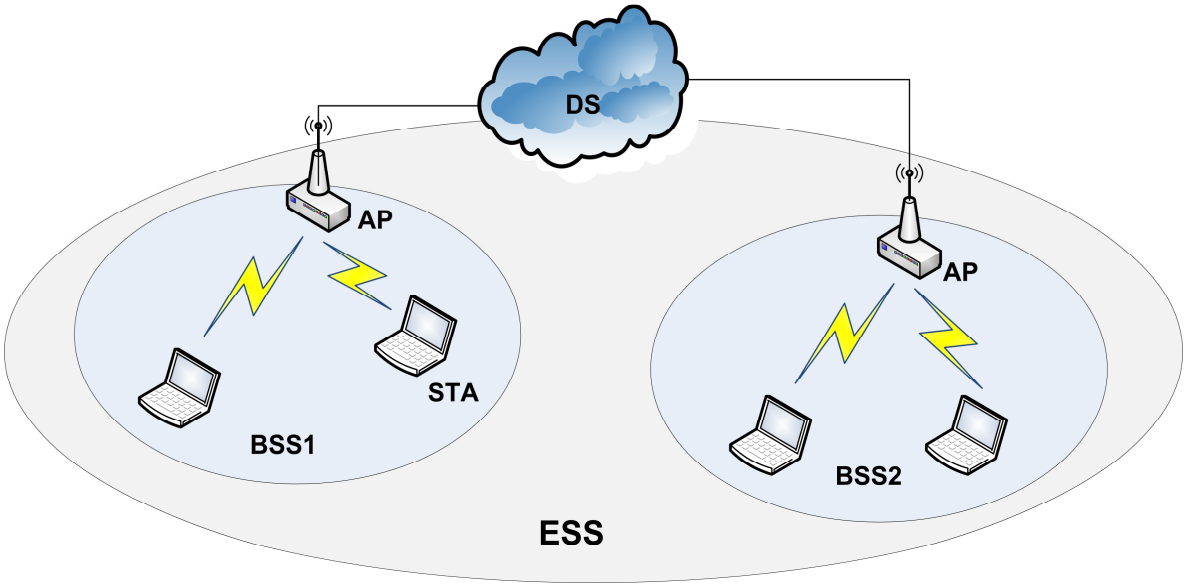

Figura 9. Arquitectura de red IEEE 802.11.

La familia IEEE 802.11 define dos entidades básicas en su arquitectura:

- Una estación (STA), es la entidad que se conecta usando el medio inalámbrico. Esta podría ser una tarjeta de red (NIC) en un PC o en portátil.
- Un punto de acceso (AP), el cual es una entidad que establece un puente entre el medio inalámbrico y la red cableada como en una LAN 802.3. El punto de acceso actúa como una estación base para los dispositivos IEEE 802.11 y los agrega en una red cableada como una LAN.

La arquitectura IEEE 802.11 (Figura 9) consta de un BSS (Basic Service Sets), el cual define un grupo de estaciones comunicándose entre sí. Hay dos modos de operación de los BSS definidos en el sistema IEEE 802.11.

El primer modo de operación definido en la arquitectura IEEE 802.11 es el IBSS (Independent Basic Service Set). En este modo, las estaciones se comunican entre ellas sin un punto de acceso (sin ninguna conectividad a la red cableada como la LAN). Esto es un ejemplo de una red ad hoc, caracterizadas por ser una red de corta duración creada para un propósito particular. Todas las estaciones puede que no sean capaces de comunicarse entre ellas y no existe ninguna función para retransmitir tráfico a otras estaciones. El estándar IEEE 802.11 provee información sobre cómo se descubren entre si estas estaciones, sincronizar todos los temporizadores en una IBSS y administrar la alimentación.

El otro modo de operación definido en IEEE 802.11 es el modo de infraestructura o BSS. Esta configuración incluye la presencia de un punto de acceso (AP) en cada BSS, el cual provee

conectividad a la red cableada. El AP ejerce el papel de una entidad de coordinación central y permite registrar las estaciones en el BSS, autenticarlos y provee funciones para el roaming de las estaciones. El AP se identifica por una dirección MAC como las estaciones inalámbricas y puede incorporar características adicionales como firewalls, NAT, servidor DHCP, cliente DHCP, seguridad y software VPN.

Para cubrir áreas más grandes, se despliegan varios puntos de acceso. Cuando múltiplos BSSs se conectan a la misma red, el conjunto se llama un ESS (Extended Service Set). A cada punto de acceso se le asigna un canal diferente para minimizar la interferencia. Si un canal debe ser rehusado, lo mejor es asignar el canal rehusado a puntos de acceso que no se interfieran entre sí. Cuando un usuario se mueve entre BSSs, se intentara conectar con el AP con la señal más fuerte y la menor cantidad de tráfico. Esto puede aliviar la congestión y ayudar a la estación en tránsito que se mueve desde un punto de acceso en el sistema a otro a no perder la conectividad.

Un ESS introduce la posibilidad de mover tráfico entre BSS sobre-la red cableada. La combinación de APs y red cableada que los interconecta se conoce como sistema de distribución (DS).

Los estándares WLAN 802.11 intentan asegurar la mínima interrupción en la entrega de datos, y proveen algunas características para cachear y retransmitir mensajes entre BSSs. La revisión 802.11i incluye algún soporte opcional para transiciones rápidas de estaciones que se mueven entre BSSs dentro de un solo ESS. Se están desarrollando especificaciones opcionales, incluyendo 802.11r, para estandarizar el roaming "rápido" mediante la reducción de la latencia durante los handoffs entre APs

Otra forma de definir una tecnología de red es mediante los servicios que ofrece. IEEE 802.11 provee nueve servicios, de los cuales solo tres son usados para transmitir datos, los otros seis son operaciones de administración que permiten a la red hacer un seguimiento de los nodos móviles y entregarles las tramas.

Ha habido tres grandes generaciones en enfoques de seguridad para WLANs. En orden cronológico de aparición estos son:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- 802.11i/WPA2 (Wi-Fi Protected Access, version 2)

Para solventar las vulnerabilidades de WEP, el IEEE estableció el grupo de trabajo 802.11i en 2001. A comienzos de 2003 se eligió WPA como una solución intermedia que se podía conseguir con el equipo existente, simplemente actualizando el firmware y el software. Las características más robustas de seguridad se implementaron en el documento final 802.11i (Julio 2004) la solución es conocida como WPA2. El cifrado más poderoso requiere una aceleración de hardware que no es soportado por equipo WLAN más antiguo. El estándar 802.11 actual define múltiples alternativas de seguridad para WLANs., estas alternativas son presentadas en la Tabla 3.

Nombre Wi-FI	Autenticación	Distribución de Claves	Cifrado	Algoritmo
(Ninguno)	Abierta	Ninguna	Ninguno	Ninguno
WEP	Abierta o Clave compartida (WEP)	Fuera de banda	WEP	RC4
WPA - Personal	Abierta, seguida por clave compartida - PSK	(PSK - PMK)	Fuera de banda TKIP	RC4
WPA - Empresarial	Abierta, seguida por 802.1x, en la cual clave compartida - certificado u otro token	PMK del servidor de autenticación	TKIP	RC4

WPA2 - Personal	Abierta, seguida por clave compartida — PSK	Fuera de banda (PSK - PMK)	CCMP	AES
WPA2 - Empresarial	Abierta, seguida por 802.1x, en la cual clave compartida - certificado u otro token	PMK del servidor de autenticación	CCMP	AES

Tabla 3. Métodos de seguridad en IEEE 802.11

La arquitectura descrita hasta este punto, también es conocida como arquitectura independiente, esta fue la primera en implementarse y en realidad es una extensión lógica de las prácticas de bridging habituales en el mundo cableado (Ethernet). Como hemos visto, con este enfoque, cada punto de acceso (AP) se configura y administra independientemente de otros APs sin importar si pertenecen o no a un mismo dominio administrativo. Este enfoque funciona bien para redes relativamente pequeñas pero se hace inviable a medida que el número de APs en la red inalámbrica aumenta.

A medida que las redes inalámbricas han crecido en tamaño, las técnicas de administración eficiente se han convertido en un requerimiento llevando de esta manera al desarrollo del Controlador WLAN y la arquitectura dependiente que lo soporta. Un controlador WLAN es un dispositivo o grupo de dispositivos diseñados para centralizar el control de las características WLAN y por tanto hacer escalable la seguridad, administración y despliegue de la red inalámbrica. Las características que se benefician de un control centralizado incluyen: autenticación, autorización, administración, detección de intrusos, optimización del desempeño y movilidad entre otros. Sin embargo, algunos aspectos de la red inalámbrica no se prestan bien a la centralización. Un ejemplo es el reencaminamiento de paquetes. Concentrar todo el tráfico de un grupo de APs a través de un solo controlador inalámbrico introduce una complejidad y coste significativo así como un solo punto de fallo. Como solución a este punto varios fabricantes proponen el uso de un clúster de controladores, en función del número de AP instalados.

Arquitectónicamente, un controlador WLAN implementa una porción de la capa MAC del protocolo 802.11 así como otras funcionalidades de niveles superiores. La idea clave detrás del controlador WLAN es que las características del punto de acceso se dividen de tal forma que algunas se llevan a cabo en el controlador en vez de hacerlas en el punto de acceso. Esta división permite al controlador la habilidad de simplificar y consolidar la administración y seguridad de redes inalámbricas grandes. La división exacta de funcionalidades entre controlador y punto de acceso depende del fabricante.

La arquitectura dependiente fue un primer paso natural para solventar los problemas de escalabilidad y administración de las redes inalámbricas. Un controlador puede "ver" todo el tráfico de los APs bajo su control directo. Algunas funcionalidades que son relativamente difíciles de implementar con la arquitectura independiente con la dependiente se vuelven de cierta forma natural. Por ejemplo, el hand off seguro de una sesión de un cliente de VoIP de un AP a otro puede ser fácilmente administrado por un controlador inalámbrico que tiene acceso a las claves de seguridad e información del estado del cliente y los dos puntos de acceso en cuestión (véase Figura 10). La arquitectura dependiente ha sido bien recibida en entornos corporativos.

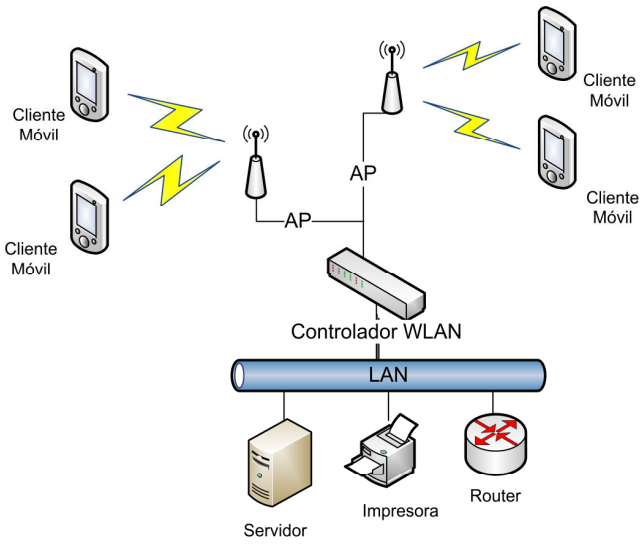

Figura 10. Ejemplo de implementación de arquitectura dependiente de red IEEE 802.11

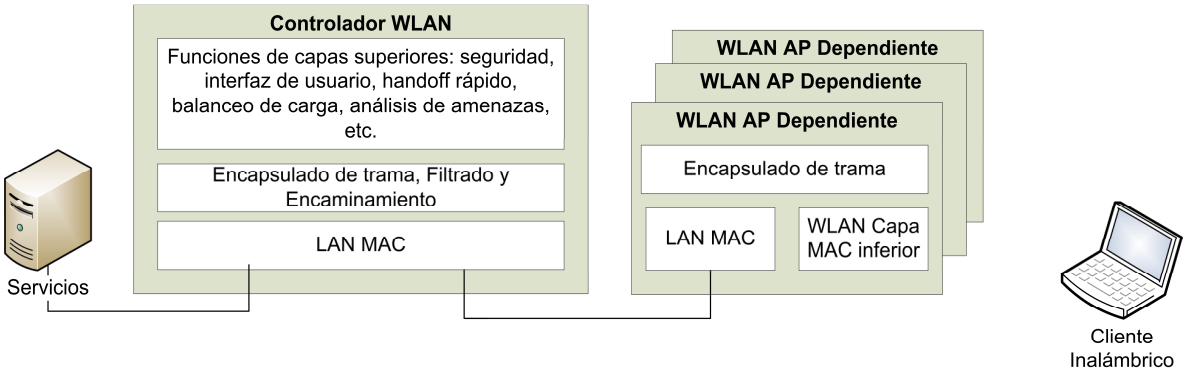

Figura 11. Una variación de la arquitectura dependiente de red IEEE 802.11

La división mostrada en la Figura 11 representa una forma de lograr los beneficios de la arquitectura dependiente. Los beneficios de este enfoque son: la facilidad de administración y la escalabilidad y sus principales desventajas son: el alto coste debido al controlador, posibilidad de cuellos de botella en el controlador.

Sin embargo, una vez solventadas las necesidades emergentes estas a su vez están forzando a nuevos requerimientos en la arquitectura de redes inalámbricas:

- La presencia ubicua de redes inalámbricas supone interferencias no solo entre redes inalámbricas adyacentes sino entre redes inalámbricas y productos del consumidor (hornos microondas, teléfonos inalámbricos, cámaras inalámbricas, etc.)
- La convergencia de redes de voz, datos y video exigen parámetros ajustados de latencia y jitter así como la necesidad de incorporar QoS para soportar VoIP y otras aplicaciones multimedia
- El surgimiento de Pymes y las redes locales administradas por el operador como distintos segmentos de mercado impulsan el requerimiento que tecnologías y características sofisticadas puedan ser fácil y rápidamente instaladas por usuarios técnicos sin experiencia.

Estos nuevos requerimientos necesitan una nueva forma de pensar acerca de las redes inalámbricas su instalación, administración y audiencia. Las redes cognitivas también conocidas como redes inteligentes [Tho05] pueden ser la solución a estos requerimientos. Las redes cognitivas son conocidas por sus propiedades de auto administración y auto solución de problemas. A continuación, se introduce el concepto de arquitectura WLAN cognitiva.

El diseño de redes cognitivas es un área de tremendo interés. El diseño de la red está basado en el ciclo OODA (Observe Orient Decide Act) [Tho05]. La idea central de una WLAN cognitiva es hacer a la WLAN verdaderamente fácil de instalar y usar. Una forma de lograr esto es mezclar los atributos de las arquitecturas independientes y dependientes y evitar las deficiencias de cada una. En breve una WLAN cognitiva debe cumplir los siguientes objetivos globales:

- Fácil de instalar y configurar por usuarios sin experiencia.
- Fácil de administrar sin el uso de herramientas de diagnóstico complejas.
- Proporciona características avanzadas.
- Auto configurable.
- Adaptable automáticamente a las condiciones RF cambiantes.
- Administración remota unificada.
- Control distribuido.
- Detección y eliminación de amenazas de seguridad
- Log de eventos RF.

Las redes WLAN cognitivas están basadas en optimizaciones cross layer que han demostrado su eficacia en la medida en que alteran los parámetros de varias capas de la pila de protocolos 802.11. Los tres componentes claves que diferencian una WLAN cognitiva de una WLAN independiente y dependiente: clustering, análisis RF y administración integral.

Los protocolos de clustering son los responsables de establecer un clúster, descubrir un clúster existentes, registrar un AP con el clúster, monitorizar, distribuir la información de configuración e intercambiar los mensajes de coordinación. En general, los protocolos de clustering permiten el flujo de control y mensajes de estado entre los participantes del clúster.

El componente de análisis RF monitoriza el entorno RF, construyendo y manteniendo una base de datos de fenómenos RF observados en el proceso. Este componente es responsable de la selección del canal, evitar interferencias, clasificación de las interferencias. Diferentes enfoques son posibles para lograr el resultado esperado del análisis RF. Sin embargo, el método más efectivo incluye el uso de hardware dedicado para monitorizar las bandas de interés de forma continua. El hardware puede ser tan simple como una interfaz WLAN dedicada usada principalmente pata el análisis o puede ser más sofisticada como es el caso de dispositivos actualmente en el mercado que pueden procesar datos espectrales en bruto y proporcionar una clasificación y análisis detallado de la señal. Este enfoque permite al AP hacer una mejor selección del canal cuando está buscando canales ya sea para evitar interferencias o para evitar interferir con otros servicios, Ej.: servicio de radar.

Un atributo útil del componente análisis RF es que elimina la necesidad de hacer site surveys. Una red WLAN cognitiva evita esto usando el componente RF para medir las señales de otros APs y ajustar la potencia de transmisión y el canal. Con un hardware de análisis RF dedicado, también se tiene la posibilidad de realizar medidas más precisas de las señales RF. Estas medidas pueden permitir aplicaciones futuras tales como localización de la fuente del emisor. La información de la localización puede ser usada para detectar la localización exacta de un rogue AP o un emisor que monta un ataque de denegación de servicio.

El componente de administración integral es responsable de mantener la integridad de las políticas y de la configuración dentro del clúster. Específicamente, el reto a superar se basa en la naturaleza distribuida del sistema. Los sistemas distribuidos no pueden garantizar la disponibilidad de cualquier nodo del clúster (AP). El tema es que un nodo que esta fuera de servicio cuando se

establecen nuevas configuraciones o políticas, este debe adquirir los nuevos parámetros antes del reestablecer el servicio. Por lo tanto, es necesario un mecanismo que asegure este tipo de información es transferida exitosamente a cada miembro del clúster. Además, la función de administración integral también debe resolver conflictos surgidos de selecciones incompatibles del usuario o de nodos fuera de servicio que se reincorporan con configuraciones y políticas desactualizadas.

Es importante resaltar que las WLAN cognitivas involucran una serie de compromisos. A cambio de la flexibilidad y la inteligencia embebida en el sistema los APs necesitan más CPU y memoria que los APs convencionales usados en las arquitecturas dependiente e independiente. La Tabla 4, resume las características y beneficios de las redes WLAN cognitivas inalámbricas tácticas para sistemas C4ISR.

Característica	Beneficio
Auto Configurable	Selecciona automáticamente parámetros RF básicos tales como potencia de transmisión y frecuencia del canal; monitoriza las bandas operativas de la WLAN en busca de interferencias y ajusta la configuración en consecuencia
Escalabilidad	La red puede crecer desde un solo AP a miles de AP, ya sea un AP a la vez o grupos de APs, mientras que use la infraestructura cableada existente
Administración unificada	La administración del clúster se logra haciendo cambios de configuración en un punto del clúster. Los cambios de la configuración son distribuidos automáticamente a todos los participantes del clúster de forma garantizada
Análisis y clasificación RF	Analiza, clasifica y graba eventos RF en log de eventos del sistema; provee visualización en tiempo real de las bandas operativas del AP
Características avanzadas	Las mismas características avanzadas que con las arquitecturas basadas en el controlador pero sin el costo y la complejidad del controlador

Tabla 4. Características y beneficios de las redes inalámbricas cognitivas

3.2.2.1.3 Estándares emergentes IEEE 802.11

Mientras que la popularidad de IEEE 802.11 crece rápidamente, nuevos estándares 802.11 están surgiendo, sobre en dos grandes categorías: especificaciones que hacen uso de tecnologías inalámbricas avanzadas en Radio Frecuencia (RF) y la capa física (PHY), tales como 802.11n y especificaciones que suplen las necesidades de administración de redes inalámbricas, medidas de desempeño, roaming rápido y necesidades en otras aplicaciones específicas y escenarios de uso. Estos incluyen 802.11k, 802.11p, 802.11r, 802.11s, 802.11t, 802.11u, 802.11v, 802.11w y 802.11y. En esta sección se describen brevemente: objetivos y ámbitos de estos estándares emergentes.

Las tecnologías emergentes así como las aplicaciones inalámbricas (tales como VoIP, Video sobre IP, servicios de localización, despliegues y administración a gran escala) imponen nuevos requerimientos sobre las capacidades de WLANs. Estos avances requieren facilidades estándar para adquirir e intercambiar estadísticas y medidas para administrar y desplegar mejor la WLAN, para utilizar mejor el ancho de banda inalámbrico para optimizar automáticamente el desempeño de la red y mejorar la fiabilidad de la WLAN.

La especificación 802.11k RRM (Radio Resource Measurement) define mejoras a las medidas de los recursos radio mediante la definición de una lista de medidas estandarizadas para los recursos radio y proveyendo mecanismos a las capas superiores en la pila de red para generar reportes de medidas radio y de red consistentes. Los mecanismos incluyen peticiones de medidas así como las MIB con una interfaz OID (Object IDentifier) para las capas superiores.

Las medidas radio suministradas pueden ser usadas para varios beneficios tales como permitir una configuración radio automática y simplificada, logrando mejores prestaciones para la WLAN, optimizando el uso de los recursos radio del cliente, alertando al administrador de red.

Las medidas RRM 802.11k incluyen: Beacons, resumen de paquetes recibidos, histogramas de ruido, estadísticas de la STA, reporte de vecinos, medidas del enlace, QoS, Cargas QBSS, retardo en el acceso, etc.

802.11k adopta un modelo de petición/respuesta a través de una capa de administración para recoger estadísticas y realizar las medidas. En general, 802.11k solamente contiene medidas que prácticamente todos los fabricantes pueden soportar a través de una actualización del firmware o del driver sin que implique modificaciones del hardware.

IEEE 802.11p define mejoras a 802.11 necesarias para soportar aplicaciones ITS (Intelligent Transportation Systems), que incluyen intercambio de datos entre vehículos a altas velocidades y entre vehículos y la infraestructura de la carretera en la banda licenciada a ITS de 5.9GHz (5.85 — 5.925 GHz). 802.11p también es conocido como WAVE (Wireless Access for the Vehicular Environment).

802.11p utiliza canales de 5 y 10MHz, la capa física es OFDM a 5.9GHz, con una máscara espectral que no se logra fácilmente con dispositivos 802.11a. También requiere una capa MAC substancialmente extendida y solo usa algunas de las facilidades de 802.11 como el mecanismo básico de acceso de EDCA.

802.11r define las mejoras a 802.11 necesarias para aportar una solución a las transiciones rápidas entre BSS. Provee una solución para hacer un handoff más rápido para solventar las necesidades de seguridad, latencia mínima y reserva de recursos QoS las cuales son necesarias para aplicaciones VoIP ampliamente distribuidas. 802.11r permitirá la conectividad a bordo de vehículos en movimiento, con handoffs rápidos entre puntos de acceso.

802.11r permite a un cliente inalámbrico establecer una asociación de seguridad y QoS en un nuevo punto de acceso antes de hacer una transición, lo que lleva a una mínima perdida de conectividad e interrupción de la aplicación. Todos los cambios en el proceso de roaming no introducen vulnerabilidades de seguridad.

802.11s define las mejoras requeridas a 802.11 para conformar una nueva topología de redes inalámbricas 802.11, las redes Mesh, las cuales permiten la entrega de tramas de salto a salto. El trabajo de 802.11s empezó en 2005 y actualmente es draft en estado de mejora.

802.11s hereda de los estándares 802.11 existentes muchas características incluyendo la seguridad, QoS y mecanismos de ahorro de energía. Por ejemplo, los enlaces seguros mesh están basados en 802.11i y la distribución de las claves usa una jerarquía de clases y un mesh KDC (Mesh Key Distributor), también es compatible con claves pre-compartidas. También adopta una variedad de conceptos tales como beacons y probe/response para anunciar el Mesh ID, protocolos de enrutamiento, capacidades de seguridad, etc.

Las nuevas características 802.11s incluyen descubrimiento de red, mantenimiento de red, recuperación o restablecimiento de rutas y una funcionalidad de enrutamiento mesh. En particular, 802.11s aporta un protocolo de enrutamiento de capa 2 para redes mesh pequeñas y medianas llamado HWMP (Hybrid Wireless Mesh Protocol), el cual es un hibrido entre dos protocolos de enrutamiento inalámbricos: Tree Based Routing y enrutamiento AODV. Las aplicaciones mesh tanto fijas como móviles están soportadas por HWMP, los intercambios de tramas empleados por HWMP incluyen:

- PANN (Portal Announcement): permite la segmentación mesh permitiendo a los nodos elegir un portal como su Gateway.

- RANN (Root Announcement): permiten la formación pasiva o activa de mesh.
- RREQ (Routing REQuest): construye ruta de encaminamiento y permite el registro de STA en el nodo.
- RREP (Routing REsPonse): construye los caminos de retorno.
- RRER (Route Error): señaliza la perdida de una ruta

El siguiente diagrama ilustra el modelo de red mesh adoptado por el grupo de trabajo 802.11s. Este define tres tipos abstractos de nodos mesh (Figura 12): el punto mesh (MP), el punto de acceso mesh (MAP) y el punto de portal mesh (MPP).

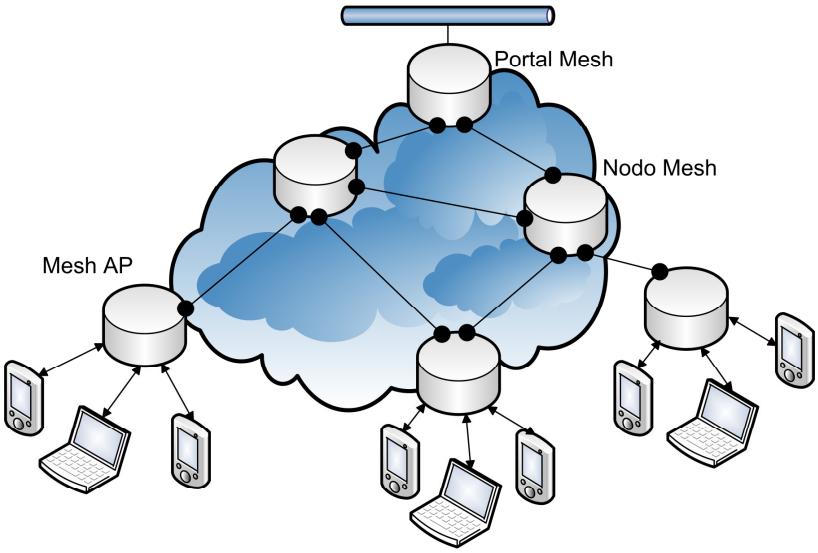

Figura 12. Modelo de red mesh propuesto por IEEE 802.11s

Los mecanismos existentes en 802.11 para la administración de la red inalámbrica son en su mayoría a través de SNMP. Sin embargo, hay algunos inconvenientes en este enfoque. Por ejemplo, no todos los clientes inalámbricos en el mercado poseen capacidades SNMP. En el caso de que un diente inalámbrico no tenga conectividad IP, la administración del dispositivo puede ser requerida pero el uso de SNMP es imposible. Además, las complejidades de un AP 802.11 necesitan más capacidades de administración que las provistas por MIBs SNMP. Por lo tanto, es necesario crear más MIBs o buscar un nuevo enfoque más avanzado que SNMP.

802.11v aporta las mejoras a la administración de redes inalámbricas 802.11. Extiende el trabajo previo de 802.11k en medidas de recursos radio para formar una interfaz coherente y completa a las capas superiores para la administración de STAs por los APs. Mientras que 802.11k aporta los mensajes para obtener la información, el 802.11v aporta la habilidad para configurar estaciones.

Finalmente, en el ámbito táctico la utilización de 802.11 puede ser una buena opción en determinados casos por los anchos de banda que ofrece, bajo coste y fácil despliegue. Sin embargo, la escasez de certificaciones de seguridad, los rangos cortos y la sensibilidad a interferencias pueden llegar a ser puntos en contra. Una acertada elección, particularizada a un ámbito espacial, operacional y radioeléctrico concreto y sobretodo combinada con otras tecnologías de red, puede ser muy adecuada en muchos escenarios. Este caso es la denominada 'burbuja WIFI' que se establece alrededor de un vehículo para la extensión de servicios, utilizada, por ejemplo, en el sistema norteamericano Force XXI Battle Command Brigade And Below (FBCB2) [Mor04].

3.2.2.2 WiMAX IEEE 802.16

El estándar WiMAX (Worldwide Interoperability of Microwave Access) se corresponde a la especificación IEEE 802.16 [IEEE802.16-2004] haciendo referencia a un sistema BWA (Broadband Wireless Access) de alta tasa de transmisión de datos y largo alcance (hasta 50 Km.), escalable, y que permite trabajar en bandas del espectro tanto "licenciado" (bandas de frecuencias: 700MHz, 2.3GHz, 2.5GHz, 3.5GHz, 4.9GHz) como "no licenciado" (bandas de frecuencias: 2.4GHz, 5.7GHz). El servicio, tanto móvil como fijo, se proporciona empleando antenas sectoriales tradicionales o bien antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance.

WiMAX es una tecnología de red inalámbrica de área metropolitana orientada a la interconexión de WIFI hotspots así como el acceso de banda ancha de última milla. Podemos encontrar dos ramas básicas dentro del estándar IEEE 802.16: a) 802.16-2004(d) diseñado para modelos de uso de acceso fijo y que incluye a 802.16a y 802.16c, con tasas de transferencia efectivas de 40Mbps, OFDM 256-FFT y mejoras en el MAC para el soporte de QoS b) IEEE 802.16e [IEEE802.16e], reforma al estándar 802.16-2004 que añade movilidad. 802.16e conserva todas las actualizaciones de WiMAX fijo, añadiendo un soporte robusto para broadband móvil. Por otra parte, la capa MAC esta optimizada para enlaces de larga distancia ya que tolera grandes retardos y jitters.

Las principales diferencias de 802.16e respecto a 802.16-2004 son las siguientes (la lista no es exhaustiva):

- Aparece la estación móvil (MS). Una estación en un servicio de telecomunicación móvil está pensado para ser usado mientras se está en movimiento o durante paradas en puntos sin especificar. Sin embargo, en 802.16e una MS también es una estación subscriptora (SS).
- Procedimientos de handover a nivel MAC.
- Modos de ahorro de energía (para MSs que soportan movilidad): modo idle y modo sleep.
- SOFDMA (Scalable OFDMA). De manera general, la capa PHY OFDMA del estándar 802.16, se reescribió por completo entre 802.16-2004 y 16e. Aunque la palabra SOFDMA no aparece en el documento 802.16e, es el tipo estandarizado de OFDMA.
- Seguridad. La seguridad del 802.16-2004 se actualiza por completo.
- Las técnicas MIMO (Multiple-Input Multiple-Output) y AAS (Advanced Antenna System), ambas introducidas en el 802.16-2004, tienen varias mejoras y detalles de implementación en 802.16e.
- Una nueva clase de QoS: ertPS (enhanced real time Polling Service), esta clase soporta flujos de tiempo real que generan paquetes de datos de tamaño variable de forma periódica, por ejemplo: VoIP con supresión de silencio.

WiMAX es una tecnología con mucho potencial y con un número elevado de aplicaciones, desde su uso más básico por operadores utilizando la tecnología para hacer enlaces punto a punto backhaul entre dos o más ubicaciones o bien soportando islas de cobertura WIFI siendo WIMAX su troncal. Hasta el uso de WiMAX en aplicaciones de telemedicina, monitorización ambiental, prevención de incendios, tal como se definió y probo mediante diferentes testbeds en el marco del proyecto europeo WIERD (WiMAX Extension to Isolated Research Data Networks) [WIERD]. Otra aplicación importante de esta tecnología es su uso para reestablecer redes de comunicaciones en situaciones de emergencia, en [Don05] se define el concepto de 'fly-away communications kit', el cual describe un sistema de comunicaciones basado en una combinación de Wi-Fi, WiMAX y comunicaciones vía satélite para dar soporte de comunicaciones a los first-responders en zonas devastadas por una catástrofe y en la cual se ha perdido toda la infraestructura de red.

El uso de WiMAX no se limita a comunicaciones terrestres, existen varias iniciativas y soluciones para el uso de WiMAX en comunicaciones marítimas, ya sea para la comunicación entre embarcaciones o entre embarcación y puerto. Ejemplo de esto es el proyecto TRITON (TRI-media Telematic Oceanographic Network) [TRITON], el objetivo es desarrollar un sistema que aporte la infraestructura de comunicaciones a diversas aplicaciones como: video vigilancia, prevención de la

piratería, detección de contaminación, seguridad marítima, comunicaciones de voz y datos en general, etc. La red TRITON está basada en el modo mesh de IEEE 802.16-2004 y operando en la frecuencia de 5.8 GHz. La red mesh se conectara a redes terrestres a través de estaciones en el Puerto. En áreas sin cobertura suficiente o en el mar donde no haya un relay en el Puerto se usaran satélites para completar la red [Zho09].

En el campo de salvamento marítimo, en [Gar09] se hace el análisis de una red WiMAX-Satélite para la gestión de emergencias en áreas marinas. En cuanto a soluciones comerciales del uso marítimo de WiMAX es de destacar el sistema BATS (Broadband Antenna Tracking System's) [BATS] que utilizando equipo WiMAX de Redline en la banda de 5.8GHz logra comunicaciones estables a 4.5Mbps entre barcos a 20km de distancia que se mueven a una velocidad de 13 nudos.

3.2.2.2.1 Capa de protocolos WiMAX

El estándar de red BWA IEEE 802.16 especifica la interfaz aérea de un sistema BWA fijo que soporta servicios multimedia. La capa de control de acceso al medio (MAC) soporta principalmente arquitecturas punto a multipunto (PMP), con una topología tipo mesh opcional. La capa MAC está estructurada para soportar varias capas físicas (PHY). De hecho, solo dos de ellas son usadas en WiMAX.

La arquitectura de capas de protocolo definida en WiMAX/IEEE 802.16 [IEEE802.16- 2004] puede verse en la Figura 13, como se puede observar el estándar 802.16 define solamente las dos capas más bajas, la capa física (PHY) y la capa MAC, en la capa LLC, se aplica el estándar IEEE 802.2. La capa MAC está compuesta de tres subcapas, la subcapa de convergencia (CS), la subcapa de partes comunes (CPS) y la subcapa de seguridad.

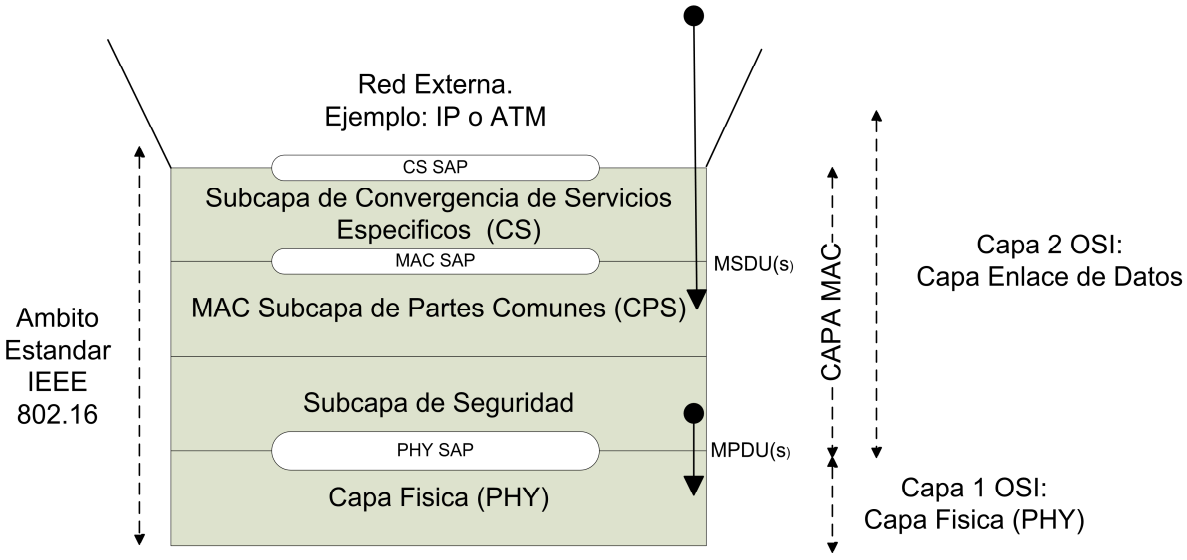

Figura 13. Capas de protocolo del estándar 802.16 BWA

La subcapa de convergencia de servicios específicos (CS), está por encima de la subcapa CPS y utiliza sus servicios a través del punto de acceso al servicio (SAP) MAC (ver Figura 13). La subcapa CS realiza las siguientes funciones:

- Acepta PDUs de capas superiores. En la versión del estándar IEEE802.16-2004, se definen especificaciones CS para dos tipos de capas superiores: CS para asynchronous

transfer mode (ATM) y CS para paquetes, en el último caso los protocolos de capa superior pueden ser IP versión 4 o 6.

- Clasificación y mapeo de MSDUs en los CIDs (Connection IDentifier) apropiados. Esta es una función básica de los mecanismos de administración de calidad de servicio (QoS) de 802.16 BWA.
- Procesamiento (de ser requerido) de las PDUs de nivel superior basado en la clasificación.
- Una función opcional de la. subcapa CS es PHS (Payload Header Supression), esto es, el proceso de suprimir partes repetitivas de los encabezados del payload en el emisor y restaurar estos encabezados en el receptor.
- Entregar PDUs CS al MAC SAP apropiado y recibir PDUs CS de la entidad peer.

La subcapa de partes comunes (CPS) reside en medio de la capa MAC. Esta subcapa representa el corazón del protocolo MAC y es responsable de:

- Asignación de ancho de banda
- Establecimiento de conexiones
- Mantenimiento de conexiones entre dos sitios

El estándar 802.16-2004 define un conjunto de mensajes de administración y de transferencia. Los mensajes de administración se intercambian entre los SS y la BS antes y durante el establecimiento de la conexión. Cuando la conexión se establece, los mensajes de transferencia se intercambian para permitir la transmisión.

La subcapa CPS recibe datos de varios CSs, a través del MAC SAP, clasificado para conexiones MAC particulares. La QoS se tiene en cuenta para la transmisión y la planificación de datos sobre la capa física. La subcapa CPS incluye muchos procedimientos de diferentes tipos: construcción de la trama, acceso múltiple, asignación de ancho de banda, administración de recurso radio, administración de QoS, etc.

La subcapa MAC también contiene una subcapa de seguridad separada (ver Figura 13) la cual provee autenticación, intercambio seguro de claves, cifrado y control de la integridad a través del sistema BWA. En el estándar 802.16, el cifrado de las conexiones entre los SS y la BS se hace con un protocolo de cifrado de datos que se aplica en ambos sentidos de la comunicación.

Se usa el protocolo de PKM (Privacy Key Management), como protocolo de autenticación para la distribución segura de claves desde la BS a los SS. Los mecanismo de privacidad básicos se refuerzan añadiendo autenticación del SS basada en certificados digitales. Además, la BS utiliza el protocolo PKM para acceso condicional a los servicios de red. La enmienda 802.16e define PKMv2 el cual tiene el mismo framework que PKM, renombrándolo PKMv1, con algunas mejoras como nuevos algoritmos de cifrado, autenticación mutua entre el SS y la BS, soporte de handover y un nuevo algoritmo de control de la integridad.

La capa física (PHY) de WiMAX, establece la conexión física entre ambos extremos, a menudo en las dos direcciones (uplink y downlink). Como 802.16 es evidentemente una tecnología digital, la capa física es responsable de la transmisión de secuencias de bits. Esta capa define el tipo de señal usada, la clase de modulación y demodulación, la potencia de transmisión y también otras características físicas.

El estándar 802.16 considera la banda de frecuencia de 2 - 66 GHz, esta banda se divide en dos partes:

- El primer rango está entre 2 y 11GHz y está destinada para transmisiones NLOS. Esta se definió previo al estándar 802.16a. En la actualidad existe equipamiento WiMAX certificado a partir de la banda de 700MHz.

- El segundo rango está entre los 11 y 66 GHz y está destinado para transmisión LOS. No se usa en WiMAX.

Se definen 5 interfaces físicas en el estándar 802.16. Estas interfaces están resumidas en la Tabla 5. Las cincos interfaces físicas están cada una descrita en una sección del estándar 802.16 (o en sus enmiendas). Los sistemas 802.16 pueden usar tanto FDD (Frecuency Division Duplexing) como TDD (Time Division Duplexing).

Se dan algunas especificaciones para la banda de frecuencias no licenciadas usadas por 802.16-2004 en el marco de la capa física WirelessHUMAN (High-speed Unlicensed Metropolitan Area Network). Para las bandas de frecuencias no licenciadas, aparte de las características mencionadas en la Tabla 5, el estándar requiere mecanismos como la selección dinámica de frecuencia (DFS) para facilitar la detección y evitar la interferencia con otros usuarios. WiMAX solamente considera las capas físicas OFDM y OFDMA de 802.16.

Denominación	Banda de Frecuencias	Duplexing	Opciones MAC
WirelessMAN-SC	10 - 66 GHz (LOS)	TDD y FDD	
WirelessMAN-SCa	Por debajo de 11GHz (NLOS); licenciada	TDD y FDD	AAS, ARQ, STC, movilidad
WirelessMAN-OFDM	Por debajo de 11GHz (NLOS); licenciada	TDD y FDD	AAS, ARQ, STC, mesh, movilidad
WirelessMAN-OFDMA	Por debajo de 11GHz (NLOS); licenciada	TDD y FDD	AAS, ARQ, HARQ, STC, movilidad
WirelessHUMAN	Por debajo de 11GHz (NLOS); No licenciada	TDD	AAS, ARQ, STC, mesh

Tabla 5. Interfaces físicas definidas en el estándar IEEE 802.16

3.2.2.2.2 Arquitectura WiMAX

La arquitectura WiMAX está basada en el uso de protocolos IP estandarizados y marcos como el IP Multimedia Subsystem (IMS). Dos grupos de trabajo del WiMAX Forum definen la arquitectura y las funcionalidades asociadas: el Network Working Group (NWG) crea las especificaciones de red y el Service Provider Working Group (SPWG) ayuda a definir las prioridades y requerimientos.

El conjunto de especificaciones emitidas por estos dos grupos incluyen varias alternativas para el mapeo de diferentes funcionalidades requeridas a equipos físicos, permitiendo al mismo tiempo implementaciones dependientes del fabricante y también puntos de interoperabilidad a nivel de red gracias al uso de interfaces abiertas estandarizadas [WMFT32-09] [WMFT33-09].

La arquitectura de referencia de WiMAX ha sido creada basada en los siguientes requerimientos:

- Una red basada en paquetes de alto desempeño con divisiones funcionales asegurando una máxima flexibilidad basada en los protocolos estándares de IEEE e IETF.
- El soporte de una amplia gama de servicios y aplicaciones.
- El soporte de roaming e interoperatividad con otras redes fijas y móviles.

En términos de aplicaciones y servicios, una red WiMAX está diseñada para que sea capaz de soportar:

- Voz sobre IP (VoIP), multimedia (usando IMS) y otro servicios obligatorios como llamadas de emergencia.
- Acceso a una gran variedad de proveedores de aplicaciones de servicio.
- Interfaces con una variedad de pasarelas de red para convertir servicios antiguos (circuitos de voz, MMS) en IP y transportarlos sobre redes de acceso radio WiMAX.

Además, considerando la interconexión de redes y el roaming, varios escenarios deben ser soportados:

- Poca dependencia con las redes tableadas (DSL) o inalámbricas (redes móviles 3GPP o 3GPP2)
- Roaming global entre operadores WiMAX (esto incluye, entre otras cosas, un uso consistente del servidor AAA, entre operadores WiMAX para la autenticación y facturación).
- Una variedad de métodos de autenticación de usuarios (usuario/password, certificados digitales, basados en SIM)

3.2.2.2.3 Modelo de referencia de red

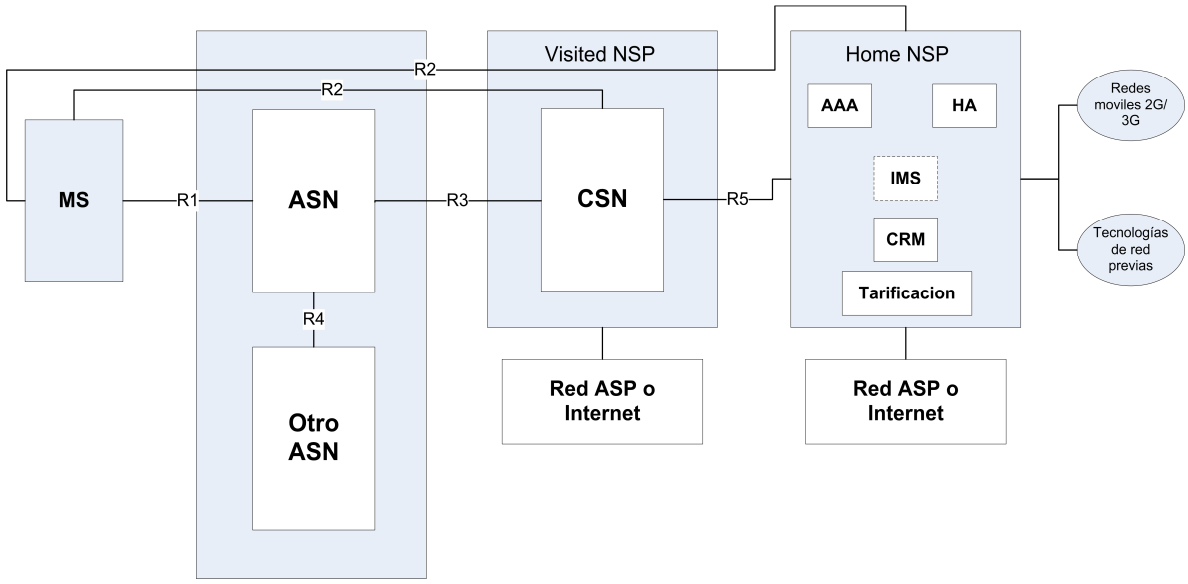

Figura 14. Modelo de referencia de red WiMAX con componentes (MS/ASN/CSN), puntos de referencia (RI a R5) y actores (NAP/NSP/ASP)

El modelo de red de referencia de WiMAX (Figura 14) consta de tres componentes interconectados por interfaces estandarizadas o puntos de referencias R1 a R5, estos tres componentes son:

- La estación móvil (MS)
- La red de acceso a servicios (ASN)
- La red de conectividad de servicios (CSN)

La estación móvil (MS) es un equipo móvil genérico que provee conectividad entre el equipamiento subscriptor y una BS WiMAX. La red de acceso a servicios (ASN) incluye un conjunto de funcionalidades que proveen conexiones de acceso radio a los subscriptores WiMAX. Una o más

ASN, se interconectan a través del punto de referencia R4. Un proveedor de acceso a servicios (NAP) provee infraestructuras de acceso radio a uno o varios proveedores de servicios de red (NSP). El NSP es una entidad de negocio que permite la conectividad IP y servicios WiMAX a los subscriptores WiMAX de acuerdo a los acuerdos de servicios (SLA) establecidos.

El NSP implementa la red de conectividad de servicios (CSN), la cual provee la conectividad IP para subscriptores WiMAX. En la parte de la red de acceso radio, los servicios WiMAX se proveen a través de acuerdos contractuales con uno o varios NAP. En la parte de aplicaciones, los servicios WiMAX se prestan gracias a acuerdo contractuales con proveedores de servicios de aplicaciones (ASP) y/o a través de conexiones directas a Internet. Adicionalmente, un NSP en un país dado puede llegar a acuerdos de roaming con otros NSPs, los cuales pueden estar en países distintos. Por lo tanto, un subscriptor WiMAX puede estar registrado en un Home-NSP o a un Visited NSP, es decir un NSP con el cual Home-NSP tiene un acuerdo de roaming.

El ASN incluye todas las funcionalidades que permiten la conectividad radio con los subscriptores WiMAX. Como consecuencia, el ASN provee principalmente:

- Conectividad a nivel de capa 2 con los subscriptores WiMAX (a través del interfaz aéreo WiMAX).
- Mecanismos de administración de los recursos radio (RRM) tales como control y ejecución del handover.
- Gestión de la movilidad y del paging (en el supuesto de servicios de portabilidad/ movilidad).
- Funciones de retransmisión al CSN para el establecimiento de conectividad a nivel 3 con subscriptores WiMAX (procedimientos AAA, asignación de direcciones IP)
- Tunelización de datos y señalización entre el ASN y el CSN a través del punto de referencia R3.
- Descubrimiento de red y elección del NAP/NSP preferido

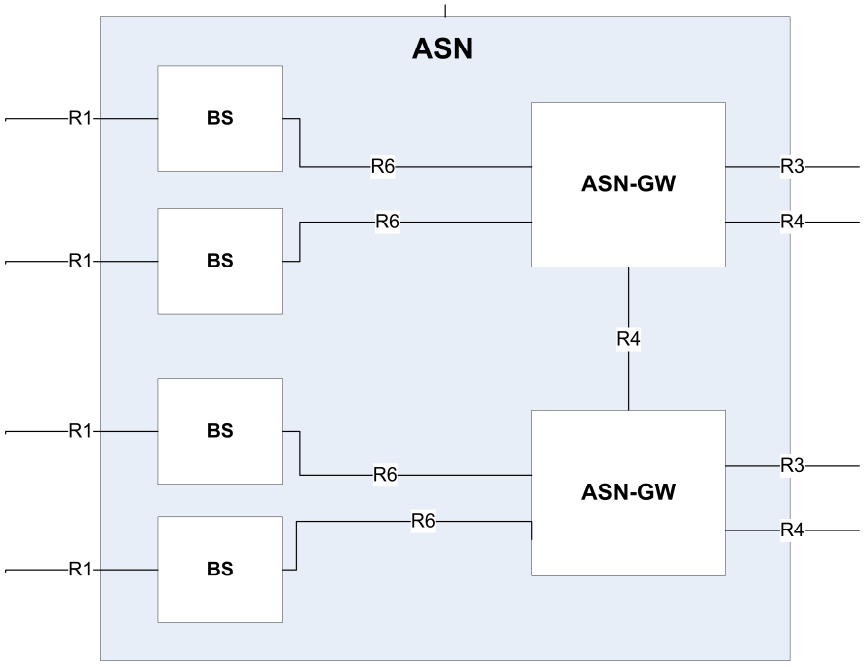

Figura 15. Modelo de referencia de ASN genérico.

El ASN usualmente consta de varias estaciones base (BS) conectadas a varios ASN Gateways (ASN-GW), como se muestra en la Figura 15. Dentro del ASN, se describen 2 puntos de referencias adicionales: el R6 que define interfaz de comunicación entre BS y ASN-GW, esta

interfaz se encarga de la gestión del túnel IP con el fin de conectar y desconectar la conexión con el MS. El R8 define la interfaz de comunicación entre BS y se encarga de hacer Mobile Handoffs

La BS es la entidad que implementa las características MAC y PHY tal como los definen los estándares 802.16, la estación base también está a cargo de la planificación de usuarios y de los mensajes de señalización intercambiados con el ASN-GW a través de la interfaz R6, también puede incorporar otras funciones de acceso de acuerdo al perfil ASN.

En una red de acceso WiMAX, una instancia de BS se define en términos de un sector y una frecuencia asignada. En el caso de varias frecuencias asignadas a un sector, el sector incluye tantas instancias de BS como frecuencias tenga asignadas. La conectividad a múltiples ASN-GW puede ser requerida en el caso de balanceo de carga o para propósitos de redundancia.

El ASN-GW actúa como un punto de decisión para funciones nonbearer plane (ejemplo: administración de recursos radio) y como un punto de refuerzo para funciones bearer plane. Para propósitos de implementación, la descomposición de las funciones ASN en estos dos grupos es opcional. Si esta descomposición se hace, los dos grupos están separados por el punto de referencia R7. Como en todo sistema de telecomunicación, el ASN-GW puede ser diseñado para proveer redundancia y balanceo de carga entre distintos ASN-GW.

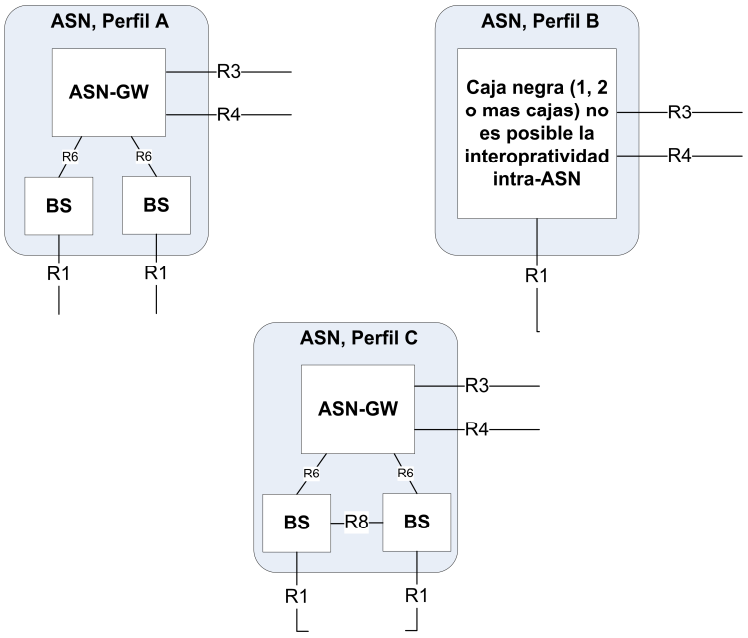

Figura 16. Perfiles ASN A, B y C.

Hay tres opciones de implementación de ASN: perfiles ASN A, B y C (Figura 3-14). De acuerdo a los perfiles, algunas funcionalidades están implementadas en la BS o en el ASN-GW (perfiles A y C) o por una caja negra en el caso del perfil B ASN. En particular, la implementación del perfil A incluye:

- Control de handover dentro del ASN-GW, lo cual permite un control más fácil de los recursos radio durante el procedimiento de handover y la preparación de las rutas de reencaminamiento a nivel 3.
- Control de recurso radio (RRC) dentro del ASN-GW (es posible el balanceo de carga entre BSs)

La movilidad ASN Anchored se logra a través de los puntos de referencia R6 y R4. Esta movilidad se refiere a handovers donde el punto de anclaje para el MS que está en el ASN no cambia.

La implementación del perfil C tiene la misma estructura del perfil A, la diferencia entre ellos es que las BSs tienen muchas más funcionalidades. Una implementación del perfil C incluye.

- El control del HO (Handover) se encuentra en la BS.
- Las funcionalidades de control de recursos radio (RRC) se encuentra en la BS, habilitando la gestión de recursos radio RRM dentro de la BS.

El perfil B no especifica ninguna división funcional, de haber alguna es decisión del fabricante. Como consecuencia, no es posible la interoperatividad intra-ASN con el perfil B.

La red CSN proporciona los servicios de conectividad IP a los clientes WiMAX. Proporcionando las siguientes características principales:

- Control de Políticas y Admisión basándose en perfiles de suscripción de clientes
- Tunelización (basado en protocolos IP) con otros equipos/redes (soporte ASN CSN Tunnelling, inter-CSN Tunnelling para Roaming).
- Soporte de movilidad basado en Mobile IP (Home Agent (HA) funcionalidad para movilidad inter-ASN).
- Tarificación del cliente e interoperabilidad entre distintos Operadores.
- Servicios WiMAX, tales como acceso a Internet, los servicios basados en la localización, conectividad para servicios "peer-to-peer", provisioning, etc.
- Direccionamiento IP a los MS y localización de parámetros de punto final para las sesiones de usuario.

Para lograr estas funciones, la red CSN, puede estar compuesta de los siguientes equipos:

- Routers (con una eventual funcionalidad HA (Home Agent) para la movilidad inter-ASN Gateway)
- Servidores DHCP y DNS
- Servidores/proxies AAA y bases de datos de usuarios WiMAX para acceso, autenticación, autorización, tarificación y aprovisionamiento
- Pasarelas para la integración/interoperatividad de la red WiMAX con otras redes (ej.: una red 3GPP o PSTN).
- Firewalls para proteger a los equipos de la red WiMAX mediante el refuerzo de políticas de acceso en el tráfico desde y hacia la red externa (especialmente usada para la detección/prevención de denegación de servicio)

El modelo de referencia de red WiMAX define varios puntos de referencia (RPs) entre varias entidades en la red WiMAX. Estos RPs introducen puntos de interoperatividad entre equipos de distintos fabricantes.

El punto de referencia R1 define el interfaz radio entre la MS y el ASN, como consecuencia de ello incluye todas las características físicas y MAC definidas en los perfiles WiMAX del estándar IEEE 802.16. El R1 transporta tanto tráfico como mensajes de control del plano de usuario

El punto de referencia R2 es una interfaz lógica entre la MS y el CSN. Contiene todos los protocolos y otros procedimientos relacionados con la autenticación (usuario y dispositivo), autorización de servicios y configuración IP de los dispositivos. Esta interfaz lógica se establece entre la MS y el H-NSP y algunos protocolos (tales como la administración de direcciones IP) puede ser ejecutadas por el V-NSP en el caso de roaming.

El punto de referencia R3 es la interfaz lógica entre el ASN y el CSN. Este punto transporta tanto los mensajes del plano de control (métodos AAA, políticas de refuerzo de la QoS de extremo a extremo, mensajes de administración de la movilidad) e información del plano de datos a través del túnel entre el ASN y el CSN.

El punto de referencia R4 interconecta dos ASN (ASN perfil B) o dos ASN-GW (perfiles ASN A o C). Este punto transporta mensajes tanto del plano de control como de datos, especialmente durante el handover de un usuario WiMAX entre ASNs/ASN GWs o durante los procedimientos de actualización de la localización en el modo Idle. Este RP es el único punto de interoperatividad entre ASNs de distintos fabricantes.

El punto de referencia R5 es la interfaz que interconecta dos CSNs. Consta de un conjunto de métodos en el plano de control y de datos entre el CSN de una red propia (H-NSP) y una red visitante (V-NSP).

El punto de referencia R6 conecta la BS y el ASN-GW. Este punto transporta tanto mensajes de control (para el establecimiento, modificación, control y liberación de la ruta de datos de acuerdo con la movilidad del MS) como información del plano de datos (enlace de datos intra-ASN entre BS y ASN-GW). El método de tunelling utilizado es GRE, MPLS o VLAN. Esta interfaz también transporta, en conjunto con R4, la información del estado MAC transportada por el punto de referencia R8 cuando la interoperatividad R8 entre BSs no está disponible.

El punto de referencia R7 es una interfaz lógica opcional entre la función de decisión y la función de refuerzo del ASN-GW.

El punto de referencia R8 es una interfaz lógica entre BSs. Transporta el intercambio de datos en el plano de control que es usada para habilitar el handover rápido y eficiente entre BSs. Opcionalmente el R8 puede transportar información en el plano de datos durante la fase de handover. Es de anotar que una interfaz física directa no es necesaria entre BSs. Los métodos R8 pueden ser transportados a través, por ejemplo, del ASN GW.

3.3 Modelos de QoS

La calidad de servicio (QoS) no es una necesidad única de las redes inalámbricas, la distribución estadística de la infraestructura de red entre servicios de tiempo real y servicios IP normales (como correo electrónico, FTP), de una manera eficiente ha adquirido una notable importancia con el aumento de aplicaciones multimedia con flujos simultáneos de datos diferentes con distintos requerimientos de tiempo real.

Servicios como voz sobre IP y distribución de contenidos multimedia resaltan la necesidad de administrar, controlar, diferenciar y garantizar los niveles de servicios deseados durante la comunicación. La percepción del usuario de calidad está determinada por factores de extremo a extremo como latencia, jitter, throughput, tasa de errores y ancho de banda. La gestión de QoS asociada a mecanismos de ingeniería de tráfico logran los niveles de servicio deseados.

Un modelo de QoS describe un conjunto de servicios de extremo a extremo, los cuales permiten a los clientes seleccionar una serie de garantías que gobiernan propiedades tales como tiempo, planificación y fiabilidad. El modelo de QoS especifica la arquitectura que nos permite ofrecer un mejor servicio que el modelo tradicional de best-effort. Esta arquitectura debe tener en cuenta las limitaciones impuestas por el tipo de redes inalámbricas que son objeto de estudio de la presente tesis, tales como, topología dinámica, retardo y fiabilidad.

El IETF ha propuesto dos modelos de QoS para las redes cableadas:

- Differentiated services (DiffServ) [RFC2474] [RFC2475]: que es un mecanismo de granularidad gruesa basado en la clase. La unidad fundamental es el paquete que se clasifica en función del tipo de servicio al que se quiere adscribir al flujo al que el paquete pertenece. Es una aproximación simple. La clasificación de paquetes y el comportamiento por salto (PHB: Per Hop Behavior) son los bloques principales de las redes DiffServ. Se definen dos PHB, EF (Expedited Forwarding) [RFC2598] para datos en tiempo real sensible al retardo y AF (Assured Forwarding) [RFC2597] para datos no críticos, este último se subdivide en 4 subclases más. La clasificación de los paquetes se hace utilizando códigos DSCP que se mapean a niveles de servicios deseados. Los nodos DiffServ reencaminan los paquetes y determinan la precedencia de descarte en caso de congestión basados en los códigos DSCP. Varios mecanismos tales como: colas de prioridad, colas basadas en clase pueden ser usados para implementar PHB.
- Integrated Services (IntServ): que es un mecanismo de granularidad fina basado en el flujo. La unidad fundamental es el flujo, sobre el que se opera y sobre el que realizan reservas de recursos, para las que existe un protocolo específico RSVP (Resource ReSerVation Protocol) [RFC2205], a lo largo de todo el camino de transmisión. Es una aproximación compleja.

El modelo IntServ/RSVP, no tiene en cuenta las limitaciones de recursos impuestas por las redes inalámbricas. La señalización del protocolo RSVP es muy voluminosa en comparación con el ancho de banda disponible en este tipo de redes. Además, el proceso de mantenimiento de rutas es ineficiente cuando consideramos el carácter dinámico de este tipo de redes.

El modelo DiffServ parece más apropiado, pero fue concebido para redes con una topología de red relativamente estática y con suficiente ancho de banda en los enlaces troncales.

Para resolver este problema, varios autores han propuesto diversas soluciones que se ajustan mejor a las redes inalámbricas. Las aproximaciones fundamentales son relativas a las colas de entrega de paquetes (ya sea en nodos individuales o en hardware específico de red), en los protocolos de acceso al medio y en encontrar y mantener rutas QoS de forma distribuida. Atacando estos elementos es como se consigue una predictibilidad en los tiempos de entrega de los paquetes.

En lo referente a protocolos MAC podemos diferenciar entre aproximaciones centralizadas y distribuidas, el objetivo de estos protocolos es coordinar de forma eficiente y compartir de manera justa el ancho de banda disponible entre los nodos [KUM06], [GRO99]. Como ejemplo de protocolos mac centralizados tenemos TDMA [ZHUO2], CDMA [CHE97], FDMA y CSMA [SOB99] que estarán disponibles dependiendo de la tecnología de comunicación utilizada.

Las soluciones QoS basadas en protocolos MAC centralizados involucran la planificación de slots de tiempo y/o división de frecuencias. Estas aproximaciones requieren de una autoridad central que controle las comunicaciones así como una sincronización precisa entre los nodos. En [Lin99], se utiliza un esquema CDMA sobre una red TDMA para reducir la interferencia entre las distintas transmisiones. Mediante el uso del protocolo de enrutamiento DSDV se calcula la información del ancho de banda disponible así como la diseminación de rutas cortas en la red por lo cual se pueden calcular rutas QoS. En enfoque similar se propone en [CHE97]. Una versión modificada de AODV se utiliza para aporta QoS en redes inalámbricas basadas en TDMA en [ZHUO2].

Debido a la naturaleza dinámica y móvil de las redes inalámbricas los protocolos MAC distribuidos son ampliamente utilizados en estos escenarios. Aunque, en esta aproximación calcular el ancho de banda disponible en la red es una tarea más complicada ya que no existe una autoridad central y cada nodo tiene que hacer el cálculo teniendo en cuenta el ancho de banda utilizado por sí mismo y por sus vecinos. En [XUE03], se propone un método para calcular el ancho de banda disponible para un nodo, donde el ancho de banda agregado del nodo i, está dado por el ancho de

banda utilizado por sí mismo, la suma del tráfico entre dos nodos vecinos y la suma del tráfico entre un nodo vecino y un nodo fuera del rango del nodo i.

En [SOB99] se propone un esquema de prioridad para 802.11 basado en el concepto BB (Black Burst) para aportar mecanismos de prioridad de QoS para aplicaciones de tiempo real en redes inalámbricas, este concepto consiste en definir una zona que retardos de extremo a extremo acotados para transmisiones de video y voz, también es de destacar el protocolo Q-MAC [LIU05], que aporta QoS mediante la diferenciación de servicios de red basados en niveles de prioridad que reflejan las prioridades de la capa de aplicación y los recursos disponibles.

En el ámbito de la planificación de paquetes existen múltiples planificadores de uso extendido en routers (y en general en cualquier máquina con capacidades de routing, por ejemplo un kernel de Linux o Windows 2000 server) cuya principal funcionalidad es la de garantizar una entrega equilibrada de los paquetes de los distintos flujos que reciben. Cabe destacar fair-queueing [Nag87], Weighted Fair Queueing [Sti98], Random Early detection (RED) [F1o93], Stochastic Fairness Queueing (SFQ) [Mck90], Token Bucket Filter (TBQ), [SriO4] amén de las clásicas políticas de asignación equiprobables FIFO, LIFO y Round Robin. Sobre estos mismos planificadores se puede llevar a cabo una planificación por prioridades de los paquetes atendiendo, básicamente, a parámetros como los campos de DiffServ en la cabecera IP.

Respecto a los protocolos de enrutamiento para redes inalámbricas tácticas, en la sección 3.4 de la presente tesis, se abordan con detalle distintas soluciones, además de estos cabe destacar el algoritmo de enrutamiento CEDAR (Core Extraction Distributed Ad-hoc Routing) [SIV99] y el framework INSIGNIA [Lee00] el cual propone el uso de señalización en banda, en la cual se incluye información de parámetros de QoS y el estado de los nodos dentro de los paquetes de datos (en este caso, en la cabecera del paquete IP).

En lo referente a tecnologías radio militar como pueden ser radios VHF y HF con capacidades IP ninguna de estas funcionalidades está implementada y además son desarrollos cerrados donde no se permite la modificación de ninguno de sus parámetros. La única intervención es garantizar a nivel IP o nivel de aplicación determinados parámetros que acoten el tiempo de comunicación de mensajes. Detalles sobre la implementación de QoS sobre estos sistemas, que forman parte de la arquitectura expuesta en la presente tesis, se verá en capítulos posteriores.

A continuación, describiremos los modelos de QoS que implementan las tecnologías de comunicaciones civiles probadas en esta tesis (comunicaciones celulares 3G, WLAN y WiMAX) y para cada una de ellas describiremos los innovaciones que se están llevando a cabo en lo referente a QoS y que constituirán la nueva generación de estos sistemas.

3.3.1 QoS en redes WLAN

El estándar IEEE 802.11 solamente soportaba servicio best-effort a través de sus mecanismos de acceso DCF (Distributed Coordination Function) y PCF (Point Coordination Function). La necesidad de mejores mecanismos de acceso que permitieran diferenciación de servicios y soporte de aplicaciones multimedia lleva a la creación del estándar 802.11e.

El estándar 802.11e introduce el HCF (Hybrid Coordination Function) el cual implementa un mecanismo basado en contención (EDCA: Enhanced Distributed Channel Access) y un mecanismo basado en poolling (HCCA: HCF Controlled Channel Access). El soporte de QoS en EDCA se logra a través del concepto de categorías de tráfico (TC) para distinguir entre clases de tráfico diferentes, dándole a cada una ellas diferentes prioridades de acceso al medio. Cada TC tiene su propia cola de transmisión y su propio conjunto de parámetros de canal de acceso (Figura 17).

La diferenciación de servicio entres TCs se refuerza fijando parámetros diferentes de la ventana de contención (CWmin, CWmax), AIFS (Arbitrary Inter-Frame Space) y límite de duración de la oportunidad de transmisión (TXOPlimit) (Figura 17). Una TC de mayor prioridad tendrá un AIFS,

CWmin o CWmax más corto que le den una mayor probabilidad de acceder al medio o de transportar una carga mayor. TC3 y TC2 están reservadas para aplicaciones de tiempo real (transmisión de voz y video) mientras que TC1 y TC0 esta destinadas a tráfico best-effort y background, es decir, tráfico sin requisitos de QoS.

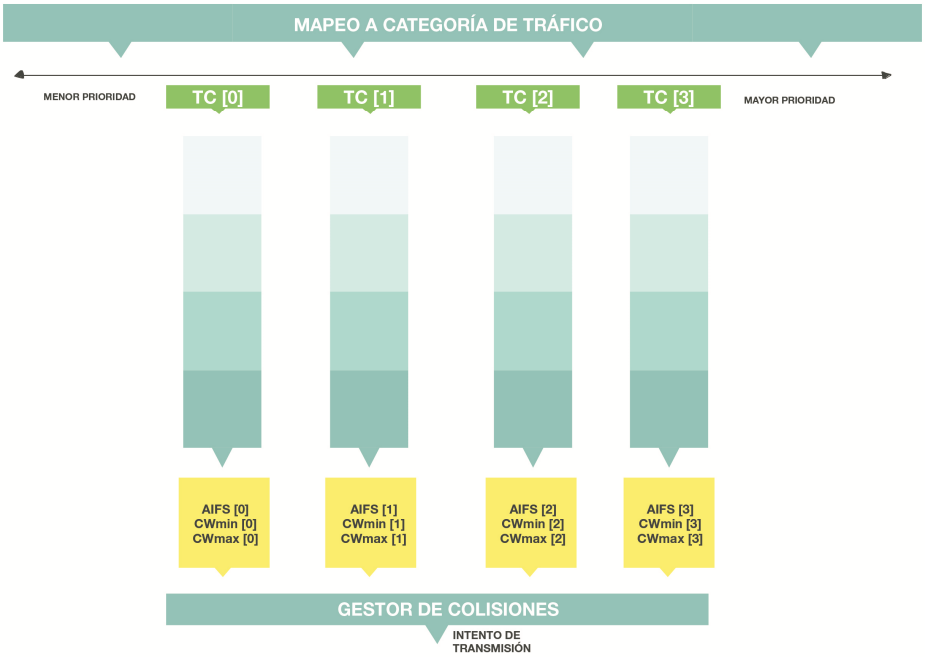

Figura 17. Clasificación y mapeo de tráfico en IEEE 802.11.

En las redes WLAN 802.11 surge un buen número de dificultades añadidas que afecta directamente a la QoS. Así, la ausencia de un control centralizado, el menor y variable ancho de banda, la mayor tasa de error en los canales radio y la movilidad de los nodos con la consiguiente inestabilidad topológica, conducen a dificultar las garantías de tiempo real en ese tipo de redes. El efecto del movimiento tiene una incidencia muy destacada puesto que, al variar la topología de manera dinámica e impredeciblemente puede introducir perturbaciones considerables.

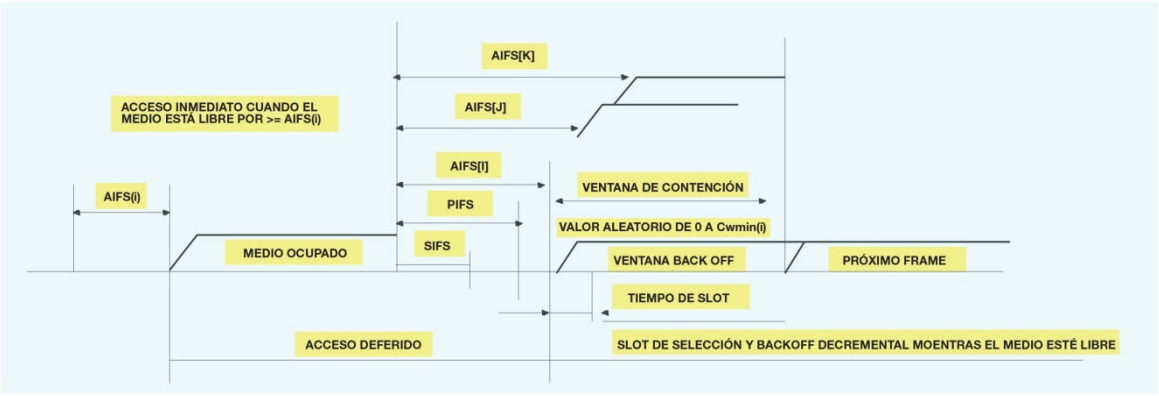

Figura 18. Mecanismo de acceso EDCA

Existen protocolos síncronos como por ejemplo Clúster TDMA [Lin97], Clúster Token [Lin96] o SRMA/PA (Soft Reservoir Multiple Access with Priority Assignment) [Alm00] que salvan la carencia de un nodo central pagando el precio de requerir una sincronización temporal.
Por otra parte, existen toda una serie de protocolos asíncronos que no requieren un tiempo global y por lo tanto son más flexibles para un entorno Wireless. Utilizan unas ventanas temporales muy pequeñas y algoritmos muy optimizados para evitar las colisiones de forma que se acoten los retardos y el ancho de banda entregado. Además, los paquetes tienen estampado un deadline de forma que cuando un nodo comprueba que ha expirado los descarta, evitando que consuman recursos. Además soportan una aproximación de servicios diferenciados, con colas de prioridad. Ejemplos de estas aproximaciones son Real Time MAC (RT-MAC) [Ba199], Distributed Coordination Function - Priority Classes (DCF-PC) [Den99], Enhanced Distributed Coordination Function (EDCF) [Ben01].

Otros protocolos asíncronos adoptan la aproximación de realizar una reserva de recursos de forma que cada nodo tiene unos slots temporales asignados para garantizar retardos acotados. Es el caso de Multiple Access Collision Avoidance with Piggyback Reservations (MACA/PR) [Ger97] y Dynamic Bandwidth Allocation Sharing Extension (DBASE) [She01]

3.3.2 QoS en WiMAX

WiMAX cuenta con excelentes mecanismos de QoS que permiten lograr una calidad de servicio diferenciada para distintas aplicaciones. En primer lugar la arquitectura de calidad de servicio de WiMAX utiliza las clases de servicio a fin de diferenciar las conexiones procedentes de diferentes aplicaciones con diferentes requisitos de QoS. Cada conexión se clasifica en una clase de servicio que corresponde a su tipo de aplicación. Este proceso se llama clasificación. Una vez clasificados se pueden aplicar métodos y algoritmos de planificación entre las diferentes clases de servicio o incluso dentro de la misma clase.

El proceso de clasificación estándar del IEEE 802.16, donde se asocia cada paquete con un flujo de servicio (SF), contiene la característica de QoS que lo distingue de otros protocolos de red inalámbrica, como 802.11 o 3G [WOO06]. El clasificador definido en la SS por la arquitectura WiMAX QoS clasifica las conexiones procedentes de una capa de aplicación, basado en el campo de identificador de conexión (CID), y luego reenvía cada conexión a la cola adecuada [CHO05]. Esto permite que se soporte una política de calidad de servicio por conexión. En WiMAX, dado que la capa MAC es orientada a la conexión, cada flujo de servicio se le asigna un identificador (ID). Hay dos tipos de identificadores para cada flujo de servicio de entrada: el identificador de flujo de servicio (SFID) y el identificador de conexión (CID). El SFID es un campo de longitud de 32 bits temporalmente asignado a cada flujo de servicio, mientras que CID es un campo de longitud de 16 bits asignado a un flujo de servicio admitido o activo. Ambos SFID y CID son proporcionados por la BS.

Se pueden definir dos tipos de clasificadores: el clasificador UL que se aplica en la SS y clasifica los flujos de servicio de la SS antes de ser transmitido en el canal de UL, y el clasificador DL que se aplica en la BS y tiene como objetivo clasificar los flujos SF antes de transmitirlos en el canal DL [GAK05].

De acuerdo a las características de trafico de diferentes servicios, se han definido cinco tipos de servicios de planificación para el interfaz WiMAX: unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), extended real-time polling service (ertPS) y el servicio best effort (BE). Entre ellos UGS, rtPS y ertPS son usados para tráfico de tiempo real y trafico interactivo tales como: video y juegos online (rtPS), VoIP sin supresión de silencio (ertps), mientras que nrtPS y BE son utilizadas para tráfico no critico corno transferencias de fichero (nrtPS), correo electrónico y navegación Web (BE).

Cada uno de estos servicios de planificación tiene un conjunto obligatorio de parámetros de QoS que deben ser incluidos en la definición del SF. La Tabla 6 muestra los parámetros de QoS obligatorios para cada uno de los servicios de planificación

Servicio de Planificación	Tasa de tráfico máxima sostenida	Tasa de tráfico mínima sostenida	Política petición / transmisión	Jitter tolerado	Latencia Máxima	Prioridad Tráfico
UGS	■	(puede estar presente)	■	■	■	
ertPS	■	■	■		■	
rtPS	■	■	■		■	
nrtPS	■	■	■			■
BE	■		■			■

Tabla 6. Parámetros QoS obligatorios de los servicios de planificación definidos en WiMAX.

En las redes WiMAX, la BS administra los recursos de ancho de banda entre las conexiones derivadas de SSs diferentes. Se utilizan distintos métodos para solicitar ancho de banda para una conexión. La BS puede hacer una asignación a la SS, o dar una oportunidad de transmisión unicast para que la SS envíe su solicitud de ancho de banda en el canal de UL. El período de contención en la subtrama de UL, que se produce justo después de la solicitud de ranging, se reserva sólo para las conexiones que no son de tiempo real, tales como, SF nrtPS y BE con el fin de enviar su solicitud de ancho e tan el mecanismo de contención. Las conexiones en tiempo real como UGS, rtPS y ertPS se les asignan una o más ranuras de tiempo en el canal de UL por la BS para fines de solicitud de ancho de banda y por lo tanto no utilizan el mecanismo de contención. En consecuencia, el protocolo IEEE 802.16 garantiza más calidad de servicio para el tráfico de datos en tiempo real, ya que sus peticiones de ancho de banda no entran en la fase de contención razón por la cual no chocan posteriormente con otras peticiones de ancho de banda.

WiMAX tiene una capa MAC centralizada. Todas las peticiones de ancho de banda para las aplicaciones en el uplink (UL), tienen que ser planificadas y asignadas por la estación base (BS) en la interfaz aérea. Por lo tanto, la planificación en UL sobre la interfaz aérea juega un papel importante para satisfacer las limitaciones de QoS de extremo a extremo de aplicaciones heterogéneas en redes WiMAX.

Al entrar en la red y después de pasar las fases de autorización y registro, la SS envía sus requisitos de ancho de banda y los parámetros de QoS para cada conexión a la BS, con mensajes específicos de control. Si la BS cree que puede soportar la petición de la SS en términos de reserva de ancho de banda y calidad de servicio, la conexión se admite, de lo contrario se rechaza o entra en una etapa de retroceso (backoff) para que lo reintente. Cuatro son los métodos utilizados para la asignación de ancho de banda a un flujo de servicio: unsolicited bandwidth grants, piggyback grant request, contention based y unicast polling [NUA07]. Estos mecanismos de asignación de ancho de banda definidos permiten a los fabricantes optimizar el rendimiento del sistema mediante el uso de diferentes combinaciones de estas técnicas, mientras que se mantiene la interoperabilidad. La Tabla 7 resume las opciones disponibles de petición/concesión para cada uno de los servicios de planificación.

Servicio de Planificación	Piggyback grant request	Bandwitdth Stealing	Unicast Polling	Contention-based Polling
UGS	No permitida	No permitida	Puede ser usado Bit PM (Poll-me)	No permitida
ertPS	Extended piggyback	Permitida	Permitida	Permitida
rtPS	Permitida	Permitida	Permitida	Permitida
nrtPS	Permitida	Permitida	Permitida	Permitida
BE	Permitida	Permitida	Permitida	Permitida

Tabla 7. Opciones de petición/concesión para cada uno de los servicios de planificación definidos en WiMAX.

Una SS puede enviar una petición de ancho de banda total o incremental. Cuando la BS recibe una petición global, esta sustituye su percepción de las necesidades de ancho de banda de la conexión con de la cantidad de ancho de banda requerido. Si recibe una solicitud de ancho de banda incremental, entonces añade la cantidad de ancho de banda requerido a su percepción actual de las necesidades de ancho de banda de la conexión.

WiMAX también aporta mecanismos para que las aplicaciones negocien la QoS requerida para la aplicación en cuestión. Para lograr esto el WiMAX forum ha desarrollado el concepto de USI (Universal Services Interface), el cual es un API que expone el operador WiMAX, donde la gran mayoría de aplicaciones Web como YouTube, Skype, etc., pueden usar esta interfaz para solicitar la QoS requerida para sus servicios de la red WiMAX.

En la Figura 19, se muestra la arquitectura básica QoS de WiMAX descrita hasta ahora. En esta figura se muestra la conexión UL típica entre SS y BS, en ella la SS pide una concesión de ancho de banda para la transmisión en el UL. El planificador está en la BS.

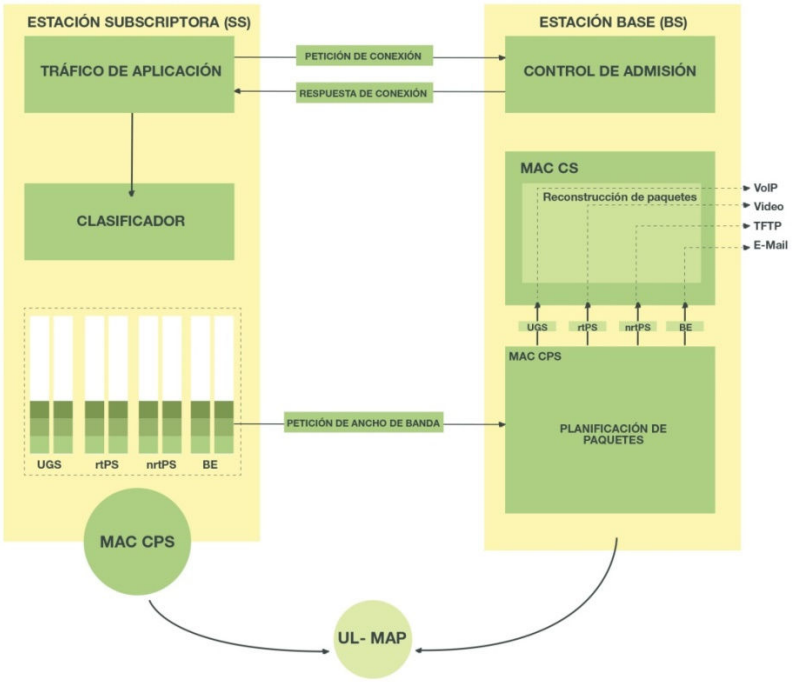

Figura 19. Arquitectura básica QoS WiMAX

3.3.2.1 Funcionamiento de QoS de extremo a extremo en redes WiMAX

Como vimos en la sección anterior para conseguir QoS de extremo a extremo, WiMAX cuenta con un framework de QoS que le aporta una serie de mecanismos y funciones tanto a nivel físico como a nivel MAC. A nivel físico, cuenta con funciones como: adaptación del enlace, HARQ, planificación dependiente del canal, retroalimentación de la calidad del canal, control de potencia y adaptación de potencia que están diseñadas para contribuir a proporcionar la QoS requerida.

En la capa MAC tanto de WiMAX fijo como de WiMAX móvil, la QoS se presta a través de service flows (SF). Esto es, un flujo de paquetes unidireccional que se le asigna un conjunto particular de parámetros de QoS. Un SF provee transporte unidireccional de paquetes ya sea en el uplink o el downlink. El SF está caracterizado por una serie de parámetros como el service flow identifier (SFID), nombre de clase de servicio (UGS, rtPS, ertPS, nrtPS o BE) y parámetros de QoS (tales como tasa de trafico máxima sostenida, tasa de trafico mínima reservada y latencia máxima).

En la Figura 20, se muestra el modelo de red WiMAX que proporciona QoS de extremo a extremo, para mayor detalle sobre los elementos de la arquitectura consulte la sección 3.2.2.4.2 del capítulo 3 de la presente tesis. En la figura los elementos claves son el MS, el ASN y el NSP (Network Service Provider) local y remoto. El NSP es equivalente al núcleo de la red. El NSP remoto (V-NSP) es equivalente al NSP local cuando el MS no está en roaming. El ASN es equivalente a la red de acceso radio (RAN). El ASN está compuesto por la BS y ASN-GW.

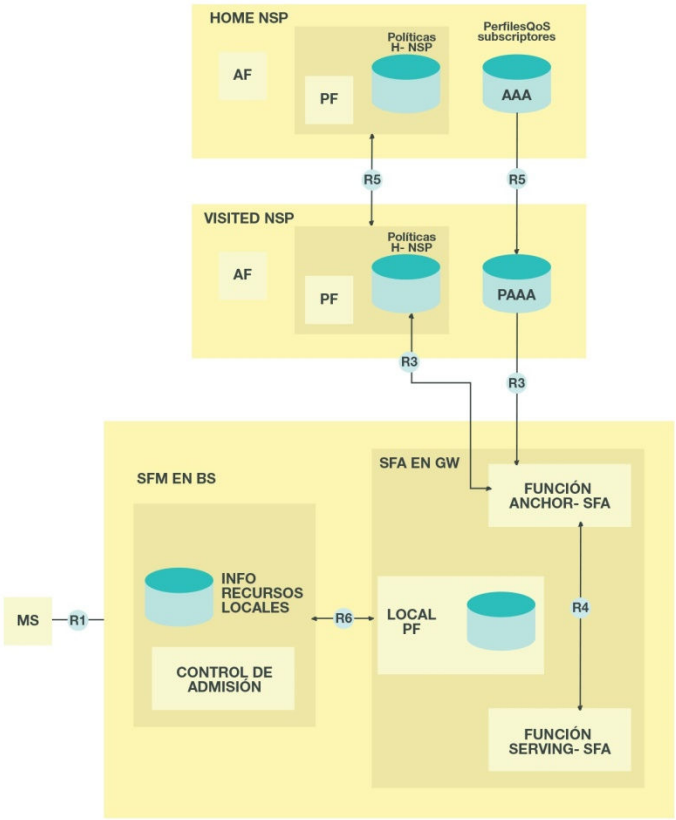

Figura 20. Arquitectura QoS WiMAX extremo a extremo

La BS en el ASN incorpora una función de QoS llamada SFM (Service Flow Management). El SFM es una entidad lógica responsable de la creación, admisión, activación, modificación y borrado de SF 802.16. Esta consta de una función de control de admisión (AC) y la información local de recursos asociada. El AC se usa para decidir si un nuevo SF puede ser admitido basado en el uso de los recursos locales.

El ASN-GW en el ASN implementa una función QoS llamada SFA (Service Flow Authorization). En el caso que el perfil QoS del usuario se descargue de un servidor AAA a la SFA en la fase de entrada a la red, la SFA es responsable de evaluar cualquier petición de servicio contra el perfil QoS del usuario. También se pueden suministrar SF a través de un NMS (Network Management System).

En función de la configuración, la información suministrada puede incluir parámetros adicionales tales como prioridad del usuario, la cuales se utilizan para reforzar prioridades relativas entre usuarios. Por ejemplo, la prioridad del usuario se puede tener en cuenta en situaciones donde las peticiones de SF entre todos los usuarios exceden la capacidad de los recursos radio y por tanto un subconjunto de estos debe ser rechazado.

3.3.2.2 Avances en mecanismos de QoS en redes WiMAX

La investigación sobre este tema no está cerrada y hay muchos estudios de análisis y simulaciones acerca del soporte de QoS sobre redes WiMAX, cabe destacar los estudios realizados en [Cha09] sobre mecanismos de planificación sobre redes Mobile WiMAX, en [Fi108] se introduce un algoritmo "rápido y eficiente de transmisión adaptativo de QoS para redes Mobile WiMAX, el estudio presentado en [Tal08] hace un análisis exhaustivo de QoS en redes WiMAX y [Nev08] aporta estudios de simulación de diferenciación de QoS en redes WiMAX.

De igual manera se están desarrollando mecanismos avanzados de QoS para la nueva generación de WiMAX 802.16m [IEEE802.16m]. Un ejemplo de tales mecanismos es el aGPS (adaptative Granting and Polling), el cual ajusta los intervalos de polling y concesión en función del tráfico, de tal manera que se optimice la sobrecarga que genera el proceso de polling. Otro ejemplo es el mecanismo Group Scheduling que se utiliza para usuarios de VoIP. Además, la nueva generación soporta de manera eficiente los procesos de beam forming, modo MIMO y mitigación de las interferencias. Estas características contribuyen a la capacidad y calidad de VoIP.

Otro aspecto de QoS que está siendo mejorado en 802.16m es el diseño de un canal de contención ultra rápido con mínima latencia, de tal manera que el usuario final pueda pedir ancho de banda de forma incremental a medida que su aplicación lo necesite. A nivel global, la próxima generación de WiMAX promete una serie de innovaciones que ayudaran a que el usuario final tenga servicios interactivos de tiempo real con excelente calidad de servicio.

3.4 Enrutamiento en redes de datos inalámbricas para entornos tácticos

Las redes inalámbricas en entornos tácticos constan de un conjunto de nodos móviles (hosts) que están conectados por enlaces inalámbricos. La topología de red en tales entornos puede variar constantemente de manera aleatoria. Los protocolos de enrutamiento que se utilizan en redes cableadas no pueden ser usados de forma directa en este tipo de redes inalámbricas debido a la naturaleza altamente dinámica de la topología, el ancho de banda restringido de los enlaces inalámbricos y la ausencia de una infraestructura centralizada de administración. A lo largo de estos años, se han propuesto una serie de protocolos enrutamiento para este tipo de redes inalámbricas. En esta sección se realiza un análisis de los retos que conlleva el diseño de protocolos de enrutamiento para este tipo de redes, luego se presenta una clasificación y una breve discusión del funcionamiento de los distintos protocolos de enrutamiento.

3.4.1 Retos de diseño

Los mayores retos que tiene que superar un protocolo de enrutamiento diseñado para una red inalámbrica de uso táctico son la movilidad de los nodos, un canal propenso a errores, limitación de recursos y problemas por terminales ocultos.

La topología de red en una red inalámbrica de uso táctico cambia constantemente debido a la movilidad de los nodos, por lo tanto una sesión de datos sufre cortes frecuentes a lo largo del camino. La interrupción ocurre ya sea debido al movimiento de los nodos intermedios en el camino o debido al movimiento de los nodos finales. Tales situaciones no suceden en los enlaces fiables de las redes cableadas donde todos los nodos son estáticos. Aunque pueden producirse cortes en el camino, los protocolos de redes cableadas acaban encontrando una ruta por la cual dirigir el tráfico y la tasa de error debido a falta de rutas es muy pequeña. Sin embargo, los protocolos de enrutamiento de redes inalámbricas en entonos tácticos deben gestionar de manera eficiente y efectiva la movilidad de los nodos.

Las redes cableadas tienen abundante ancho de banda sobre todo si utilizan fibra óptica combinada con tecnología WDM (Wavelength Division Multiplexing). Pero en una red inalámbrica, el ancho de banda a nivel radio es limitado, por lo tanto, la velocidad de datos que ofrecen es mucho menor que la ofrece una red cableada. Esto obliga a que los protocolos de enrutamiento usen el ancho de banda de forma óptima manteniendo el overhead lo más bajo posible. La disponibilidad limitada de ancho de banda también impone restricciones en la forma en que los protocolos de enrutamiento mantienen la información topológica. Debido a los cambios frecuentes de topología, mantener una información topológica consistente en todos los nodos implica más transacciones de control las cuales se traducen en mayor uso de ancho de banda. Como los protocolos de enrutamiento eficientes de las redes cableadas requieren una completa información topológica en todo momento, no son adecuados para el enrutamiento en redes inalámbricas de uso táctico.

La naturaleza Broadcast del canal radio plantea un reto importante en la redes inalámbricas de uso táctico. Los enlaces inalámbricos poseen características variables en el tiempo en términos de capacidad del enlace y probabilidad de errores en el enlace. Esto obliga a los protocolos de enrutamiento de redes inalámbricas tácticas a interactuar con la capa MAC para encontrar rutas alternativas a través de enlaces de mejor calidad. Esto se atribuye a problemas con terminales ocultos [Fu197]. Por lo tanto, es necesario que los protocolos de enrutamiento en redes inalámbricas de uso táctico encuentren rutas alternativas con menor grado de congestión.

Otra restricción que ha tenerse en cuenta, es la capacidad de procesamiento de los nodos en la redes inalámbricas de uso táctico. Los dispositivos usados en este tipo de redes tienen requisitos estrictos de portabilidad y por lo tanto tienen restricciones de dimensiones y peso, así como restricciones sobre la alimentación y condiciones climáticas adversas. Incrementar la capacidad de procesamiento puede implicar el uso de equipos más pesados y menos portables.

Debido a los problemas discutidos hasta el momento en las redes inalámbricas en entornos tácticos, los protocolos de enrutamiento de las redes cableadas no pueden ser usados, son necesarios protocolos de enrutamiento especializados que solucionen los retos anteriormente descritos. Un protocolo de enrutamiento para una red inalámbrica de uso táctico debe tener las siguientes características:

- Debe ser totalmente distribuido, dado que el enrutamiento centralizado implica un elevado tráfico de control y por lo tanto no es escalable. El enrutamiento distribuido es más tolerante a fallos que el enrutamiento centralizado, el cual involucra el riesgo de un solo punto de fallo.
- Debe adaptarse a los frecuentes cambios de topología causados por la movilidad de los nodos.
- El cálculo y mantenimiento de las rutas debe implicar a un número pequeño de nodos. Cada nodo en la red debe tener un acceso rápido a las rutas, esto es, un tiempo de establecimiento de conexión mínimo.
- Debe estar libre de bucles y libre de rutas erróneas.

- El número de colisiones de paquetes debe mantenerse en un mínimo limitando el número de broadcasts realizados por cada nodo. Las transmisiones deben ser fiables para reducir la perdida de mensajes y prevenir la ocurrencia de rutas erróneas.
- Deben converger a rutas optimas una vez la topología de red sea estable. La convergencia debe ser lo más rápida posible.
- Debe utilizar de manera óptima recursos limitados tales como ancho de banda, memoria y capacidad de procesamiento.
- Cada nodo en la red debe intentar almacenar información solamente sobre la topología local estable. Los cambios que ocurran en partes de la topología de red con las cuales el nodo no tiene ninguna correspondencia de tráfico, no deben afectar de ninguna manera al nodo, es decir, cambios en partes remotas de la red no deben producir actualizaciones en la topología de la información mantenida por el nodo.
- Debe aportar un cierto nivel de calidad del servicios (QoS) requerida por las aplicaciones y también debe ofrecer soporte a tráfico con restricciones temporales (voz y video)

3.4.2 Clasificación de protocolos de enrutamiento

Los protocolos de enrutamiento para redes inalámbricas en entornos tácticos pueden ser clasificados en diferentes tipos basados en diferentes criterios. Alguna de las clasificaciones, sus propiedades y las bases de la clasificación se tratan en esta sección. La clasificación no es mutuamente excluyente y algunos protocolos caen en más de una clase. Los protocolos de enrutamiento para redes inalámbricas en entornos tácticos pueden ser clasificados en cuatro categorías, basados en:

- Mecanismos de actualización de la información de enrutamiento
- Uso de información temporal para enrutamiento
- Topología de enrutamiento
- Utilización de recursos específicos

En la categoría de clasificación basada en el mecanismo de actualización de la información de enrutamiento pueden ser clasificados a su vez en tres sub-categorías, estas son:

- *Protocolos de enrutamiento proactivos:* En este tipo de protocolos de enrutamiento, cada nodo mantiene la información de la topología de red en forma de tablas de enrutamiento intercambiando periódicamente información de enrutamiento. La información de enrutamiento se inunda en toda la red, cuando un nodo necesita una ruta a un destino, ejecuta el algoritmo de localización de rutas sobre la información de topología que mantiene.

  Los protocolos de enrutamiento DSDV (Destination Sequenced Distance-Vector) [Per94], WRP [Mur96] (Wireless Routing Protocol), OLSR (optimized link state routing) [Cla01], CGSR (Cluster-head Gateway Switch Routing protocol) [Chi97] y STAR (Source-Tree Adaptative) [Gar99], son algunos ejemplos de protocolos que pertenecen a esta categoría.

- *Protocolos de enrutamiento reactivos o bajo demanda:* los protocolos que caen en esta categoría no mantienen la información de la topología de red. Obtienen la ruta necesaria cuando es requerido, usando un proceso de establecimiento de la conexión. Por lo tanto, estos protocolos no intercambian información de enrutamiento periódicamente.

  Ejemplos de protocolos que pertenecen a esta categoría son el protocolo de enrutamiento DSR (Dynamic Source Routing protocol) [Joh96], en el cual el nodo fuente inunda la red con paquetes RouteRequest cuando la ruta no está disponible para el destino deseado. Se pueden obtener múltiples rutas a diferentes destinos a partir de un solo RouteRequest.

AODV (Ad hoc on-demand distance vector) [Per91], este utiliza números de secuencia de destino para identificar la ruta más reciente. TORA (Temporally ordered routing algoritm) [Par97], es protocolo de enrutamiento bajo demanda iniciado por la fuente que utiliza un algoritmo de inversión de enlace (link reversal) y proporciona múltiples rutas sin bucles a un nodo destino. LAR (Location-aided routing protocol) [Ko98], utiliza la información de localización del nodo para mejorar la eficiencia del enrutamiento reduciendo el tráfico de control, LAR asume la disponibilidad de GPS para su funcionamiento. El protocolo ABR (Associativity-based routing) [Toh97], el cual selecciona las rutas basado en la estabilidad del enlace inalámbrico.

- *Protocolos de enrutamiento híbridos:* Los protocolos que pertenecen a esta categoría combinan las mejores características de las dos categorías anteriores. Los nodos dentro de una cierta distancia del nodo en cuestión, o dentro de una región geográfica en particular, se dice que están dentro de la zona de enrutamiento de un nodo dado. Para enrutar dentro de esta zona, se utiliza un protocolo reactivo. Para los nodos que están localizados más allá de esta zona, se usa utiliza un protocolo bajo demanda.

  El protocolo ZRP (Zone routing protocol) [Haa97], El concepto clave empleado en este protocolo consiste en utilizar un sistema proactivo de enrutamiento dentro de una zona limitada a r-saltos de todos los nodos, y el uso de un sistema de enrutamiento reactivo para los nodos fuera de esta zona. El protocolo de enrutamiento intrazona (IARP: intra-zone routing protocol) se utiliza en la zona donde un nodo en particular emplea enrutamiento proactivo. El protocolo de enrutamiento reactivo utilizado más allá de esta zona se conoce como protocolo de enrutamiento inter-zona (IERP: inter-zone routing protocol). La zona de enrutamiento de un nodo dado es un subconjunto de la red, dentro de la cual todos los nodos son alcanzables a menos de o al radio de la zona de saltos.

  Otro ejemplo es el protocolo de enrutamiento ZHLS (Zone-based hierarchical link state) [Joa99], es un protocolo de enrutamiento hibrido jerárquico que utiliza la información de la ubicación geográfica de los nodos para formar zonas que no se superpongan. Se emplea un direccionamiento jerárquico que está formado por un identificador de zona y otro de nodo. Cada nodo requiere la información de ubicación, a partir de la cual puede obtener su identificación de zona. La información sobre la topología dentro de una zona se mantiene en todos los nodos dentro de esta, y para las regiones fuera de la zona, sólo se mantiene la información de conectividad de la zona. .

En la categoría de clasificación basada en el uso de información temporal para el enrutamiento, los protocolos de enrutamiento tienen en cuenta el uso de información temporal con respecto el tiempo de vida de los enlaces inalámbricos y el tiempo de vida de las rutas seleccionadas. En este caso los protocoles se dividen en dos sub-categorías, estas son:

- *Protocolos de enrutamiento que utilizan información temporal pasada:* estos protocolos de enrutamiento utilizan información acerca del estado pasado de los enlaces o del estado de los enlaces en el momento del enrutamiento para tomar decisiones de enrutamiento. Por ejemplo, una métrica de enrutamiento basada en la disponibilidad del enlace inalámbrico (la cual aquí seria la información actual/presente) junto a algoritmo del camino más corto, aporta una ruta que puede ser eficiente y estable en el momento de la búsqueda de la ruta. Los cambios topológicos pueden romper inmediatamente el enlace, haciendo que la ruta pase por un proceso de reconfiguración costoso en términos de recursos.

  Ejemplos de este tipo de protocolos son. DSDV (Destination Sequenced DistanceVector), STAR (Source-Tree Adaptative), WRP (Wireless Routing Protocol), DSR (Dynamic source routing protocol) y AODV (Ad hoc on-demand distance vector).

- *Protocolos de enrutamiento que utilizan información temporal futura:* los protocolos que pertenecen a esta categoría utilizan información acerca del estado futuro esperado de los enlaces inalámbricos para hacer decisiones de enrutamiento. Aparte del tiempo de vida de los enlaces inalámbricos, la información de estado futuro también incluye información respecto al tiempo de vida del nodo (la cual está basada en el nivel de batería restante y la tasa de descarga de la batería), predicción de la localización y predicción de la disponibilidad del enlace.

  Ejemplos de este tipo de protocolos son: RABR (Route-Lifetime Assessment-Based Routing) [Aga00] y LBR (Link Life-Based Routing Protocol). [Man01].

Las redes inalámbricas en entornos tácticos, debido a la cantidad relativamente pequeña del número de nodos, pueden utilizar ya sea una topología plana o una topología jerárquica para el enrutamiento. Basados en la topología de enrutamiento nos encontramos los siguientes tipos de protocolos:

- Protocolos de enrutamiento de topología plana: los protocolos que caen en esta categoría hacen uso de un esquema de direccionamiento plano similar al usado en redes LAN IEEE 802.3. Asumen la presencia de mecanismos de direccionamiento únicos globalmente (o al menos únicos a la parte conectada a la red) para los nodos en la red inalámbrica. Ejemplo de este tipo de protocolo son: DSR (Dynamic source routing protocol), SSA (Signal Stability-based Adaptative) y AODV (Ad hoc on-demand distance vector).
- Protocolos de enrutamiento de topología jerárquica: los protocolos que pertenecen a esta categoría hacen uso de una jerarquía lógica en la red y un esquema de direccionamiento asociado. La jerarquía puede estar basada en información geográfica o puede estar basada en el número de saltos.

  El protocolo de enrutamiento HSR (Hierarchical State Routing) [Iwa99], es un protocolo de enrutamiento jerárquico distribuido multinivel que utiliza clustering a distintos niveles con la administración eficiente de miembros en cada nivel de clustering. El uso de clustering mejora la asignación de recursos y la gestión. HSR opera mediante la clasificación de los diferentes niveles de clustering. Los dirigentes electos en cada nivel de conforman los miembros del nivel inmediatamente superior. Diferentes algoritmos de clustering, tales como el propuesto en [Chi97], se emplean para la elección de dirigentes en todos los niveles.

  El protocolo FSR (Fisheye State Routing) [Iwa99] es una generalización del protocolo GSR (Global State Routing) [Ger98]. FSR utiliza la técnica fisheye para reducir la información requerida para representar datos, aplicada a la reducción de tráfico de enrutamiento. El principio básico detrás de esta técnica es la característica de los ojos de un pez que puede capturar información de los píxeles con mayor precisión cerca del punto focal de su ojo. Esta precisión se reduce con un aumento de la distancia desde el centro del punto focal. Esta propiedad se trastada al enrutamiento en redes inalámbricas mediante un nodo que mantiene información precisa sobre los nodos de la topología local e información no muy precisa acerca de nodos lejanos, la exactitud de la información de la red disminuye al aumentar la distancia.

Finalmente en la categoría de protocolos de enrutamientos basados en la utilización de recursos específicos tenemos:

Enrutamiento asistido por información geográfica: los protocolos que pertenecen a esta categoría incrementan su rendimiento y reducen la sobrecarga de tráfico control mediante

la utilización efectiva de la información geográfica disponible. El protocolo LAR (Location-Aided Routing) es un ejemplo de este tipo.

Enrutamiento basado en consumo de potencia: esta categoría de protocolos de enrutamiento basan sus decisiones de enrutamiento en la reducción del consumo de potencia ya sea de forma local o global en la red. Por ejemplo el protocolo PAR (Power-Aware Routing) [Sin98].

3.4.3 Enrutamiento multicast

Las redes inalámbricas en entornos tácticos tiene aplicación en operaciones civiles (computación colaborativa y distribuida), operaciones de búsqueda y rescate, operaciones de refuerzo de la ley y situaciones de guerra donde establecer y mantener una infraestructura de comunicaciones puede ser difícil o muy costoso. En todas estas aplicaciones, la coordinación y comunicación entre un numero dado de nodos son necesarias. Los protocolos de enrutamiento inalámbricos juegan un papel importante en redes inalámbricas en entornas tácticos dado que siempre es más ventajoso usar multicast que múltiples enlaces unicast, especialmente en la transmisión de video y audio sobre este tipo de redes donde el ancho de banda es muy escaso.

Los protocolos de enrutamiento IP multicast de la redes cableadas tales como DVMRP [Wai98], MOSPF [Moy94], CBT [Ba193] y PIM [Dee96], no funcionan bien en redes inalámbricas de entornos tácticos debido a la naturaleza dinámica de la topología de red. El cambio dinámico de topología sumado a enlaces inalámbricos de bajo ancho de banda y poco fiables, causan tiempo de convergencia largos y pueden llevar a la formación de bucles de enrutamiento transitorios que consumen rápidamente el ancho de banda limitado disponible.

En una red cableada, el enfoque básico adoptado para hacer multicast consiste en establecer un árbol de enrutamiento para un grupo de nodos que constituyen una sesión multicast. Una vez establecido el árbol de enrutamiento, un paquete enviado a todos los nodos del árbol, atraviesa a cada nodo y a cada enlace en el árbol una sola vez. Tal estructura multicast no es apropiada para la redes inalámbricas en entornos tácticos por que debido a la elevada movilidad el árbol, se puede romper fácilmente.

Esta sección discute el problema del enrutamiento multicast (el problema de determinar cuáles nodos en la red deben participar en la recepción de paquetes de datos multicast, es decir, transmitidos de una fuente a un conjunto seleccionado de receptores) y presenta varios protocolos de enrutamiento multicast para redes inalámbricas en entornos tácticos.

3.4.3.1 Retos de diseño en protocolos de enrutamiento multicast

La disponibilidad limitada del ancho de banda, un canal broadcast propenso a errores, la movilidad de los nodos, el problema de terminales ocultos y la seguridad limitada hacen del diseño de protocolos de enrutamiento multicast para redes inalámbricas de uso táctico una tarea complicada. Debido a la movilidad de los nodos, los fallos en el enlace son muy comunes, en este tipo de redes. De tal manera, que los paquetes de datos enviados por la fuente pueden ser descartados, lo cual resulta en una tasa de entrega de paquetes muy baja. Por lo tanto, un protocolo de enrutamiento multicast debe ser lo suficientemente robusto para soporta la movilidad de los nodos y lograr una tasa de entrega de paquetes alta.

En un entorno de red táctica, donde el ancho de banda es limitado, la eficiencia del protocolo multicast es muy importante. La eficiencia multicast está definida como la relación del número total

de paquetes de datos recibidos por los receptores sobre el número total de paquetes (datos y control) transmitidos en la red.

Para poder hacer un seguimiento de los miembros de un grupo multicast, se requiere el intercambio de paquetes de control. Este consume una cantidad considerable de ancho de banda. Por lo tanto, el diseño de protocolos multicast para este tipo de redes debe asegurar que el número total de paquetes de control transmitidos para mantener el grupo multicast se mantenga en mínimos.

Una de las aplicaciones importantes de las redes tácticas es su uso en aplicaciones estratégicas/militares. Por lo tanto, aportar calidad de servicio (QoS) es un aspecto importante de los protocolo de enrutamiento multicast aplicados a este tipo de redes. Los parámetros principales que se tienen en cuenta son el throughput, retardo, duración del retardo y fiabilidad.

Si un protocolo de enrutamiento multicast necesita dar soporte a un protocolo de enrutamiento en particular, entonces será difícil que el protocolo multicast funcione en una red heterogénea. Por lo tanto, es deseable que el protocolo de enrutamiento multicast sea independiente de cualquier protocolo de enrutamiento unicast.

3.4.3.2 Clasificación de protocolos de enrutamiento multicast

Los protocolos de enrutamiento multicast para redes inalámbricas en el ámbito táctico pueden ser clasificados en dos tipos: protocolos multicast genéricos/independientes de la aplicación y protocolos multicast dependientes de la aplicación. Mientras que los protocolos multicast genéricos son usados para hacer multicast convencional, los protocolos multicast dependientes de la aplicación están enfocados a las aplicaciones específicas para las cuales han sido diseñados. Los protocolos independientes de la aplicación pueden ser subclasificados en tres dimensiones diferentes.

Basados en la topología: los enfoques actuales usados por protocolos de enrutamiento multicast en redes inalámbricas pueden ser clasificados en dos tipos basado en la topología multicast: basado en árboles y basados en malla. En los protocolos de enrutamiento basados en árboles, solamente existe un ruta entre el par fuente-receptor, en tanto que en los protocolos de enrutamiento multicast basados en malla, puede haber más de una ruta entre el par fuente-receptor. Los protocolos multicast basados en árboles son más eficientes comparado a los protocolos multicast basados en malla, pero los protocolos multicast basados en malla son robustos debido a la disponibilidad de múltiples caminos entre fuente y destino.

Los protocolos multicast basados en árboles pueden ser divididos en dos tipos: los protocolos multicast cuya raíz del árbol está en la fuente de los datos y los protocolos multicast de árbol compartido, en este tipo de protocolos un solo árbol se comparte entre todas las fuentes dentro del grupo multicast y su raíz la tiene en el nodo llamado el nodo núcleo. Los protocolos multicast cuya fuente es la raíz del árbol funcionan mejor que los protocolos con un árbol compartido cuando son sometidos a una carga excesiva de tráfico, esto se debe a la distribución eficiente del tráfico, pero los últimos son más escalables. El problema principal de los protocolos multicast basados en árboles compartidos es que dependen mucho del nodo núcleo, por lo tanto, un solo fallo en este nodo afecta el funcionamiento del protocolo multicast.

Los protocolos de enrutamiento BEMRP (Bandwidth efficient multicast routing protocol) [Oza99], MZRP (Multicast Zone Routing Protocol) [Dev01], ABAM (Associativity-Based ad hoc Multicast routing) [Toh00], DDM (Differential Destination Multicast) [Ji00], WBM (Weight-Based Multicast) [Das00], MAODV (Multicast Ad hoc On-demand Distance Vector) [Roy99], [Roy00], AMRIS (Ad hoc Multicast Routing protocol utilizing Increasing id-numberS) [Wu98] y AMRoute (Ad hoc Multicast Routing protocol) [Born98] son algunos ejemplos de los protocolos que pertenecen a esta categoría.

Como ejemplo de protocolos de enrutamiento multicast basados en malla tenemos: ODMRP (On-Demand Multicast Routing Protocol) [Lee99], DCMP (Dynamic Core¬based Multicast routing Protocol) [Das02], FGMP-RA (Forwarding Group Multicast Protocol - Receiver Advertising) [Chi98], NSMP (Neighbor Supporting ad hoc Multicast routing Protocol) [Lee00] y CAMP (Core-Assisted Mesh Protocol) [Gar99].

Basados en la inicialización de la sesión multicast: la formación del grupo multicast puede ser iniciada tanto por la fuente como por los destinatarios de los datos. En un protocolo multicast, si la formación del grupo solamente la inicia el nodo fuente, entonces se denomina protocolo de enrutamiento multicast iniciado por la fuente y si es iniciado por los receptores entonces es llamado protocolo de enrutamiento multicast iniciado por los clientes. Algunos protocolos multicast no distinguen entre fuente y destino para la inicialización del grupo multicast, llamamos a estos protocolos de enrutamiento multicast iniciados por la fuente o por destino.

Basado en el mecanismo de mantenimiento de la topología: el mantenimiento de la topología multicast puede hacerse a través de una aproximación soft-state o de una hard-state. En la aproximación soft-state, los paquetes de control se inundan periódicamente para refrescar la ruta, lo cual lleva a una alta tasa de entrega de paquetes a costas de una elevada carga de trafico de control, sin embargo en la aproximación de hard-state, los paquetes de control son transmitidos (para mantener rutas) solo cuando se cae un enlace, lo que resulta en una sobrecarga de trafico de control más baja a expensas de una baja tasa de entrega de paquetes.

Tal como se mencionó anteriormente, hay algunos protocolos de enrutamiento multicast que se adaptan a las diferentes necesidades de un usuario en función del escenario de uso. Ejemplo de esto es el protocolo CBM (Content-Based Multicasting) [Zho00], el cual se utiliza en áreas en las que el conjunto de fuentes y de destinos de la información van cambiando de forma dinámica en función del contenido de la información y la movilidad de los propios receptores. Un ejemplo de este tipo de aplicación está en un campo de batalla donde los soldados en movimiento deben ser actualizados continuamente sobre las amenazas inminentes que pueden ocurrir dentro de un período determinado (por ejemplo, en los siguientes diez minutos) o que pueden estar presentes en una cierta distancia (por ejemplo, a 5 Km.) del soldado. Información sobre la presencia de sus aliados también pueden ser de utilidad para ellos.

Sensores autónomos desplegados en la zona de combate se pueden utilizar para recopilar la información requerida. Así, en el modelo CBM, se puede suponer que los nodos están interesados en obtener información sobre las amenazas y recursos que están: (i) a un tiempo t lejos de su ubicación actual y / o (ii) a una distancia d.

En la parte del sensor-push del esquema, los nodos sensores generan información y las pasan al líder del bloque en que se encuentran por medio de mensajes de alerta de amenazas. Con base en la ubicación y la velocidad de la amenaza, esta información es enviada a otros bloques por el líder del bloque. En la parte receiver-pull, si la especificación temporal es t, entonces el nodo receptor envía un PullRequest al líder del bloque en el que se espera que estén presentes después del período de tiempo t. En el caso en que el líder tenga información incompleta sobre la amenaza, genera más mensajes PullRequest a los líderes de bloque en la dirección de la amenaza, recupera la información sobre amenazas (en caso de haberla) y la envía al receptor solicitante.

Otro ejemplo de protocolos multicast dependientes de la aplicación, es el protocolo LBM (Location-Based Multicasting) o geocasting, el cual es una variante del multicast convencional que utiliza la información geográfica para hacer multicast.

Aquí, un grupo de nodos presentes en una región geográfica en particular, constituyen el grupo multicast receptor. Un nodo utiliza su GPS para obtener sus coordenadas de latitud, longitud, altitud. Geocasting tiene varias aplicaciones, como el envío de mensajes de emergencia a las personas dentro de un área pequeña, como edificios, localización de una persona que se sabe

está localizada en un área geográfica pequeña, como el suburbio de una ciudad, y el envío de publicidad destinada sólo a una región en particular. Algunos de los sistemas multicast basados en la localización se describen a continuación.

En [Ko99], se proponen dos sistemas que utilizan un enfoque inundación modificado para geocasting. Estos sistemas utilizan el concepto de regiones de reenvío. En el primer esquema, un rectángulo que abarca la fuente y el receptor de la región multicast, y cuyos lados son paralelos a los ejes X e Y, constituye la región de reenvío. Cuando un nodo, recibe un mensaje multicast, lo reenvía solamente si se encuentra dentro de la región de reenvío. De lo contrario, el mensaje se descarta.

En el segundo esquema, la región de reenvío no se forma ninguna forma definida. Cuando cualquier nodo J recibe un paquete multicast, que ha sido originado por un nodo S, de un nodo I, solo se reenvía el paquete si está a una distancia d del centro de la región multicast, del nodo I. La distancia se calcula de la siguiente manera. Antes de transmitir un paquete de datos, los nodo fuente inserta sus propias coordenadas (Xs, Ys) y las coordenadas del punto central de la región multicast (Xc, Yc) en el paquete. Un nodo de recepción, ya que conoce sus propias coordenadas mediante GPS, calcula su distancia (Xc, Yc), y también la distancia entre el nodo anterior y (Xc, Yc). Si la distancia es como máximo, d más que la distancia de su nodo anterior (nodo de origen) del centro de la región multicast, se envía el paquete, de lo contrario, se descarta el paquete. Antes del reenvío, el nodo sustituye las coordenadas del nodo anterior en el paquete con sus propias coordenadas, de modo que el próximo nodo receptor pueda calcular las dos distancias por medio de las cuales se toma la decisión sobre si debe o no reenviar el paquete un salto más.

3.5 Sistemas de gestión, operación y mantenimiento

3.5.1 Estado actual de la gestión de red

Los NMS (Network Management Systems) actuales se basan en el protocolo SNMP. La mayoría de los componentes de red y sistemas operativos comerciales llevan incorporados agentes SNMP. Sin embargo, los NMS actuales, sufren de varias limitaciones. Una de las limitaciones del sistema de gestión basado en SNMP es que los valores de los objetos gestionados se define como valores escalares. El protocolo de gestión basado en OSI, CMIP, está orientado a objetos. Sin embargo, no ha tenido éxito debido a la complejidad de las especificaciones de los objetos gestionados y la limitación de grandes cantidades de memoria en los sistemas informáticos del pasado.

Otra limitación de la gestión basada en SNMP es que es un sistema basado en consultas. En otras palabras, el NMS consulta a cada agente sobre su estado o para obtener cualquier otra información que necesita para la gestión de la red. Sólo un pequeño conjunto de operaciones las inicia un agente de administración a un NMS en forma de alarmas. Para detectar fallos rápidamente, o para obtener buenas estadísticas, el NMS debe hacer consultas más frecuentes a los agentes, lo cual genera mayor tráfico de red. Hay una solución alternativa a este problema, que consiste en desplegar monitores remotos.

Algunas de las restricciones sobre la gestión basada en SNMP han sido resueltas por los sistemas de gestión de red emergentes. La tecnología orientada a objetos ha llegado a una etapa madura y la capacidad de hardware para manejar pilas orientadas a objetos está disponible en el mercado. Por lo tanto, la gestión de redes orientada a objetos está siendo reconsiderada. Esto tiene aplicación potencial en la gestión de redes de telecomunicación. Los sistemas de gestión de red se construyen actualmente con protocolos orientados a objetos y con esquemas, como el protocolo CORBA (Common Object Request Broker Architecture) y el esquema XML (Extended Markup Language).

Una red activa, que es la dirección de las redes de nueva generación, incluirá aplicaciones integradas de gestión de red, Además del avance de la investigación y el desarrollo en la gestión de la red en cuanto a estándares, protocolos, metodología, y las nuevas tecnologías, existe una actividad considerable en las aplicaciones de gestión. De particular importancia son las tecnologías de correlación de eventos en la gestión de fallos y la securización de red y comunicaciones en la gestión de seguridad.

Existe gran cantidad de investigaciones que intentan desarrollar estándares para protocolos de gestión alternativos específicamente para redes inalámbricas en entornos tácticos tipo MANET. A pesar de estos esfuerzos, SNMP sigue siendo el protocolo de gestión de referencia. Algunas de las características de las redes inalámbricas en entornos tácticos tales como reconfiguración frecuente de la red debido a la movilidad de los nodos que a su vez cambian la topología, representan un reto para los sistemas de gestión por SNMP comerciales. Uno de los muchos retos en redes tácticas es reducir el tráfico de gestión debido al troughput limitado en los enlaces inalámbricos. Una alternativa para ello es el Adhoc Network Management Protocol (ANMP), el cual es compatible con SNMP y usa un clúster de nodos jerárquicos para reducir el número de mensajes que se intercambian entre gestor y agentes [Che99].

Otro sistema alternativo es el Yelp Announcemement Protocol (YAP) el cual permite al agente reportar periódicamente al gestor, en lugar de ser el gestor quien pregunte periódicamente [Cha04]. Otros esfuerzos que no se centran en el protocolo específico utilizado, se basan en crear un sistema descentralizado que es capaz de gestionar una relación peer-to-peer activa dentro de la red MANET [Bru04]. El hecho que no exista un estándar alternativo para redes inalámbricas en entornos tácticos, indica que aunque SNMP puede no ser ideal, es el protocolo de gestión más común; por lo tanto SNMP puede ser adaptado al entorno táctico como una forma de estandarizar como los objetos presentan la información a través del uso de una MIB [Her10].

Un NMS robusto combinado con los conceptos de NCW puede potencialmente conducir a una red adaptativa donde sea posible la integración de clústeres auto-organizados de sensores semiautónomos y vehículos no tripulados bajo el comando de un tomador de decisiones humano. En este entorno predominantemente mesh, cada nodo tiene el potencial de servir como relay de otros nodos y es capaz de formar o reparar la red basado en el SA adquirido del estado y capacidades de sus nodos vecinos, información obtenida a través del NMS.

3.5.2 Estándares de gestión de red

En la actualidad están en uso varios estándares para gestión de red. La Tabla 8 enumera cuatro estándares, junto con una quinta clase basadas en tecnologías emergentes, y sus puntos más destacados. Los primeros cuatro son el modelo OSI, el modelo de Internet, TMN, y IEEE LAN / MAN. Un tratamiento detallado de las diversas normas se puede encontrar en [Bla95].

Estándar	Beneficio
OSI/CMIP	• Norma internacional (ISO / OSI) • Gestión de redes de comunicación LAN y WAN • Se ocupa de las siete capas OSI • Más completa • Orientado a objetos • Bien estructurado y en capas • Consume grandes recursos en la ejecución
SNMP/Internet	• Estándar IETF • Originalmente pensado para el manejo de componentes de Internet, actualmente adoptado para WAN y sistemas de telecomunicaciones • Fácil de implementar

	• Mayor implementación
TMN	• Norma internacional (ITU-T) • Gestión de la red de telecomunicaciones • Basado en el framework de gestión de red OSI • Aborda aspectos administrativos y de red de la gestión
IEEE	• Estándares IEEE adoptados internacionalmente • Aborda la gestión de LAN y MAN • Adopta las normas OSI significativamente • Se ocupa de las dos primeras capas del modelo OSI
Tecnologías Emergentes	• WBEM (Web-Based Enterprise Management) • JMX (Java Management Extension) • Gestión de red basada en XML • Gestión de red basada en CORBA

Tabla 8. Estándares de gestión de red

La primera categoría en la Tabla 8, el estándar de gestión OSI (Open System Interconnection), es el estándar adoptado por la Organización Internacional de Normalización (ISO). El protocolo del estándar de gestión OSI es CMIP (Common Management Information Protocol). El protocolo de gestión de OSI tiene incorporado el servicio CMIS (Common Management Information Service), el cual especifica los servicios básicos necesarios para realizar las diversas funciones en las siete capas OSI. Las especificaciones son orientadas a objetos y por tanto los objetos administrados están basados en clases y reglas de herencia. Además de especificar los protocolos de gestión, CMIP/CMIS también define las aplicaciones de gestión de red. En el momento de su definición los mayores inconvenientes del estándar de gestión OSI eran su complejidad y que la pila CMIP era grande. Aunque en la actualidad estos aspectos no son impedimentos para la implementación de CMIP/CMIS, SNMP se ha convertido en el protocolo de mayor implementación.

El protocolo SNMP (Simple Network Management Protocol), tiene su origen en un estándar del IETF. En SNMP, los objetos administrados están definidos como objetos escalares: Estaba pensada para gestionar componentes de Internet, pero en la actualidad se usa para administrar redes WAN y sistemas de telecomunicaciones. Es fácil de implementar, lo que lo ha convertido en el sistema de gestión de red con mayor presencia en la actualidad.

La tercera categoría en la Tabla 8 es TMN, el cual está diseñado para gestionar la red de telecomunicaciones y está orientado a cumplir las necesidades de los operadores y proveedores de servicios. TMN es un estándar de la UIT (Unión Internacional de Telecomunicaciones) y se basa en las especificaciones OSI CMIP/CMIS. TMN extiende el concepto de gestión más allá de la gestión de redes y componentes de red. Sus especificaciones abordan temas de servicios y negocios (M3000).

eTOM (Enhanced Telecommunications Operations Map) es una guía para los procesos de negocio en la industria de las telecomunicaciones. Es una extensión de TMN que está siendo desarrollada por el TM Forum (TeleManagement Forum) como un componente del NGOSS (New Generation OSS) [Rei05]. La diferencia principal entre los enfoques TMN y eTOM es que el primero ha sido desarrollado a partir de las redes y equipos de red (de abajo hacia arriba), mientras que eTOM es un enfoque de arriba hacia abajo. El marco eTOM se ha incorporado en el marco de TMN como un conjunto de normas (M.3050.x).

Los estándares IEEE para redes de área local (LAN) y red de área metropolitana (MAN) las especificaciones que aparecen en la Tabla 8 se refieren únicamente a las capas OSI 1 (físico) y 2 (enlace de datos). Estas especificaciones están estructuradas de forma similar a las especificaciones del modelo OSE. Tanto OSI/CMIP como Internet/ SNMP utilizan las normas IEEE para las capas inferiores.

La última categoría de la Tabla 8 lista las tecnologías emergentes en gestión. Una de ellos se basa en el uso de tecnología Web, se usa un servidor Web para el sistema de gestión y navegadores Web en los nodos de administración de red. En la gestión basada en Web, el modelo organizacional utiliza la arquitectura servidor-Web/navegador-Web. Un ejemplo de esto es el estándar WBEM (Web-Based Enterprise Management), desarrollado por el DMTF (Desktop Management Task Force), está basado en modelo de datos CIM (Common Information Model) y utiliza para transporte CIM sobre http.

JMX (Java Management Extension) es una tecnología abierta basada en Java para la gestión. Esta define la arquitectura de gestión, las interfaces de programación de aplicaciones (API), y los de servicios de gestión, en una sola especificación. Fue desarrollado bajo la iniciativa JMAPI (Java Management API) de Sun Microsystems.

XML es un lenguaje de meta-marcado estandarizado por el W3C (Worldwide Web Consortium) para el intercambio de documentos en la Web. Los sistemas de gestión basados en XML se basan en un método de gestión de red, el cual define la información de gestión por XML y el intercambio de datos para la gestión en la forma de un documento XML, y utiliza un método estándar de procesado de documento XML para el procesamiento de datos.

Los sistemas de gestión basados en CORBA (Common Object Request Broker Architecture) son modelos cliente-servidor orientados a objetos que utilizan CORBA. Los objetos se definen utilizando el lenguaje IDL (Interface Description Language) y utilizan una arquitectura MO (Managed Objects) distribuida.

3.5.3 Sistemas de gestión basados en web

3.5.3.1 Interfaz web y gestión vía Web

La tecnología Web se puede utilizar tanto para reunir como para mostrar datos de gestión de redes. Esto se logra al tener un servidor Web incorporado en el dispositivo. El dispositivo que soporte la gestión basada en Web debe tener un servidor Web incorporado, páginas HTML con el contenido requerido, y aplicaciones de gestión. Con este enfoque, un operador con un PC y un navegador pueden conectarse a la URL del servidor Web del dispositivo y obtener páginas HTML con información de fallos, la información de rendimiento, etc. y realizar operaciones de configuración detallada. También se puede ver información gráfica de gestión.

Este enfoque adolece de varios inconvenientes. Las representaciones basadas en mapas de topología de red, las funciones de gestión de alto nivel, tales como análisis de tendencias, la correlación entre dispositivos, notificaciones, etc., no son posibles. La escalabilidad se convierte en un problema si una estación de administración tiene que conectarse a los dispositivos de forma individual, cuando miles de ellos tienen que ser configurados. Así, aunque este enfoque es una mejora a la gestión de configuración a través de SNMP, se ha llegado a la conclusión que no puede ser un reemplazo para SNMP.

Dado que SNMP es una tecnología firmemente arraigada y tiene sus ventajas en cuanto a la supervisión de fallos y rendimiento, muchas aplicaciones de gestión de red combinan la gestión vía SNMP con la administración basada en Web para obtener las ventajas de ambos enfoques. Es posible tener un sistema de gestión centralizado con una vista gráfica basada en mapas de la topología de red y utilizar la interfaz basada en Web para conectarse a los dispositivos que usando HTTP para las operaciones de configuración detalladas relacionadas con la gestión. En este enfoque, SNMP se utiliza para la monitorización de fallos y rendimiento y HTTP se utiliza para la configuración. Muchos productos NMS utilizan este enfoque cuando el dispositivo lo soporta.

3.5.4 Sistemas de gestión basados en XML

En una aplicación de gestión de red es importante contar con un modelo de gestión de la información claramente definido, protocolos para intercambio de datos, conectividad de base de datos, etc. El conjunto de herramientas XML, las especificaciones basadas en XML y las aplicaciones XML existentes sirven como bloques constructivos para implementar una amplia gama de aspectos de gestión de red.

Aparte de las ventajas que ofrece como una tecnología de gestión, XML puede tener un efecto muy beneficioso en el desarrollo de software de gestión de red, donde muchas de las operaciones de gestión se pueden modelar en un documento XML. El enfoque puede pasar gradualmente de escribir código para las aplicaciones de gestión a crear documentos XML que representen las operaciones de gestión. La Figura 21, muestra la arquitectura de gestión generalizada para el uso de XML en la gestión utilizando el kit de herramientas XML (esquemas XML o DTD (Document Type Definitions), DOM (Document Object Model) y SAX (Simple API for XML), XSL (Extensible Style Sheet Language) y XPath (XML Path XML), SOAP y WSDL).

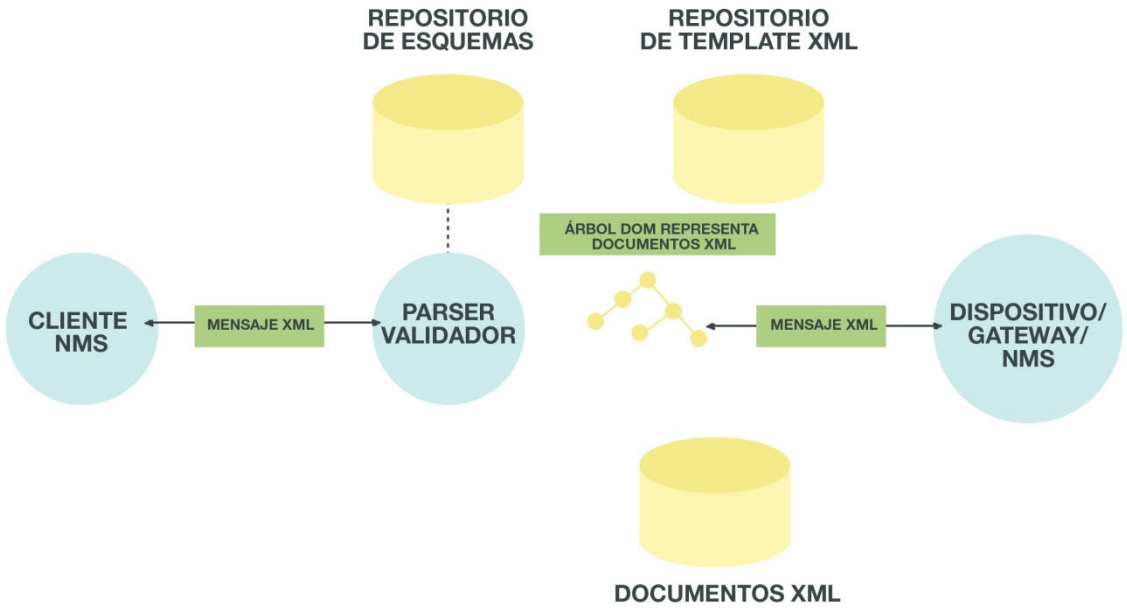

Figura 21. Arquitectura de gestión de red generalizada basada en XML

3.5.4.1 Arquitectura de sistemas gestión basados en XML

La Figura 22 muestra a tres arquitecturas posibles para la gestión basada en XML. La Figura 22(a), representa un enfoque basado puramente en XML para la gestión de red. Aquí el NMS está totalmente basado en XML y el dispositivo también es compatible con una interfaz XML para la comunicación gestor-agente. A la larga, una arquitectura totalmente basada en XML que involucra a todas las entidades en una red administrada promete los mayores beneficios. Sin embargo, hay una gran cantidad de elementos de red instalados que soporta los protocolos antiguos. Además, a partir de estudios comparativos de rendimiento llevados a cabo por diversos investigadores, SNMP, CMIP, etc., se encuentran en una clara ventaja desde el punto de vista de la eficiencia y la puntualidad. Así, en el corto y mediano plazo, las necesidades más apremiantes de las ventajas de XML surgen en el lado de los gestores, donde los operadores podrían beneficiarse del procesamiento basado en XML para la gestión de la información. Esta situación exige la integración de los nodos administrados basados en SNMP en un lado y sistemas de gestión basados en XML, al otro lado.

La arquitectura basada en Gateway de la Figura 22(b) muestra este enfoque. La aplicación de administración dispone de una interfaz basada en XML para comunicarse con los elementos de la red y se desarrolla aprovechando las ventajas de las herramientas basadas en XML. Hay un Gateway entre el NMS y el dispositivo que hace la traducción entre XML en el lado de los gestores y SNMP en el lado de los elementos de red.

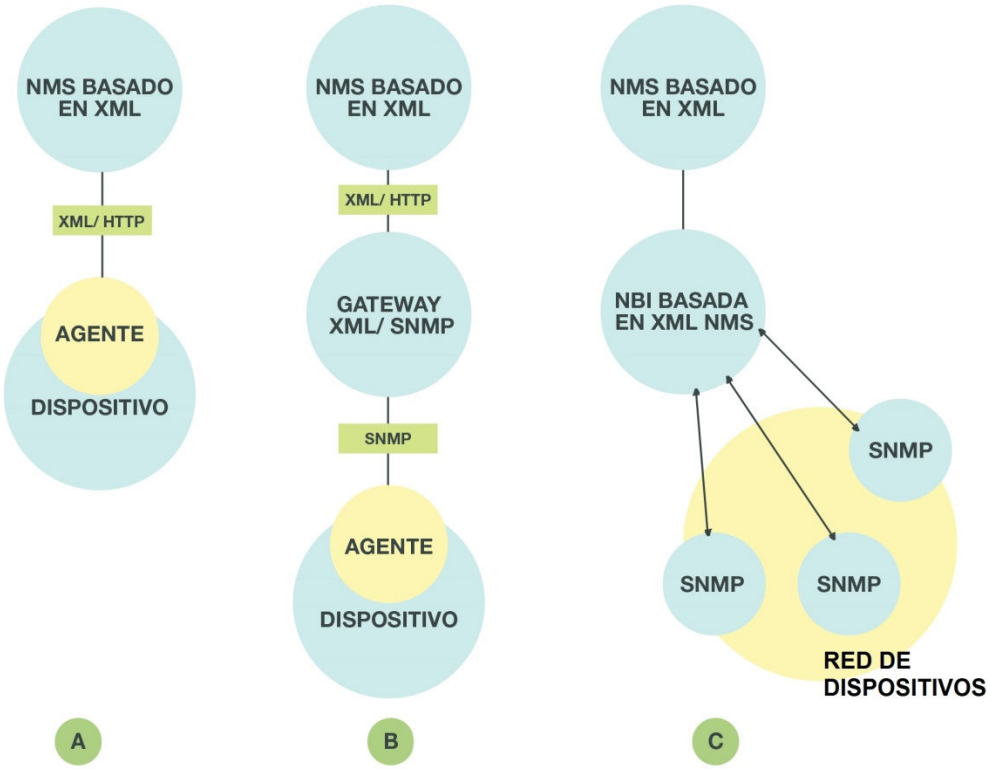

Figura 22. Tres ejemplos de arquitecturas basadas en XML

La arquitectura basada en Gateway de la Figura 22(b) muestra este enfoque. La aplicación de administración dispone de una interfaz basada en XML para comunicarse con los elementos de la red y se desarrolla aprovechando las ventajas de las herramientas basadas en XML. Hay un Gateway entre el NMS y el dispositivo que hace la traducción entre XML en el lado de los gestores y SNMP en el lado de los elementos de red.

La Figura 22(c), representa un enfoque muy interesante para la gestión basada en XML en el cual el sistema de cara a la red tiene la flexibilidad de usar cualquier protocolo para comunicarse con el elemento a gestionar. Esto tiene la ventaja de que los elementos existentes en la red no tienen por qué someterse a cambios radicales para adaptarse a una tecnología totalmente nueva. Además, permite que los protocolos de nivel inferior sean más eficientes, oportunos y tengan un impacto menor y se pueden seguir utilizando. Sin embargo, la aplicación de gestión (EMS o NMS) que se comunica con el elemento de red directamente tiene que implementar un NBI (North Bound Interface), que pueda comunicarse con el NMS. Este NBI debe estar basado en XML. Los mensajes intercambiados entre el EML y NML son semánticamente más ricos y se pueden corresponder a vanas operaciones a nivel inferior. Esto permite la implementación de mensajes SOA y XML que pueden ser intercambiados entre el EMS y el NMS.

3.5.4.2 Estado actual de los sistemas de gestión basados en XML

Se han hecho muchas investigaciones y trabajos para explorar el potencial de XML como una tecnología de gestión. Esto incluye iniciativas y consorcios de la industria, iniciativas de investigación y de organismos de estandarización que están trabajando en esta dirección.

Varios fabricantes de equipos han añadido la compatibilidad con XML a sus dispositivos. Los líderes del mercado como Juniper Networks, Cisco, 2Wire, etc., ya tienen soporte para la comunicación basada en XML. Juniper Networks fue uno de los primeros en soportar XML para las operaciones de gestión. El soporte a la gestión basada en XML se ha incorporado en el elemento de red, tal como se muestra en la figura 3-25, y los RPCs basados en »EL pueden ser intercambiados entre la aplicación de gestión y el elemento de red. Un RPC XML consiste en una petición y la respuesta correspondiente, transmitida durante una sesión orientada a la conexión usando cualquier protocolo de transporte. La información de configuración se puede descargar, modificar y volver a cargar. 2Wire ha proporcionado soporte basado en XML para la configuración de sus dispositivos DSL usando XML a través de SSL. Esto ha sido presentado en el Foro DSL. Varios modelos de dispositivos de Cisco proporcionan una interfaz basada en XML para la gestión de la configuración. Cisco ofrece la posibilidad de exportar de la información de inventario en XML.

Varios grupos de investigación han investigado cómo se puede utilizar XML para la gestión de elementos de red y algunos han puesto en marcha prototipos como prueba de concepto. Se centran en la descripción de la estructura de gestión de la información como documentos XML. En algunos casos esta estructura consiste en proporcionar una representación XML de las actuales MIB SNMP, incluidas las operaciones de mejora sobre estas. En esta sección se describen los métodos propuestos por algunos de estos grupos y algunas de las decisiones de diseño que han tomado [Ju02]; [Men04]; [Str04]; [rooD3].

3.5.4.3 Gestor basado en XML

La Figura 23 muestra una representación esquemática de la arquitectura general de un sistema de gestión basado en XML. Los componentes funcionales necesarios en una aplicación de gestión basada en XML se describen a continuación:

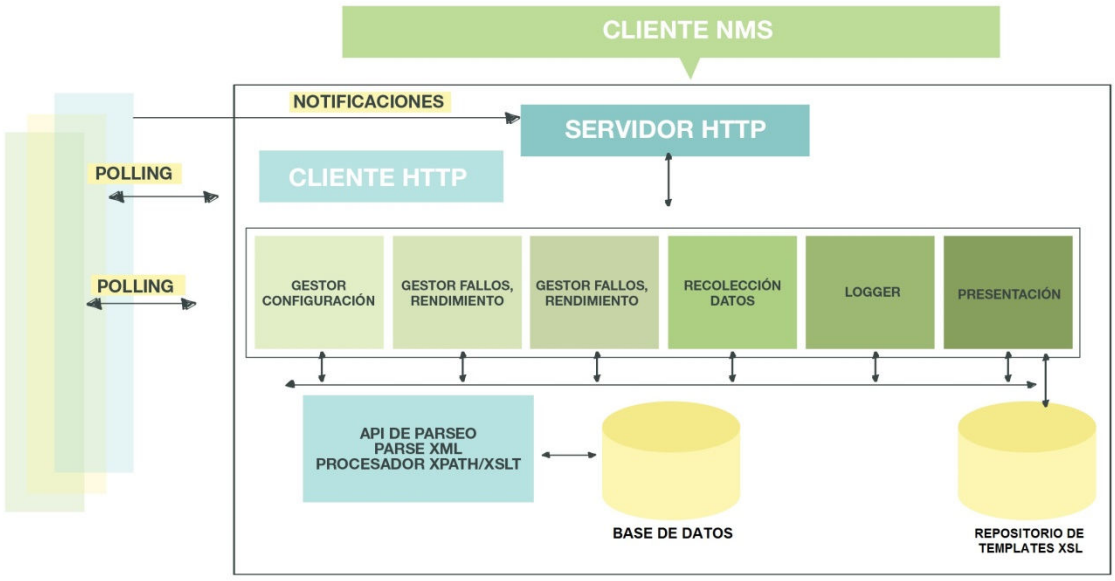

Figura 23. Arquitectura general de un sistema de gestión de red basado en XML

Componente de recopilación de datos: El diseño de este componente viene dado por el hecho de que el modelo de comunicación utilizado es XML sobre HTTP. Es posible utilizar cualquier protocolo orientado a la conexión, pero como muchos de estos dispositivos cuentan un servidor Web incorporado y el soporte directo de la gestión de red basada en HTTP/HTML, gran parte de la infraestructura necesaria para la gestión basada en Web que ya estaría presente. Para la obtención de datos de gestión basado en consultas, la aplicación NMS tiene un cliente HTTP que periódicamente envía una petición HTTP al agente del dispositivo para la gestión de la información. La respuesta recibida es bien procesada o almacenada en la base de datos. Para recibir notificaciones del dispositivo, se incluye un servidor Web en el NMS y un cliente Web en el dispositivo. El servidor Web se utiliza para recibir notificaciones XML/HTTP de los elementos de red o del dispositivo/Gateway/EMS y facilitar vistas basadas en un GUI Web de la información de gestión a los operadores.

El modelado de información de gestión se basa en XML, y las características de los dispositivos tienen que estar representados como un documento XML. El modelado de dispositivos puede seguir la MIB SNMP existente para el dispositivo (MIB-Module/Group/Table/TableEntry/RovvIndex) o ser rediseñado y hacerse más expresiva y de gran alcance. Por ejemplo, en el caso de la arquitectura se muestra en la Figura 22(c), donde el NMS basado en XML es un gestor de gestores, sería conveniente definir un esquema XML adecuado para modelar el dispositivo desde una perspectiva de más alto nivel. Tal perspectiva se traduciría en una vista "basada en la red" de la red en lugar de la habitual vista centrada en el dispositivo.

La estructura de los datos de gestión en los documentos XML puede ser descrita usando Document Type Definition (DTD) o un esquema XML. Ambos enfoques son apropiados para la mayoría de los documentos, pero el esquema XML se utiliza con más frecuencia.

Los documentos XML en una aplicación de gestión serían de dos tipos: uno perteneciente a la configuración, de la aplicación del -gestor y el otro que tiene la información de configuración/modelado del dispositivo. En caso de que la gestión de XML se construya sobre la gestión de SNMP, por ejemplo, la parte del documento de modelado del dispositivo sería una traducción de la MIB del dispositivo a XML. Varios grupos de investigación han desarrollado tales traductores.

Direccionamiento de dispositivos de red: Cuando el NMS quiere obtener información específica de un determinado dispositivo, el dispositivo se identificada por su dirección IP, el protocolo de transporte es TCP y el protocolo de capa de aplicación puede ser cualquiera: telnet, ssh, http, etc. El protocolo más utilizado es HTTP. El mensaje XML recibido de la red puede ser analizado por la aplicación de gestión utilizando una de las muchas opciones. Las tecnologías basadas en XML también proporcionan varios mecanismos para la obtención de información del MO. Las expresiones XPath o XQuery se pueden utilizar para acceder a determinadas partes del mensaje XML. Los OIDs SNMP y CMIP se tienen una buena correspondencia con las expresiones XPath.

Las operaciones de gestión también están representadas en un documento XML y una pregunta que surge aquí es cuales transacciones deben estar representadas como atributos y cuáles deben ser elementos XML. Existen ciertas reglas básicas que se utilizan cuando se debe tomar la mencionada decisión. En general, las entidades que son como objetos se representan como elementos, es decir, los casos en los que habrá varias instancias. Los 'datos que tienen un valor único serán representados como atributos. El diseño debe ser tal que el documento XML sea fácil de leer, el esquema XML para la validación es simple, y es adecuado para la búsqueda a través de una expresión XPath.

Aplicaciones funcionales de gestión: Esto incluye aplicaciones para lograr la funcionalidad FCAPS. Incluye algunas aplicaciones como el filtrado, correlación, logging, etc. Dado que la información de gestión está representada en XML, estas también deben usar algún parser como DOM o SAX. También habrá un repositorio de plantillas XSL para mostrar dinámicamente la información de gestión.

3.5.4.4 Agente basado en XML

El componente básico del agente basado en XML es un servidor Web incorporado, algunos de los componentes relacionados con el procesamiento XML (parser de XML, XPath controlador), y el motor de cliente HTTP, además de la aplicación estándar integrada que el agente necesita para acceder al valor actual de los datos solicitados y entregar las notificaciones.

Dado que los componentes que residen en el dispositivo son aplicaciones integradas y están sujetas a mayores limitaciones de recursos que los componentes de la aplicación gestor, es común escribir los parsers XML compactos en lugar de usar DOM o incluso SAX. Por ejemplo, en dispositivos de Juniper, se utiliza un parser personalizado para analizar datos. La figura 3-27 muestra la arquitectura típica de un agente.

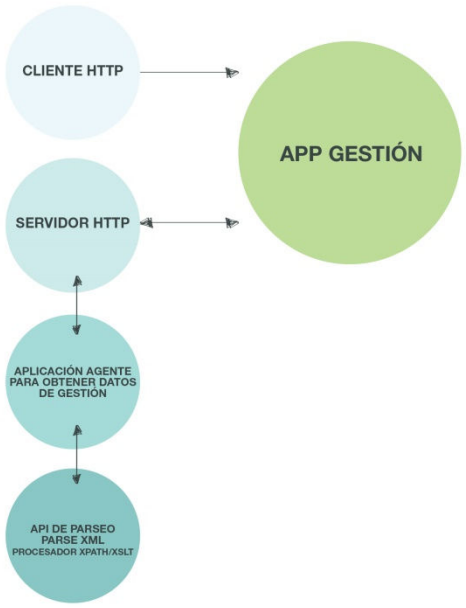

Figura 24. Arquitectura del agente basado en XML

Una transacción típica petición-respuesta entre gestor y agente incluye las siguientes operaciones:

- Se envía la petición HTTP GET del parámetro de gestión para la obtención de datos. La solicitud HTTP GET tiene un parámetro que describe la petición en detalle. El gestor identifica el MO como una expresión XPath o XQuery. HTTP POST se utiliza para las operaciones de configuración con los parámetros de configuración en el cuerpo de la petición POST.
- Se hace la validación de la operación utilizando un parser de XML y el esquema. Dos parsers comunes disponibles son DOM y SAX. El parser DOM construye una representación del árbol de todo el documento XML y por lo tanto hace uso intensivo de memoria y procesador. El parser SAX es un parser por eventos de streaming y es más ligero, pero aun si consume muchos recursos.
- La petición se envía al agente/gateway como una petición HTTP a través del cliente HTTP de la aplicación gestor. El agente evalúa la expresión XPath y obtiene el último valor del MO solicitado.
- La respuesta se envía de nuevo al NMS como un mensaje XML y los datos se almacenan en la base de datos del NMS
- Las notificaciones o trap se envía a través del cliente HTTP del dispositivo y es recibido por el servidor HTTP en el NMS. Es procesado por la aplicación funcional de gestión en cuestión (controlador de notificación en la figura 3-26

3.5.4.5 Web Services para la gestión basado en XML

Los servicios Web son el siguiente paso lógico en el que la gestión basada en XML se está moviendo, ya que da una estructura adicional para la gestión basada en XML y define una forma independiente de la máquina para la aplicación de gestión y el agente intercambien mensajes.

Los servicios Web son un marco basado en XML para la construcción de aplicaciones distribuidas basadas en protocolos abiertos. La plataforma básica de servicios Web es XML + HTTP y los elementos de la plataforma de servicios Web son: SOAP es un protocolo de comunicación sencillo basado en XML para acceder a los servicios Web y está diseñado para su uso a través de Internet. WSDL es un lenguaje basado en XML para describir servicios Web y es un estándar del W3C. WSDL también se utiliza para localizar servicios Web. Este documento expone las operaciones, cuales parámetros se pasan a una operación, a través de que protocolos se puede acceder una operación, y en qué lugar (es decir, la dirección IP o, nombre de dominio) reside el servicio Web. UDDI es un servicio de directorio donde las organizaciones pueden registrarse para buscar servicios Web. Es un directorio para almacenar la información de interfaces de servicios Web descrito por WSDL.

Varios investigadores [Pra04] han hecho trabajos sobre el uso de los elementos de administración Web basada en servicios. OASIS (Organization for the Advancement of Structured Information Standards) es una organización de estandarización para la definición de servicios Web, y de esta han surgido varias normas, tales como MUWS (Management Using Web Services), MOWS (Management of Web Services), etc_ Los servicios Web predominantemente se ocupan de la gestión de sistemas.

3.5.5 Gestión en redes inalámbricas

En las redes satelitales, el NMS por lo general se encuentra en el hub/modern y monitoriza el hub/modem y los equipos en cada emplazamiento. Los datos de gestión se adquieren a través del enlace satélite compartiendo el ancho de banda con la carga útil de datos.

Los objetos a ser gestionados son parámetros asociados con la antena, transmisores, convertidores de frecuencia y amplificadores de potencia. Puesto que el ancho de banda total disponible está en el rango de 128 kbps a 2 Mbps (En el mejor de los casos), suponiendo un límite del 5% de uso para la gestión de datos, el ancho de banda disponible en los enlaces por satélite para la gestión es del orden de unos pocos kilobits por segundo. El uso de SNMP en este marco no es adecuado, y por lo tanto se utilizan protocolos eficientes propietarios. Las características de gestión y los parámetros que están implementados también están limitados debido a la limitación de ancho de banda.

3.5.5.1 Gestión en comunicaciones satelitales

En las redes satelitales, el NMS por lo general se encuentra en el hub/modem y monitoriza el hub/modem y los equipos en cada emplazamiento. Los datos de gestión se adquieren a través del enlace satélite compartiendo el ancho de banda con la carga útil de datos.

Los objetos a ser gestionados son parámetros asociados con la antena, transmisores, convertidores de frecuencia y amplificadores de potencia. Puesto que el ancho de banda total disponible está en el rango de 128 kbps a 2 Mbps (En el mejor de los casos), suponiendo un límite del 5% de uso para la gestión de datos, el ancho de banda disponible en los enlaces por satélite para la gestión es del orden de unos pocos kilobits por segundo. El uso de SNMP en este marco

no es adecuado, y por lo tanto se utilizan protocolos eficientes propietarios. Las características de gestión y los parámetros que están implementados también están limitados debido a la limitación de ancho de banda.

3.5.5.2 Gestión en redes Wireless LAN 802.11

Hay varios problemas asociados con el despliegue y la gestión de WLAN. Estos incluyen la escalabilidad, el aprovisionamiento, el flujo de datos tanto en tiempo real como en tiempo no real, amplia accesibilidad, gestión de energía, la interferencia de otros sistemas que operan en la misma frecuencia, tales como Bluetooth, gestión de la seguridad y la gestión de calidad de servicio. Hemos abordado algunos de estos en capítulos anteriores, a continuación abordaremos la manera de gestionar de forma centralizada una red de WLAN.

El uso de WLAN ha ido creciendo significativamente y las especificaciones 802.11 se han normalizado. Un AP de cualquier fabricante puede trabajar con la tarjeta de cualquier otro fabricante de WiFi. Sin embargo, esto se aplica sólo a conjunto de funciones básicas. El RFC 3990 define el planteamiento del problema en la configuración y aprovisionamiento de un punto de acceso inalámbrico. Se realizó un estudio y los resultados indicaron que la terminología, así como las funciones, eran divergentes y por lo tanto no era fácil definir una MIB que pudiera ser utilizada para administrar una red 802.11 [RFC4118].

Como preludio al desarrollo de una MIB que hace que todos los componentes de WLAN, incluyendo puntos de acceso, sean interoperativos, el amplio conjunto de funciones de AP se ha dividido en dos categorías: las funciones de 802.11, que incluyen aquellas funciones requeridas por los estándares IEEE 802.11, y las funciones de configuración y aprovisionamiento (CAPWAP: Configuration and Provisioning of Wireless Access Point), las cuales incluyen aquellas que no son obligatorias en IEEE 802.11, pero que se consideran esenciales para el control, configuración y gestión de redes WLAN 802.11 a nivel de gestión centralizada. Otro término que ha causado una ambigüedad considerable es "punto de acceso", que por lo general indica una caja que tiene antenas, pero que no tenía un conjunto uniforme de funcionalidades externas consistentes entre múltiples fabricantes. Para eliminar esta ambigüedad, el AP ha sido redefinido como el conjunto de funciones 802.11 y CAPWAP, mientras que el equipo físico que termina la capa PHY 802.11 se llama WTP (Wireless Termination Point).

Los estándares IEEE tienen una MIB bien definida para tecnologías inalámbricas como 802.11 y 802.16. Sin embargo, las arquitecturas inalámbricas centralizadas actuales de la mayoría de fabricantes no utilizan las MIB estándares IEEE, en cuyo lugar utilizan sus MIBs privadas. El esfuerzo de IETF CAPWAP es unir las MIB WLAN IEEE e IETF y hacer una red LAN inalámbrica que contengan productos de múltiples fabricantes interoperables.

El protocolo CAPWAP [RFC4564], [RFC5415], [RFC5416], define un protocolo estándar e interoperable, que permite a un controlador de acceso (AC) gestionar un conjunto de WTPs, como se muestra en la Figura 25. El NMS se comunica con AC utilizando SNMP. El AC se comunica con el WTP utilizando el protocolo CAPWAP. En la Figura 25, cada WTP coordina a las estaciones de su BSS.

Con el fin de hacer compatible la MIB IEEE con la MIB IETF CAPWAP, se necesita una asignación de uno a uno entre las dos [Yan07]. Esto se logra mediante el mapeo de la interfaz abstracta ifIndex en MIB II a una interfaz inalámbrica, definida como interfaz virtual radio, con un identificador único. La interfaz inalámbrica se muestra como la radio PHY en la Figura 25 y se le asigna un identificador único mediante la combinación del número de serie del WTP y el identificador radio para el servicio inalámbrico en el BSS. El lado izquierdo de la figura muestra la relación uno a uno entre ifIndex y la interfaz de radio virtual. Por lo tanto, en la Figura 25 para las tres interfaces virtuales WTP 1, 2 y 3, hay tres PHY Radio 1, 2 y 3, respectivamente, y también ifIndex 1, 2 y 3 correspondientes.

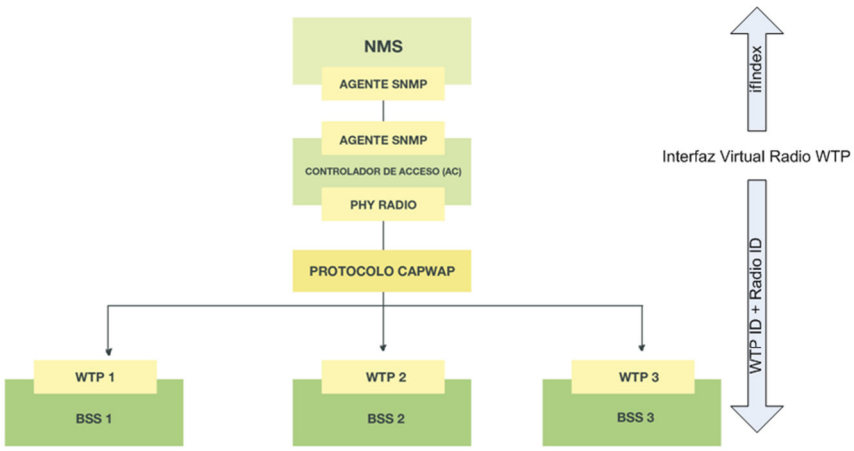

Figura 25. Arquitectura de gestión centralizada en redes WLAN

La MIB CAPWAP-Base, le será asignada un número por la IANA bajo la mib-2 [Shi09]. Hay 5 grupos bajo capwapBaseMIB.

- El grupo capwapBaseAc define los objetos del controlador de acceso.
- El grupo capwapBaseWtps define los objetos del WTP.
- El grupo capwapBaseParameters define los parámetros asociados con la base.
- El grupo capwapBaseParameters define los parámetros asociados con la base.
- El grupo capwapBasestats define las estadísticas del sistema.
- El grupo capwapBaseNotifrVarObjects define los objetos usados para las notificaciones.

3.5.5.3 Gestión en redes WiMAX

La Figura 27 muestra el modelo de referencia de gestión de redes WiMAX [Cho04]; [Dud04] definido en la enmienda 802.16f, la cual aporta mejoras a 802.16-2004, definiendo una MIB (Management Information Base) para las capas MAC y PHY y los procedimientos de administración asociados.

Se trata de un sistema de gestión de red (NMS), nodos administrados BS y SSs, y una base de datos de service flows. La base de datos de service flows contiene el service flow y la información de calidad de servicio asociada con que tienen que ser asignados BS y SS cuando se les dota de servicio, o un SS móvil cuando entra en la zona de cobertura de la BS. Los SSs pueden ser gestionados directamente por NMS o indirectamente a través de la BS, que actúa como proxy SNMP. La información de gestión entre el SS y la BS se realizara sobre un segundo CID (connection ID) de gestión para el SS administrado.

La BS y los SS recogen y almacenan los objetos gestionados en el formato de la WirelessMan Interface MIB y la wmanDevMib, definida en el documento 802.16f, los cuales se ponen a disposición del NMS a través de protocolos de gestión, come el SNMP (Simple Network Management Protocol).

La Figura 26, muestra la estructura de la MIB wmanIfMib de 802.16 y su nodo 184 bajo transmission (mib-2 10). Aquí se define la tabla interfaz para una interfaz inalámbrica MAN. wmanIfMibObjects en wmanIfMib tiene tres subnodos: wmanIfBsObjects (1) tiene las tablas asociadas con la BS; wmanIfSsObjects (2) tiene las tablas asociadas con los SS, y winanIfCominonObjects (3), las tablas asociadas con los objetos comunes.

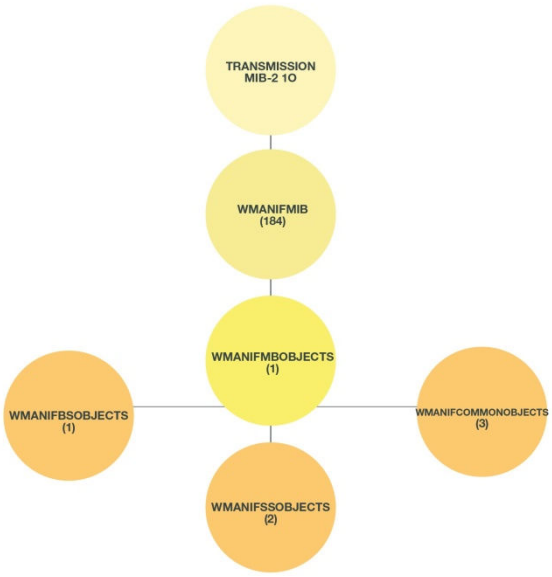

Figura 26. Esquema de la WMAN IF MIB definida en IEEE 802.16f

El agente SNMP puede ser implementado en el controlador de la BS o en el controlador del sector. Hay una entrada para cada BS si el agente SNMP se implementa en un controlador BS común. Sólo hay una entrada para el sector BS si el agente SNMP se implementa en el regulador del sector.

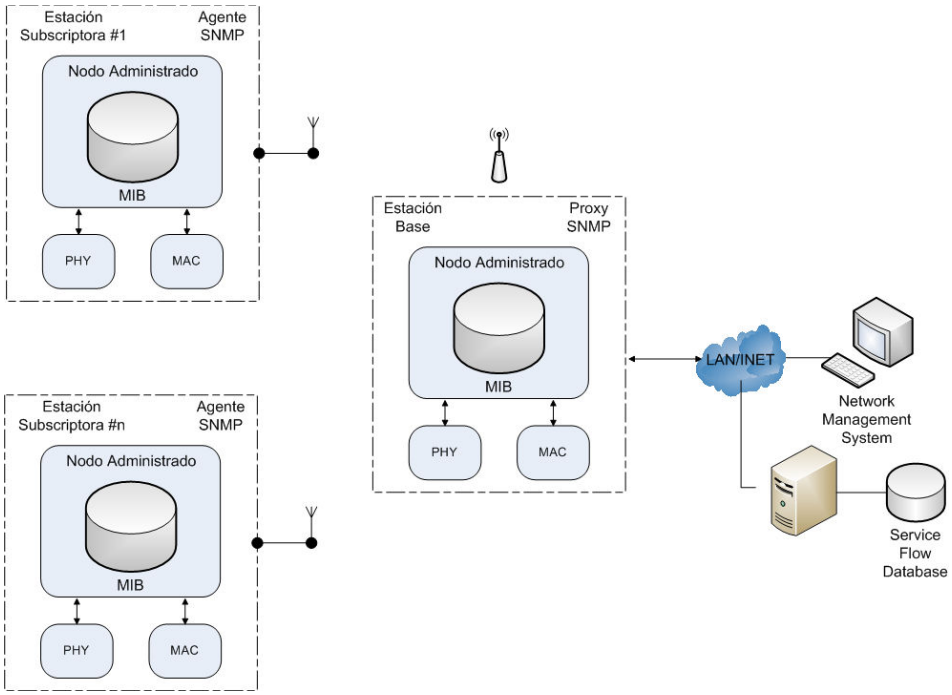

Figura 27. Modelo de referencia de administración de red corno se define en 802.16f

El estándar IEEE 802.16 solamente define las capas PHY y MAC. Como consecuencia de ello para asegurar la interoperabilidad entre vendedores para operaciones tales como roaming, es importante definir estándares sobre un amplio rango de interfaces y equipos, como en los estándares móviles 3GPP y 3GPP2. Por lo tanto, el WiMAX Forum aparte de definir las características del acceso radio entre estaciones bases y clientes de distintos fabricantes basados en los estándares 802.16, también busca proveer una arquitectura de red IP de extremo a extremo de alto desempeño que soporte usuarios fijos, nomádicos, portables y móviles.

4 Diseño e implementación de una arquitectura de comunicaciones inalámbricas para sistemas C4ISR

4.1 Arquitectura de comunicaciones propuesta

Tras la evaluación previa realizada en el estado del arte se estimó que es necesario un nuevo enfoque a la hora de proponer una arquitectura de comunicaciones para cualquier sistema de mando y control de pequeñas unidades a desarrollar. En concreto, se determinó que muchas de las soluciones existentes poseían las siguientes deficiencias a subsanar:

- Dependencia muy estricta del medio de transmisión subyacente.
- Utilización de protocolos propietarios
- Arquitecturas en capas sin señalización cross-layer, asociadas a sistemas monolíticos y poco flexibles
- Falta de inclusión de información multimedia
- Escasa utilización de COTS (Common Off-The-Shelf)
- Inclusión de políticas y soluciones de tiempo real muy rígidas
- Rigidez, que se traduce en falta de flexibilidad, agilidad y capacidad de adaptación en sistemas y consecuentemente en procedimientos

El enfoque de trabajo para esta tesis se centra en diseñar la arquitectura de comunicaciones para un sistema de mando y control de pequeña unidad, por tanto se propone una arquitectura cognitiva, cross-layer, multicapa y modular que permita la comunicación continua o casi-continua entre los componentes implicados (dispositivos de red, ordenadores, vehículos, personas, etc.) y teniendo en cuenta la estructura jerárquica (y por lo tanto la distribución geográfica) de los operativos implicados, utilizando para ello los medios inalámbricos disponibles en cada localización y con la habilidad de migrar a un medio inalámbrico distinto cuando sea requerido o necesario, logrando de esta manera auto adaptación a las condiciones cambiantes del entorno.

Para el desarrollo de la arquitectura cross-layer, se ha utilizado un enfoque basado en una entidad paralela encargada de coordinar la interacción entre los distintos planos a través de una API (Application Protocol Interface), entendiendo un API como un conjunto de Objetos, Primitivas y Servicios. Los objetos definen cuales datos pueden ser intercambiados a través del API y su formato. Los objetos pueden ser por ejemplo parámetros propietarios de una capa, un paquete de datos o una variable específica, como el SNR (Signal to Noise Ratio) en el receptor. Las primitivas son las funciones a cargo de interactuar con los objetos. Las primitivas pueden ser invocadas por cualquiera de las capas involucradas y finalmente, un servicio es una secuencia de primitivas invocadas para la obtención de un objeto o conjunto de objetos específicos.

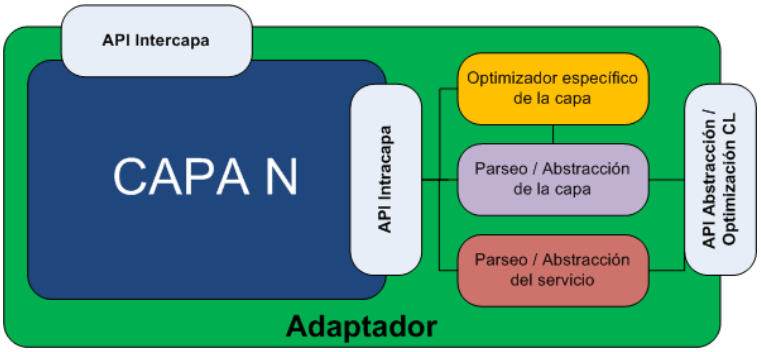

Figura 28. Detalle de la definición de una capa cross-layer

En la Figura 28 se muestra una vista general de las entidades utilizadas en la solución implementada, en la cual cada capa está envuelta en un Adaptador especifico de la capa, este será el encargado bien sea de optimizar los parámetros que se exponen a otras capas o funcionar como desacoplador de la tecnología subyacente.

En la Figura 28, también se puede apreciar un API Intercapa, el cual expone los servicios a las capas vecinas. A pesar de la representación gráfica, el API está concebido para conectar tanto hacia las capas superiores como a las inferiores.

Cada capa también está prevista de un API Intracapa, el cual lo podríamos ver como una "Caja Blanca" utilizada para exponer todos los parámetros internos de la capa al Adaptador. Los otros módulos internos son los encargados de realizar las funcionalidades específicas de la capa. El rol del optimizador específico de la capa está bien definido, sin embargo, los otros requieren una explicación más detallada.

Conceptualmente, es posible dividir una capa en dos aspectos: a) su "forma", la cual está dada por las variables que definen la estructura de la capa y b) la información que pasa a través de ella, definida por ejemplo por las medidas de desempeño realizada por la capa. El primer aspecto se tiene en cuenta en el Paseador de la capa, usado para traducir las variables internas y forma de la capa en un conjunto de variables desacopladas de la tecnología subyacente que se ponen a disposición de la entidad paralela. Claro que esto también es válido a la inversa, es decir, que cada vez que la entidad paralela realiza una optimización cross-layer global y proporciona los nuevos valores optimizados las variables generalizadas, el parser interno debe trasladar esos requisitos para que puedan ser usados por el optimizador local.

Por el contrario, el segundo aspecto, se cubre en el Parseador del servicio que realiza la misma operación de abstracción. La única diferencia subyace en el hecho que este tipo de variables se utilizan dentro de las métricas de optimización, pero no están sujetas a optimización por sí mismas, dado que están compuestas por medidas. Esto hace que la operación de parseo se simplifique mucho.

Por último, el API Cross-Layer (CL) proporciona la interfaz horizontal cross-layer hacia la entidad paralela, la cual se describe a continuación.

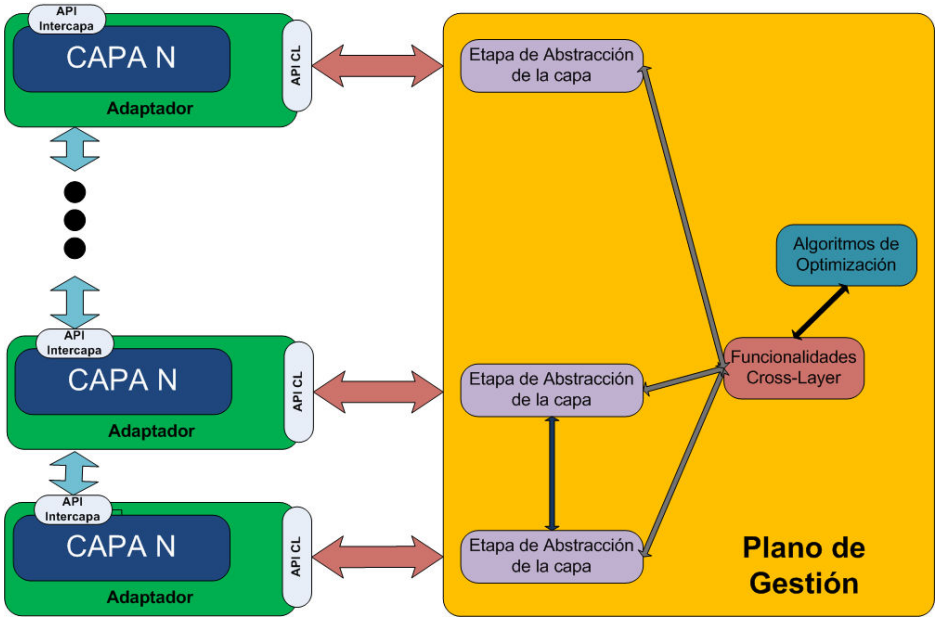

Figura 29. Esquema general de la arquitectura cross-layer propuesta

En la Figura 29, se muestra el esquema general de la solución implementada para la arquitectura multinivel. En la parte izquierda se aprecia la arquitectura en capas tradicional, con cada capa envuelta dentro de un Adaptador. Se convierte por lo tanto en la primera capa de la arquitectura, mientras que la segunda capa está compuesta de un gestor de la arquitectura o plano de gestión. Esta entidad contiene tanto una representación abstracta de las capas y servicios disponibles en la pila, así como las funcionalidades y adaptadores cross-layer. Tal como se muestra en esta figura, la estructura se define a partir de una representación basada en gráficos. La motivación para utilizar este enfoque son dos fundamentalmente. La primera que permite tener una arquitectura compleja con una gran modularidad que permiten reemplazar o expandir una funcionalidad. La segunda motivación es debido a la necesidad de un diseño orientado al desarrollo que permita implementar de una forma ágil la arquitectura propuesta.

La arquitectura global propuesta ha sido dividida en tres planos: un plano de red, un plano software o de componentes de proceso y un plano de gestión cross-layer, el cual se encarga de administrar los cambios debido al entorno o reconfiguraciones de los dos primeros. Con esta división se ha intentado desacoplar al máximo las tres arquitecturas así como poder especificar con mayor detalle sus características e interrelaciones.

En la Figura 30, se puede ver un esquema general de la arquitectura de comunicaciones propuesta e implementada en el sistema de mando y control SIMACOP, cada uno de los planos y módulos implementados, así como sus interrelaciones se describirán en detalle en las siguientes secciones.

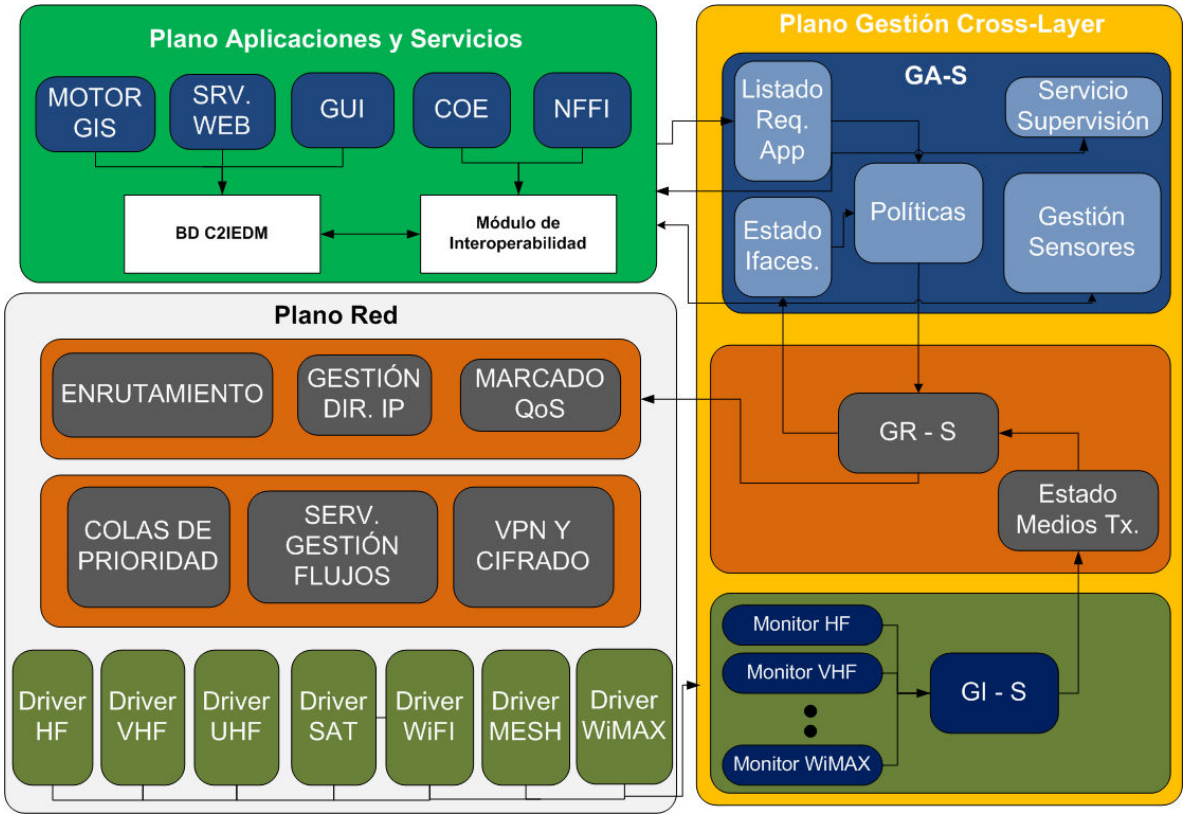

Figura 30. Arquitectura General cross-layer implementada en Simacop

Es importante destacar que el corazón de la arquitectura de comunicaciones propuesta es la arquitectura de red que determinará las capacidades y funcionalidades que aquella poseerá. Además, la aproximación propuesta es dual y puede ser utilizada tanto en un ámbito civil como en uno militar. La modularidad permite un elevado grado de independencia respecto a tecnologías de red subyacentes y, en definitiva, una mayor flexibilidad.

En definitiva el objetivo que impulsa y dirige el comportamiento de la arquitectura es doble, por un lado mantener la estructura y adaptarse a los cambios pero en ambos casos limitados (y complementariamente dirigidos) por el objetivo global que es la efectividad de la misión. Gracias a este enfoque consideramos que la arquitectura desarrollada refuerza y lleva la agilidad a un nivel superior.

4.1.1 Arquitectura de red

La arquitectura de red propuesta tiene un carácter multinivel, su estructura general se puede observar en la siguiente figura:

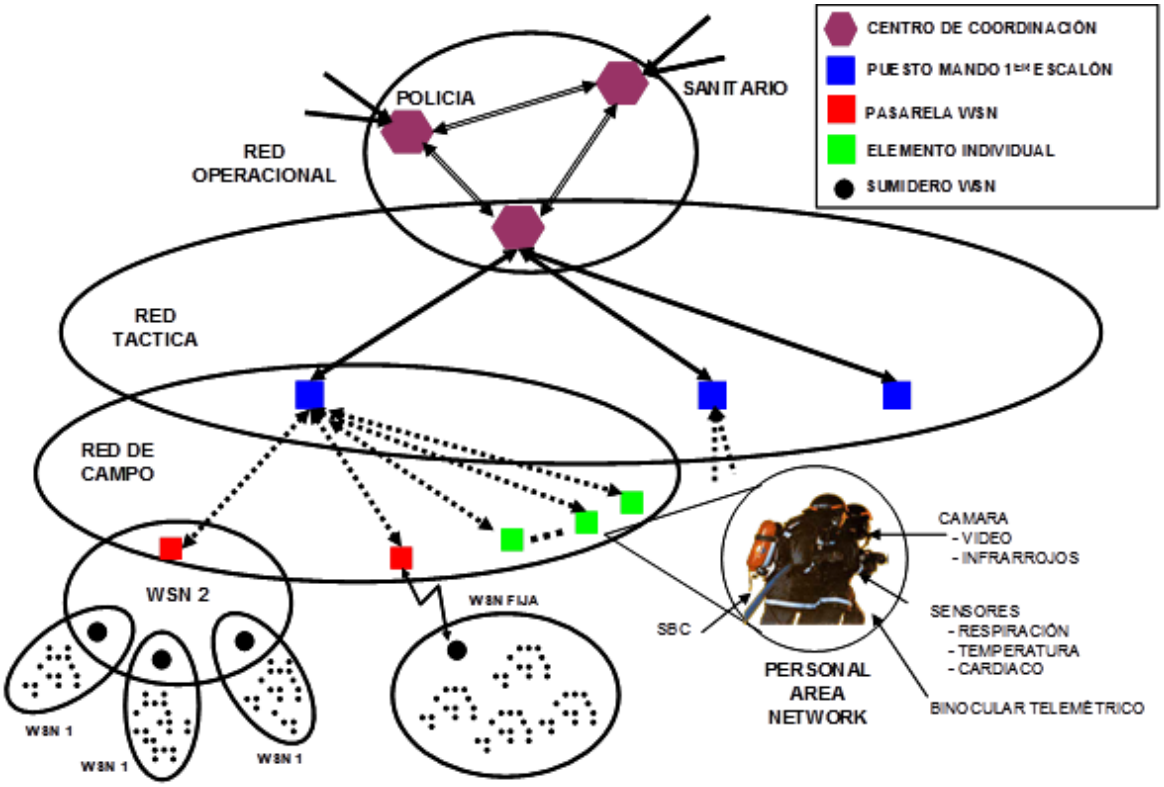

Figura 31. Arquitectura de red propuesta.

Tal como se puede apreciar, la arquitectura define 4 niveles de red ordenados jerárquicamente que a su vez están compuestos por 5 subredes distintas:

Nivel de interconexión de sensores. Este es primer nivel de red y está compuesto por:

1) Una red de área personal (PAN, por sus siglas en inglés: Personal Area Network) que como su nombre indica es una red de ámbito muy reducido entorno a un operativo individual y que engloba todos los sensores que puede acarrear (particularmente vídeo, GPS, telemetría y bio-sensores). En dicha red siempre se dispondrá de un dispositivo computacional de mayor jerarquía que recoge toda la información sensorizada, le aplicará un determinado procesamiento y hará de pasarela hacia la red de campo/combate para la distribución de dicha información.

   La red a este nivel se encarga de conectar los sensores que porten unidos a su cuerpo los operativos con el Single Board Computer (SBC) o PDA que gestiona todos los flujos a nivel de operativo. Este tipo de sensores se comunicará mediante tecnología inalámbrica, básicamente BlueTooth y Ultra Wide Band (UWB).

2) Redes de sensores (WSN, por sus siglas en inglés: Wireless Sensor Network), en este caso, tendrían una funcionalidad similar a la que tienen las PAN en la figura previa pero sin implicar a un operativo humano. Dicha red puede incluir una única WSN o bien aglutinar varias, como se observa en la esquina inferior izquierda de la figura. Dichos sensores son desplegados por los operativos humanos durante la intervención o bien desplegados pseudo-aleatoriamente sobre la zona previo a la intervención por medios especiales, por ejemplo en el caso de incendios o emergencias con vertidos altamente tóxicos donde los operativos humanos no pueden acceder con facilidad. En este mismo caso los sensores

pueden ser incluidos en vehículos aéreos no tripulados (UAV por sus siglas en inglés, Unmanned Aerial Vehicles) siempre atendiendo al payload que puede soportar como restricción fundamental y que permiten la monitorización y telemedición de zonas potencialmente muy peligrosas para operativos humanos.

La posición de los sensores no tiene porque estar predeterminada o diseñada, lo que permite el despliegue rápido y aleatorio en terrenos inaccesibles o en operaciones de crisis o gestión de desastres. Una característica a destacar de las WSN es la capacidad de auto organización y de realizar esfuerzos cooperativos, así como la tolerancia a fallos que exhiben en el comportamiento global y su bajo coste.

Los sensores están equipados con procesadores, lo que permiten que en lugar de enviar los datos tal y como son capturados sean capaces de realizar un cierto procesado, permitiendo acelerar los mecanismos de fusión de datos. Este mismo papel realizaba el nodo aglutinador en la PAN.

En esta subred se permitirá la transferencia de información entre sensores y la auto organización de la misma, siempre atendiendo a parámetros de consumo energético, tanto en la operación de los nodos individuales como en el enrutamiento de datos. Tecnologías como ZigBee (802.14) [ZIG] y Ultra Wide Band (UWB) [ISO26907] se utilizarán existiendo nodos pasarela que transferirán información de la WSN al nivel superior, principalmente por tecnología Wifi.

Nivel de red de campo/combate. Este nivel interconecta a las distintas unidades individuales entre sí y con el mando o visto de otro modo interconecta a las distintas PAN y WSN. Este nivel debe soportar todos los flujos multimedia de un conjunto de operativos. Dadas las características de los enlaces a éste nivel y la naturaleza de las operaciones a llevar a cabo, dicha red tiene la premisa de interconectar todos los nodos con todos, por cuestiones de redundancia y fiabilidad. Esto se ha probado con la utilización de tecnologías 802.11, aproximación ad-hoc, y tecnologías de red mallada (radios SpearNet de ITT y radios Rajant BreadCumb) y WiMAX móvil (IEEE 802.16e) como se verá posteriormente.

Nivel de red táctica. Este nivel es el encargado de interconectar distintas redes de campo/combate, es decir, conecta al personal de primer escalón de mando con los mandos de las diferentes unidades operativas, para que estos transmitan la información destinada a cada uno de los individuos en la zona de actuación a través de la red de combate. Además es el corazón de toda la arquitectura de red pues interconecta a las distintas unidades embarcadas en vehículos estableciendo las mallas de los distintos niveles jerárquicos. Se emplea tecnología inalámbrica WLAN, redes móviles comerciales (UMTS, GPRS), WiMAX fija (IEEE 802.16 -2004 d) y/o móvil o comunicaciones vía satélite, dependiendo de la cobertura y despliegue de las unidades operativas.

En el caso de soluciones militares se empleará comunicaciones VHF, HF y los medios satélites anteriormente citados. Es de destacar que en el caso de VHF y HF el ancho de banda disponible cae drásticamente constituyendo en ese caso los enlaces cuellos de botella que determinan la existencia de 'islas de información', principalmente multimedia. En cualquier caso, la información relevante para un sistema de mando y control requiere poco ancho de banda y siempre será transportada.

Nivel de red operacional, es el encargado de la interconexión de distintas redes tácticas de una misma organización o agencia. El caudal de datos a transportar y procesar suele ser mayor pero también lo son las capacidades de los medios a éste nivel. Se utiliza fundamentalmente enlaces satélite o de fibra óptica. En el caso de existir varias redes estratégicas debería existir flujo de información entre los centros de coordinación de nivel superior, por lo que se podría plantear la existencia de una red estratégica de coordinación global o red operacional de coordinación.

Nivel de red operacional de coordinación, permite conectar las redes operacionales de distintas agencias, permitiendo la compartición de información respecto a lo que está ocurriendo en el teatro de operaciones. En este nivel serán fundamentales los protocolos y tecnologías de interoperabilidad para poder permitir la transferencia de datos, siempre con unas restricciones particulares de entrega, entre organismos implicados en una operación conjunta.

Como se puede observar la arquitectura ha sido diseñada de manera muy modular para poder intercambiar en todo momento tecnologías de red a la hora de conectar los distintos escalones. Por otra parte las características principales de la arquitectura de red y que han determinado el diseño de cada uno de los elementos en las distintas soluciones son las siguientes:

- Tolerancia a fallos para garantizar la robustez de las distintas subredes: Los distintos elementos de la arquitectura han sido diseñados para que sean capaces de recuperarse ante fallos o variaciones críticas del entorno.
- Multicast para garantizar la escalabilidad, siempre y cuando sea posible. Esto se ha llevado a cabo en redes wifi (a/b/g) pero sin embargo no se podido implementar, por limitaciones tecnológicas, en redes de HF, VHF, WiMAX y satélite. Sin embargo en dichos casos se ha seguido la aproximación de segmentar la red en mallas de muy pocos nodos (típicamente 4-5) para limitar los dominios de colisión e incorporando nodos que hacen de pasarela y router entre mallas.
- Inclusión de protocolos de tiempo real como RTP/RTCP/RTSP reforzados por estrategias de planificación y asignación de recursos de tiempo real en los sistemas operativos, tanto en cada nodo particular como a nivel distribuido. Esto se verá en detalle en puntos posteriores.
- Las redes de campo/combate y red táctica son MANETs (Mobile Ad-hoc Networks). Esto se probó fundamentalmente en la versión del sistema embarcado que implementaba una tecnología mesh o mallada. Esta aproximación se estima muy adecuada para las características de dicho nivel de red y de los procedimientos aplicados en dicho escalón jerárquico, tanto en agencias civiles como militares.
- Suficiente ancho de banda para transmitir todos los flujos implicados, principalmente los multimedia. Monitorización y gestión del ancho de banda para el caso en el que este sea un recurso limitado, ya sea de un orden de magnitud tal que con muchas restricciones permite al menos un flujo multimedia o bien que no sólo no los permita sino que introduzca dificultades incluso para el transferencia de simples posiciones.
- Integración de tecnologías de red heterogéneas: IEEE 802.11a/b/g, Bluetooth, WiMAX, HF, VHF, mesh propietario, GSM/GPRS, UMTS, fibra óptica y comunicaciones satélite de manera completamente transparente para el usuario y fácilmente conmutable. Todo esto ha sido probado y validado.

4.1.2 Arquitectura de software

Por otra parte, toda la arquitectura del sistema C4ISR ha sido diseñada cumpliendo las especificaciones del framework para desarrollo de arquitecturas C4ISR [C4I97] [C4I07] del departamento de defensa de los Estados Unidos. Este framework aporta una mejor gestión y control sobre los productos y ciclos de desarrollo y una adecuada correlación entre los objetivos de sistemas, operativos y tecnológicos.

Se han establecido las siguientes premisas para el desarrollo de la arquitectura software:

- Los componentes utilizados para cada área de desarrollo deben estar basados en estándares siempre que sea posible.
- Debe utilizar sistemas y arquitecturas de software basado en código libre (OSS, por sus siglas en ingles Open Source Software), siempre que sea posible
- Debe usar modelos de datos que garanticen la Interoperabilidad.

- Por último, todos los flujos a entregar, tanto datos sensorizados como órdenes, deben cumplir requerimientos de tiempo real. Es por ello que se ha desarrollado la arquitectura para utilizan sistemas operativos de tiempo real (RT-Linux) y protocolos de red de tiempo real, como RTP y RTSP.

Basados en estas directrices se propone la siguiente arquitectura software genérica para los elementos de proceso:

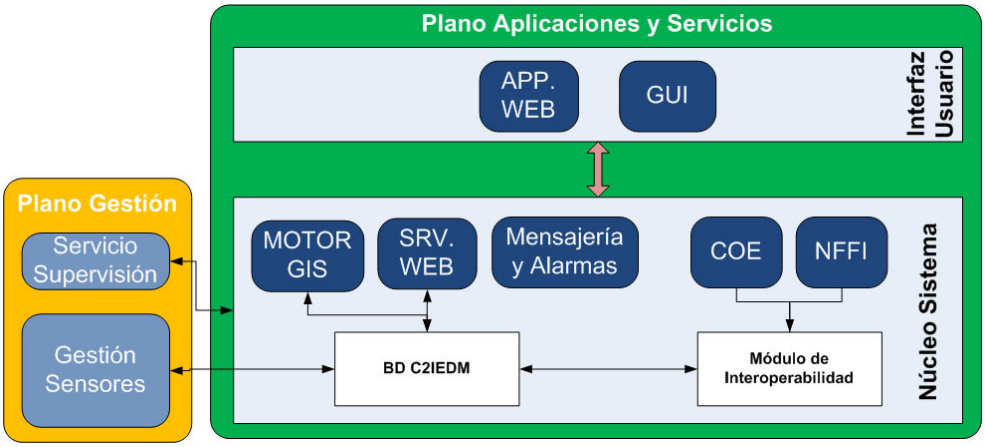

Figura 32. Arquitectura software para caso de configuración desembarcada

La arquitectura se descompone en dos elementos principales: el nivel de aplicación y el núcleo del sistema. De esta manera se ha buscado la modularidad y el desacoplo entre componentes software.

- En el nivel de aplicación se deben ubicar los distintos módulos que permiten la representación de la información sobre el teatro de operaciones a los usuarios. En la arquitectura software propuesta se ha optado por la utilización de aplicaciones basadas en tecnologías Web. Gracias a ello se permite la flexibilidad y modularidad puesto que pueden ser utilizadas desde cualquier sistema operativo e incluso desde máquinas que carezcan de base de datos o servidor Web. Así, cualquier nodo dotado de un navegador puede acceder a la COP, si está autorizado para ello. El diseño del GUI se recomienda que siga los principios de las teorías cognitivas más en boga, como por ejemplo [Rot01] [Sch00] para facilitar el acceso a la información, minimizar la sobrecarga cognitiva y facilitar la automatización de tareas.

  En la Figura 33, se puede ver la pantalla principal de la aplicación SIMACOP, la cual se compone de cuatro campos: una barra de información general ubicada en la parte superior de la pantalla, la botonera principal, el GIS y el mini mapa.

  En dicho interfaz de usuario se observan unos botones básicos para interactuar con el GIS (ZOOM IN, ZOOM OUT, IR A y MEDIR), un botón para acceder al filtrado jerárquico de la información (ORBAT), un botón de información extendida (INFO) y otro para la administración del sistema, tanto a un nivel básico como avanzado. Por último se pueden observar cuatro botones con funcionalidades extra como son las alarmas, los mensajes, las amenazas y los objetos. En todo momento un oficial puede detectar un evento prioritario y crítico, como puede ser un ataque y para señalizarlo a toda la red simplemente deberá pulsar en el botón de alarmas que le conducirá a una pantalla donde se mostraran las alarmas preconfiguradas existentes más dos configurables.

  Las amenazas siguen un algoritmo de validación por parte de unidades de nivel jerárquico superior respecto a amenazas generadas por unidades de un nivel jerárquico inferior. Similares a las amenazas, aunque sin validación y sin símbolo sino simplemente una cadena textual referenciada a un punto en el mapa, se encuentran los objetos. Su principal

utilidad se puede encontrar para señalar elementos o eventos no críticos detectados en el teatro de operaciones como un puente o un hospital.

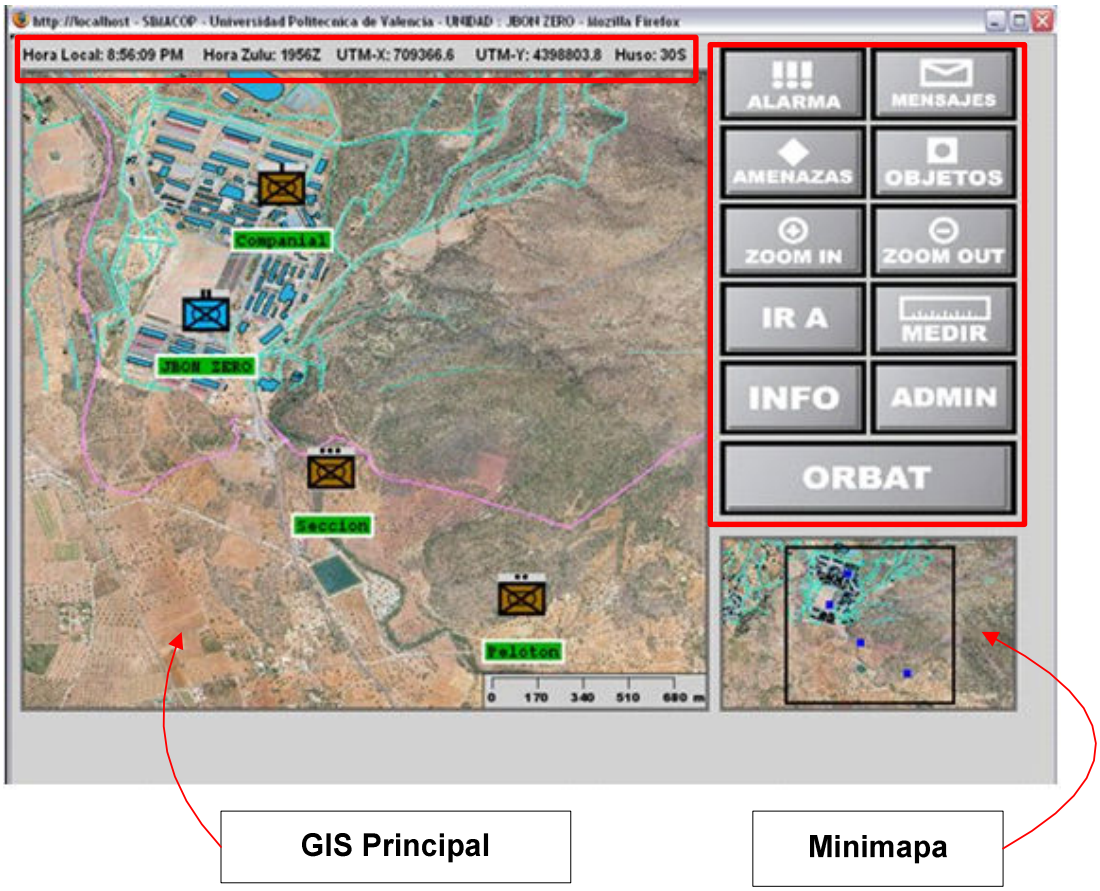

Figura 33. Interfaz principal de SIMACOP

Por último cabe destacar la funcionalidad de mensajería o 'chat táctico' que permite la comunicación textual entre nodos. Esta herramienta ha sido destacada como de extremada utilidad por parte de los usuarios finales para la sustitución, en múltiples ocasiones, de las comunicaciones vocales. Piénsese, por ejemplo, que en las configuraciones multimalla los usuarios de una malla no pueden comunicarse directamente con usuarios de otra distante más de un salto vía voz, sin embargo el sistema SIMACOP hace de enrutador y permite la comunicación entre mallas, independientemente de la distancia entre ellas. Así el 'chat táctico' es una herramienta muy rápida de envío de órdenes y reportes entre distintas unidades.

Dichos flujos de información (mensajes, alarmas, amenazas y objetos) van por caminos distintos entre sí y respecto a las posiciones de forma que se establecen una serie de colas a nivel de pila TCP/IP como políticas de planificación en cuanto a los procesos y servicios que las atienden para poder priorizar unos flujos respecto a otros. Todo esto se verá con más detalle en el punto de tiempo real.

Otro elemento importante en la aplicación es la utilización de cartografía vectorial. Con la misma se ofrece la facilidad al usuario de utilizar superponibles sobre la marcha y poder poner y quitar, en caliente, diversos elementos geográficos o logísticos como pueden ser carreteras y comunicaciones, conducciones de gas o de agua, cultivos, líneas e infraestructuras eléctricas o de telecomunicaciones, etc.

- Inmediatamente bajo nos encontramos el nivel del núcleo del sistema. En el mismo se encuentran los componentes software fundamentales de todo sistema de mando y control

a nivel de nodo. Así, en el mismo debe existir un módulo de Sistema de Información Geográfica (SIG) que trate, almacena y facilite la representación de toda la información geográfica. Fuertemente acoplado con el mismo estará un Sistema de Gestión de Bases de Datos (SGBD) donde se almacene toda la información relevante a una operación. La recomendación para la arquitectura software propuesta es la utilización del estándar OTAN C2IEDM (Command and Control Information Exchange Data Model) [C2I] y que se facilite la adaptación al futuro estándar JC3IEDM (Joint C3 Information Exchange Data Model) [JC3] cuando éste esté plenamente desarrollado.

Otro módulo incluido en el núcleo del sistema será el que gestione los servicios avanzados más allá de la mera replicación de posiciones dentro de un sistema de seguimiento de fuerzas propias, esto es, servicios como la detección, diseminación y validación de amenazas, envío de alarmas prioritarias o servicios de mensajería o 'chat táctico'.

Por último, dentro de éste núcleo del sistema se propone la inclusión de un módulo de interoperabilidad que, gracias a soportar determinados mecanismos y protocolos estándar, permita la interconexión del sistema con otros equipos de otras agencias y organismos, desarrollados con arquitecturas potencialmente muy distintas, de forma que se pueda establecer un intercambio efectivo de información relevante para el cumplimiento de la misión.

4.1.3 Plano de gestión cross-layer

Finalmente en el plano de gestión se definen tres "gestores": El gestor de aplicaciones y servicios de SIMACOP, el gestor de redes y el gestor de interfaces. En este plano es donde reside la "Inteligencia" o capa "cognitiva" de la arquitectura. Los servicios del núcleo de SIMACOP interactúan con el plano de gestión para establecer los recursos necesarios para la trasmisión. Estos parámetros se utilizan para adaptar los parámetros de trasmisión tanto en la capa de red como en las interfaces de transmisión.

En lo referente a la gestión las decisiones de acciones a ejecutar sobre el sistema se hacen de acuerdo a la disponibilidad específica de un medio de transmisión en un momento dado o de acuerdo a las preferencias establecidas por el usuario o administrador del sistema.

En la figura se puede ver los distintos gestores y su interrelación con el resto de componentes de la arquitectura.

El Gestor de Aplicaciones de SIMACOP (GA-S) es el responsable de administrar los recursos disponibles entre las aplicaciones y servicios del núcleo de SIMACOP y los medios de transmisión disponibles. Para lograr este objetivo mezcla información de la lista de medios de comunicación disponible (provista por el GR-S, acrónimo de Gestor de Redes de SIMACOP) y los requisitos de la aplicación o servicio, basado en estos parámetros genera las políticas necesarias que se envían al GR-S para tomar la acción adecuada, tal como se puede ver en la siguiente figura:

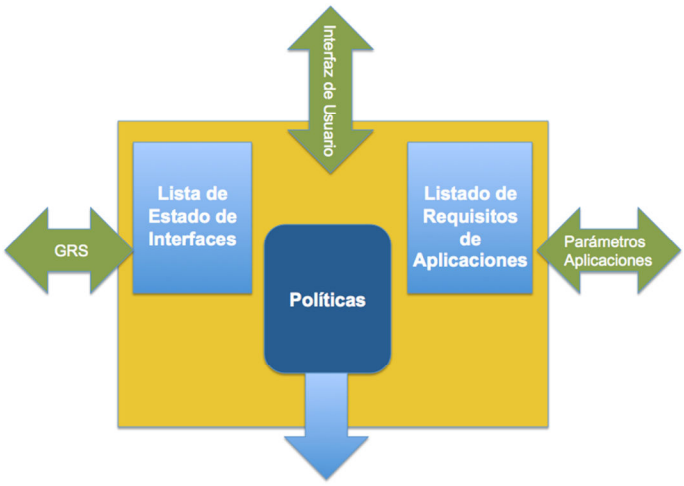

Figura 34. Detalle del módulo gestor de aplicaciones de simacop.

Como parte del Gestor de Aplicaciones (GA-S), también se define la existencia de un módulo de supervisión de fallos y recuperación de caídas, en este nivel se encarga del funcionamiento intra-nodo. Este módulo proporcionar los mecanismos para monitorizar el estado de un nodo y su funcionamiento, así como las condiciones de su entorno y las preferencias del usuario y dependiendo de las políticas definidas modificar la configuración local de SIMACOP y/o la de otros nodos que dependan de él. Por otra parte, en cada nodo hay un proceso de monitorización que verifica el estado de otros procesos críticos como el subsistema de video, subsistema de GPS, etc., y si se llegase a detectar cualquier posible estado erróneo recuperar el sistema a un estado consistente.

Siguiendo este enfoque se han desarrollado dos soluciones para cada una de las arquitecturas software implementadas, es decir, una para la configuración desembarcada y otra para el sistema vehicular. En el primer caso, el sistema se ejecuta sobre hardware embebido (SBC o PDA), el cual se debe mantener en funcionamiento sin intervención humana y recuperarse de fallos (reinicios por batería o cortes de red, etc.) de forma autónoma.

En este caso existen dos niveles de operación: nivel de sistema operativo y nivel de código. En el nivel de sistema operativo hay varios procesos que monitorizan el estado de procesos claves (servidor vídeo, servidor GPS y servidor de señales) y la evaluación de los flujos de datos desde y hacia los nodos, esto puede verse en la siguiente figura:

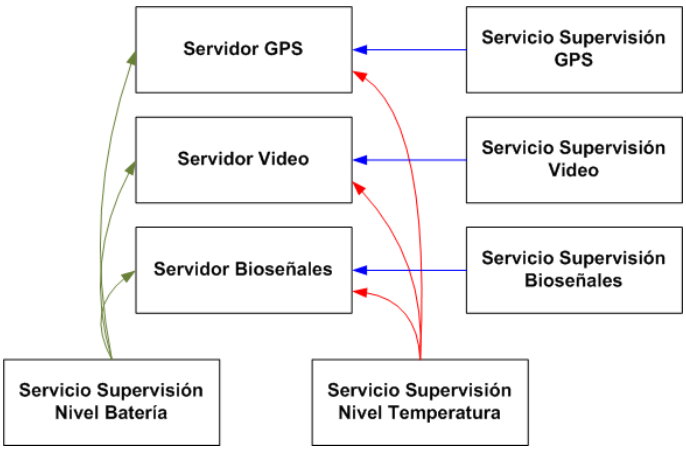

Figura 35. Gestión de procesos a nivel operativo

A nivel de código hay procesos que detectan los cambios del entorno y modifican el código en ejecución para que se adapte. Este es el caso, por ejemplo, de movimiento o cambios de iluminación en video que hacen que el servidor debido reduzca la tasa de transmisión. Otro ejemplo, es cuando el SBC se acerca a una red de sensores previamente desplegada y se puede comunicar vía ZIGBEE con sus nodos y reconfigura su estructura e información de enrutamiento siguiendo una función de ahorro de energía. En estos casos, el sistema reescribe algunas partes de su código para adaptarse ya que en la arquitectura desembarcada (tanto SBC como PDA) no hay un compilador por lo tanto el código que se reescribe es código interpretado.

En la versión vehicular, también hay procesos que monitorizan el correcto funcionamiento de los sensores y reinician el servidor para llevarlo a un estado consistente en caso de detectar errores. Por otra parte, el proceso de re-escritura de código on-the-fly tiene más relevancia en esta solución, dado que estos nodos son los que implementan el núcleo de las funcionalidades de los procesos de auto configuración intra-nodo e inter-nodo. Por lo tanto, el sistema reacciona a las entradas monitorizadas (bien sea del entorno o del usuario) para ganar eficiencia y flexibilidad.

Por ejemplo, el código se rescribe para cambiar de una configuración de GPS a otra (dependiendo de las entradas del usuario o ante datos de GPS erróneos)

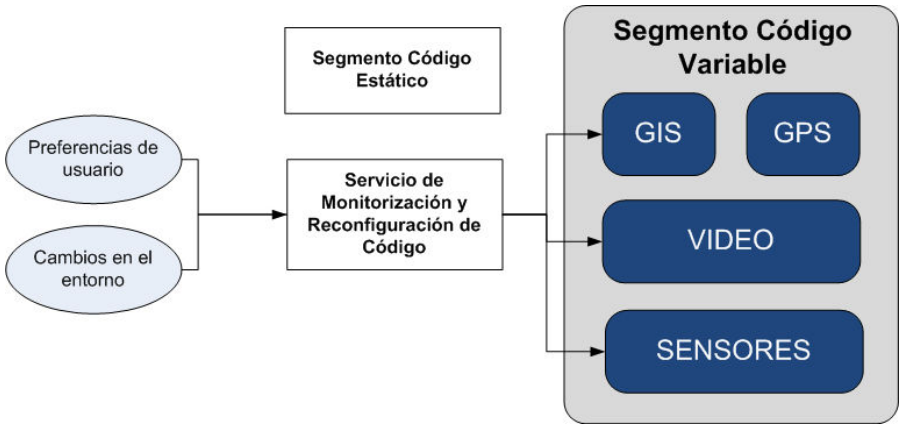

Figura 36. Proceso de reescritura de código intra-nodo

Este gestor también está provisto de un módulo de gestión de sensores, el cual permite la conexión de gran número de sensores (fuentes de vídeo, GPS, señales biomédicas, información telemétrica, integración con datos de redes de sensores, etc.) y la obtención de información e integración de la misma en la arquitectura propuesta.

Además, dicho módulo debe permitir la fusión de dicha información sensorial para elaborar conocimiento a partir de datos crudos permitiendo entregar a cada nivel de mando la información que realmente precisa en cada momento. Dicho módulo software de fusión sensorial, ubicado en cada nodo, trabajará cooperativamente con los módulos de sensores de otros nodos para elaborar ese conocimiento de manera distribuida, como aproximación más eficiente.

En definitiva, este módulo proporciona un “servicio de integración de sensores”, que interconecta distintos sensores y sus flujos asociados con los nodos de cómputo donde la información será procesada y el conocimiento elaborado así como con los nodos donde hay puestos de mando y control donde será representada. Esto se puede ver en el siguiente esquema:

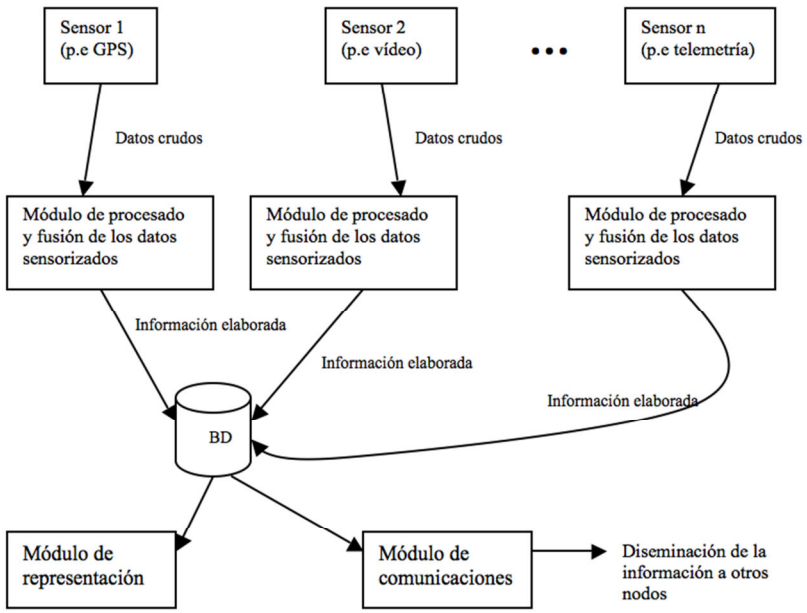

Figura 37. Arquitectura de gestión de sensores

El Gestor de redes de SIMACOP (GR-S) es el responsable de varias tareas, primero que todo es el enlace entre uno o más medios de transmisión y uno o más servicios de Simacop (que pueden estar ejecutándose de forma simultánea), es decir, es el responsable del envío y recepción entre un proveedor de datos y un servicio de Simacop, en base a los requisitos de QoS que obtiene de la capa de Gestión de Aplicaciones de Simacop.

Este módulo también es responsable de:

- Notificar a la capa GA-S de cualquier cambio en la disponibilidad de un medio de transmisión.
- Actualizar la tabla de enrutamiento cuando sea necesario o cuando la capa GA-S lo solicite.
- Gestionar el direccionamiento IP del nodo.
- Marcar cada flujo de datos de acuerdo a las políticas de QoS definidas en la capa GA-S.
- Gestionar el intercambio entre dos medios de transmisión distintos.

Dos de las funciones más importantes de este módulo son la gestión de QoS y la gestión del enrutamiento. A nivel de QoS, se ha optado por una solución cross-layer que genera colas de prioridad diferenciada en función del tipo de flujo y del medio de transmisión. Funciona de la siguiente manera, el módulo GA-S genera las políticas de temporización para cada flujo y se pasan al módulo GR-S.

El módulo de GR-S en base a las políticas que recibe genera políticas de QoS basado en servicios diferenciados (DiffServ) [RFC2474] [RFC2475], lo que consiste en generar una cola tipo DSMARK a nivel 3 del modelo OSI para cada política, este tipo de cola marca los paquetes usando el campo DSCP del paquete IP con un valor adecuado para los requerimientos de calidad de servicio de cada tipo tráfico, tras modificar la cabecera IP, se pasa el paquete IP a la capa MAC, en dicha capa se mapean los valores del campo DSCP a valores clases de servicio (CoS, por las siglas en ingles de Class of Service) y son asignados a colas o clases de servicios distintas para cada tipo.

Finalmente, cada una de estas clases de servicio tiene valores diferentes dependiendo del medio de transmisión que corresponda, por ejemplo en WiFI implicaría valores distintos para ventana de

contención, oportunidad de transmisión, etcétera, mientras que en WiMAX se traducirá en asignar los flujos a una de las clases de servicio disponibles, como rtPS o UGS, las cuales se mapean a valores diferenciados para retardo mínimo, jitter garantizado, etc. En medios de transmisión puramente militares como HF o VHF dado que la implementación a nivel MAC no es estándar, son capas propietarias cuyos parámetros no se pueden moldear desde un software externo o desde campos IP, en este caso la QoS se maneja únicamente desde la capa de aplicación con la temporización de cada uno de los servicios. En el punto 4.2 de la presente tesis se detalla la implementación de QoS para cada uno de los medios de transmisión.

A cuanto al enrutamiento, el módulo GR-S es responsable de gestionar el direccionamiento IP de la subred entre el nodo y las interfaces radio disponible y también es responsable de crear y actualizar la tabla de enrutamiento del nodo. En este punto cabe destacar que debido a la naturaleza jerárquica de los elementos implicados, sólo tiene sentido que se comuniquen nodos del nivel jerárquico N con los de nivel jerárquico N-1 o N+1, por lo tanto en el diseño se optado por un esquema de comunicación en 'clústeres' o dominios de transmisión acotados, de forma que un nodo dado, durante el curso de una operación, se comunica con y sabe de la existencia de muy pocos nodos de los existentes, esto se explicara en detalle en el punto de esquemas de replicación de datos.

El modulo GR-S también en responsable de asignar a cada medio de transmisión un peso en función de su tasa de transferencia, el ancho de banda y el modo dúplex, entre más grande sea este valor, mejor será el canal para comunicación de datos. Además de esto, cada nodo mantiene el modulo GR-S, una matriz que relaciona todos los medios de transmisión activos con los nodos vecinos y los posibles medios de respaldo organizados por peso, dicha información se consulta y actualiza cada vez que hay cambios en la topología de red.

Finalmente, el Gestor de Interfaces de SIMACOP (GI-S) es el responsable de determinar cuáles medios de transmisión están disponibles en cada momento y verificar los parámetros del enlace (calidad de la señal, tasa de transmisión, etc.) siempre que sea posible.

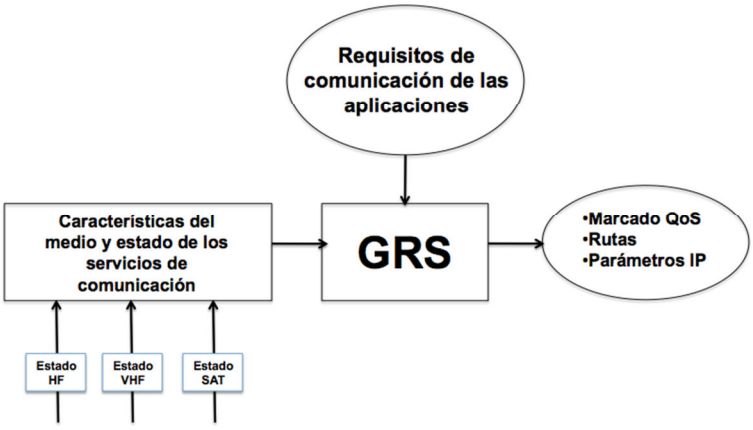

Figura 38. Módulo de gestión de redes de SIMACOP

El gestor de interfaces es el encargado de notificar a la capa superior (GRS) si algún medio deja de estar disponible y establece las colas de prioridad en el medio de transmisión elegido basado en las políticas que obtiene de la capa superior.

4.1.4 Esquemas de replicación de datos

Una característica fundamental de los sistemas de comunicaciones en sistemas C4ISR, como se ha visto en el capítulo 2, es el uso de medios con muy limitado ancho de banda debido a su

utilización en escenarios tácticos. Esto incide claramente en los servicios disponibles y fundamentalmente en los retardos de réplica, que son elevados y de varianza difícilmente caracterizable. Es por ello que se precisan mecanismos de réplica y de calidad de servicio adecuados a un entorno con estas características. En el presente punto se detalla el esquema de replicación de datos propuesto e implementado en el sistema de seguimiento de fuerzas propias que valida la arquitectura propuesta al permitir la réplica de información entre todos los nodos en tiempo útil.

Entre las características elegidas para el esquema de replicación de datos podemos destacar:

La característica fundamental que se ha perseguido en el diseño de la réplica de datos ha sido, como en prácticamente todos los puntos del presente trabajo, la simplicidad. El mecanismo debe ser extremadamente simple tanto en su implementación como en su funcionamiento para no sobrecargar a los nodos ni a la red con información excesiva.

Por lo tanto, en el esquema de replicación se ha optado por minimizar la información transferida a lo imprescindible, eliminando cualquier tipo de redundancia. Como consecuencia de esto, se realizan envío de datos de reducido tamaño y a ráfagas, buscando adecuarse a las características del canal radio disponible en cada momento.

Eliminar el uso de retransmisiones, protocolos de comunicación y transferencia a varias bandas y reducir el número de ACKs al mínimo imprescindible, por lo tanto, no se precisa que estén de acuerdo y estrictamente coordinados temporalmente emisor y receptor. Además, para los tipos de datos a tratar en esta solución la pérdida eventual de algún paquete no es grave. Por ejemplo, si se pierde un paquete con una posición ésta quedará invalidada por la siguiente que se generará tras n segundos fijados en el periodo de muestreo. Lo mismo sucede con un stream de vídeo o cualquier tipo de información multimedia que pueda enviarse (aunque esto sólo puede llevarse a cabo en medios con el adecuado ancho de banda, como satélite, WiMAX, etc.).

Para el caso de la propagación de alarmas, amenazas y mensajes, que sí pueden precisar un mecanismo de ACK, se optó por una estrategia mixta basada en que si un nodo no consigue enviar una determinada información, salvo casos muy concretos, acabará estando en condiciones de volver a enviar dicha información, todo esto combinado con el uso de ACKs, pero muy particulares para no sobrecargar. Por ejemplo en el caso del envío de amenazas, aunque estimado como menos prioritario, existía un requerimiento de usuario de una validación o ACK a nivel operativo por parte de oficiales de nivel superior respecto a oficiales de nivel inferior, lo cual sí se implementó. Debido a este punto y al anterior, se utiliza el protocolo UDP que no precisa ACKs a nivel de transporte, permite la pérdida de paquetes y es unidireccional.

Esto conduce también al diseño de una arquitectura muy desacoplada entre emisores y receptores. El emisor comprueba que posee información para enviar y la envía por los medios que sabe que están disponibles para la comunicación con los receptores. Los mismos lo único que hacen es estar a la escucha por los canales habilitados y al recibir información la insertan en sus bases de datos. La aproximación se puede considerar muy distribuida y ‘stateless’ pues en todo momento los nodos desconocen el estado general de la red.

Al hilo del punto anterior hay que destacar que se optó por un esquema de comunicación en ‘clústeres’ o dominios de transmisión acotados de forma que un nodo dado, durante el curso de una operación se comunica con y sabe de la existencia de muy pocos nodos de los existentes. Esto es debido, inicialmente, a un requisito operativo de diseño puesto que dada la naturaleza jerárquica de los elementos implicados, sólo tiene sentido, en principio, que se comuniquen nodos del nivel jerárquico N con los de nivel jerárquico N-1 o N+1 (Figura 39). Esto desde el punto de vista de las limitaciones radio citadas es una gran ventaja pues un nodo acaba comunicándose con 4-5 nodos a lo sumo con el beneficio adicional de que, al pertenecer a un nivel jerárquico próximo, es muy probable que la distancia no sea muy grande y por tanto las probabilidades de una buena conectividad radio son mayores. En el caso de unidades de nivel jerárquico elevado (piénsese en

nivel de batallón o compañía) donde esto no se cumple y en la práctica se ha observado un mayor grado de conmutación entre medios radio al perderse la conectividad o bien directamente en estos niveles los enlaces con el inferior son HF permitiendo la comunicación a largas distancias de 'islas' de VHF, más próximas entre sí geográficamente. Este último punto se pudo constatar en las maniobras LIVEX'08 en el campo de maniobras de Chinchilla que se comentan en el capítulo 5 del presente trabajo.

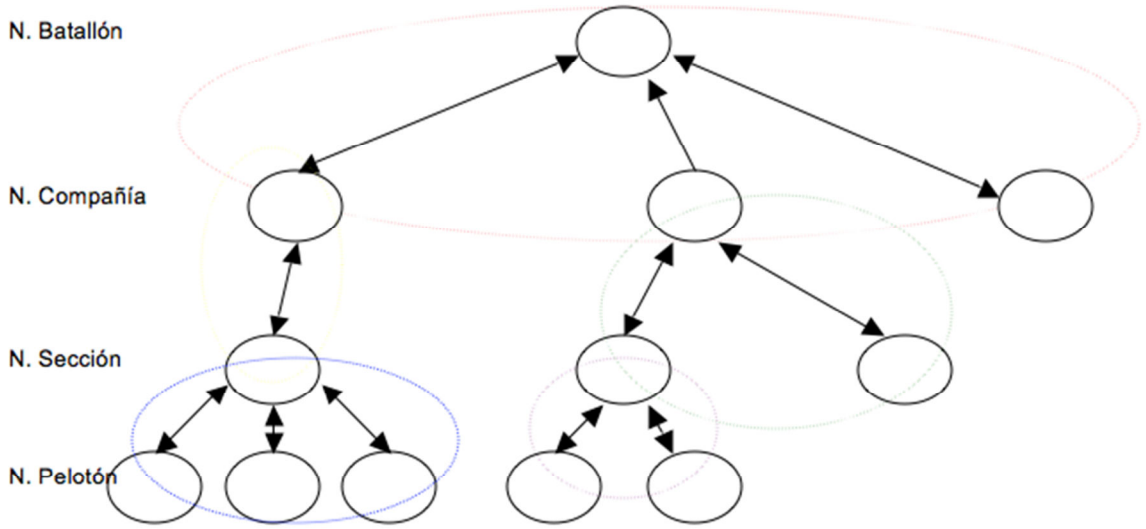

Figura 39. Clúster o Dominios de comunicación por niveles jerárquicos en la operativa

En la Figura 39, se puede observar una configuración bastante típica en la tenemos un batallón del que dependen tres compañías. De la primera de ellas depende una sección a la cual están asociados tres pelotones. De la segunda compañía dependen dos secciones de la primera de las cuales penden dos pelotones mientras de la segunda ninguno. Por último tenemos una compañía de la que no depende ninguna unidad. Se puede observar que la comunicación se establece únicamente dentro de los clústeres marcados (colores con puntos discontinuos) de forma que un nodo únicamente conoce y se comunica con nodos accesibles a nivel radio, es decir, se comunica dentro de uno o como mucho dos clústeres (depende de su ubicación).

De esta forma, el procedimiento de funcionamiento del algoritmo es muy simple. En cada nodo existen servicios de Windows con una temporización adecuada al medio por el que van a transmitir y al tipo de flujo de datos concreto que van a enviar, que periódicamente se activan y comprueban si ha habido alguna actualización en su base de datos, bien sea posiciones, alarmas, amenazas objetos o mensajes. En tal caso formatea el mensaje a enviar para cada tipo de datos y lo pone en la cola correspondiente. El proceso de envío, basado en la información que proporciona la capa de gestión, evalúa que nodos susceptibles de recibir datos están disponibles y procede, cuando corresponde al envío de datos.

Por otra parte en cada nodo existen servicios receptores, independientes de los emisores, que están a la escucha de manera continuada por puertos particulares. En el caso de recibir datos los insertan en la base de datos.

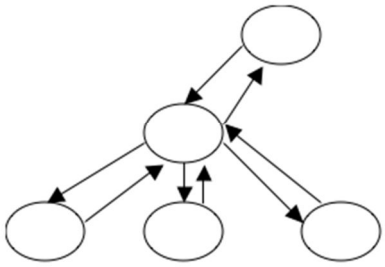

Figura 40. Flujos de comunicación entre nodos adyacentes jerárquicamente

En la Figura 40, se puede observar el procedimiento de diseminación de la información entre nodos de jerarquía adyacente. Los nodos de nivel inferior (1) entregan (es de destacar que no existe una sincronización estricta entre ellos) al nodo superior las actualizaciones de datos en períodos preconfigurados recibiendo a su vez de dicho nodo las actualizaciones que el mismo disponga (2). Éste repite el proceso con el nodo de jerarquía superior. La información acaba por morir y se hacen comprobaciones estrictas para que no haya bucles o efectos de 'rebote'.

El esquema de replicación de datos también es el encargado de mantener la estructura de la red consistente a la vez que se adapta a los cambios externos, esto significa que es el encargado de mantener las características principales del sistema tales como, el intercambio de mensajes y la COP Conjunta, durante y después de una reestructuración o cambio a nivel de red. Estos cambios pueden ser inserción de nuevos nodos, eliminación de nodos existentes, cambios en medio de transmisión entre otros.

El corazón principal de SIMACOP y alrededor del cual se articula todo es el fichero de misión (FDM), el cual refleja la orgánica así como la estructura de red de una manera flexible. En dicho fichero se encuentra toda la información imprescindible de una operación concreta como puede ser las unidades implicadas, sus características orgánicas, sus características de red, sensores, filtros, etc. Esta información se genera con una simple herramienta integrada en la aplicación SIMACOP, en el modo administrador y se salva en un fichero de texto que suele tener un tamaño entorno a los 40-50 KB.

Este fichero se distribuye a todas a las unidades implicadas para que lo instalen y compartan la estructura de la operación y puedan comunicarse entre ellas. Dicha estructura de información también puede ser modificada en el curso de una operación, siendo entonces diseminada por medios radios por un canal destinado a la señalización y el control. Por lo tanto, para reconfigurar el estado de la red, está información debe ser consistente entre los nodos por lo tanto es necesario establecer unos procedimientos de intercambio.

A continuación se describen en detalle los procesos de reconfiguración de red. En el primer caso, consideremos lo que sucede cuando un nodo se une a la red. Cuando una nueva unidad se une a una misión, el nodo necesita saber una información mínima del despliegue de red ya sea por medio del FDM o al menos la información de contacto de su unidad superior.

El primer paso del proceso es contactar a la unidad superior para registrarse en la misión (ORBAT_JOIN_MSG) como se muestra en la Figura 41, la unidad superior recibe la petición y valida al subordinado a través de un token de autenticación, después de la autenticación exitosa, la unidad superior actualiza la base de datos con la nueva unidad subordinada y envía un fichero de misión modificado a sus subordinados (ORBAT_UPDATE_MSG) así como a sus unidades superiores (en caso que existan). La unidad superior también actualizará su base de datos y reenviará el mensaje ORBAT_UPDATE_MSG al resto de unidades subordinadas, de esta manera los cambios se irán propagando a lo largo de la red.

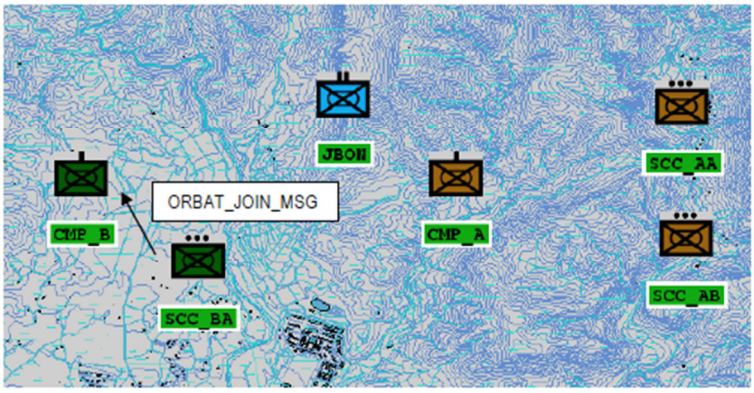

Figura 41. Una nueva unidad se une a la operación

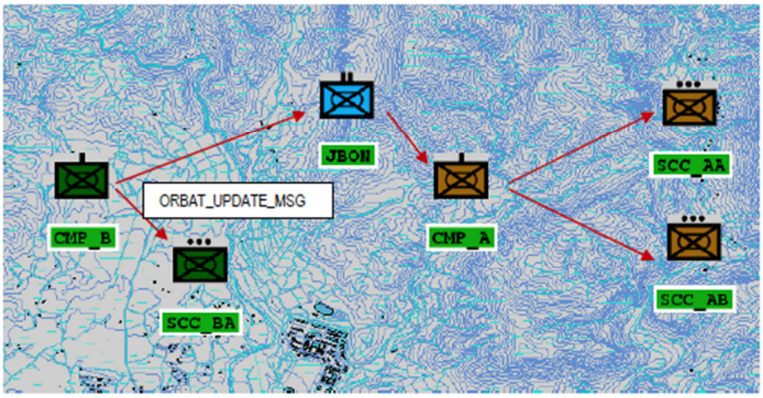

Figura 42. La unidad superior actualiza el ORBAT

Cuando todas las unidades subordinadas en un nivel han actualizado su información local, enviarán un mensaje de ORBAT_APPLYOK_MSG a la unidad superior (Figura 43). A la recepción de este mensaje por la unidad de coordinación global (GCU) desde sus subordinados esto significará que todos los nodos en la red han actualizado su base de datos local con la información de la nueva unidad, por lo tanto la GCU inunda la red con un mensaje ORBAT_UPDT_MF_MSG (Mensaje de actualización del FDM). Hasta este momento los cambios son a nivel de base datos más no a nivel de aplicación, por lo tanto, cuando un nodo recibe este mensaje entra en juego la reconfiguración intra-nodo, la aplicación volverá a leer la base de datos y generará el código necesario para hacer visible está nueva unidad en el GIS, en caso que el nodo no tenga unidades subordinadas, enviará un ORBAT_APPLYOK_MF_MSG a la unidad superior. En el caso que sí que tenga unidades subordinadas, les reenviara el mensaje y esperará hasta que todas las unidades confirmen antes de reportarlo a la unidad superior. Cuando la unidad de coordinación global (GCU) recibe este mensaje de todas las unidades subordinadas, significará que todos los nodos en la red han actualizado y reescrito su aplicación, a partir de este momento la unidad está completamente operativa en la red (Figura 44). Después de este punto, toda la red se habrá reconfigurado para adaptarse al cambio y el flujo de información entre los nodos, no se habrá visto afectado por la modificación.

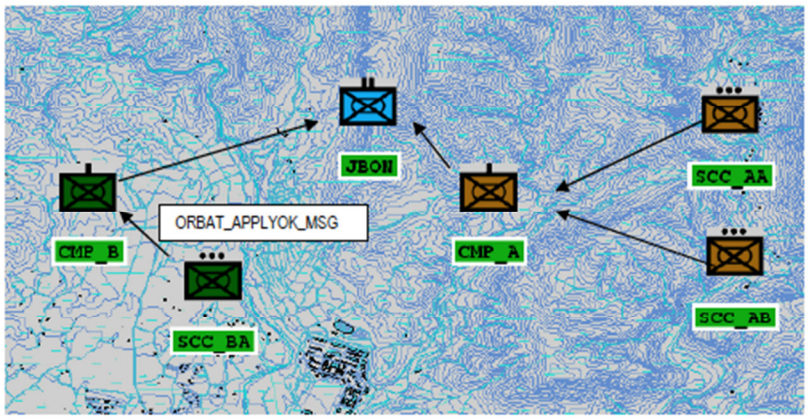

Figura 43. Confirmación de cambios en el ORBAT

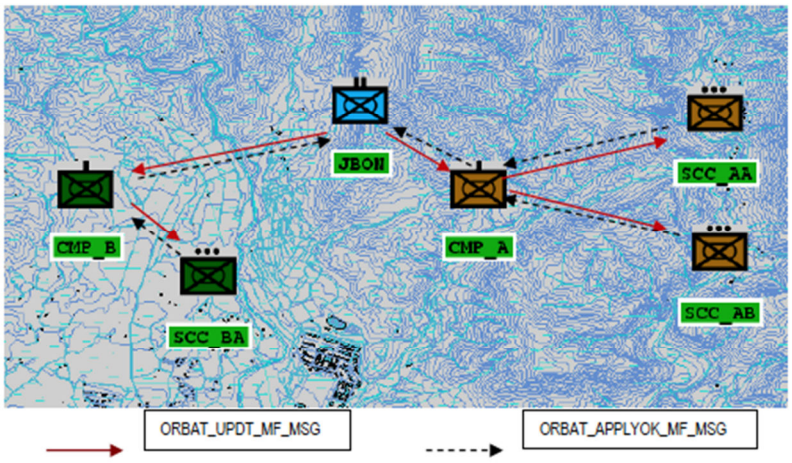

Figura 44. Redistribución del FDM y autoconfiguración intra-nodo

En el caso de una modificación del estado de un enlace, ocurrirá una reconfiguración inter-nodo pero tendremos que diferenciar dos casos: a) Un nodo quiere acceder a una red con un medio de transmisión distinto definido previamente en el FDM y b) un nodo necesita acceder a una red con un medio de transmisión no declarado previamente en el FDM.

En el primer caso, la capa de gestión GI-S monitoriza el estado del medio de transmisión, en el caso de un fallo en el enlace, utilizará el próximo medio de transmisión disponible para contactar a la unidad. Como se explicó previamente, cada medio de transmisión se le asigna un peso en función de su tasa de transferencia, el ancho de banda y el modo dúplex, entre más grande sea este valor, mejor será el canal para comunicación de datos. Además de esto, cada nodo mantiene una matriz que relaciona todos los medios de transmisión activos con las unidades vecinas y los posibles medios de respaldo organizados por peso.

Cuando hay un fallo de enlace, el nodo intentará contactar al nodo vecino a través del siguiente medio de transmisión disponible mediante el envío de una petición CHG_TX_MED_REQ y esperará por la respuesta del tipo TX_CHANGE_RES. El nodo receptor actualizará su base de datos, reiniciara los servicios de replicación hacia la unidad y hará un acuse de recibo TX_CHANGE_RES, de ahora en adelante la comunicación y replicación de datos se realizará a través de este canal. Si el nodo falla en responder al CHG_TX_MED_REQ, la unidad intentará con el resto de medios de transmisión disponible en modo round-robin, hasta que obtenga una respuesta en cualquier de los medios disponibles, la Figura 45, se ilustra este procedimiento.

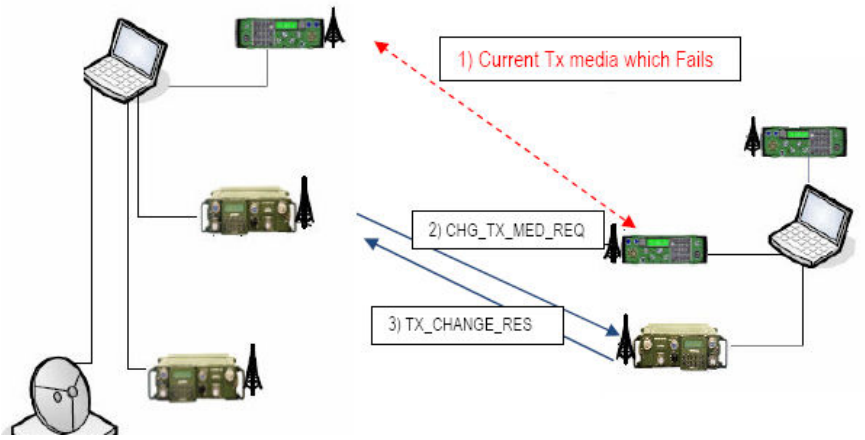

Figura 45. Cambio del medio de transmisión debido a un fallo

La reconfiguración inter-nodo también ocurrirá cuando una unidad quiere acceder a una red con un medio de transmisión diferente no declarado previamente en el fichero de misión, en este caso es necesario que el operador configure todos los detalles necesarios del medio de transmisión como dirección IP, nombre de la conexión, etc. Lo cual actualizará la base de datos local del nodo.

Para continuar el proceso, tenemos que diferenciar entre dos casos, si la unidad está cambiando de medio de transmisión hacia sus subordinados o hacia el nodo superior. En este último caso, el nodo envía una petición JOIN_NET_REQ a través de este nuevo medio de transmisión, a la recepción de este paquete, la unidad superior actualiza su BBDD, reiniciara los servicios de replicación hacia la unidad y hará un acuse de recibo con la respuesta ACCEPT_JOIN_RES de ahora en adelante la comunicación y replicación de datos se realizará a través de este canal.

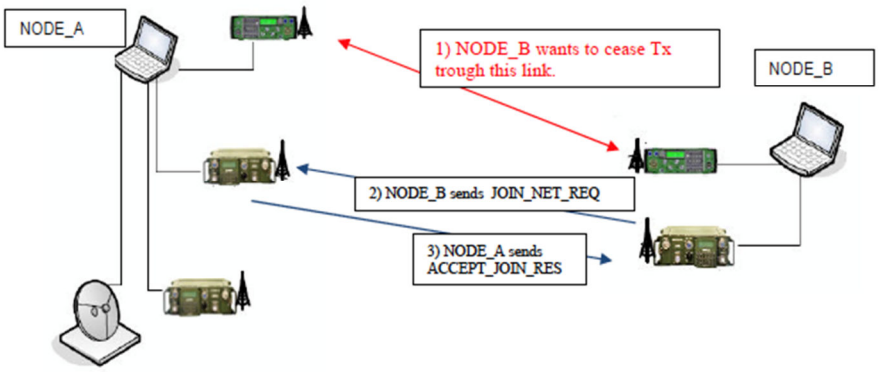

Figura 46. Cambio del medio de transmisión hacia unidades superiores

En el primer caso, es decir, cambio de medio de transmisión hacia unidades subordinadas, asumiendo que al menos uno de los subordinados también el mismo tipo de radio en el nuevo canal de comunicación, la unidad superior enviará un mensaje UPDT_NET_MSG a sus subordinados, el nodo receptor actualizará su base de datos, reiniciara los servicios de replicación hacia la unidad y hará un acuse de recibo con la respuesta APPLYOK_NET_RES, de ahora en adelante la información de réplica y comunicaciones se realizará a través de este canal. Este cambio en la configuración de red, afectará únicamente a los nodos que pertenezcan a esta malla y no se esparcirá por el resto de la red, reduciendo de esta manera el consumo de ancho de banda. La Figura 47 ilustra este proceso.

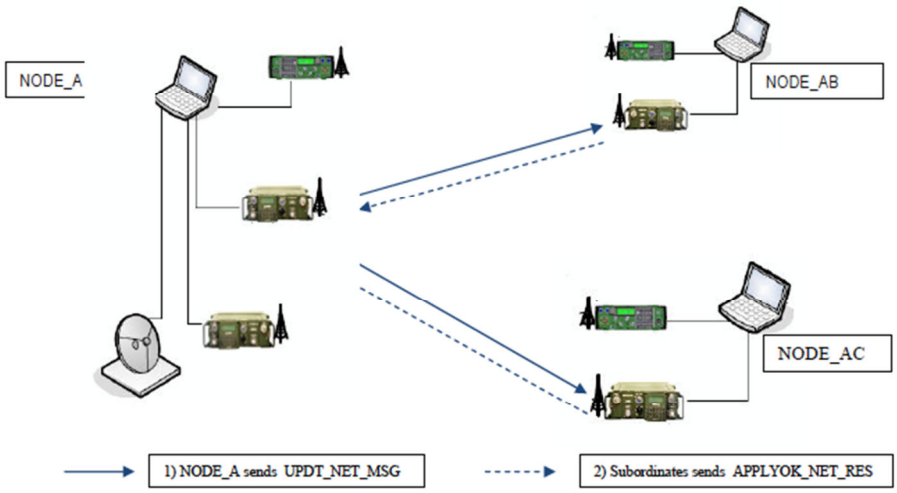

Figura 47. Cambio del medio de transmisión hacia unidades subordinadas

Este último caso pone de manifiesto uno de los principios de diseño establecidos, que es auto-configuración y adaptación a nivel de red a la vez que se mantiene la consistencia a nivel de red.

4.2 Implementación de los módulos de comunicaciones inalámbricas

En cuanto a medios de comunicación Simacop en su versión vehicular incluye distintos módulos de comunicaciones inalámbricas que permiten la interacción con todos los medios de transmisión tácticos actualmente en uso en el Ejército de Tierra, estos son:

- Radios HF Harris 5800
- Radios VHF PR4G V2 y V3.
- Satélites militares en banda X: TLB, TLX y SoTM (Satcom on the move)
- Radios Spearnet de ITT

Simacop en su versión civil (GESTOP) también utiliza medios de comunicación civiles por ejemplo:

- Satélites de cobertura global en banda L: Inmarsat, Iridium y Thuraya
- Tetrapol
- UMTS/GPRS
- Wifi y WiMAX

Cada uno de estos interfaces de comunicaciones ofrece distintas posibilidades para su integración que varían en función del dispositivo, fundamentalmente los servicios disponibles en el sistema C4ISR se ven limitados en función del ancho de banda disponible en cada medio de transmisión.

En adelante cuando nos referimos a una radio de combate táctica IP, por ejemplo radios HF o VHF, hablamos de un dispositivo que implementa las capas física, MAC y DLL del modelo OSI y que ofrece un interfaz IP al cual se puede conectar cualquier dispositivos COTS con interfaz IP.

4.2.1 Caracterización del medio radio

A continuación se detalla un estudio que pone de manifiesto las limitaciones de los medios radios a utilizar en la arquitectura del sistema con solución vehicular. Dicho estudio se llevó a cabo de manera iterativa con el desarrollo y pruebas del sistema y condujo a la determinación de un tipo concreto de algoritmo de réplica y retransmisión de datos.

En concreto para las radios PR4G F@astnet VHF se llevaron a cabo una serie de mediciones para caracterizar las prestaciones que daba el canal radio a la hora de transportar la información de la aplicación. Dichas mediciones se tomaron con una o varias radios, cada una de ellas con una computadora asociada en la que se ejecutaba la aplicación SIMACOP y los servicios de réplica de datos. Todas las radios están, lógicamente en la misma malla PR4G (misma frecuencia y dominio de broadcast). Hay que destacar que los resultados obtenidos con radios Harris 5800 de HF son todavía peores pues el ancho de banda utilizable es menor y el canal es simplex.

Inicialmente se mostrarán medidas de retardos en distintos modos. Todas las medidas se tomaron con las radios estáticas a distancias de 100-200 metros.

En la siguiente figura se observan los retardos para dos radios PR4G IPMUX punto a punto en la misma malla con 10 bytes y 50 bytes de PDU.

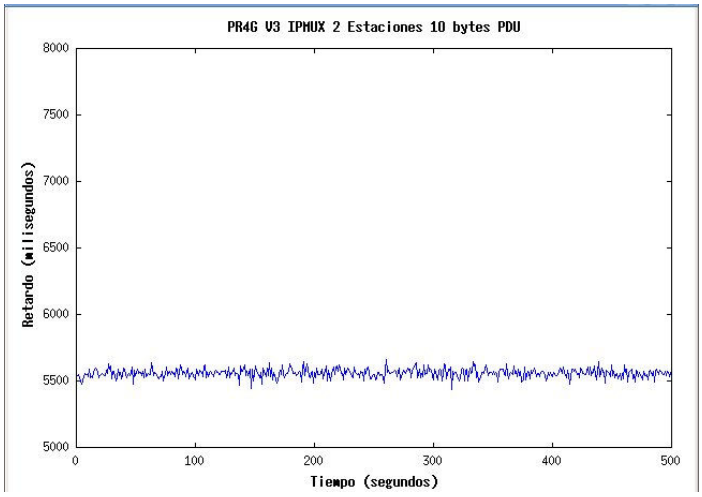

Figura 48. PR4G IPMUX 2 estaciones 10 bytes PDU

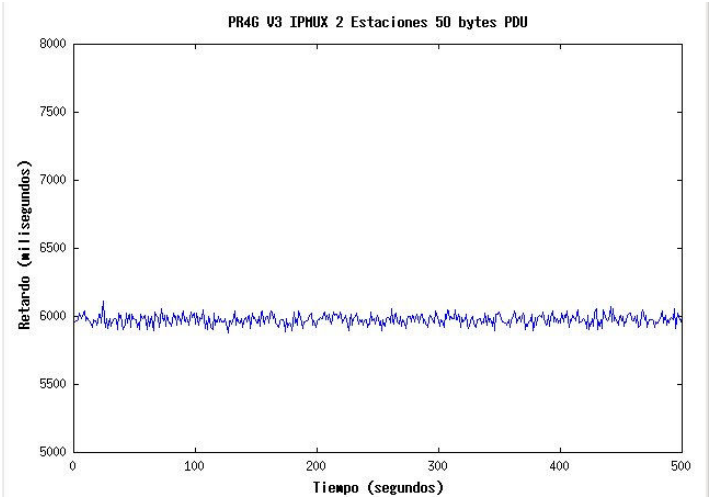

Figura 49. PR4G IPMUX 2 estaciones 50 bytes PDU

Mientras que para una PDU de 100 bytes se obtuvieron los siguientes valores:

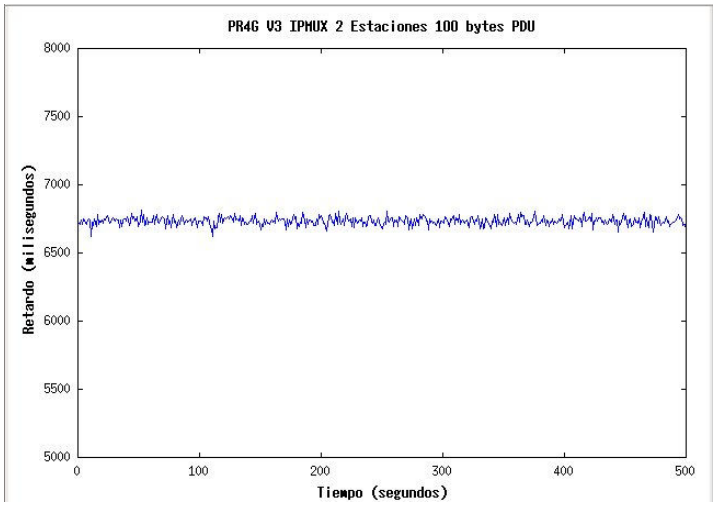

Figura 50. PR4G IPMUX 2 estaciones 100 bytes PDU

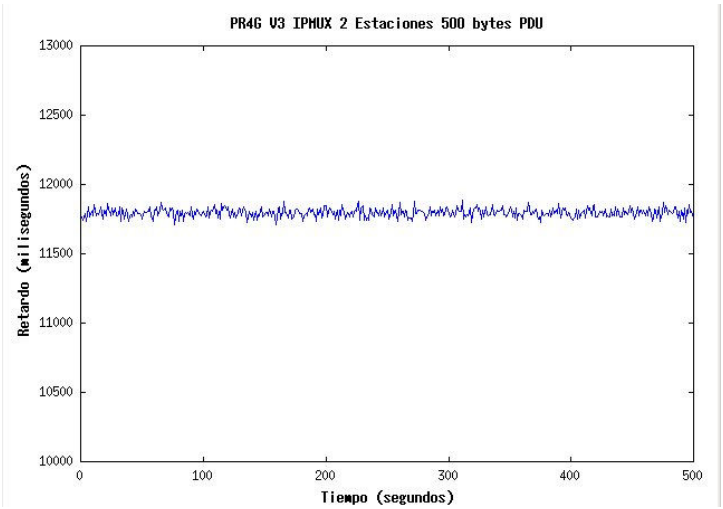

Figura 51. PR4G IPMUX 2 estaciones 500 bytes PDU

Lo expuesto en las anteriores gráficas se puede observar en la siguiente tabla:

	10 bytes PDU	**50 bytes PDU**	**100 bytes PDU**	**500 bytes PDU**
Media retardo en ms	5560,70	5977,38	6737,45	11798,59
Varianza retardo en ms	1123,46	1299,84	937,20	886,02

Tabla 9. Estadísticas de retardo con 2 estaciones PR4G

Para el caso de la configuración de varias radios conectadas una a n, una como directora y las otras como subordinadas se obtuvieron muestras en un escenario de 1 a 3. Las siguientes gráficas muestran los retardos para las mismas configuraciones que en el caso anterior, esto es PDU de 10, 50,100 y 500 bytes.

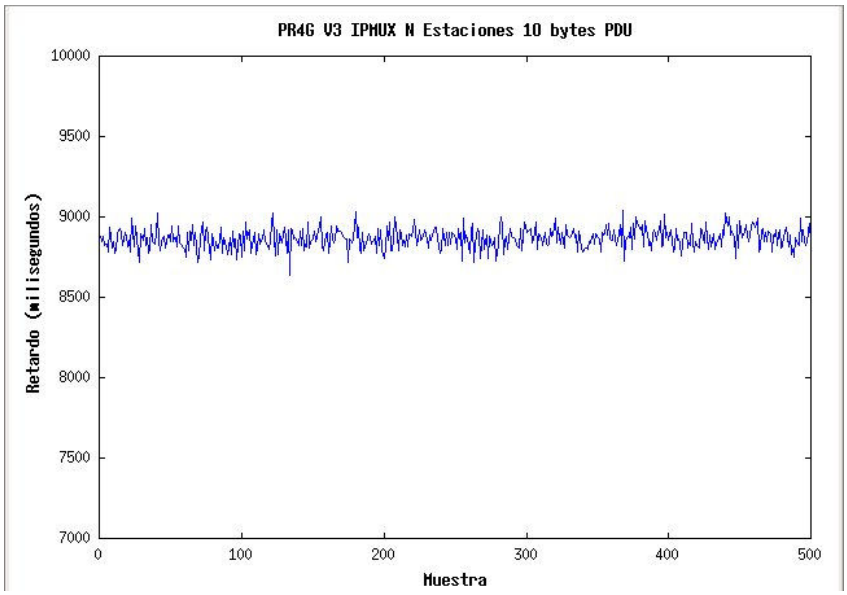

Figura 52. PR4G IPMUX N estaciones 10 bytes PDU

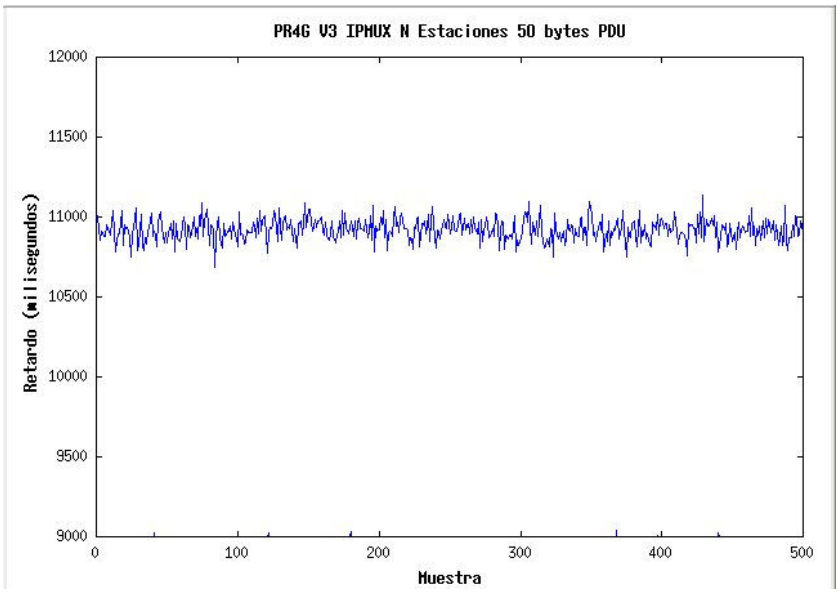

Figura 53. PR4G IPMUX N estaciones 50 bytes PDU

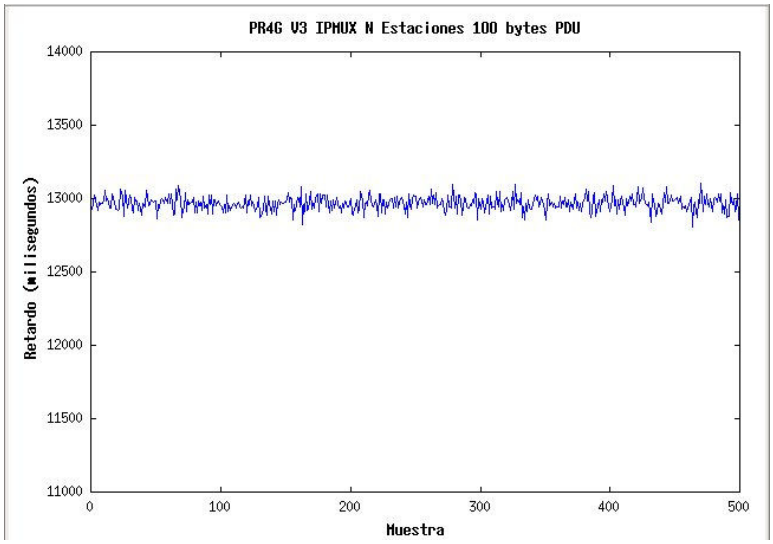

Figura 54. PR4G IPMUX N estaciones 100 bytes PDU

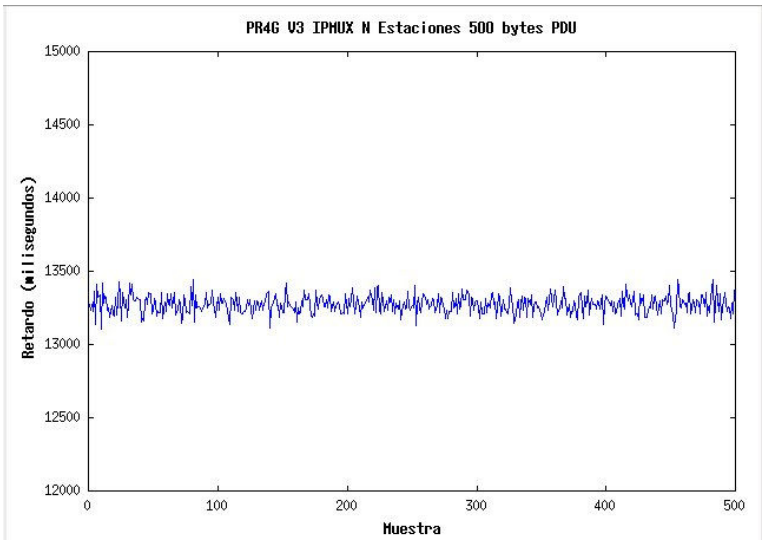

Figura 55. PR4G IPMUX N estaciones 500 bytes PDU

En este caso los estadísticos presentaron los siguientes valores:

	10 bytes PDU	**50 bytes PDU**	**100 bytes PDU**	**500 bytes PDU**
Media retardo en ms	8871,30	10923,50	12966,13	13273,21
Varianza retardo en ms	3561,40	4592,69	2239,36	3542,66

Tabla 10. Estadísticas de retardo para N estaciones PR4G

Respecto al ancho de banda ofrecido por estas radios es de destacar que el ancho de banda medido nunca excedió de 1200bps en modo IPMUX. Existen otros modos de funcionamiento de las radios como por ejemplo IPSAP, y en concreto, los resultados de las medidas, tanto de retardos como de ancho de banda, son algo mejores (40% en ancho de banda y 35% en retardo) pero IPSAP no es viable puesto que no permite simultanear voz y datos.

En las dos siguientes figuras se pueden ver los resultados de ancho de banda para una transmisión en modo IPMUX. En el primer caso sólo hay un flujo de datos en la malla y en el segundo caso el ancho de banda se comparte entre varios.

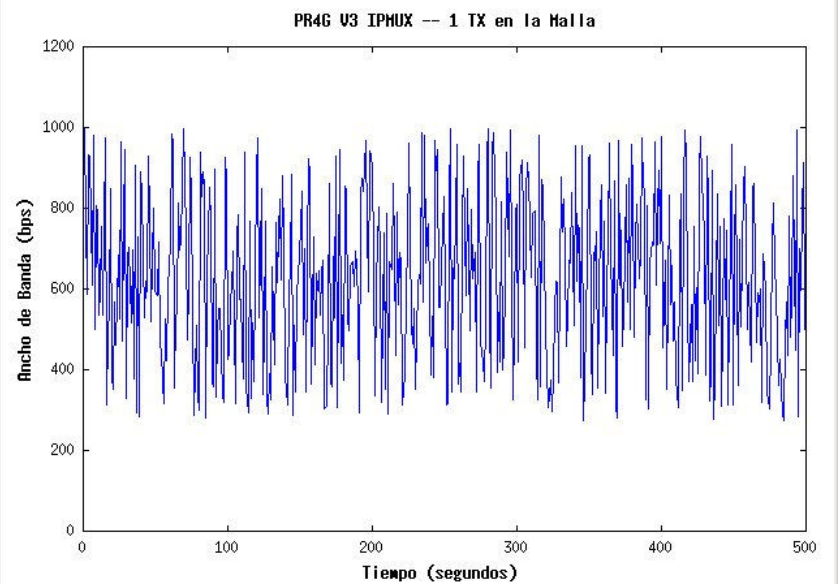

Figura 56. Ancho de banda experimentado (1 transmisión en la malla)

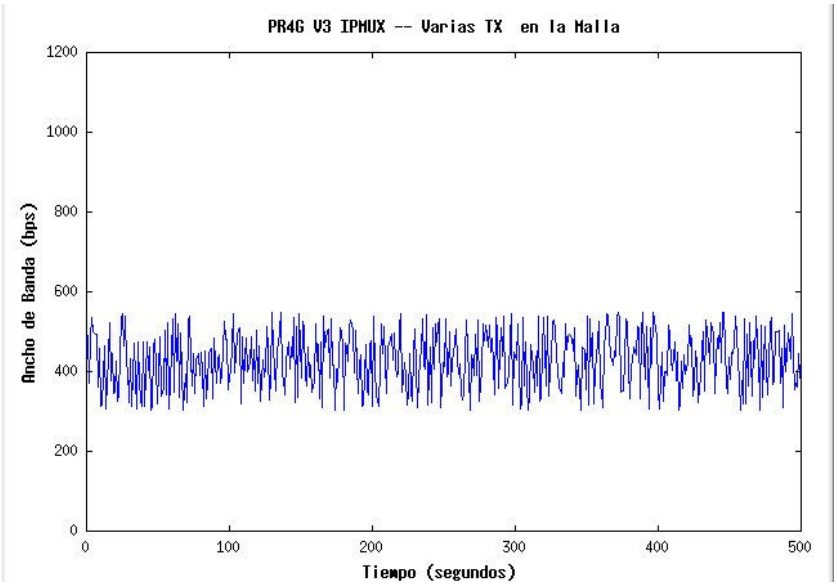

Figura 57. Ancho de banda experimentado (varias transmisiones en la malla)

Como se puede observar los medios de transmisión VHF son extremadamente restrictivos y limitantes para el sistema a desarrollar. Como se ha comentado previamente los medios radios HF y los medios de VHF de anterior generación aún son más limitadores. Estas limitaciones estudiadas, junto con otros requisitos de diseño condujeron a la elaboración de una serie de algoritmos y políticas de replicación de la información entre nodos.

4.2.2 Módulo HF

Este módulo proporciona comunicaciones sobre redes de radio HF. En general las radios HF ofrecen un canal simplex de elevada latencia y polling secuencial en el acceso al canal compartido (lo que conduce a un aumento en la distancia entre slots para el acceso al mismo para una estación conforme aumenta el número de las mismas).

En el caso de solución vehicular se utilizó el dispositivo HARRIS RF-5800H. Este dispositivo aporta diferentes interfaces de datos y control remoto: PPP sobre RS-232 y/o DTE sobre RS-232. Admite STANAG 5066 e incluye ALE (establecimiento Automático de Llamada) de 2ª generación. Incorpora a nivel hardware IP en el aire y protocolo STANAG 4538 y ALE de 3ª generación. Se trata de un canal cuyo ancho de banda no supera los 9600 bps.

Para la integración de esta radio se ha utilizado el interfaz IP que proporcionan las radios por PPP sobre RS-232. A parte de utilizar este interfaz para comunicar los datos del nodo conectado a ellas, también se utiliza para obtener la posición GPS tanto de la radio local, como de las radios remotas en la misma malla de transmisión en caso de que no tengan un nodo de mando y control asociado. La información de posicionamiento GPS se obtiene periódicamente y luego es procesada por el módulo de gestión de sensores y las posiciones resultantes se ingresan en la base de datos para ser distribuidas finalmente por el servicio de réplica de posiciones al resto de nodos.

Estas radios no admiten gestión de QoS en la capa MAC ya que utiliza protocolos propietarios, por lo tanto la QoS se maneja únicamente desde la capa de aplicación con la temporización de cada uno de los servicios que marca la GA-S. Cada uno de los servicios de réplica tiene un slot de transmisión cada T_{REPL} (segundos), que puede variar en función del servicio y del nivel jerárquico del nodo. En la Tabla 11, se recogen los diversos parámetros y temporizadores preconfigurados utilizados para este medio de transmisión, en cualquier caso, estos parámetros son modificables por el usuario desde el GUI, en cuyo caso se aplica un factor de ponderación de acuerdo al nivel jerarquico de la unidad.

Parámetro	Pelotón	Sección	Compañía	Batallón
T_{REPL_alm}	25	30	45	180
T_{REPL_pos}	25	30	45	180
T_{REPL_ao}	120	120	120	120
T_{REPL_MSJ}	240	240	240	240

Tabla 11. Parámetros de réplica para radio HF

En la tabla, el parámetro T_{REPL_alm} hace referencia al período de réplica de alarmas. T_{REPL_ao} representa el período de réplica de amenazas y objetos. T_{REPL_pos} representa el tiempo replica de posiciones. Finalmente T_{REPL_MSJ}, representa el tiempo de réplicas de mensajería de texto

El módulo de comunicaciones HF fue evaluado y validado en diversas pruebas, por nombrar solo una de ellas, pruebas por parte de JCISAT en Abril de 2008. El detalle de los distintos escenarios de pruebas realizadas se puede consultar en el capítulo de validación.

4.2.3 Módulo VHF

Este módulo se implementó sobre radios VHF PR4Gv2 y radios PR4Gv3.

Interfaz de Comunicaciones VHF PR4G v2. Proporciona comunicaciones sobre redes de radio VHF con un ancho de banda de hasta 19200 bps. Dispone de una interfaz de datos RS-232 sobre la que se debe montar la red IP, en este caso únicamente por software.

Interfaz de Comunicaciones VHF PR4G v3. Proporciona comunicaciones sobre redes de radio VHF. Al igual que el dispositivo de comunicaciones HF, dispone de diferentes interfaces de datos (nivel de enlace) y control remoto: PPP, Ethernet, DTE sobre RS-232, etc. A nivel hardware incorpora IP en el aire. Esta interfaz alcanza un ancho de banda de hasta 43000 bps.

Para la integración de ambas radios (PR4Gv2 y PR4Gv3) se ha utilizado el interfaz IP que proporcionan las radios. Al igual que en el caso de las radios HF, aparte de utilizar este interfaz para comunicar los datos del nodo conectado a ellas, también se utiliza para obtener la posición GPS tanto de la radio local, como de las radios remotas en la misma malla de transmisión que no tengan un nodo conectado.

Estas radios no admiten gestión de QoS en la capa MAC ya que utiliza protocolos propietarios, por lo tanto la QoS se maneja únicamente desde la capa de aplicación con la temporización de cada uno de los servicios que marca la GA-S. Cada uno de los servicios de réplica tiene un slot de transmisión cada T_{REPL} que varía en función del servicio y del nivel jerárquico del nodo. Tabla 12 se recogen los diversos parámetros y temporizadores preconfigurados utilizados para este medio de transmisión, en cualquier caso, estos parámetros son modificables por el usuario desde el GUI, en cuyo caso se aplica un factor de ponderación de acuerdo al nivel jerarquico de la unidad.

Parámetro	Pelotón	Sección	Compañía	Batallón
$T_{REPL\ alm}$	15	20	35	160
$T_{REPL\ pos}$	15	20	35	160
$T_{REPL\ ao}$	120	120	120	120
$T_{REPL\ MSJ}$	240	240	240	240

Tabla 12. Parámetros de réplica para radio VHF

El módulo de comunicaciones VHF fue evaluado y validado en diversas pruebas, por nombrar alguna de ellas, pruebas por parte de JCISAT en Abril de 2008, así como por del Regimiento de Caballería Ligera Lusitania 8 en el campo de maniobras de Chinchilla, Albacete en Mayo de 2008. Los detalles de las pruebas realizadas se pueden consultar en el capítulo de validación.

4.2.4 Módulo UHF

Este módulo se probó sobre radios personales Spearnet de la empresa ITT, las cuales operan en la frecuencia militar de 1.2 GHz con un ancho de banda máximo de 1Mbps, en este caso las radios no sólo se utilizaron como medio de comunicación sino como dispositivo computacional, ya que cuentan con un sistema operativo Linux con kernel 2.6.11 basado una distribución desarrollada a partir de busybox [BUS1] sobre un procesador ARM PAX 270. Sobre el cual se empotro: el servidor de GPS, la gestión del streaming de video (pues la codificación, en esta ocasión, se llevó a cabo en cámaras IP de la empresa Axis), la codificación de voz y la gestión de todos estos flujos.

Con estás radios se pudo estudiar con mayor profundidad las capacidades de la redes MANET ya estas radios poseen toda una serie de funcionalidades extra que no se pueden encontrar en medios que implementen 802.11 en modo ad-hoc, 802.11s o tecnologías mesh estándar. En concreto, un interfaz radio, sin estar conectado a una computadora, ya sea un PC, un SBC o el equipo embebido que llevan las radios, simplemente con ser alimentada eléctricamente empieza a enviar paquetes por el medio radio para descubrir qué otros nodos con el mismo interfaz están próximos, establece tablas de rutas a los mismos y monta toda una infraestructura de red, mediante el envío de paquetes propietarios en capa 2 ISO/OSI. Esto permite liberar a las capas superiores de dichas responsabilidades y resulta extremadamente eficiente en el descubrimiento de la red y ágil en la reconfiguración.

Otras dos ventajas asociadas a lo descrito de esta tecnología de radio son la capacidad de actuar como relay de las radios y la subsiguiente extensión lineal del rango de comunicaciones y la ganancia en robustez al proporcionar multicamino. La funcionalidad de relay es muy útil en general pero muy particularmente para operaciones tácticas muy concretas como pueden ser las llevadas a cabo por cuerpos de bomberos o las propias de enfrentamientos en entornos urbanos. En muchas de las operaciones de ambos casos el despliegue de los operativos se lleva a cabo sobre una línea recta por ejemplo en subterráneos, calles estrechas, etc. donde además cada intersección puede suponer serios obstáculos para la propagación radio. Esta funcionalidad permite que la unidad más avanzada sólo precise conectividad radio con otra próxima que retransmitirá todas sus comunicaciones con el resto de unidades en la malla y hacia el mundo exterior.

A nivel de QoS dado que estas radios sí que implementan una pila TCP/IP completa es posible utilizar la solución completa de QoS cross-layer propuesta en la arquitectura, de manera que aparte de mantener los temporizadores de transmisión de datos también se clasifican los paquetes IP por el campo DSCP, luego los valores del campo DSCP se mapean a valores CoS y son asignados a 4 colas o clases de acceso predefinidas una para tráfico de vídeo (WME_AC_VID), una para audío (WME_AC_VOI), una para tráfico de alramas (WME_AC_ALM) y otra para tráfico de mensajes, posiciones GPS, amenazas y objetos (WME_AC_BE). En este caso, el módulo de marcado QoS, mostrado en la arquitectura, se basa en la utilización de herramientas de 'traffic control' y 'traffic shaping' en Linux, tanto a nivel de kernel como a nivel de espacio de usuario. El esquema de colas de prioridad por nodo es el siguiente:

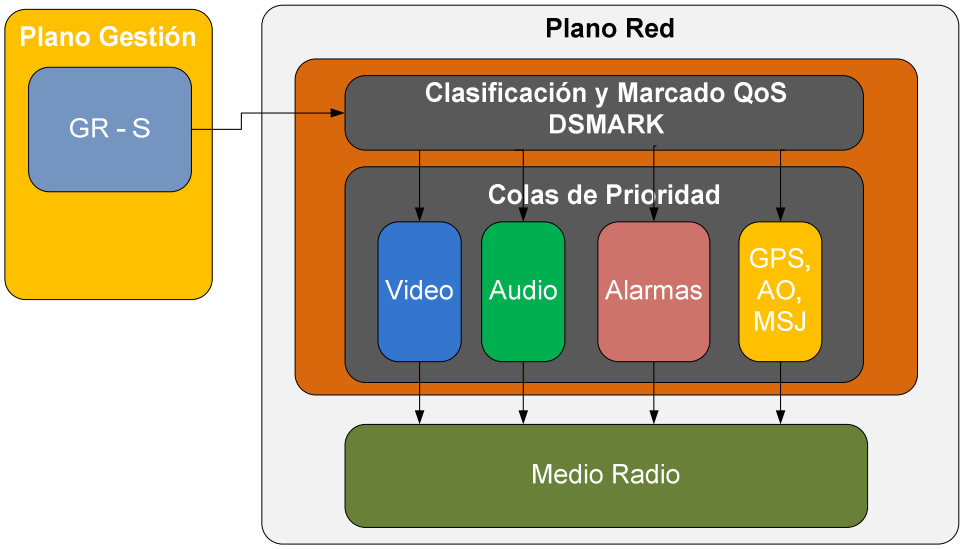

Figura 58. Colas de prioridad en la solución mallada

Con una prioridad decreciente de izquierda a derecha. Para dicha aproximación la descripción de las colas se puede ver en el siguiente script:

```
#!/bin/sh

tc qdisc del dev mea0 root

tc qdisc add dev mea0 handle 1:0 root dsmark indices 64



tc class change dev mea0 classid 1:1 dsmark mask 0x3 value 0x98 #audio

tc class change dev mea0 classid 1:2 dsmark mask 0x3 value 0x90 #GPS

tc class change dev mea0 classid 1:3 dsmark mask 0x3 value 0x88 #video
```

```
tc class change dev mea0 classid 1:4 dsmark mask 0x3 value 0x0 #otros flujos GPS,


tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dport 2000 0xffff flowid 1:1
tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dport 2001 0xffff flowid 1:1
tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dport 2002 0xffff flowid 1:2
tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dport 2031 0xffff flowid 1:3
tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dport 2004 0xffff flowid 1:2
tc filter add dev mea0 parent 1:0 protocol ip prio 1 u32 match ip dst 10.0.0.0/8 flowid 1:2
```

Tabla 13. Colas de prioridad en la solución desambarcada integrada en radios UHF de ITT

Esta priorización de los distintos flujos transmitidos se reforzó con la priorización de los procesos que los gestionaban, dentro del sistema operativo en cada nodo. De esta forma el proceso servidor de vídeo tenía una mayor prioridad que procesos que transmitían paquetes no prioritarios. Es de destacar que en las versiones del kernel 2.6, si se compilan con la opción RT_SCHED, permiten muchas facilidades de soft real time, así como una mayor predictibilidad en las llamadas al sistema, funcionalidad que también se implementó en esta versión.

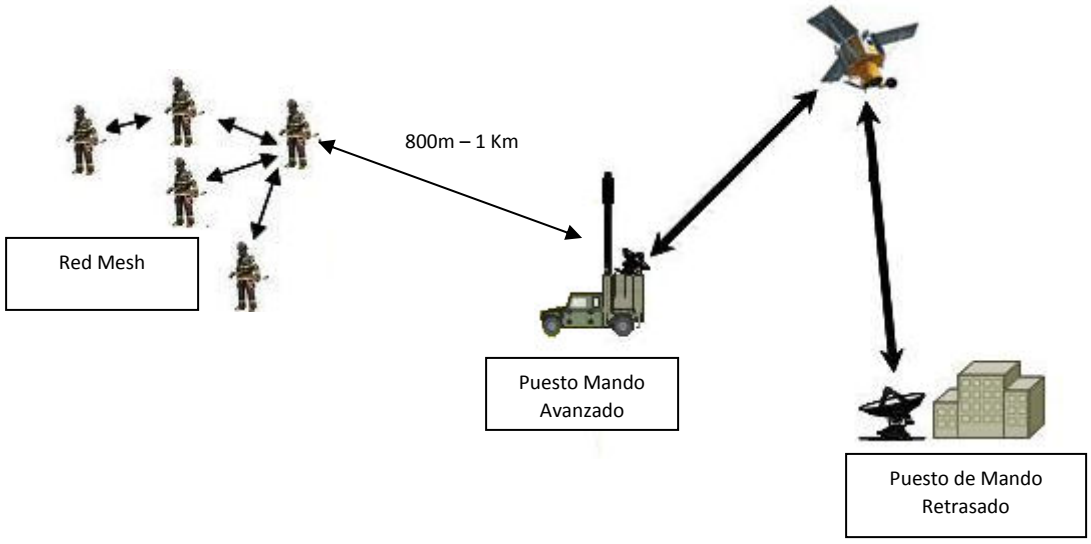

Figura 59. Topología de red Típica con red mallada en UHF

Esta arquitectura fue probada en Mayo de 2007 en el cuartel general de la Unidad Militar de Emergencias (UME) en una demostración conjunta con la empresa ITT, cuya topología de red mallada se muestra en la Figura 59. El mismo prototipo, pero utilizando tecnología mesh mediante tarjetas civiles del fabricante Motorola en banda de 2.4 GHz y SBC, es decir sin empotrar el software en las radios, fue el empleado en las pruebas de CWID08 nacional con la guardia civil. Estos puntos quedan reflejados en el capítulo de validación.

4.2.5 Módulo de comunicaciones satelitales

Este módulo se ha probado sobre terminales BGAN de Inmarsat, teléfonos satelitales Thuraya e Iridium así como satélites militares en banda X. En este caso, el ancho de banda es variable y dependiente del dispositivo. Además cada dispositivo utiliza diferentes interfaces de integración a nivel de enlace y físico, como por ejemplo Ethernet y RS-232 respectivamente.

En el caso de los satélites, dado que algunos son satélites civiles es necesario que la arquitectura solucione dos inconvenientes, en primer lugar, la asignación de direcciones IP es muchas veces dinámica y no controlable por el administrador, por lo general la IP cambia cada vez que se restablece la comunicación por un fallo de conectividad, esto puede ocurrir muy frecuente sobre todo con teléfonos satelitales como Thuraya en zonas de poca cobertura. En segundo lugar, al tratarse en varios casos de satélites comerciales es necesario cifrar todos los datos que transitan por este medio.

Para solucionar este problema, la arquitectura propuesta incluye un módulo de VPN y cifrado de datos, el cual se activa desde la capa GR-S, cuando desde el interfaz de usuario o desde el fichero de misión se añade un medio satélite, es módulo designa a uno de los nodos como el maestro del clúster a nivel de VPN y el resto como clientes, el maestro establece un túnel VPN para las comunicaciones que mantiene las IP para cada uno de los equipo que se une al túnel y además cifra las comunicaciones extremo con AES-256.

El uso de satélites bien sea comerciales o militares permite crear un gran número de topologías de red, por ejemplo enlaces punto a punto, en estrella (punto a multipunto) o hub and spoke, con un ancho de banda suficiente para incluir flujos de vídeo en el sistema de mando y control. Esto permite implementar y validar el concepto NEC (Network Enabled Capabilities) de "Sensor en la red". Expliquemos mejor este último concepto, por lo general, cada sensor en el campo de batalla se asocia a la plataforma de armas que hace uso de ella. Sin embargo, en la visión NEC de mando y control, los sensores aprovechan el alto grado de conectividad de red disponible y ya no están vinculados a una plataforma en particular, sino que están disponibles para cualquier sistema que necesite y quiera hacer uso de ellos en cada momento. Este paradigma de gestión de información se conoce como "Post and Smart Pull".

Esto módulo de la arquitectura fue probado exitosamente en Mayo de 2007 en el cuartel general de la Unidad Militar de Emergencias (UME) y en el escenario de pruebas de las EPCIS en 2009. El detalle de las pruebas realizadas se puede consultar en el capítulo de validación.

4.2.6 Módulo Wireless LAN 802.11

Este módulo se ha probado sobre redes IEEE 802.11g y 802.11a, las cuales operan en la frecuencias de 2.4 GHz y 5GHz respectivamente, con un ancho de banda máximo de 54Mbps. Para la prueba se ha desarrollado un prototipo del bucle Puesto de mando y control (1er escalón) ⇔ operativo y posterior interconexión entre puestos de mando. El prototipo implementa las redes PAN y red de campo/combate así como la red táctica pero con tan sólo una malla para la interconexión de puestos de mando. Dicho prototipo fue probado y evaluado en mayo de 2006, dentro de las pruebas CWID'06. Este prototipo fue el principal resultado del proyecto del plan nacional de I+D TIN2004-03588.

Dicho prototipo entrega los flujos de:

- Posición GPS (1 muestra/segundo)
- Señales biomédicas:
  - electrocardiograma (100 muestras/segundo)
  - temperatura (1 muestra/segundo)
- Vídeo en perspectiva subjetiva a 25 frames por segundo.
- Audio (mpeg1, mpeg4)

Este prototipo, mostrado en la Figura 60, utiliza como hardware un SBC (Single Board Computer) en los nodos operativos que recopila la información de sensores GPS, audio y cámara de vídeo, todos ellos COTS, conectados mediante Bluetooth, constituyendo la PAN. El jefe de la brigada de rescate lleva consigo una PDA para conocer en cada momento la posición de los miembros de su

brigada. Por otro lado, los distintos SBC se interconectan entre ellos y al puesto de mando y control mediante interfaces 802.11a/g y, como puede verse en la figura, mediante un punto de acceso con antena externa de ganancia añadida, para aumentar las coberturas.

Los flujos obtenidos de los sensores son procesados en el SBC para elaborar y estructurar la información que se precisa: se obtienen latitud, longitud y se codifica el vídeo y el audio. En el puesto de mando y control, los flujos se sincronizan y la información se elabora a más alto nivel para entregar la visión del teatro de operaciones a la aplicación de mando y control.

Toda la información sensorizada se recoge en bases de datos pudiendo ser utilizada para propósitos de análisis post-operación. Evidentemente esto supone un gran volumen de información por lo que se establecen filtros para discriminar la información que se debe almacenar permanentemente y la que se descarta tras caducar su vigencia.

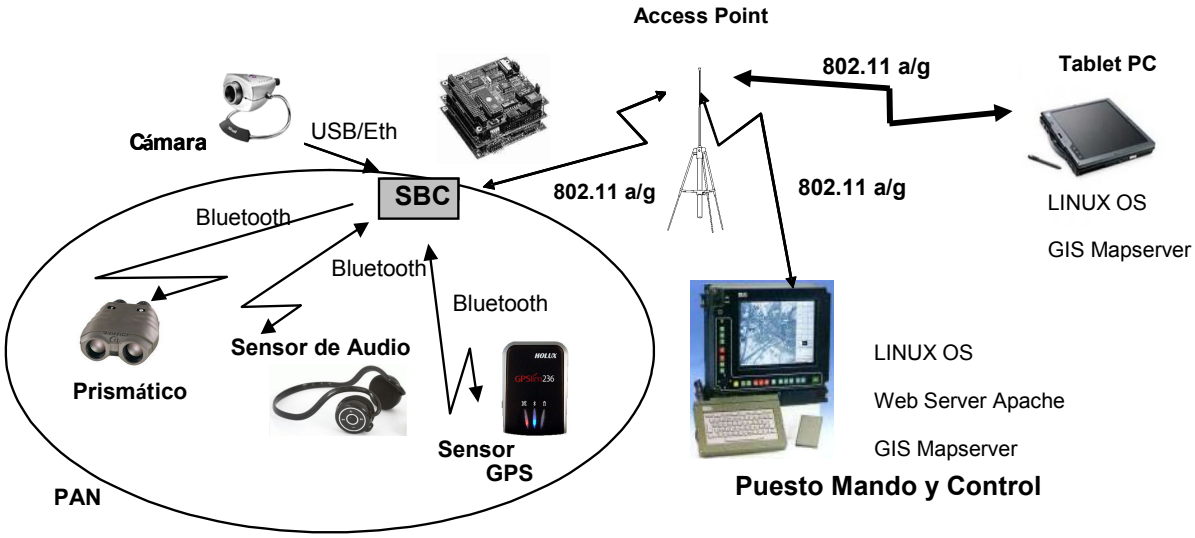

Figura 60. Implementación del módulo IEEE 802.11 sobre solución basada en SBC

A nivel de QoS, el prototipo del SBC con comunicaciones wifi, donde el SBC actúa como nodo de procesado y como dispositivo de comunicaciones, sí que es posible utilizar la solución completa de QoS cross-layer propuesta en la arquitectura, de manera que aparte de mantener los temporizadores de transmisión de datos también se clasifican los paquetes IP por el campo DSCP, luego los valores del campo DSCP se mapean a valores CoS y son asignados a 4 colas o clases de acceso predefinidas una para tráfico de alarmas (WME_AC_ALM), una para amenazas y objetos (WME_AC_AO), una para tráfico de posiciones GPS (WME_AC_GPS) y otra para tráfico de mensajes (WME_AC_MSJ). Los valores utilizados para el marcado se muestran en la Tabla 14.

Aplicación	Clasificación a Nivel 3 (DSCP)	Clasificación a Nivel 2 (CoS)
Alarmas	EF	5
Amenazas y Objetos	AF41	4
GPS	AF11	1
Mensajes y Resto de Trafico	0	0

Tabla 14. Valores DSCP y CoS usados para la clasificación por QoS del tráfico generado.

Cada una de estas clases de acceso tiene valores diferentes para la ventana de contención, oportunidad de transmisión, etc. Estos valores se utilizan para determinar el tiempo de back off para cada paquete. Como regla general, los paquetes con mayor prioridad tienen periodos de

back off más cortos. Los valores elegidos para los campos ventana de contención mínima y máxima y tiempo de trama se muestran en la Tabla 15.

Clase de Servicio	Ventana de Contención Min	Ventana de Contención Max	Fixed Slot Time	Oportunidad de Transmisión
Background	4	10	6	0
Best Effort	4	10	2	0
Video <100ms Latencia	3	2	1	3008
Voice <100ms Latencia	2	3	1	1504

Tabla 15. Valores de configuración de AC en el SBC.

4.2.7 Módulo MESH.

Este módulo se ha probado sobre terminales tarjetas Motorola WMC 6300, estas tarjetas trabajan en la banda de 2.4GHz y tienen un ancho de banda efectivo de 1Mbps e implementa un protocolo propietario para formar la red Mesh.

El módulo también se ha probado sobre radios BreadCrumb JR de Rajant Corporation, las cuales utilizan el estándar de red 802.11g para formar una red de inalámbrica mallada auto-configurable, full-duplex, flexible y segura. Estas radios operan en la banda de frecuencia de 2,4 GHz y utilizan por defecto el canal 11 (2462 MHz). Estos dispositivos adicionalmente cuenta con una interfaz Ethernet 10/100 Base-TX e interfaz de datos GPS.

Figura 61. Access Point Rajant: BreadCrumb_JR

Estas radios cuentan con un ancho de banda de 54Mbps. Gracias al ancho de banda disponible es posible integrar en el sistema de Mando y Control, servicios de VoIP para la comunicación entre los miembros del equipo y vídeo subjetivo desde las unidades en el teatro de operaciones, lo cual ayuda a mejorar la conciencia situacional y la toma de decisiones.

La solución de QoS es similar a la utilizada en redes Wlan 802.11 y descrita en el punto anterior. En Enero de 2013 se realizó una exitosa prueba de campo con estas radios para validar la arquitectura de comunicaciones propuesta, en este escenario así como sus resultados obtenidos se describen en el capítulo de validación.

4.2.8 Módulo WiMAX 802.16d

Tal como se ha visto hasta el momento en el desarrollo de la tesis, las capacidades de los sistemas de transmisiones tácticas impiden en la práctica la integración de servicios de voz, vídeo y datos. La tecnología de redes de datos inalámbricas WiMAX permiten la integración de estos servicios de forma eficiente, dando soporte a las necesidades de los modernos sistemas de información para mando y control, C4ISR.

En el mercado existen algunos productos WiMAX con características de aplicación táctica. Entre ellos destaca el producto de Tadiran. Sin embargo, estos productos están concebidos para interconectar puestos de mando de grandes unidades, hasta división, en el caso de Tadiran. Su uso en el campo de las pequeñas unidades, o unidades que combaten (brigada, batallón e inferiores), no está contemplado.

Los tres componentes fundamentales del sistema propuesto son (ver Figura 62):

- Hardware de estación base (BS)
- Hardware de estación suscriptora (SS)
- Aplicación de gestión, que se ejecuta de forma distribuida en la BS y en las SS

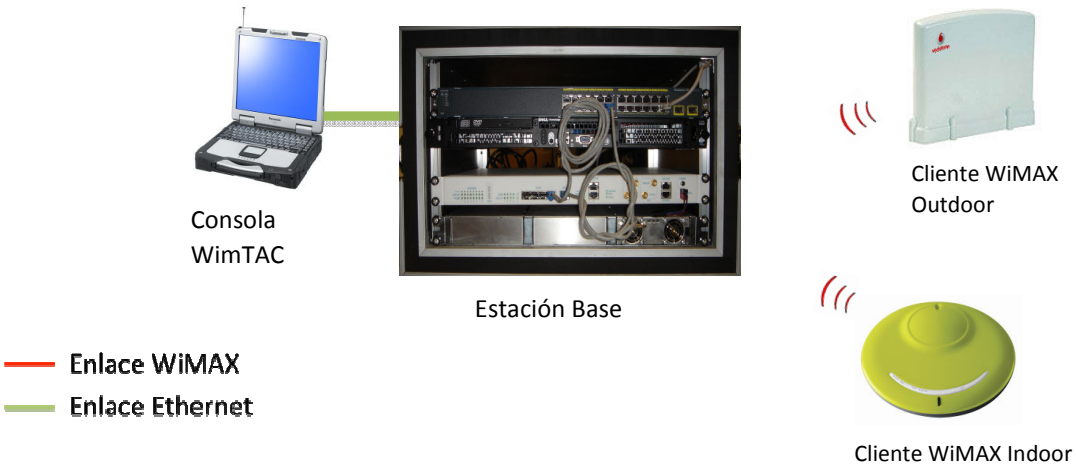

Figura 62. WimTAC: Componentes del sistema

La estación base de WiMTAC no debe entenderse como un centro nodal tradicional. Por una parte aporta las capacidades y funciones propias de una estación base o punto de acceso de red inalámbrica (como las estaciones base de UMTS, GSM o WiFi), recogidas en el correspondiente estándar IEEE 802.16. Pero por otra, su concepción táctica, hace que se prime en el diseño de la arquitectura características fundamentales como la ligereza, la movilidad, la seguridad y el soporte a los servicios de los sistemas C4ISR.

Algunas aplicaciones funcionales de un sistema como WiMTAC serían:

- Interconexión de puestos de mando de nivel brigada con nivel batallón
- Interconexión de puestos de mando de nivel batallón con niveles inferiores, compañía y sección
- Cobertura WiMAX de un puesto de mando de gran unidad tipo división o cuerpo de ejército
- Soporte a sistemas de seguimiento de fuerzas propias, FFT, a nivel de vehículos o plataformas finales de combate, a nivel de combatiente individual formado parte de un

sistema como SIMACOP de la UPV, o como burbuja móvil WiMAX en conjunción con un sistema SATCOM "on the move".
- Soporte de comunicaciones para sensores terrestres o aéreos (UAVs)
- Interconexión de alta capacidad punto-multipunto entre radares, sistemas de control de fuego o de tiro y baterías antiaéreas (misiles y cañones AA)
- Cobertura inmediata en operaciones costeras (desembarcos anfibios) o a instalaciones portuarias
- En el ámbito civil sería utilizable en la zona de una emergencia en ausencia de otros medios de comunicación o en grandes concentraciones o eventos para dar conectividad inmediata y de alta capacidad a vehículos de policía local, bomberos, protección civil o personal sanitario

WiMTAC aporta los siguientes beneficios:

- Extrema ligereza que le confiere un marcado carácter táctico que permite su uso en el ámbito de las pequeñas unidades, particularmente en el entorno militar en escenarios de guerra asimétrica en entorno urbano o en el ámbito civil para gestión de emergencias en ausencia de otros medios de comunicación.
- Aplicación de gestión extremadamente sencilla que posibilita su utilización por personal cuya especialidad fundamental no necesariamente tiene que ser Transmisiones.
- Capacidad para integrar servicios de voz, vídeo y datos, soporte fundamental de sistemas C4ISR, dando conectividad a redes de sensores visuales y numéricos, terrestres (sensores "stand alone", montados o manejados por observadores avanzados y combatientes individuales, o bien sobre vehículos) o aéreos como UAVs.

WimTAC integra una herramienta de configuración y gestión para redes WiMAX, especialmente diseñada para ser usada en entornos tácticos, convirtiéndose en el complemento perfecto para la red misma.

La aplicación de gestión de WimTAC proporciona un interfaz simple e intuitivo, especialmente diseñado para uso en el teatro de operaciones, que permite la configuración de estaciones base y CPEs, en función de las necesidades operativas. WimTAC se centra en la usabilidad y en facilitar tareas administrativas en esencia complejas.

El desarrollo de WimTAC está basado en un framework de gestión de red basado en políticas (PBNM, por sus siglas en ingles Policy-Based Network Management). En un framework de gestión basado en políticas, el gestor traduce tareas de gestión complejas en una colección de políticas de alto nivel que proporcionan la monitorización de la red y producen automáticamente las acciones apropiadas. En general, las políticas se definen mediante reglas Evento – Condición – Acción (ECA), por ejemplo, durante el evento E, si la condición C es verdadera, entonces se ejecuta la acción A. Esto encaja con bucle de control Sense-Analyze-Adapt que forma el bloque constituyente de un sistema de gestión de red (NMS) adaptativo. Además las políticas no hacen referencia a un dispositivo en específico y solo hacen referencia a la acción a realizar ante un conjunto EC. Esto permite al agente poner en contexto su entorno y decidir la mejor forma de cumplir con una política dada.

Al combinar la gestión de red basada en políticas con la conciencia del contexto (context-awareness), el framework PBNM, no solo permite trasladar la intención del mando en políticas de gestión de red, sino que también proporciona la capacidad de emular el proceso cognitivo humano al percibir eventos y actuar sobre ellos de acuerdo a las órdenes.

Por esta razón, se ha decidido utilizar el Framework PBNM ya que refleja los conceptos naturales de mando y control que se pueden encontrar en entornos tácticos y se convierte de esta manera en una solución adecuada para implementar la gestión sobre un red WiMAX táctica con nodos muy

distribuidos que se adaptan automáticamente a las condiciones cambiantes del entorno, complementando de esta manera las operaciones a nivel táctico.

WimTAC está implementado como un sistema de gestión basado en XML que consta de: 1) Un gestor XML que implementa un Framework PBNM, 2) Agentes SNMP distribuidos tanto en la BS como en la SS, 3) Consola WimTAC que es la aplicación de escritorio desde la cual se gestiona toda la red. En la Figura 63, se puede ver la arquitectura de gestión implementada en WimTAC.

El gestor NMS Wimtac se ejecuta sobre Windows Server y en él reside la base de datos de service flows, la cual contiene los perfiles de transmisión y la información de calidad de servicio asociada que tienen que ser asignados tanto a la BS como a los SS cuando se les dota de servicio, o cuando un SS entra en la zona de cobertura de la BS. También implementa un gateway que cuenta con dos interfaces uno hacia la red WiMAX y a través del cual recoge y almacena los objetos gestionados en el formato de la WirelessMan Interface MIB y la wmanDevMib (802.16f) a través de SNMP tanto de la BS como de los SS, y por el otro interfaz expone los métodos de configuración, consulta y alertas de la red WiMAX a través de un Web Service SOAP. Por lo tanto, el NMS actúa como traductor de las políticas de configuración que recibe desde la consola WimTAC a primitivas SNMP y perfiles de transmisión que serán distribuidos a los distintos elementos de la red WiMAX.

La consola WimTAC es una aplicación de escritorio que funciona sobre sistemas operativos Windows XP o superior. Los administradores se pueden conectar directamente a la BS o remotamente a través de un ordenador conectado a la red WiMAX. Las funcionalidades principales ofrecidas por WimTAC son:

- Gestión de la configuración de la estación base (BS) y de las estaciones subscriptoras (SS). La cual permite:
  - Generar una lista de los sectores de trasmisión configurados en la BS
  - Generar una lista de los perfiles de transmisión (Service Products) de la BS
  - Generar una lista de las configuraciones de los clientes WiMAX (SS) registrados en la estación base WiMAX
  - Generar una lista de las VLANs presentes en la estación base WiMAX
  - Generar una lista de los perfiles de VLANs para clientes WiMAX (SS) presentes en la estación base WiMAX
  - Obtener el estado de aprovisionamiento de una estación subscriptora (SS)
- Distribución de distintos tipos de tráfico en la red WiMAX. La cual permite:
  - Distribuir un perfil de transmisión (SP) a una estación subscriptora (SS)
  - Activar / Desactivar los servicios de transmisión de una estación subscriptora (SS) que se registra en cualquier sector de la BS WiMAX
  - Eliminar un perfil de transmisión (SP) de una estación subscriptora (SS)
- Gestión de fallos en la estación base (BS). La cual permite:
  - Generar un listado completo de las alarmas activas en la BS
  - Validar una alarma activa en la estación base (BS) WiMAX
  - Eliminar una alarma activa en la estación base (BS) WiMAX
  - filtrar las alarmas activas en la estación base (BS) WiMAX en función del sector de transmisión de la estación base (BS)
  - filtrar las alarmas activas en la estación base (BS) WiMAX en función de la mac de la BSDU (Base Station Distribution Unit)
  - filtrar las alarmas activas en la estación base (BS) WiMAX en función de la hora y/o fecha en que se generaron
- Consultar la topología de red activa

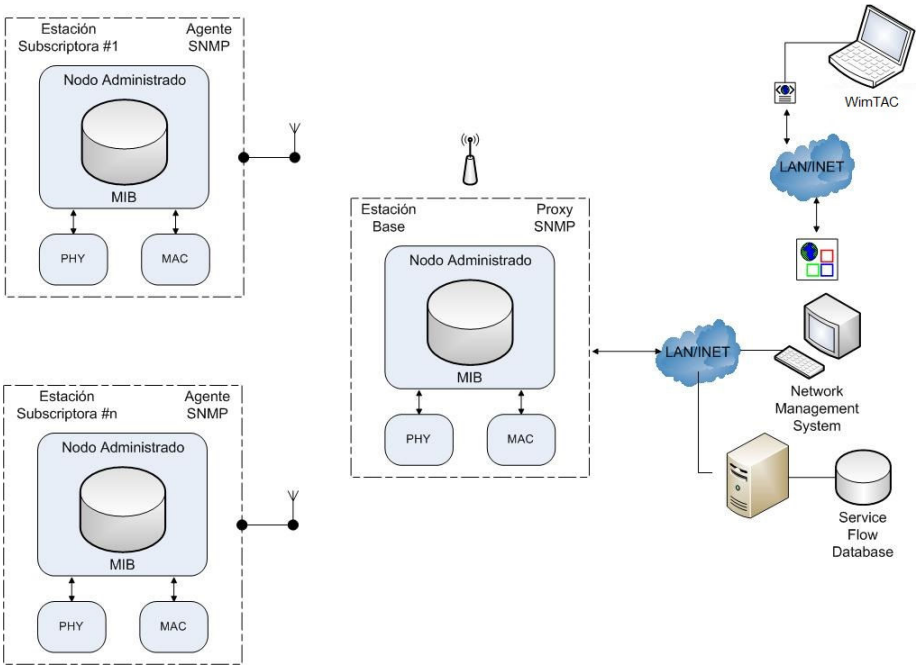

Figura 63. WimTAC: Arquitectura de gestión

En la Figura 64 se puede ver la pantalla principal de la aplicación WimTAC, tal como se puede ver se trata de un interfaz de usuario extremadamente simple e intuitivo, donde toda acción está claramente separada de otra y como máximo a la distancia de dos clics. El interfaz está pensado para ser usado por operadores civiles o militares con conocimientos básicos de WiMAX en condiciones muy adversas, ya sean estas escasa visibilidad, golpes y saltos bruscos, dificultad para pulsar teclas o botones, etcétera.

Figura 64. WimTAC: Interfaz de usuario

En la Figura 65, se puede ver la vista de topología que muestra el software una vez se han registrados distintos clientes (SS) en la BS.

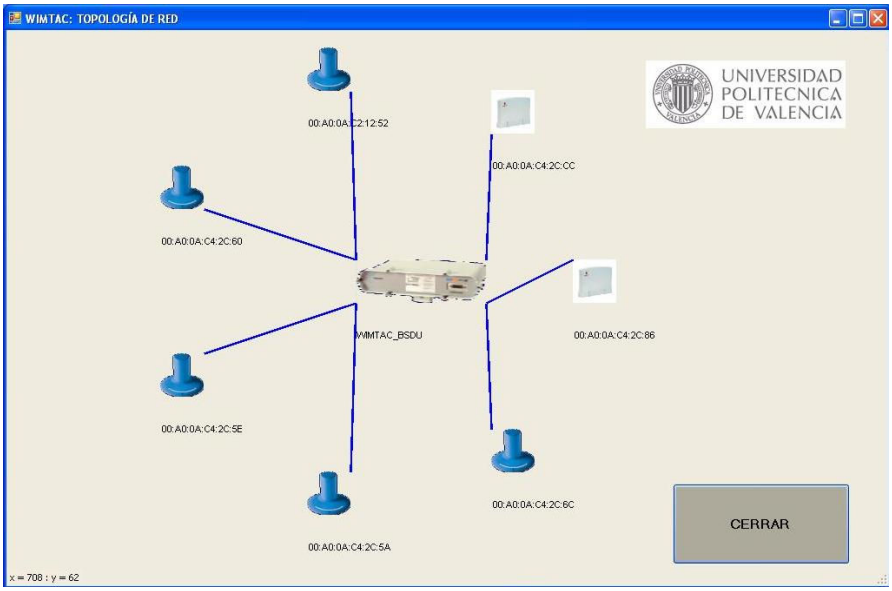

Figura 65. WimTAC: Vista de topología con varias SS registradas en BS

Tal como se ha comentado previamente un posible escenario de uso de WimTAC en el ámbito militar sería la interconexión de puesto de mando nivel batallón/compañía con puestos de mando de nivel sección, es decir, proporcionar una WMAN basado en WiMAX, la estación base podría estar en el propio vehículo de puesto de mando de batallón/compañía, que a su vez, de forma ideal podría dar conectividad "reach-back" a un puesto de mando retrasado mediante un terminal SATCOM.

Las estaciones suscriptoras estarían montadas sobre los vehículos de sección soportando diferentes servicios como VoIP para reemplazar las comunicaciones por radio HF/VHF, streaming de video desde los vehículos de sección para mejorar la SA e información de mando y control (ver Figura 66). Este último punto se pudo constatar en las pruebas llevadas a cabo en la unidad de Artillería Antiaérea (AAA) que se describen en el capítulo 5 del presente trabajo.

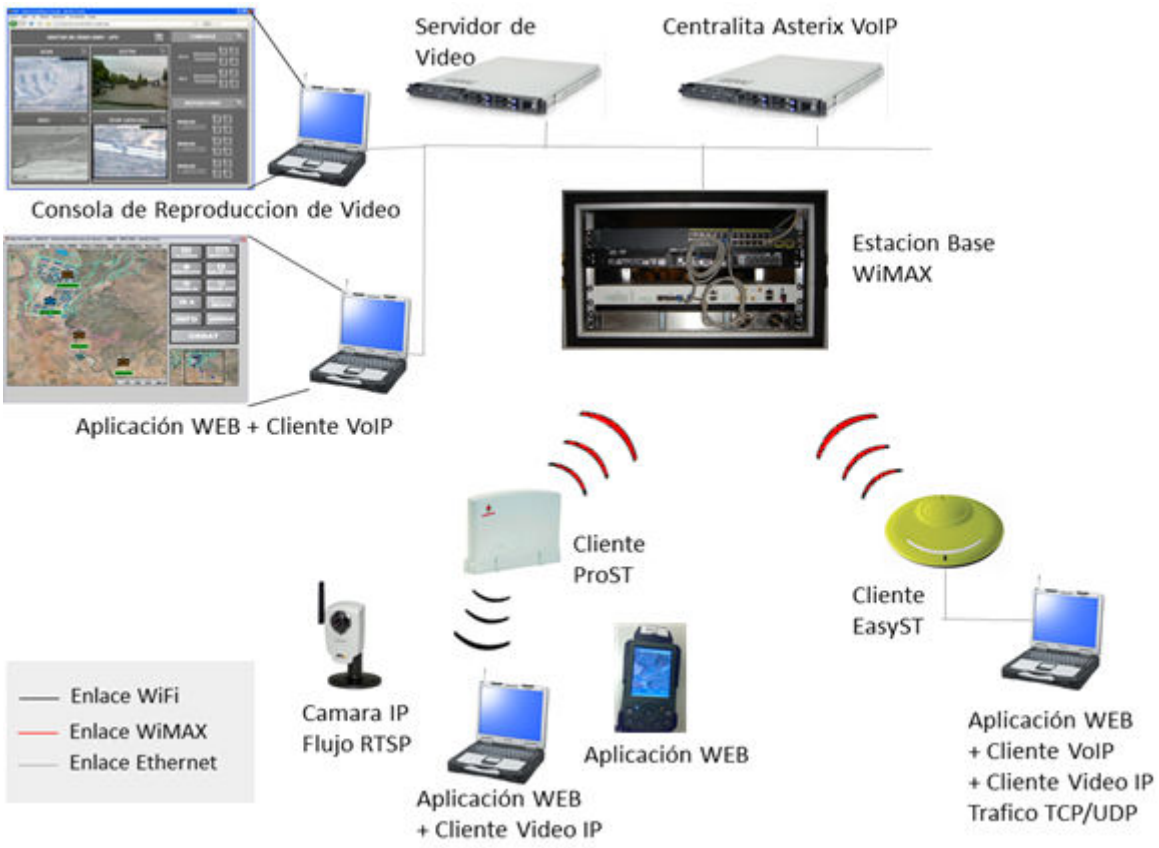

Figura 66. Topología de interconexión con distintos flujos de transmisión sobre red táctica WiMAX

5 Validación de la arquitectura de comunicaciones inalámbricas para sistemas C4ISR

5.1 Introducción a los escenarios de prueba

La arquitectura de comunicaciones propuesta en esta tesis ha sido probada desde sus primeras versiones por el Ejército de Tierra Español en diversas demostraciones y pruebas, así como en varios proyectos europeos y eventos internacionales del ámbito de gestión de emergencias. En el presente capítulo, en primer lugar, se describen las pruebas de campo realizadas al sistema SIMACOP enfocándose en particular en la arquitectura de comunicaciones utilizada sobre medios tácticos, así como los resultados obtenidos por SIMACOP en las evaluaciones de las mismas. Como ya se destacó en el capítulo precedente, SIMACOP es el acrónimo de "SIstema de MAndo y COntrol para Pequeñas unidades" y se corresponde a la implementación, en sus distintas versiones, de la arquitectura para su validación.

De igual forma se describen las pruebas realizadas sobre una variante de SIMACOP, denominada GESTOP, el cual es el acrónimo de "Sistema de Gestión de Operativos de Emergencia", al estar basado sobre SIMACOP utiliza la misma arquitectura de comunicaciones, pero su interfaz y funcionalidades están adaptadas a operaciones de emergencias y se utilizan medios de comunicaciones disponibles en el medio civil.

Durante las pruebas que describen en este capítulo, se demostrará la viabilidad, buen funcionamiento y aceptación-aprobación por parte de usuarios finales, de los diseños obtenidos como fruto de la investigación realizada en la presente tesis doctoral y que el sistema SIMACOP lleva incorporados e integrados en su arquitectura de comunicaciones.

5.2 Escenario 1: Comunicaciones tácticas sobre múltiples tecnologías de transmisión

5.2.1 Descripción y evolución del escenario de pruebas

En este apartado se describen las pruebas de campo, demostradores y pruebas oficiales de certificación y validación, por parte de organismos tanto nacionales como internacionales, en los que ha participado y ha sido sometido el sistema SIMACOP.

A lo largo de las distintas pruebas se puede ver la evolución de la arquitectura de comunicaciones utilizada, inicialmente se probaron los conceptos sobre redes inalámbricas wifi y luego se fueron incorporando medios inalámbricos tácticos como VHF, HF, UHF y medios satelitales. En concreto, las pruebas y demostradores que se van a describir en este apartado son los siguientes:

- Demostración del sistema SIMACOP en el ejercicio Coallition Warrior Interoperability Demonstration (CWID) nacional 2006
- Pruebas y demostrador en el cuartel general de la Unidad Militar de Emergencias (UME) en Mayo de 2007. Integración con las radios SpearNet de ITT. Pruebas y sistema demostrado en CWID 2007 nacional.
- Integración del sistema SIMACOP en el demostrador del proyecto europeo MARIUS. Descripción de la demostración llevada a cabo en Julio de 2007
- Evaluación del sistema SIMACOP por parte de la JCIS y AT del ET en el regimiento de transmisiones tácticas 21 (RT-21) en Abril de 2008 y Julio de 2008.
- Evaluación del sistema SIMACOP por parte del Regimiento de Caballería Ligera 8 (RCL-8) Lusitania en el campo de maniobras de Chinchilla en Mayo de 2008.

- Demostración del sistema SIMACOP en las Escuelas Prácticas CIS (EPCIS) del Ejército de Tierra 2008 en el regimiento de transmisiones tácticas 21 (RETAC-21).

Tal como se ha visto en el capítulo anterior el sistema se ha desarrollado en el marco de diversos proyectos de investigación europeos y nacionales así como en convenios con empresas punteras en el ámbito del mando y control. Por otra parte las evaluaciones las han llevado a cabo organismos de certificación nacionales, como JCIS y AT, e internacionales como la agencia NC3A, perteneciente a OTAN. La satisfactoria evaluación del sistema hacia un producto maduro y la superación de las pruebas de certificación han conducido a su adquisición por parte del Ejército de Tierra, y de forma directa y evidente valida la arquitectura de comunicaciones propuesta.

5.2.1.1 Demostración sobre el sistema SIMACOP en el ejercicio CWID nacional 2006

En Mayo de 2006 se llevó a cabo la demostración del sistema desembarcado versión SBC y con tecnología de red 802.11a/g y sensores de GPS, vídeo de alta calidad y biosensores, en la base "General Almirante" de Marines, Valencia. Dicha demostración estaba enmarcada en las pruebas CWID 06 y los evaluadores fueron personal del regimiento de transmisiones así como oficiales de los regimientos próximos de artillería y caballería. En la siguiente figura se pueden apreciar los diversos elementos constituyentes de dicha demostración:

Los componentes de la arquitectura de comunicaciones utilizada durante las pruebas fueron los siguientes:

- Un nodo de segundo nivel (Secciones) con un puente WIFI 802.11g para conectar con los dos nodos de primer nivel con el objeto de replicar los datos actualizados en el interfaz común de datos y tener una COP más amplia.
- Dos nodos de primer nivel (Sección/Pelotones), equipados con puntos de acceso WIFI 802.11a conectados con sus patrullas y un puente WIFI 802.11g para conectar los dos nodos con el objeto de replicar los datos actualizados en el interfaz común de datos.
- Una patrulla real compuesta por dos soldados con su completo equipamiento (SBC con enlace WIFI 802.11a, GPS Bluetooth, video cámara en el casco, sensores biométricos y un Tablet PC para el jefe de la patrulla.
- El resto de los elementos de la demostración son simulados.

En la demostración se intentaron probar y validar por parte de los usuarios finales conceptos en boga en la investigación en mando y control, en particular el concepto de la auto sincronización. Para ello se probaron las dos configuraciones que se pueden ver en las dos siguientes figuras, modo autosincronizado y modo jerárquico.

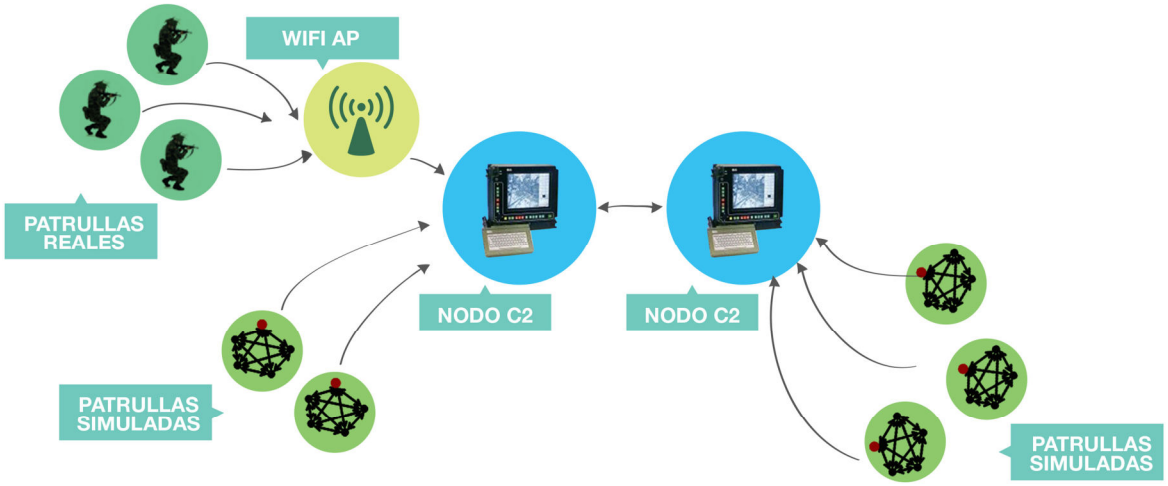

Figura 67. Arquitectura de comunicaciones en Modo Auto sincronizado.

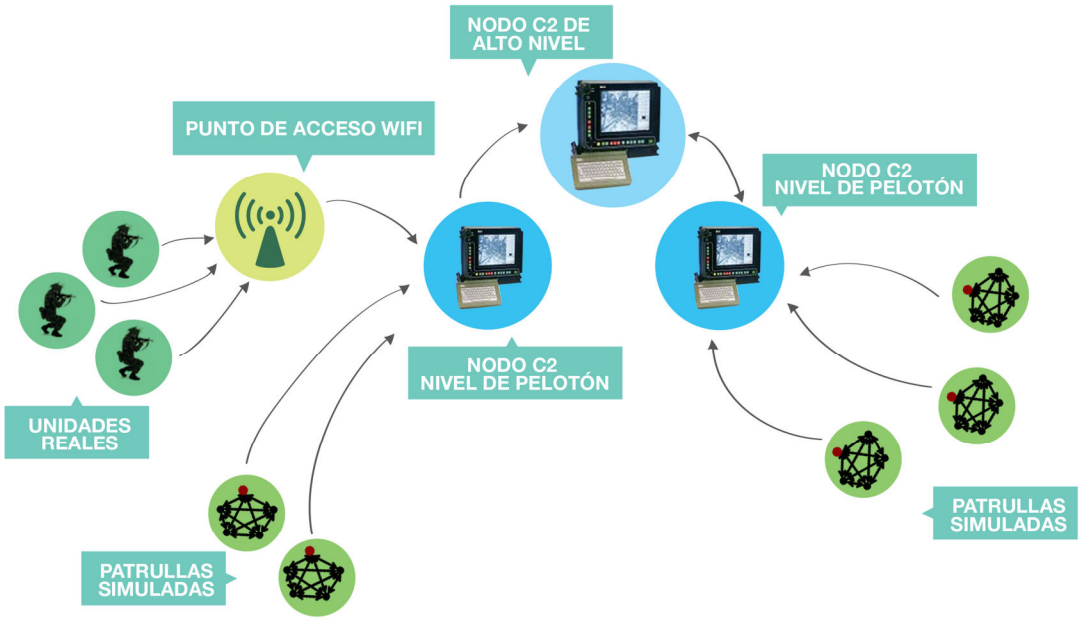

Figura 68. Arquitectura de comunicaciones en Modo Jerárquico.

En la Figura 69, podemos ver la patrulla compuesta por las dos unidades de tropa del regimiento de transmisiones 21, con todo el equipamiento descrito anteriormente.

Figura 69. Equipamiento de unidad individual

En la Figura 70, podemos ver un vehículo Rioja especialmente dedicado a las comunicaciones. En este vehículo se han instalado las antenas sectoriales (Ver número 1 en la Figura 70), que cubrirán el enlace WIFI 802.11a entre las unidades de tropa y el nodo C2 de SIMACOP de nivel de Sección/Pelotones (Ver número 3 en la Figura 70), que las monitoriza y que replica la información que recibe de ellas a los demás nodos de la red.

Esta réplica de información hacia los demás nodos de la red se realiza a través de la antena parabólica (Ver número 2 en la Figura 70), también instalada en el vehículo y que cubre el enlace WIFI 802.11g entre el nodo C2 de nivel de Sección/Pelotones y el nodo C2 de nivel de secciones.

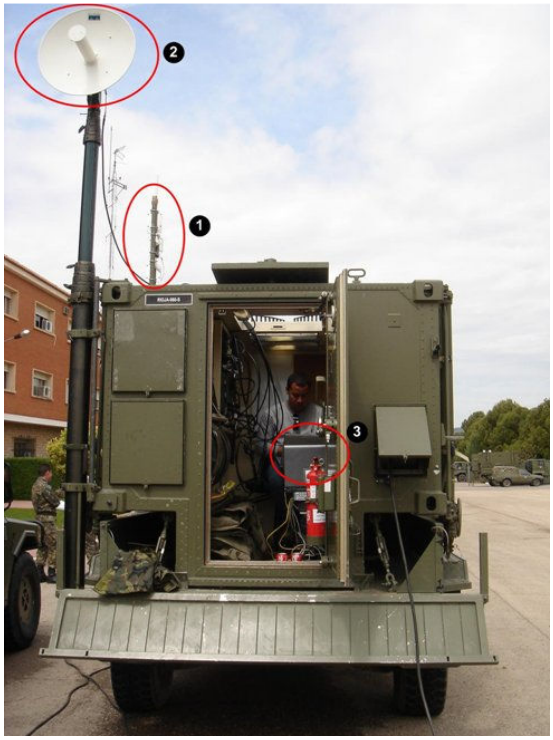

Figura 70. Vehículo de comunicaciones Rioja

Como ya se ha mencionado anteriormente en este trabajo, la réplica de posiciones y de datos biométricos se llevaba a cabo mediante las herramientas de réplica en tiempo real que incorporan las bases de datos MySQL mientras que la distribución de vídeo se llevaba a cabo mediante una solución ad-hoc basada en multicast.

Un detalle de la transmisión de video en directo desde el nodo C2 avanzado lo podemos ver en la Figura 71, donde se observa que mientras en el nodo de nivel superior (Ordenador de la izquierda), se siguen viendo las posiciones de las unidades de tropa, en el segundo nodo de nivel Sección/Pelotones (Ordenador de la derecha) se puede ver el video y las posiciones de las unidades de tropa (esquina inferior derecha del PC de la derecha) replicadas desde el nodo de nivel de Sección/Pelotones avanzado.

Cabe destacar, como puede verse en la Figura 71, la alta calidad de la imagen del video que proporciona el sistema SIMACOP pese al poco ancho de banda que consume su streaming de video, esto se debe a su óptimo algoritmo de codificación.

Figura 71. Vídeo de alta calidad en los puestos de mando

La evaluación del sistema se realizó mediante un cuestionario, que fue rellenado por observadores militares pertenecientes a distintas armas del ejército de tierra, que asistieron al desarrollo de la demostración.

De las quince preguntas efectuadas a los observadores de la prueba del sistema SIMACOP y calificadas de 1 a 5, de peor a mejor, se exponen los resultados de la evaluación:

Calidad percibida del vídeo en el puesto de mando	4.5
Calidad en la distinción de obstáculos y características del terreno	4.6
Nivel de confianza del posicionamiento de los efectivos	4
Valoración de la percepción de la situación desde el PC.	4
Valoración de la COP para la toma de decisiones	4.1
Valoración como ayuda a la toma de decisiones	4.5
Facilidad de utilización de la aplicación.	4.5
Valoración de la utilidad del Tablet PC al Jefe de Pon.	4.2
Valoración de la información del estado vital de los efectivos	3.3
Valoración de la ergonomía para el soldado	3.3
Operatividad del sistema para el Jefe de Pon.	4
Operatividad del sistema para el PC.	4.3
Valoración del funcionamiento de forma aislada.	4.1

Valoración del funcionamiento auto sincronizado.	4.4
Valoración del funcionamiento jerárquico.	4.4

Tabla 16. Validación QoE realizada por observadores militares

En la validación se destacaron los siguientes puntos, por parte de los evaluadores:

- La apreciación global de este sistema es muy buena y se ve que tiene un campo interesante a seguir desarrollando en el seguimiento y ayuda al Jefe de Pelotón y Jefe de Sección para dirigir sus efectivos.
- Destaca el GIS y la representación gráfica de obstáculos, edificios y la situación de los efectivos. Pues se abre un gran campo para la ayuda a la toma de decisiones a bajo nivel del Jefe de Sección y Pelotón para avanzar, defender y sobre todo saber si sus efectivos están vivos y dónde.
- Es muy interesante la capacidad de captar vídeo, pues facilita la comprensión en el PC. de lo que está sucediendo dónde está el soldado, observatorio o vehículo de exploración. Sobre todo de cara a la inteligencia militar y la 2ª sección que puede valorar mejor la situación en la faceta del enemigo.

Como puntos débiles destacaron, referido al prototipo demostrado:

- El soporte de comunicaciones no es el adecuado, la prueba se hizo con un enlace de Wifi, dando limitaciones en alcance y coberturas. Sería recomendable tomar dos opciones:
  - Para mantener la capacidad de captar vídeo habría utilizar WiMAX.
  - Con objeto de mejorar los alcances se debería pasar la información de posición, vital, la de designación de enemigo, etc. toda menos el vídeo, que requiere un ancho de banda mayor que los datos simples, por vía radio VHF.

Es de destacar que estas observaciones ya han sido subsanadas en siguientes versiones desarrolladas del sistema, como ya se ha indicado.

5.2.1.2 Pruebas UME 2007 y en la academia de infantería de Toledo sobre radios personales UHF tipo MESH

En estas pruebas, llevadas a cabo en Mayo y Junio de 2007, el software de la solución embarcada que antes estaba en un SBC se integró en las radios personales Spearnet de ITT. Por otra parte también se probaron los puestos de mando de SIMACOP de sección, compañía y batallón. La descripción técnica de la arquitectura implementada se puede ver en el punto correspondiente del capítulo 4.

En Mayo de 2007 se llevó a cabo una demostración completa del sistema en el cuartel general de la Unidad Militar de Emergencias situado en la base aérea de Torrejón de Ardoz, Madrid. La configuración de la demostración se puede ver en la siguiente figura:

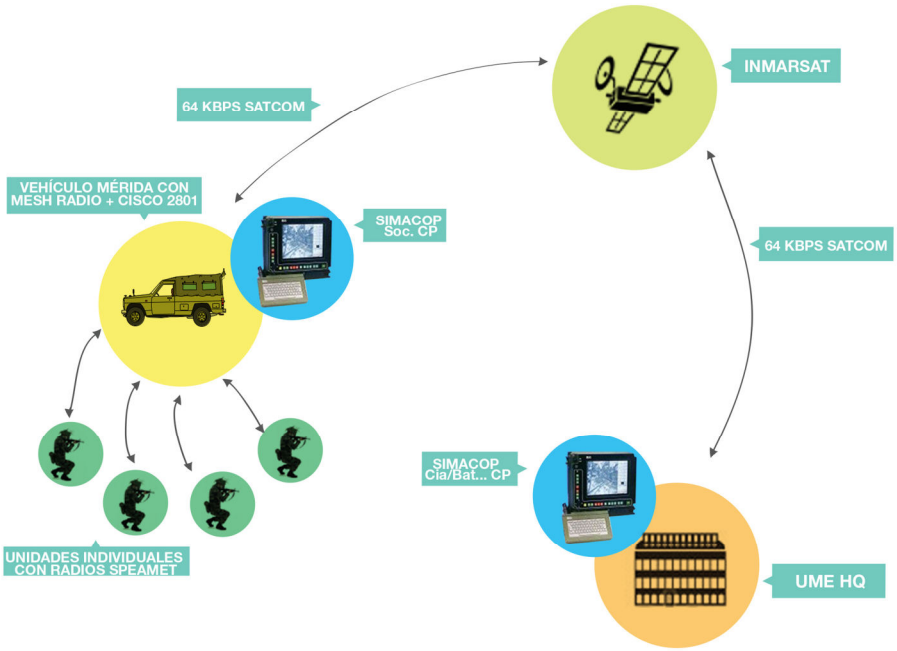

Figura 72. Esquema de las pruebas llevadas a cabo en la UME

Como se puede observar en la figura anterior se dispuso un pelotón de cuatro unidades individuales equipadas con las radios mesh Spearnet de ITT, cámara IP y el software de la UPV que se ejecutaba dentro de las radios. Las mismas formaban una malla autónoma que permitía la transferencia de GPS, vídeo y voz entre las distintas unidades. Como quinto elemento de la malla se encontraba un puesto de mando avanzado (Sección) de SIMACOP que recogía toda esa información, la representaba en su display (unidades ubicadas en la cartografía y vídeo en tiempo real) y la envía por un enlace satélite Inmarsat al puesto de mando retrasado (Compañía/Batallón) de SIMACOP ubicado en el cuartel general de la UME, en concreto en el denominado JOC (Joint Operations Centre) que se describe en figuras siguientes. En todo momento, en ambos puestos de mando se disponía de vídeo en tiempo real de cada una de las unidades y de su posición en un GIS, así como de comunicaciones vocales.

Figura 73. Aspecto del HQ de la UME, denominado JOC, con la aplicación SIMACOP en funcionamiento

En la figura anterior se observa el video-wall del JOC y la aplicación SIMACOP ejecutándose en la parte central. En la siguiente se puede ver un momento de la demostración cuando una de las unidades individuales mira hacia otra y su cámara, en perspectiva subjetiva envía el vídeo en tiempo real. En la esquina inferior derecha se observan las posiciones de las distintas unidades en el mapa.

Figura 74. Aplicación SIMACOP mostrando la posición y el vídeo en vivo

Figura 75. Aplicación SIMACOP junto con otras en el JOC

En la Figura 75, se puede observar a una unidad individual acercándose al edificio de headquarters de la UME. Mientras que en la Figura 76, se detallan los componentes del sistema. En la parte izquierda se puede ver la cámara IP, ubicada sobre el casco y parte del sistema de audio, con auriculares sin pulso de aire sino con transmisión del sonido por vibración sobre los huesos al estimular la cóclea. En la figura de la derecha se puede ver la radio Spearnet con antena adjuntada a un chaleco y con salidas para los auriculares y la cámara IP.

Figura 76. Sistema completo con cámara y radio Spearnet

En la Figura 77, se observa el vehículo de transmisiones Mérida, donde estaba ubicado el puesto de mando avanzado de SIMACOP y donde se establecía el enlace satélite con el puesto de mando retrasado.

Figura 77. Vehículo de comunicaciones Mérida con enlace satélite

El sistema (tanto la radio personal, como el software de posicionamiento y streaming de vídeo, así como los planificadores de tareas que se incluían en la radio, todo ello desarrollado por la UPV en el presente proyecto de investigación junto con los puestos de mando y control) fue calificado como muy válido por los usuarios finales, la Unidad Militar de Emergencias. Tanto es así que recibió muy buena puntuación en el concurso de adquisición de radios personales que tenía en marcha la UME. Hay que destacar que en Junio de 2007 se llevaron a cabo pruebas muy similares en la academia de infantería de Toledo y que condujeron a la adquisición del sistema, en concreto un número determinado de radios, por parte del programa 'combatiente del futuro' del ministerio de defensa español.

5.2.1.3 Integración de SIMACOP en el demostrador del proyecto europeo MARIUS

MARIUS (Mobile Autonomus Reactive Information) es un proyecto PASR (Preparatory Actions Security Research, PASR-107900) del sexto programa marco de proyectos de investigación de la Unión Europea. En dicho proyecto participaron empresas como EADS, Thales Research, British Aerospace y Selex, entre otros. El grupo de investigación de Sistemas de Tiempo Real Distribuido participó en dicho proyecto aportando una versión modificada del sistema de mando y control SIMACOP. La idea principal de proyecto MARIUS era el desarrollar y validar con una demostración realista, un sistema de mando y control aerotransportado de rápido despliegue (menos de una hora desde que produce la emergencia) que incorporase sensores de diversa índole, sistemas de ayuda a la decisión y UAV. La arquitectura básica del sistema se puede ver en la siguiente figura:

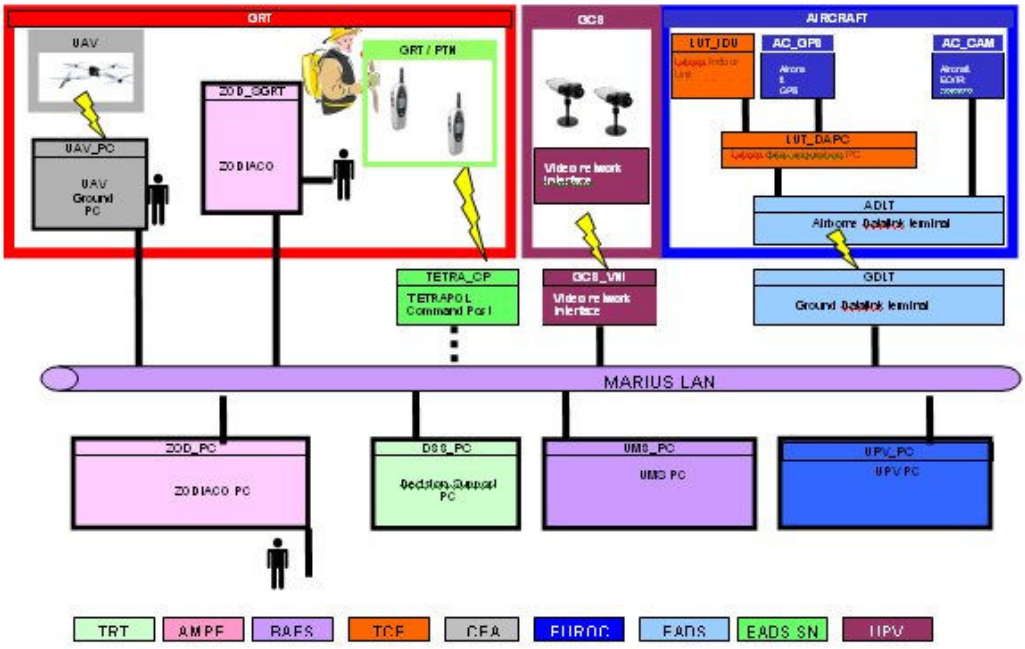

Figura 78. Arquitectura general del proyecto MARIUS

El sistema se componía de un sistema de mando y control, que se subdividía en varias consolas de representación y control, entre ellas la de la UPV, que eran transportadas en un shelter de tamaño reducido al escenario de operaciones por parte de un helicóptero. Por otra parte, por medios terrestres se transportaba a la zona donde se había producido la emergencia: un UAV y su sistema de control tierra, una infraestructura de comunicaciones TETRAPOL y un sistema de cámaras individuales y sensores de posición facilitado por la UPV (SIMACOP). Todo ello se conectaba vía inalámbrica a los puestos de mando para alimentarlos con la información sensorizada. En el helicóptero en vuelo se encontraba un sistema de la empresa Thales, Lutece, que permitía detectar heridos entre los escombros o aludes por medio de las señales emitidas por sus teléfonos móviles. Toda la información recibida era evaluada por los responsables de la toma de decisiones en la zona para poder efectuar el mando. Con posterioridad, una herramienta de ayuda a la toma de decisiones (DSS) les permitía determinar que heridos eran evacuados a qué hospitales.

SIMACOP fue introducido en el sistema como su versión desmontada con SBC. A cada bombero en la zona de operaciones se le facilitó un equipamiento de comunicaciones que permitía la transmisión tanto del video en perspectiva subjetiva como su posición, los cuales se inyectaban en dos sistemas de mando y control, el desarrollado por la empresa British Aerospace, denominado UMS y SIMACOP. La particularidad de esta versión es que el códec de video fue modificado para

que en el mismo stream MPEG viajase tanto el propio video como la información de posición para conseguir una sincronización total entre ambos flujos.

El sistema fue validado en una demostración final que se llevó a cabo en Valencia en Julio de 2007. Dicha demostración intentaba emular un escenario catastrófico en el que dos bombas explotaban en Valencia (una en exteriores y otra en un subterráneo) con gran número de heridos que debían ser evacuados. Para llevar a cabo la demostración, el consorcio de bomberos de Valencia facilitó unas instalaciones de entrenamiento que dispone en el término municipal de Ribarroja, ubicadas en un antiguo polvorín y montes aledaños.

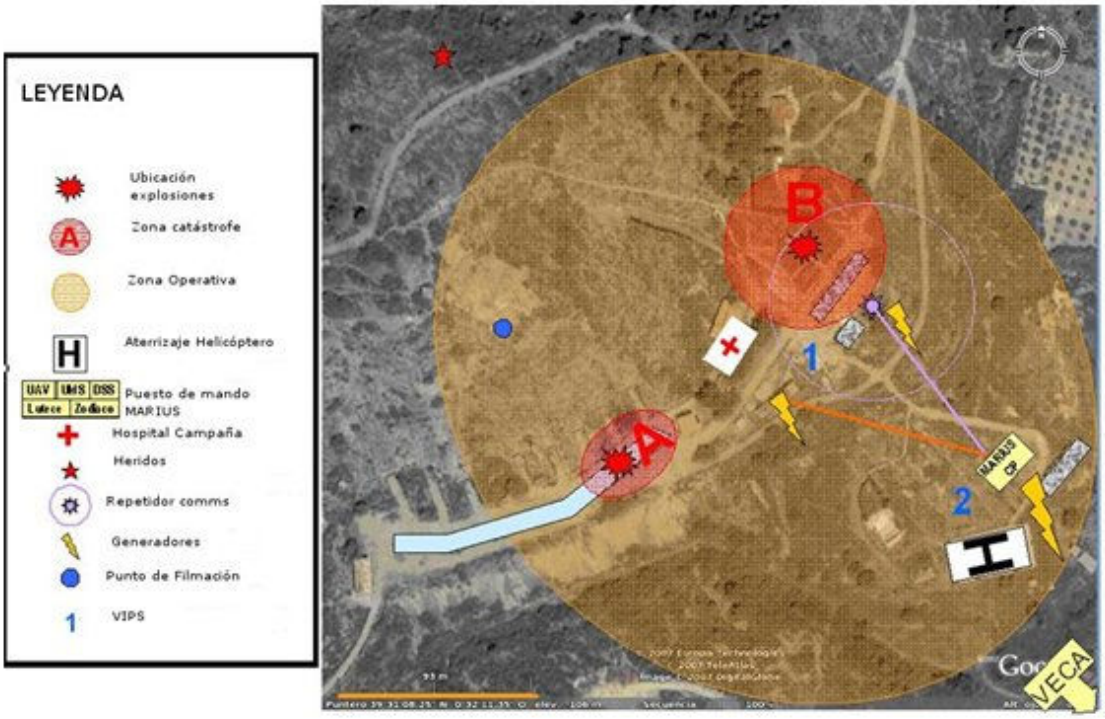

Figura 79. Escenario de pruebas del proyecto MARIUS

La UPV participó en dichas pruebas con el sistema SIMACOP embarcado para operativos individuales anteriormente citado, una consola de mando en la zona de puestos de mando (el enlace se estableció mediante tecnología mesh) y un puesto de mando retrasado ubicado a 1500 metros en el Vehículo de Coordinación Avanzada (VECA) del consorcio de bomberos y enlazado por un punto a punto wifi IEEE 802.11g con antenas parabólicas direccionales de 23 dBi de ganancia.

En las siguientes figuras se puede observar a los operativos bomberos equipados con las cámaras y SBC.

Figura 80. Detalle del SBC en el equipamiento de los bomberos

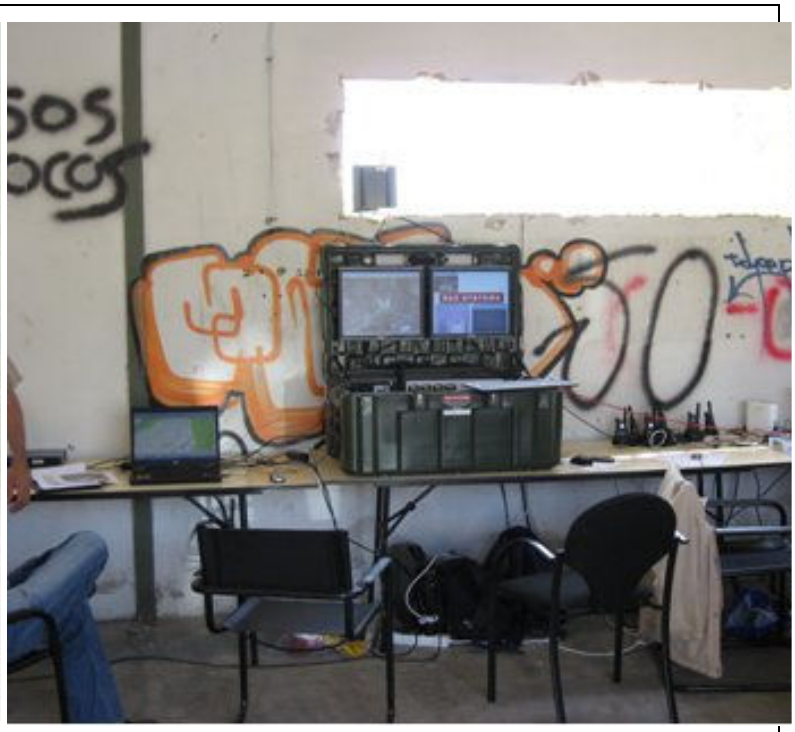

Figura 81. Consolas de Puesto de mando una vez desembarcadas en la ubicación de campaña

Figura 82. Escenario de la demostración. En la misma se pueden ver los siguientes elementos: 1) helicóptero en zona de aterrizaje; 2) edificio donde se desembarcaron y ubicaron las consolas del puesto de mando de MARIUS; 3) zona donde se produjeron las explosiones principales; 4) Ubicación del vehículo VECA

Figura 83. Helicóptero con sistema MARIUS aerotransportado

Figura 84. UAV con cámara para la inspección de túneles

Figura 85. Exteriores vehículo VECA

Figura 86. Interior vehículo VECA

El proyecto fue valorado muy positivamente tanto por los responsables de agencias de seguridad presentes en la demostración (protección civil, UME, etc.) como por los usuarios finales del proyecto (consorcio de bomberos de Valencia) así como por el officer de la Unión Europea que propuso una inmediata segunda parte y ampliación del mismo.

5.2.1.4 Pruebas JCISyAT Marines Abril 2008.

Durante la primera quincena del mes de Abril de 2008, la JCISAT (Jefatura CIS y Atención Técnica) del Ejército de Tierra decidió llevar a cabo una serie de pruebas exhaustivas sobre el sistema SIMACOP para evaluar su validez y emitir un informe de viabilidad respecto a su posterior incorporación al catálogo de sistemas de mando y control a disposición del ejército. Dichas pruebas consistieron en la evaluación del sistema de seguimiento de fuerzas propias embarcado, con todos los medios radio disponibles que se han visto en el capítulo 4, y en un escenario lo más realista posible con la utilización de hasta 15 vehículos Aníbal y Mercurio donde se instalaba el sistema SIMACOP.

En dichas pruebas se evaluaron todas las características del sistema descritas en puntos precedentes con cuestionario de hasta 400 ítems. El primer escenario evaluado fue el denominado ‘escenario 0’ de VHF donde determinados vehículos carecen de sistema SIMACOP y el resto

adquiere su posición GPS en remoto de sus radios. En la siguiente figura, se puede observar el esquema de mallas y la configuración completa para VHF:

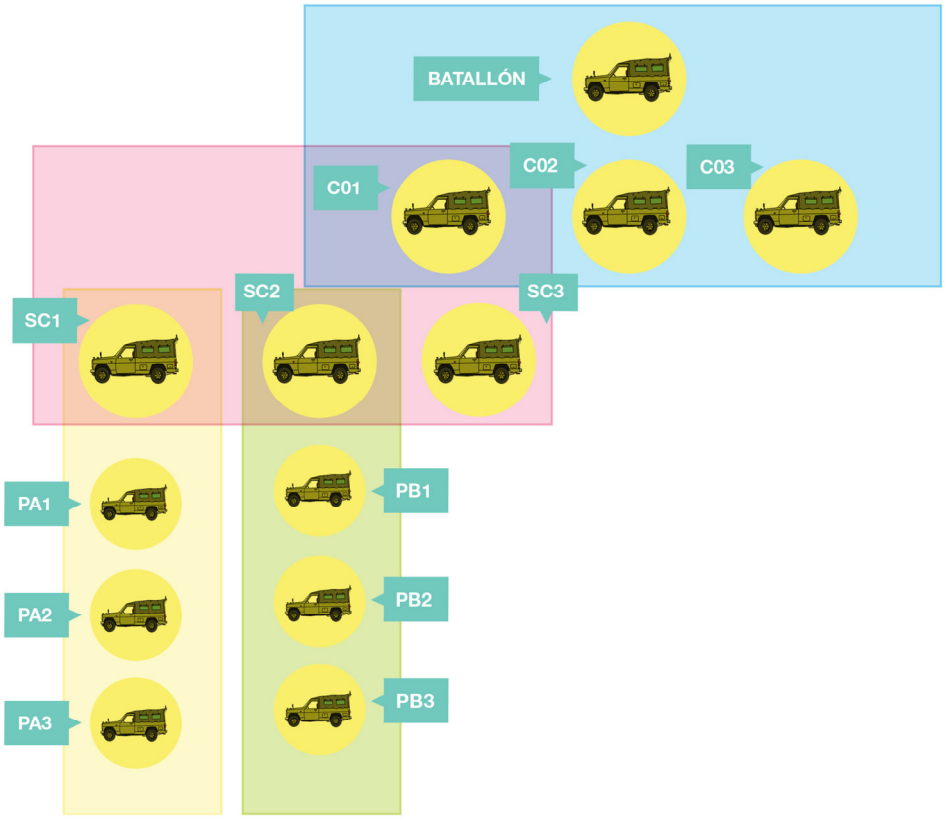

Figura 87. Esquema de mallas para la configuración completa de VHF

Hay que señalar que las mallas de VHF son dominios independientes desde el punto de vista IP ya que a nivel radio trabajan a distintas frecuencias. De esta forma no hay comunicación entre nodos de distinta malla y el sistema SIMACOP realiza el enrutamiento entre mallas a nivel de datos.

En dicho escenario se evaluaron todas y cada una de las funcionalidades del sistema y la transmisión de todos los tipos de información de cualquier nodo a otro. Debido a la naturaleza realista de las pruebas los vehículos de pelotón, sección y compañía se movieron por la base y exteriores describiendo rutas preconfiguradas. Un elemento importante era la considerable inestabilidad de las radios de VHF, que requerían reconfiguraciones periódicas, aunque luego se comprobó que esta baja de rendimiento era debida a la falta de preparación de los operarios que manejaban dichas radios y la falta de software adecuada para gestionarlas. Una vez subsanados estos problemas su rendimiento fue el adecuado.

Otro escenario que se probó a continuación fue el denominado escenario de HF, donde también se comprobaron todas las funcionalidades del sistema de manera exhaustiva, haciendo uso de radios HF. Sobre este escenario también se probaron todas y cada una de las funcionalidades del sistema. Hay que destacar las dificultades que introducen este tipo de radios a la hora de transmitir y recibir paquetes IP, como ya se ha visto en los capítulos previos de estado del arte y de especificación de la arquitectura. Problemas como la característica simplex del canal, la elevada sensibilidad a las condiciones atmosféricas o el elevado retardo introducido y escaso ancho de banda se ven compensados por las elevadas distancias que pueden lograrse.

El último escenario individual que se probó fue el denominado escenario satélite. En la siguiente figura se puede ver un esquema de dicha configuración. Se probó un punto a punto, desde un nodo de batallón a otro de compañía, para las tres tecnologías existentes, Inmarsat, Iridium y Thuraya.

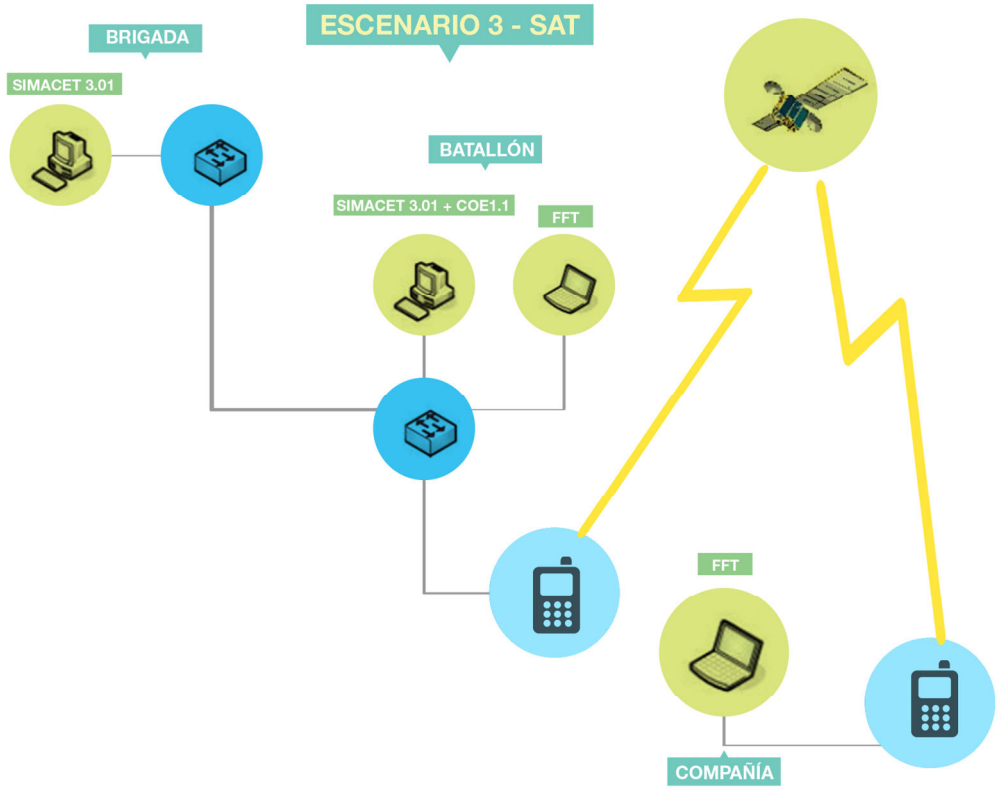

Figura 88. Esquema escenario de pruebas vía satélite

La conexión que dan los tres sistemas citados acaba consistiendo en entregar al nodo una dirección IP privada (impredecible) con visibilidad a Internet. Debido a la necesidad de identificar unívocamente los nodos existentes mediante la dirección IP, por estructura del sistema SIMACOP, y por cuestiones de seguridad, se decidió la utilización de redes privadas virtuales con cifrado para las conexiones de este tipo. Los resultados en estas pruebas fueron los mejores debido al elevado ancho de banda que entregan estos interfaces (desde 200-300 Kbps en el caso de Inmarsat hasta 64 Kbps para Thuraya) permitiéndose la actualización de posiciones y otros datos en un lapso de segundos. El principal problema encontrado fue la inestabilidad en recepción de los terminales Iridium y Thuraya que provocaba la caída de enlaces con frecuencia. Este problema no se producía con los terminales Inmarsat.

Finalmente, una vez probados de manera parcial y aislada los escenarios para cada medio de transmisión se planteó la prueba de un escenario completo con todos los medios a utilizar, para ser lo más realista posible. Sobre dicho escenario también se probaron todos los servicios y funcionalidades del sistema SIMACOP.

Dicho escenario estaba compuesto por los siguientes elementos:

- Un Batallón, utilizando como medios de transmisión VHF, HF y satélite (Inmarsat).
- Tres Compañías:
- Compañía VHF, compuesta por
  - 2 Secciones con dos pelotones cada uno.
  - Una sección sin pelotones.

- Compañía HF.
- Compañía Satélite (Inmarsat)

El esquema de mallas y tecnologías radio utilizadas se puede ver en la siguiente figura.

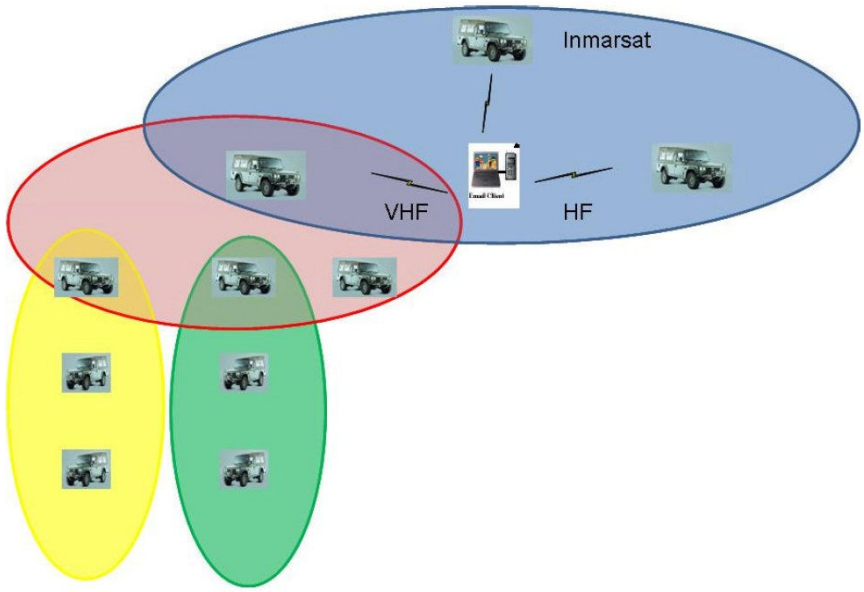

Figura 89. Arquitectura de comunicaciones con todos los medios de transmisión activos

Los resultados de la prueba del escenario completo fueron totalmente satisfactorios, permitiéndose la interconexión de nodos FFT completamente transparente mediante tecnologías de red heterogéneas y consiguiéndose desacoplar las características y problemas inherentes a cada una. En las siguientes figuras se pueden ver diversos elementos del sistema desarrollado e implementado.

Figura 90. Vehículos Aníbal equipados con antenas VHF PR4gv3

Figura 91. Aplicación SIMACOP proyectada en el centro de mando durante las pruebas de validación.

Figura 92. Vehículo de comunicaciones Mercurio con antena NVIS (Near Vertical Incident Skywave) para medios radio HF

Figura 93. Despliegue completo de Vehículos Aníbal implicados.

El resultado final de las pruebas fue altamente satisfactorio hasta el punto que el grupo de evaluación de JCIS recomendó la compra del sistema por parte del ET.

5.2.1.5 Pruebas maniobras Chinchilla Mayo 2008

En Mayo de 2008 se llevaron a cabo unas maniobras denominadas LIVEX'08 en el campo de maniobras de Chinchilla por parte del Regimiento de Caballería Ligera-8 (Lusitania) con unidades empotradas del regimiento de transmisiones tácticas 21. El grupo de investigación de Sistemas de Tiempo Real Distribuido fue invitado a dichas pruebas aportando el sistema SIMACOP para su validación por parte del personal de Caballería. Estas pruebas fueron una extensión del sistema validado en el punto anterior aplicado a unas maniobras reales y adaptadas a las peculiaridades de la orgánica de un regimiento de caballería. Desde el punto de vista técnico se probaron configuraciones completas como las vistas en el punto anterior, con todos los medios existentes operativos en un mismo ORBAT.

En estas pruebas, aparte de validar el sistema en un escenario de maniobras reales se pudieron comprobar los siguientes conceptos:

- El sistema tiene la capacidad de operación por unidades muy dinámicas y móviles, como es el caso de las unidades de caballería, con poco soporte de personal especializado. En concreto se desplazaron cinco ingenieros de la UPV y personal del RT-21 pero su apoyo fue muy limitado pues se perseguía comprobar su uso, autónomo, por parte de personal 'no técnico'.
- El sistema presenta un elevado grado de usabilidad puesto que fue rápidamente asimilado y puesto en marcha por parte del personal de caballería.
- Disminución de las comunicaciones vocales. Sustitución del control de operaciones vía ordenes vocales por el envío de mensajería mediante Chat táctico.
- Fue de gran utilidad la capacidad de reconfiguración dinámica del sistema. De esta forma, si un conjunto de unidades estaba en una malla y, dada la dispersión geográfica del campo de maniobras, se perdía enlace, se establecían con facilidad las denominadas burbujas VHF interconectadas por enlaces HF, de mayor alcance.

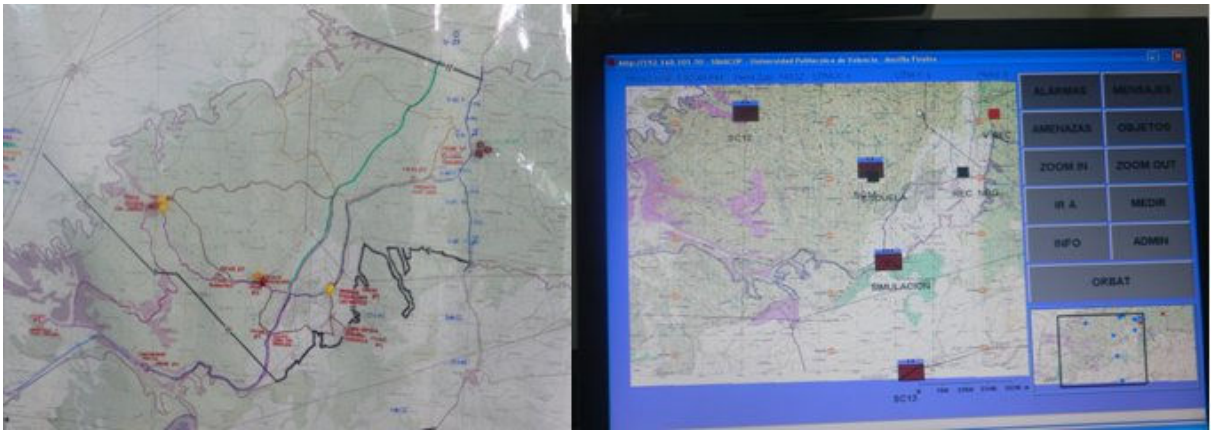

Figura 94. Sustitución del sistema de mando y control 'de pared' por uno CIS.

En la anterior figura se puede observar la evolución que introduce el sistema respecto al modo de funcionamiento clásico (mapa colgado en la pared y chinchetas representando a las unidades) por el sistema SIMACOP. Cabe destacar que a las 3 horas de desplegar el sistema los usuarios finales lo estaban usando con familiaridad y sustituyendo al sistema anterior. Una funcionalidad muy utilizada era la de mensajería.

El sistema fue evaluado muy positivamente por el personal de Caballería y por mandos de la IGECIS (Inspección General CIS) presentes en la prueba, destacando su utilidad y validez para el tipo de misiones que llevaban a cabo. Tras un breve periodo de adaptación y aprendizaje fue el único sistema de mando y control que utilizaron durante el desarrollo de las maniobras.

5.2.1.6 Pruebas EPCIS Septiembre 2008

En las escuelas prácticas CIS (EPCIS) de 2008, llevadas a cabo en Septiembre en el regimiento de transmisiones 21, Marines, Valencia, se evaluó la configuración más compleja y ambiciosa del sistema con la inclusión de flujos de vídeo de diversas fuentes, comunicadas mediante enlaces satélite y posibilitando la evaluación práctica del concepto 'sensor-on-the-net' con una aproximación 'push-and-smart-pull'.

Para ello se estableció un ORBAT que incluía tres área de operaciones (una central en España y dos en ubicaciones remotas, cada una simulando estar en un país distinto) permitiendo que todos los nodos de la red compartieran la misma visión del teatro de operaciones y pudieran, bajo demanda y en todo momento, acceder a las fuentes de vídeo que determinadas unidades incorporaban.

Para lo cual se integró en la arquitectura global de SIMACOP un sistema de captura, codificación y distribución de vídeo, desarrollado en el marco de la presente tesis y que está optimizado para su uso en entornos muy restrictivos principalmente para enlaces con 128 Kbps a lo sumo y múltiples usuarios simultáneos con solicitudes impredecibles. El ORBAT definido fue el siguiente:

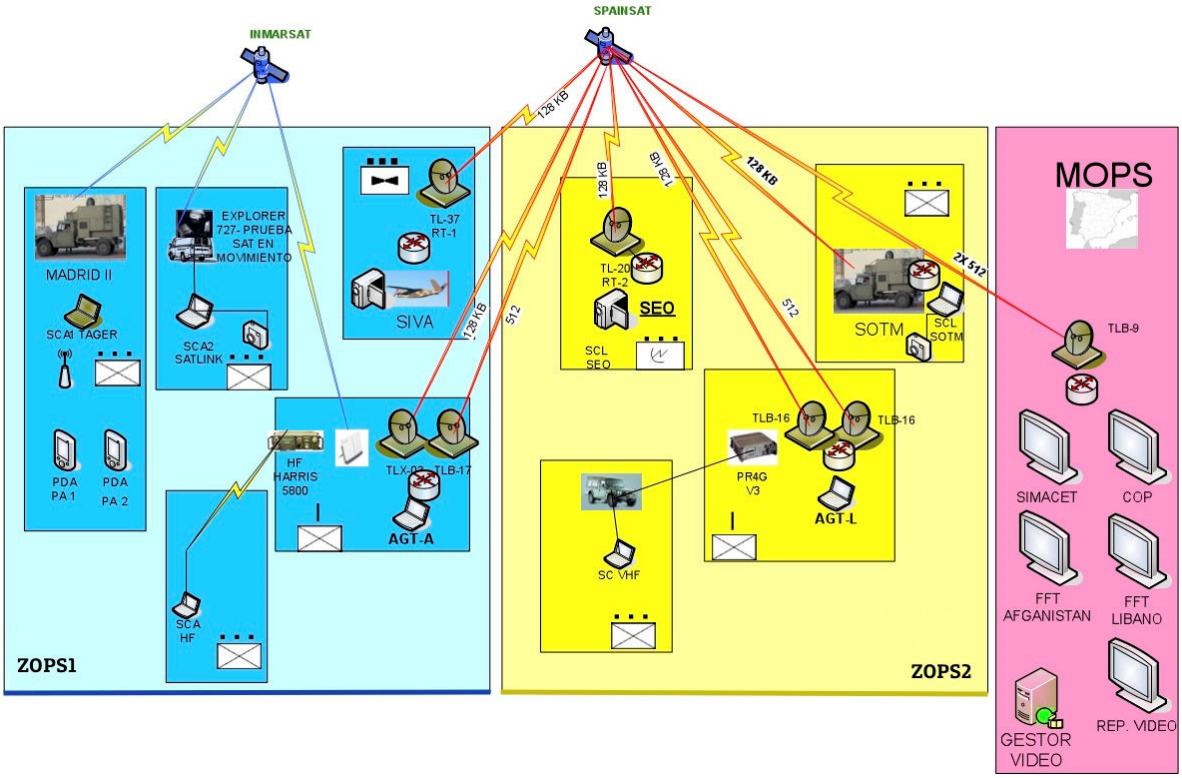

Figura 95. Arquitectura Global de comunicaciones utilizada en las EPCIS

En el esquema anterior se puede observar que existen tres áreas principales: una ubicada en territorio nacional y dos áreas remotas (ZOPS1 y 2), interconectadas todas mediante enlaces satélite y en las que existe un puesto de mando principal del que dependen determinadas unidades. Éstas últimas se interconectaban entre ellas mediante diversos medios radio: VHF (PR4G v3), HF (Harris 5800) y enlaces satélite: SATCOM on the move, TLX, TL, Inmarsat y por último wifi. En estas pruebas se pudo llevar a cabo una integración práctica de múltiples tecnologías radio y diversos flujos de datos y comprobar la viabilidad de la arquitectura propuesta en esta tesis como adecuada para gestionar un entorno de estas características.

El esquema de la arquitectura de vídeo utilizada en las pruebas fue el siguiente:

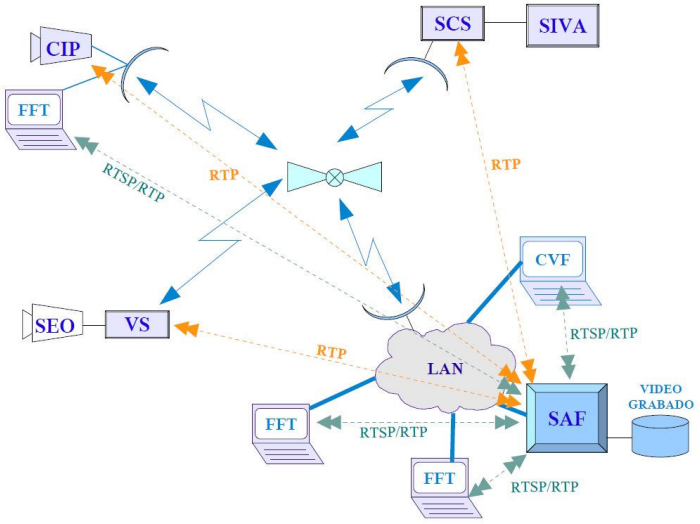

Figura 96. Esquema jerárquico de distribución de vídeo utilizado en las EPCIS

Como se puede observar existe, en la ubicación principal, un servidor de Almacenamiento de Flujos (SAF) que es el que interroga las distintas fuentes de vídeo (codificadores ubicados en los distintos emplazamientos: SEO, SIVA, etcétera) por medio del protocolo RTP. A su vez, los distintos consumidores de los flujos de vídeo (aplicación FFT con capacidades de reproducción de vídeo, consola de reproducción y gestión de flujos de vídeo (CVF por sus siglas en ingles)) solicitan, no a las fuentes, sino al SAF dichos flujos que les son entregados por medio de RTSP/RTP. Todos los emplazamientos están conectados por enlaces satélites.

En las siguientes figuras se pueden observar capturas de la aplicación con la inclusión de los flujos de vídeo. Como se ha visto en el capítulo 4, estas funcionalidades ya existían desde los primeros prototipos, adaptándose en este caso a la nueva arquitectura de servidores de vídeo.

Figura 97. SIMACOP con video integrado desde SIVA

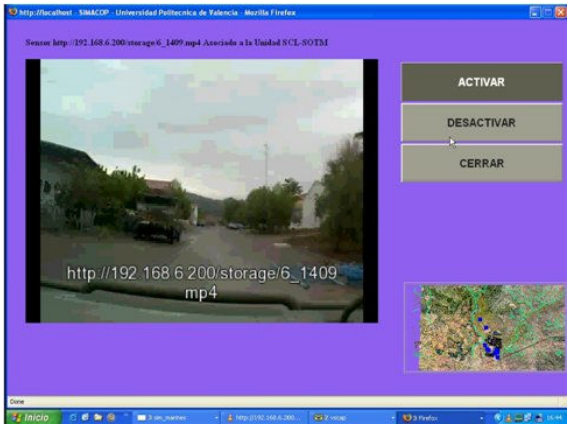

Figura 98. SIMACOP con video en primer plano y GIS sinóptico

El sistema fue evaluado muy satisfactoriamente por el personal del RT-21 durante el período de duración de las EPCIS así como por parte de las visitas destacadas, que incluyeron a oficiales de muy alta graduación como tenientes generales.

5.2.2 Conclusiones sobre la validación de la arquitectura en el escenario 1.

Las pruebas de campo a las que ha sido sometida la arquitectura de comunicaciones propuesta en la presente tesis, han comprobado la flexibilidad y la capacidad de operar en unidades tácticas muy dinámicas. Debido a la robustez de la arquitectura, se ha comprobado que no es necesario el apoyo logístico de un especialista en comunicaciones dentro de la unidad.

En los distintos escenarios de pruebas, se ha podido comprobar uno de los objetivos claves marcados en la fase de diseño de esta arquitectura que es la capacidad de utilizar cualquier medio de comunicación disponible, bien sea HF, VHF, satélite, etc. El diseño de la arquitectura le permite a SIMACOP que sea totalmente agnóstico al hardware (plataforma o medio de transmisión) sobre el cual trabaja.

La flexibilidad de la arquitectura propuesta ha permitido incluir en SIMACOP un abanico más amplio de flujos de datos, que va más allá de la transmisión de posicionamiento y navegación que normalmente se encuentra en este tipo de sistemas. Como ha quedado demostrado, la arquitectura propuesta aporta la capacidad de integración de sensores, video y telemetría, lo cual a su vez permite el desarrollo de los conceptos más avanzados de NEC sobre SIMACOP.

En las distintas pruebas, ha quedado demostrado que el uso del sistema propuesto reduce las comunicaciones vocales para reportar posicionamiento, reportes de la situación o para dar órdenes, las cuales han sido sustituidas por el servicio de mensajería instantánea mediante chat táctico.

Se ha podido comprobar la capacidad de gestionar e integrar sensores visuales (video) en operaciones reales, específicamente streaming de video desde UAV y otros sensores tácticos.
En resumen, la arquitectura de comunicaciones utilizada en SIMACOP proporciona a los mandos y a las unidades operativas una percepción conjunta de la situación, que hace posible la auto sincronización y definitivamente la reducción del flujo de reportes de mensajes y órdenes dentro la estructura jerárquica de una unidad táctica.

5.3 Escenario 2: Comunicaciones civiles sobre WiFi, WiMAX y Mesh

5.3.1 Descripción y evolución del escenario de pruebas

En la presente sección se van a describir las pruebas de campo y demostraciones, llevadas a cabo por organismos internacionales, en los que ha participado el sistema GESTOP (Sistema de Gestión de Operativos de Emergencia), el cual está basado en SIMACOP, por lo tanto, utiliza la misma arquitectura de comunicaciones, pero su interfaz y funcionalidades están adaptadas a operaciones de emergencias.

La experiencia adquirida y las lecciones aprendidas con SIMACOP, se aprovecharon para optimizar GESTOP. En el caso de GESTOP se da más relevancia a la integración de sensores, por ejemplo, se incluyen pulseras médicas para valoración inicial y triage de heridos, así como la vídeo subjetivo desde el operario de emergencia, que ayuda en la toma de decisiones a los comandantes responsables de la misión.

A nivel de comunicaciones, GESTOP ha sido probado utilizando la combinación de distintos tipos de redes inalámbricas disponibles en el medio civil, por ejemplo, IEEE 802.11, Redes tipo Mesh, enlaces microondas, 3G y WiMAX. En concreto, las pruebas y demostradores que se van a describir en este apartado son los siguientes:

- Pruebas en el simulacro internacional de emergencias de Bogotá en Octubre de 2009.
- Pruebas sobre radios Mesh en Enero de 2013. Validación de uso de VoIP sobre radios

Rajant BreadCumb.

El sistema ha sido valorado muy positivamente por los usuarios finales en las distintas demostraciones internaciones en las que ha participado. La satisfactoria evaluación del sistema por usuarios finales demuestra la vialidad del sistema global, y de forma directa valida la arquitectura de comunicaciones propuesta.

5.3.1.1 Pruebas en Simulacro Internacional de emergencias en Bogotá

Del 9 al 12 de Octubre de 2009, El grupo de investigación de Sistemas de Tiempo Real Distribuido participó en el Simulacro Internacional de Emergencias, llevado a cabo en la ciudad de Bogotá (Colombia). En este evento se probó la arquitectura de comunicaciones para gestión de emergencias, aportando una versión modificada del sistema de mando y control SIMACOP llamada GESTOP, de igual forma se pudo probar la solución de gestión de video en entornos de emergencias llamada SARF (Sistema de Almacenamiento y Reproducción de Flujos de Video).

Este simulacro fue el primero de este género en América Latina y buscaba preparar a la comunidad en respuesta ante una gran catástrofe, en concreto un terremoto. Durante 52 horas continuas, se probaron más de 62 escenarios distintos de atención de emergencias, como accidentes aéreos, incendios estructurales, colapsos, incidentes con materiales peligrosos (NBQ), rescates acuáticos y accidentes vehiculares, participaron equipos tanto de Norteamérica ()como de Suramérica (Venezuela, Chile, Ecuador, Argentina), así como participantes de Europa (Francia, España) y Asia (Japón), todos los sistemas participantes estaban bajo la coordinación de la Dirección de Prevención y Atención de Emergencias (DPAE), el organismo designado por el gobierno nacional de los temas de emergencias en Colombia. El sistema se probó exitosamente en 3 escenarios en concreto, los cuales se describen a continuación.

5.3.1.1.1 Desalojo de centro histórico ante terremoto

Este fue el principal escenario de pruebas del simulacro y demarcaba el inicio del resto de escenarios de pruebas, en este escenario se simulaba un sismo con origen en la falla Frontal de la cordillera Oriental, con una magnitud de 6,2 puntos en la escala de Ritcher, una profundidad de 23 kilómetros que causa estragos considerables en la capital, y hacía necesario como primer paso evacuar el centro histórico.

En este escenario de pruebas participamos con la arquitectura multinivel de SARF (Sistema de Almacenamiento y Reproducción de Flujos de Video), el cual permite hacer streaming de video bajo demanda desde distintas fuentes, en tiempo real, a través de enlaces con un ancho de banda reducido.

El objetivo principal de este escenario era proporcionar al personal de la DPAE encargado de la operación de evacuación, información visual que les ayudase a tomar mejores decisiones a la hora de coordinar los esfuerzos de las distintas instituciones implicadas. El esquema de comunicaciones utilizado en este escenario se puede ver en la siguiente figura:

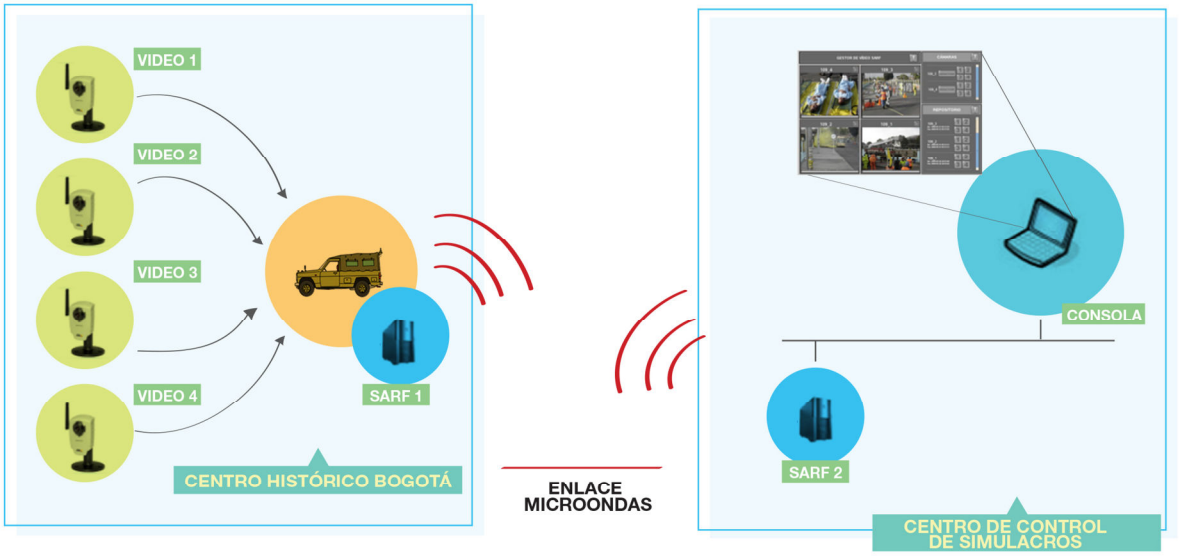

Figura 99. Esquema de comunicaciones escenario desalojo centro histórico

Tal como se puede ver en la Figura 99, en el lugar de la emergencia, se ubicaron 4 cámaras de video IP inalámbricas distribuidas a lo largo de varios puntos para monitorizar la evacuación, dichas cámaras se conectaban por un enlace inalámbrico WiFI hasta el vehículo de comunicaciones en el cual se encontraba desplegado un SARF de primer nivel, este era el encargado de almacenar los flujos de video provenientes de las distintas cámaras en el sitio de la emergencia.

El vehículo de comunicaciones contaba además, estaba equipado con un enlace microondas hacia el puesto de mando ubicado en el centro de control de simulacros, en el cual se encontraba un SARF de 2 nivel que permitía acceder a los flujos de video de las distintas cámaras bajo demanda para su reproducción en tiempo real.

Figura 100. Gestor de vídeos durante con imágenes desde distintas fuentes durante la evacuación del centro histórico

Este escenario permitió probar de forma satisfactoria la arquitectura multinivel de codificación, streaming y replicación de video desarrollada en un entorno real de gestión de emergencias en el ámbito civil.

5.3.1.1.2 Rescate de heridos tras el derrumbe en una fábrica

En este escenario de pruebas se simulaba la operación de rescate de heridos en una fábrica derrumbada tras el terremoto, en este caso SIMAGEM fue probado por un equipo de bomberos de Venezuela. La arquitectura de comunicaciones utilizada en este escenario se puede ver en la siguiente figura:

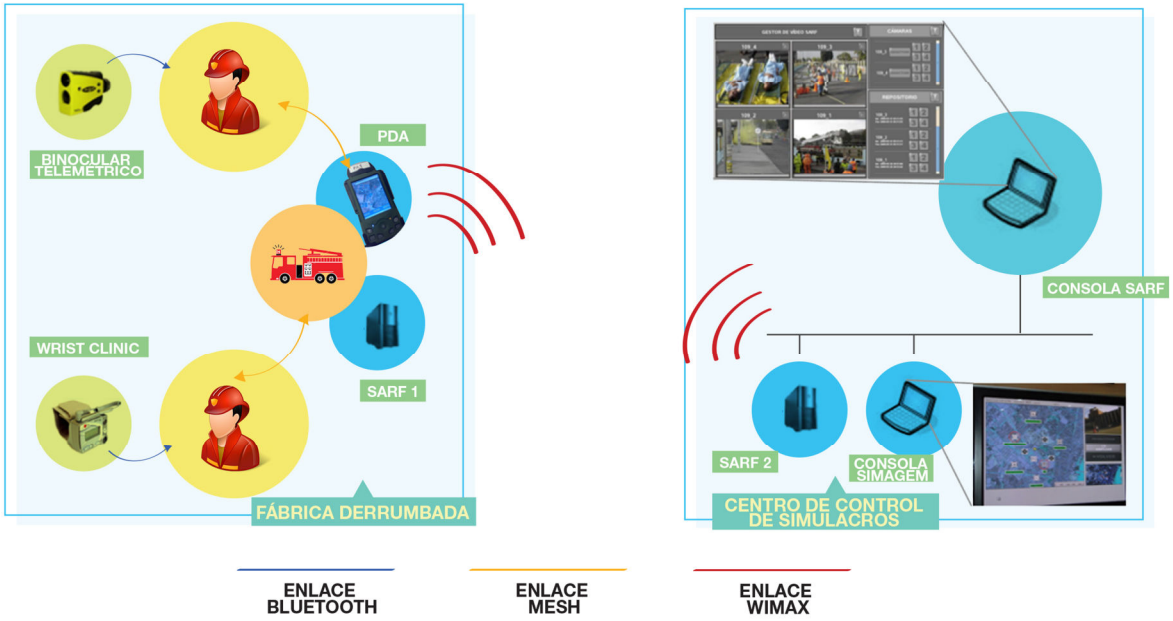

Figura 101. Esquema de comunicaciones del escenario rescate de heridos en fábrica

GESTOP fue introducido en el sistema como su versión desmontada con SBC. Como equipamiento básico, cada uno de los bomberos en la zona de operaciones estaba equipado con un SBC con GPS Bluetooth asociado y una cámara de video IP montada en su arnés para obtener el video en perspectiva subjetiva, de esta manera, tanto el vídeo como su posición se inyectaban en el sistema de mando y control, GESTOP.

Adicionalmente, uno de los bomberos llevaba un binocular telemétrico para designar objetos de interés para la misión (localización de heridos o estructuras comprometidas) y otro estaba equipado con un wrist clinic: sensor para medir frecuencia cardiaca, ECG, presión sistólica y diastólica, saturación de O2, temperatura corporal y respiración de los heridos rescatados en la zona de desastre.

Toda esta información era fusionada en único flujo en el SBC y transmitida hacia el puesto de mando de primer nivel ubicado en la zona del rescate, un vehículo de atención de emergencias equipado con un portátil rugerizado que ejecuta GESTOP, a través de un enlace mesh. En el vehículo también se encuentran un SARF de primer nivel que recibe los flujos de video las distintas cámaras de bomberos. El puesto de mando de primer nivel, fusiona la información recibida de los distintos miembros de la brigada de salvamento y los replica al puesto de mando retrasado, ubicado en el centro de control de simulacros, a través de un enlace WiMAX.

En el puesto de mando retrasado, se ejecuta la consola de GESTOP, la cual permite a los responsables de la misión (DPAE), hacer seguimiento de todos los miembros del equipo además también se encuentra el SARF de segundo nivel, el cual se comunica con el SARF de primer nivel para obtener los flujos de las distintas fuentes de vídeo (en este caso los bomberos en la zona con cámaras IP) por medio del protocolo RTP. A su vez, la aplicación GESTOP con capacidades de

reproducción de vídeo solicita, no a las fuentes, sino al SARF de segundo nivel, dichos flujos que les son entregados por medio de RTSP/RTP.

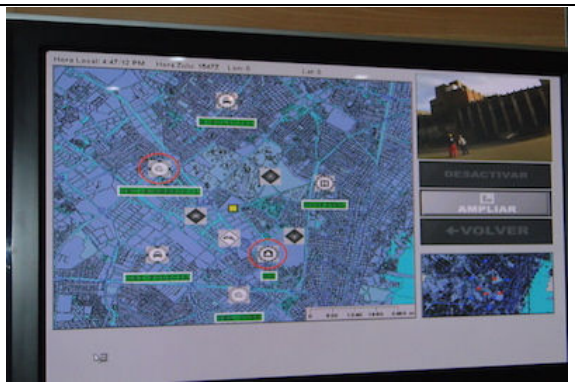

Figura 102. GESTOP en el puesto de mando retrasado, durante la misión de rescate con video subjetivo desde uno de los bomberos

Figura 103. Gestor de vídeos durante el transcurso de la misión con imágenes desde distintas fuentes durante la evacuación de heridos

Figura 104. Puesto de mando retrasado durante la misión de rescate mientras miembros de DPAE monitorizan la operación

Figura 105. Puesto de mando retrasado con video en diferido durante análisis posterior de la operación

El uso combinado de GESTOP y SARF permitió a los responsables no solamente coordinar la misión durante su ejecución, si no hacer un análisis posterior de la misma, dado que tanto los flujos de videos como el resto de información obtenida, por ejemplo, información de posicionamiento de los bomberos, objetos, muestras tomadas con los sensores, etc., quedan almacenadas en el sistema y se pueden consultar posteriormente.

5.3.1.1.3 Atención de emergencia NBQ

En este escenario de pruebas se simulaba la operación de rescate de heridos tras un ataque NBQ producto de la explosión de una bomba en las inmediaciones de un estadio de futbol, en este caso GESTOP fue probado por distintos organismos de salvamento: equipo de anti-explosivos de la armada nacional, policía nacional y DPAE entre otros. La arquitectura de pruebas utilizada en este escenario se puede ver en la siguiente figura:

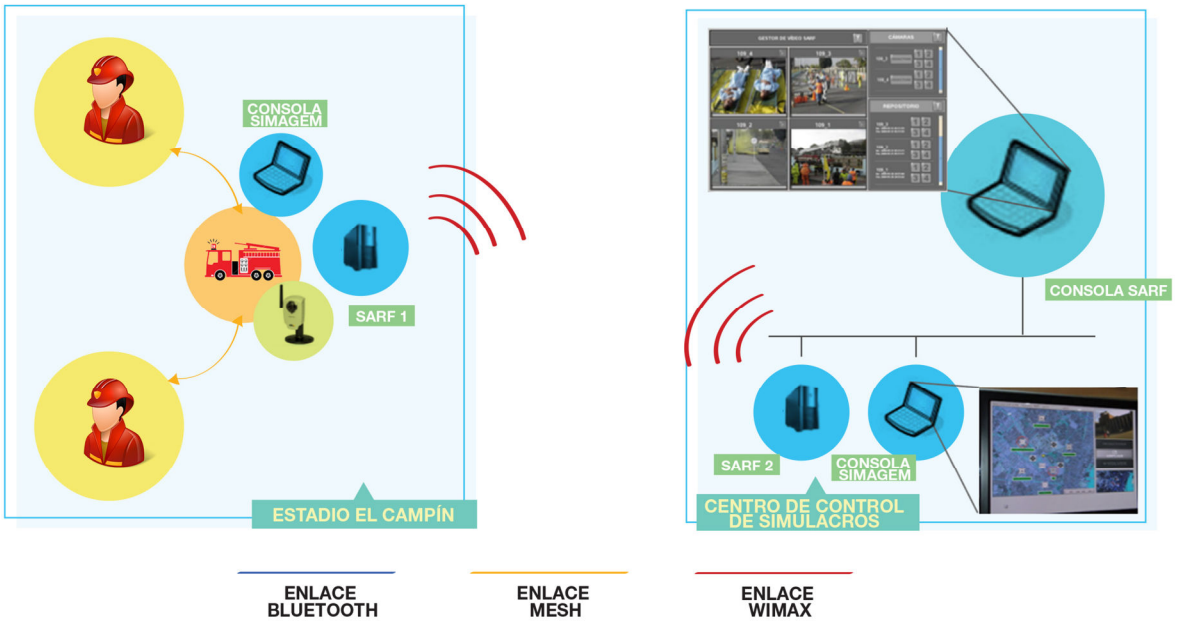

Figura 106. Esquema de comunicaciones del escenario ataque NBQ

En este escenario GESTOP fue introducido en su versión desmontada con SBC. El sistema se probó con grupo de emergencias NBQ de la policía nacional. En la zona de operaciones, cada miembro del equipo estaba equipado con un SBC con GPS Bluetooth asociado y una cámara de video IP montada en su casco dentro del traje de protección para obtener el video en perspectiva subjetiva, de esta manera, tanto el vídeo como su posición se inyectaban en el sistema de mando y control, GESTOP.

Adicionalmente se instalaron cámaras montadas en el vehículo con el puesto de mando de primer nivel para tener una visión general del escenario tras la explosión. Desde el puesto de mando retrasado, se podía visualizar el posicionamiento de los distintos miembros de la unidad NBQ, así como el video subjetivo y el video de las cámaras instaladas en los vehículos

A nivel de comunicaciones, se utilizó una red MESH para la conexión entre los miembros del equipo NBQ y el puesto de mando de primer nivel. Para la comunicación entre el puesto de mando de primer nivel y el puesto de mando retrasado se utilizó un enlace WiMAX.

Figura 107. Vehículo de comunicaciones WiMAX, con CPE Airspan para enlace hacia el puesto de mando retrasado

Figura 108. Operario NBQ con equipamiento GESTOP dentro del traje de protección

Figura 109. Captura de gestor de vídeos durante el transcurso de la misión desde el puesto de mando de primer nivel

Figura 110. Captura de GESTOP durante el transcurso de la misión desde el puesto de mando de primer nivel

5.3.1.2 Pruebas sobre radios Mesh.

En el mes de enero de 2013, se decidió probar la arquitectura de comunicaciones sobre radios MESH del fabricante BreadCrumb, adquiridas por el grupo de investigación, el objetivo de esta prueba era validar el uso de estas radios en situaciones de emergencia, en las cuales las comunicaciones comerciales, por ejemplo redes 3G / 4G, no estuviesen disponibles o estuviesen colapsadas debido a una catástrofe natural como una inundación en la zona costera. El lugar

seleccionado para realizar las pruebas ha sido la playa de El Puig ubicado en la zona costera de la Comunidad Valenciana.

Figura 111. Topología de red utilizada durante las pruebas

En la Figura 111, se muestra la topología de red utilizada durante la realización de las pruebas. En este escenario se desplegó un puesto de Mando y Control central que coordina las acciones de dos unidades móviles, que atienden la emergencia, la comunicación entre los miembros del equipo se realiza utilizando clientes de VoIP instalados en su dispositivos. Los componentes incluidos en esta operativa son los siguientes:

- **Centro de gestión de emergencias**: Es el puesto de mando y control que coordina la misión de rescate. Este puesto está equipado con un portátil rugerizado Panasonic CF-30, que ejecuta GESTOP, la aplicación localiza cada dispositivo en la unidad y le permite al comandante de la unidad utilizar cualquier funcionalidad de mando y control proporcionada por la aplicación (ej.: localización de usuarios, mensajería, etc.). En este puesto también se configuró una centralita VoIP Asterisk que permite la comunicación entre las distintas unidades.
- **Unidades Móviles**: Para estas pruebas se utilizaron dos unidades móviles, cada una de ellas equipada con 1 PDA que ejecutaba GESTOP y un soft-phone para la comunicación por VoIP y una radio Mesh BreadCrumb para la comunicación con el resto del equipo.

La red desplegada y configurada durante las pruebas soporta las necesidades de intercambio de información de los sistemas de mando y control para uso en situaciones de emergencia. La arquitectura de comunicaciones Mesh propuesta y validada durante esta prueba proporciona soporte para los siguientes flujos de datos:

- VoIP: El uso de VoIP sobre la red Mesh permite la reducción de equipos y utilizar una sola red para transportar toda la información necesaria. Para la prueba se utiliza una centralita de Asterix, con un soft-phone integrado en cada unidad.
- Intercambio de datos GESTOP, el cual requiere muy poco ancho de banda dado que ha sido diseñado para funcionar sobre radios de poco ancho de banda como VHF o HF. Tal como se ha comentado previamente el GESTOP se encarga de distribuir información relativa a posicionamiento de vehículos, alarmas, amenazas, objetos y mensajes de texto corto.

En cuanto al flujo de VoIP, el objetivo de estas pruebas era hacer mediciones de QoS en términos de ancho de banda utilizado, retardo y jitter a distintas distancias del puesto de mando y control. Se obtuvieron las medidas haciendo pruebas de movilidad para analizar la calidad de servicio de los clientes SIP en movimiento.

Para la prueba de VoIP se realizaron llamadas entre las dos unidades móviles ubicadas físicamente de manera equidistante del puesto de mando en los extremos de la red Mesh, primero se ubicaron las unidades a 100 metros de la antena central ubicada en el puesto de mando y se mantuvo la comunicación entre los extremos conforme se alejaban de puesto de control, para la prueba se establecieron puntos de control de QoS cada 100 metros hasta un máximo de 400m, de esta manera se realizaron las pruebas a lo largo de 800 metros de recorrido, analizando y obteniendo medidas QoS. El recorrido completo de las unidades se muestra en la Figura 112.

Figura 112. Ubicación inicial y recorrido realizado con las radios Mesh Breadcumb.

La comunicación que se estableció desde cada unidad en el extremo de la red se realizaba por medio de la antena central ubicada en el puesto de mando, es decir, no había una comunicación directa entre las unidades móviles, por lo que podemos asegurar que siempre se realizan 2 saltos para la conexión y el transcurso de la llamada. El número de saltos y la distancia entre las antenas afecta a los valores de latencia y jitter obtenidos durante la prueba, y ayuda a simular el comportamiento en un situación real en la cual las unidades de emergencia desplegadas en el campo sirven de relay a nivel de red Mesh para lograr una comunicación optima por VoIP entre los miembros del equipo.

De acuerdo a las recomendaciones de la ITU, en términos de QoS para llamadas de VoIP, se específica que el ancho de banda mínimo es de 80Kbps, si este es menor podría escucharse mal la voz. El máximo retardo o latencia es de 150ms de extremo a extremo, para valores mayores de retardo la comunicación se vuelve molesta por la pérdida de interactividad, si se pasa de 200ms la comunicación es imposible. El jitter máximo recomendado en una conversación es de 20ms, entre 20ms y 30ms es aceptable si se incrementa a más de 100ms sería imposible la comunicación. Las pérdidas de paquete no deberían superar 3%, según vaya aumentando el porcentaje poco a poco se verá afectada la calidad de la llamada.

Teniendo en cuenta los parámetros de referencia establecidos por la ITU, procedemos a analizar los resultados obtenidos durante la prueba. En las siguientes graficas se mostraran 4 graficas por medida de QoS, la primera grafica corresponderá a 100m(a) la segunda a 200m(b) la tercera 300m(c) y la cuarta 400m(d).

Para estimar el ancho de banda utilizado durante la prueba de VoIP el tamaño de la carga útil se estimó en base al bloque de entrega del codificador y al número de bloques a transportar en un paquete (cabeceras) [Kim11]. Para esta prueba se utilizó el códec G.711 a-Low desde los 2 clientes SIP y con un periodo de empaquetado de 20ms, el tamaño de la carga útil fue de 160 Byte y con un promedio de tasa real de transmisión o ancho de banda requerido de 87,2Kbps (con

cabeceras IP/UDP/RTP) en una llamada. En la siguiente gráfica se observa el ancho de banda consumido en cada una de las distancias establecidas como punto de control.

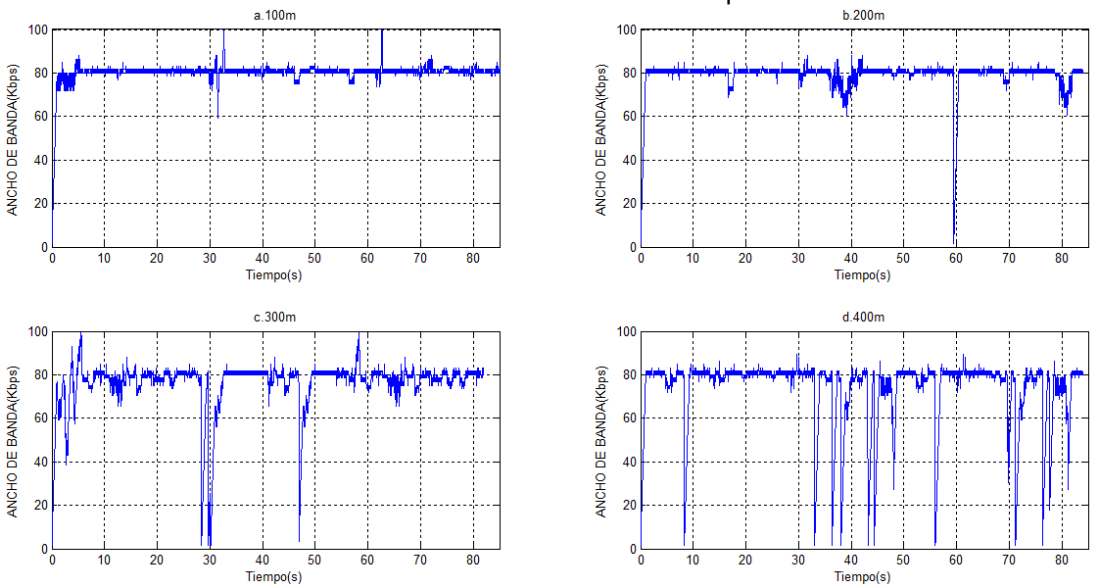

Figura 113. Ancho de banda medido.

En la primera grafica representa el ancho de banda a 100m de distancia de una antena a otra, con un promedio de 80.15Kbps, el cual se mantiene un poco constante en el trascurso de la llamada durante 80s. Este promedio está según la UIT en el ancho de banda mínimo permitido para una conversación VoIP, que es de 80Kbps. A distancias superiores (200m, 300m y 400m) se observa como ya no es constante el trafico RTP en las conversaciones, las cuales presentan fluctuaciones de alto rango de ancho de banda. Estos datos se puede ver reflejado en el promedio de estas distancias, pues a 200m se tiene un promedio de 79.04Kbps, a 300m de 76.12Kpbs y a 400m de 73.71Kbps los cuales se encuentran por debajo del ancho de banda mínimo permitido por la UIT [ITU].

En cuanto a la latencia, a continuación se muestran las gráficas obtenidas para cada una de las distancias establecidas como punto de control.

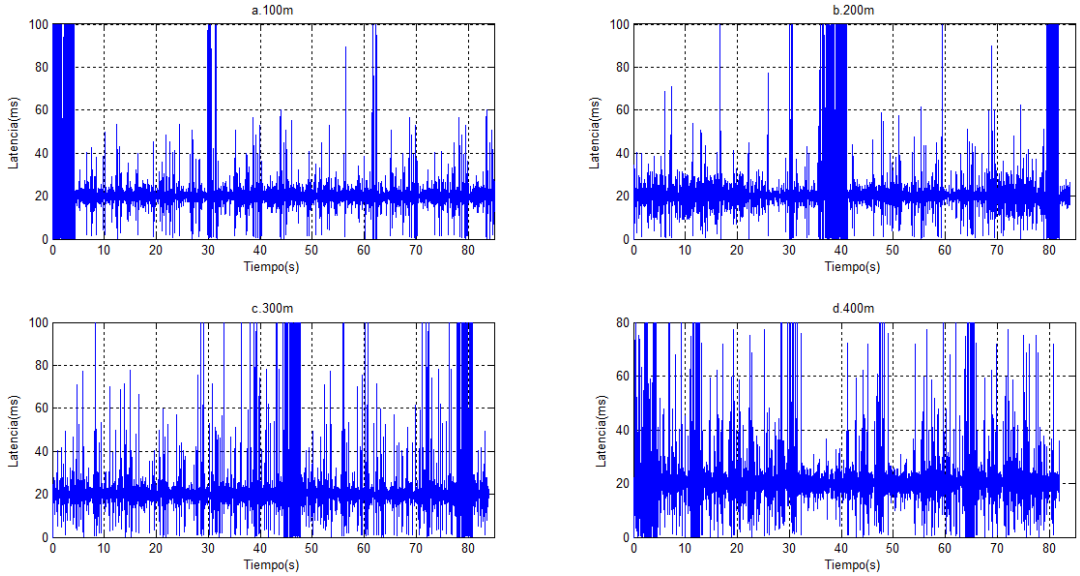

Figura 114. Latencia medida a gran escala

En la Figura 114.a se observa que la mayoría valores capturados a 100m de distancia, llegan con un retardo alrededor de 20ms, a esta distancia la comunicación fue clara, fluida y no se percibían ningún tipo de retardo al igual que la Figura 114.b en la que se sostuvo también una buena conversación sin ningún tipo retraso, en ésta los valores del retardo aumentan, ya que la mayoría de los paquetes llegan con una latencia de alrededor de los 30ms. En la Figura 114.c la latencia en muchos de los paquetes se incrementa al doble con respecto a la Figura 114.a algunos llegando a valores de los casi 50ms, a diferencia de la Figura 114.d en la que cual la conversación se mantiene menos estable con cortes de voz, teniendo más con valores de latencia por encima de 40ms. Todos los valores promedios de las gráficas están por debajo del valor máximo de retardo permitido por la ITU para llamadas VoIP, el cual es de 150 ms, pero evidentemente si hubiera más terminales Mesh estos valores aumentarían.

En cuanto al Jitter, en la Figura 115.a se muestra como se empieza con un jitter de casi 20ms pero luego el tiempo de llegada de un paquete con respecto al otro, se estabiliza más en la mayoría de los paquetes ya que se mantienen con un jitter por debajo de los 4ms, en la Figura 115.b se observa que hay más paquetes manteniéndose con valores de 4 y 5 ms, en la Figura 115.c la mayoría de los paquetes sobrepasa los valores de jitter de 5ms, también hay valores de 10ms y picos que llegan por encima de los 25ms y en la Figura 115.d hay más valores con 10ms de jitter con relación a las distancias anteriores y picos más altos que llegan hasta casi 180ms como se puede apreciar en la figura 23.

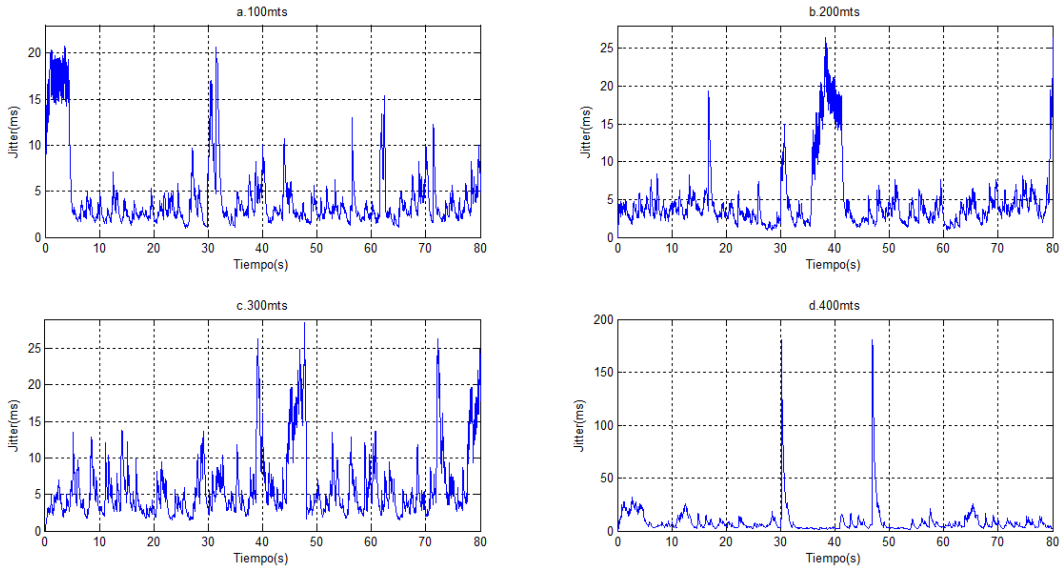

Figura 115. Jitter medido durante las pruebas

El jitter promedio medido para 100m es de 4,23ms, para 200m es de 5ms, para 300m 6,14ms y de 400m 8,56ms. Estos promedios de cada distancia están por debajo del valor máximo recomendado para mantener una excelente comunicación que es de 20ms.

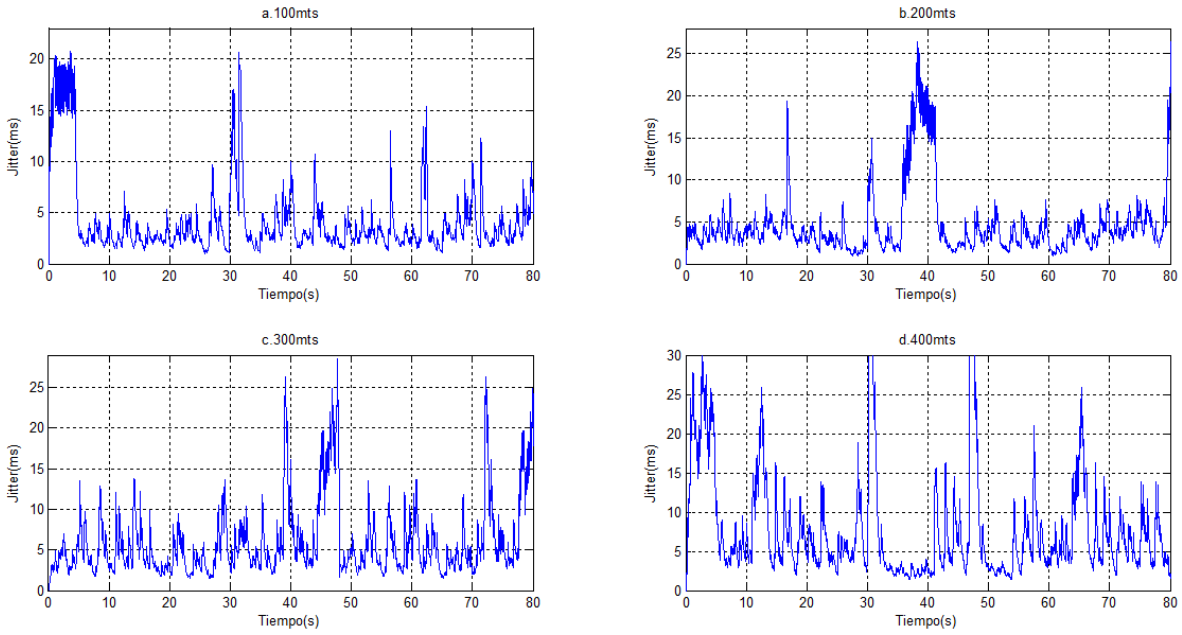

Figura 116. Jitter promedio medido durante las pruebas

Las pruebas llevadas a cabo han permitido validar el uso de Mesh como una tecnología adecuada para establecer comunicaciones de voz al interior de un equipo de atención de emergencia, sobre todo tras una catástrofe natural cuando los medios de comunicaciones habituales no están disponibles.

A pesar que de que a priori el alcance puede parecer corto, debemos tener en cuenta que al combinar la tecnología Mesh con una tecnología WMAN como WiMAX se podría cubrir áreas mucho más extensas e interconectar distintos equipos de trabajo de forma fiable y gracias al uso de tecnología COTS a un precio mucho más asequibles que otras soluciones similares.

5.3.2 Conclusiones sobre la validación de la arquitectura en el escenario 2.

En los distintos escenarios de pruebas, se ha podido comprobar una vez más la flexibilidad de la arquitectura de comunicaciones propuesta que en este caso integra a medios comunicaciones civiles como WiFi IEEE 802.11, WiMAX y Mesh, adaptándose al ancho de banda y las condiciones de QoS disponibles en el medio de transmisión subyacente.

En las distintas pruebas realizadas se pudo probar de forma satisfactoria la arquitectura multinivel de codificación, streaming y replicación de video desarrollada en un entorno real de gestión de emergencias en el ámbito civil. Y los responsables de las operaciones de emergencia valoraron muy positivamente la posibilidad de ver con sus propios ojos lo que ocurre en el terreno, lo que mejora la percepción conjunta de la situación, que hace posible la auto sincronización e incrementa su capacidad para la toma de decisiones.

También se ha podido validar el uso de VoIP sobre redes Mesh dentro la arquitectura, está tecnología es útil para la coordinación y atención de una emergencia entre los miembros del equipo de rescate cuando en una situación de catástrofe los medios de comunicación comerciales, por ejemplo redes 3G / 4G, no están disponibles o están colapsadas.

5.4 Escenario 3: Comunicaciones tácticas sobre WiMAX

El regimiento 81 de Artillería Anti-Aérea (AAA) del Ejército de Tierra, decidió probar la arquitectura de comunicaciones tácticas sobre WiMAX propuesta por la UPV, dada la necesidad de esta unidad de conectar las unidades de tiro entre ellas y con el puesto de mando. Actualmente, la unidad despliega varios Km de cable coaxial o fibra óptica, para conectar dichos componentes lo cual genera varios problemas como roturas en el cable o el tiempo necesario para el despliegue. El resto de medios inalámbricos en uso como VHF y HF no proporcionan el ancho de banda suficiente para soportar todos los servicios necesarios.

En este escenario de pruebas, se ha utilizado WiMAX como una WMAN a nivel de HQ. Además se ha utilizado la herramienta de gestión y configuración de redes WiMAX, denominada WiMTAC, explicada en el anterior capitulo y que ha sido desarrollada durante la fase de investigación de la tesis.

5.4.1 Descripción del escenario de pruebas

En la Figura 117, se muestra la arquitectura de comunicaciones utilizada durante el despliegue de la de la unidad de AAA. Como se puede ver, el centro de mando de seguimiento y disparo de una unidad AAA está compuesto de varios elementos distribuidos, cada uno de los cuales provee cierta información o control. El sistema necesita mecanismos de comunicación en tiempo real, con bajos retados y jitter controlado, además necesita un ancho de banda garantizado para ciertas aplicaciones. Los componentes incluidos en esta operativa son los siguientes:

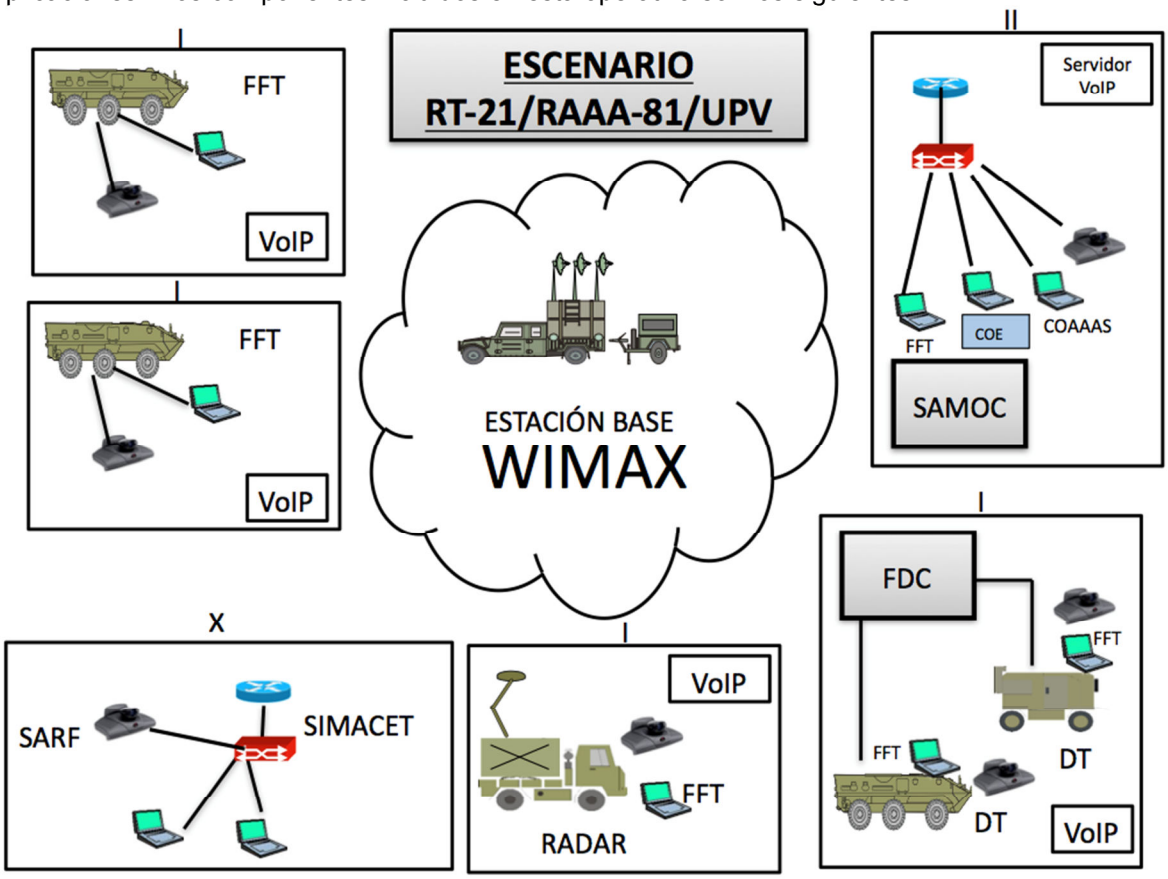

Figura 117. Despliegue de red WiMAX utilizado durante las pruebas

- **Centro de operaciones de misiles tierra-aire (SAMOC):** Es el puesto de mando y control de la unidad AAA a nivel de batallón. En el SAMOC se ejecuta un sistema C2I llamado COAAAS (Sistema del Centro de Operaciones de la AAA). El COAAAS recibe principalmente información de localización y seguimiento de los objetivos del RADAR. La aplicación COAAAS distribuye y asigna los objetivos a las baterías de dirección de tiro.

  El SAMOC también está conectado al sistema SIMACET-FFT. En el caso de la AAA, la aplicación localiza cada dispositivo en la unidad y le permite al comandante de la unidad utilizar cualquier funcionalidad de mando y control proporcionada por la aplicación (ej.: localización de objetivos o visualización de atributos). Adicionalmente, el SAMOC puede hacer uso de video streaming a través del SARF también desarrollado por la UPV y en uso por el Ejército de Tierra.

- **Centro de Dirección de tiro (FDC):** Este componente está equipado con sensores opto-electrónicos y un radar para seguimiento de objetivos de corto alcance y para hacer cálculos de disparo que son enviados a las baterías AAA. La información procedente de los sensores requiere mucho ancho de banda, además este flujo de información requiere alta prioridad y bajo retardo en la transmisión, para que los cálculos sean efectivos.
- **RADAR:** Se utiliza para obtener información de exploración, seguimiento y detección, la cual es la información principal que alimenta al COAAAS en el SAMOC. La información de este nodo es crítica para unidades de este tipo, para poder seguir a los objetivos, los datos deben estar disponibles en tiempo real en el SAMOC.
- **Baterías AAA:** La razón de existencia de una unidad AAA son las baterías. El grupo AAA utilizado durante esta prueba estaba compuesto de una batería SAM Roland con un vehículo de comando APC, vehículos de logística y dos lanzadores Roland SAM sobre un chasis AMC30 y una batería de cañones AA con dos cañones dobles Oerlikon de 35mm. Cada uno de las baterías tenía su propio FDC.
- **Estación Base WiMAX:** se utilizó una estación base WiMAX (Figura 118), para proporcionar comunicaciones de banda ancha entre los componentes distribuidos de todo el sistema. Durante las pruebas de campo se utilizaron dos modelos: Una estación base AirSpan instalada en vehículo HMMWV y una BS ultra-ligera con la parte radiante atada un mástil portátil camuflado en el área forestal. Debido a la naturaleza táctica del sistema, su utilizo una antena omnidireccional, con menor ganancia que la da una antena directiva pero que por el contrario ofrece un uso más táctico, es decir, alta movilidad de los componentes del sistema que permite una rápida reorganización para dificultar la detección y evitar la neutralización de las acciones de los enemigos.
- **Puesto de mando nivel Brigada:** En este puesto se ejecuta SIMACET (Sistema de Mando y Control del Ejército de Tierra). Este sistema recibe información del COAAAS y también del FFT y de las unidades de artillería a nivel de batallón. Este puesto de mando, también recibe información de otras unidades relacionadas con la brigada y unidades vecinas, además también puede recibir de cualquier unidad aliada a través de NFFI.

En todos los vehículos involucrados en la prueba se instaló un cliente WiMAX (CPE), en la Figura 119, se puede ver el cliente instalado en el SAMOC. Los CPEs instalados en los vehículos utilizaban antenas omnidireccionales y el utilizado en el SAMOC utilizaba una antena directiva de alta ganancia. De igual manera, el centro de logística estaba conectado con una antena directiva a la red WiMAX. Esta conexión se ha hecho con el objetivo de probar la posibilidad de tener una posición en la retaguardia conectada a cierta distancia de la unidad AAA para controlar el stock de munición.

El uso de WiMAX permitió realizar el despliegue de los diferentes componentes de la unidad distribuidos en un área de varias decenas de kilómetros, con aplicaciones que consumen gran ancho de banda y que mejora considerablemente el uso de sistemas radio actualmente en uso en este tipo de unidades militares. Las estaciones base, son lo suficientemente ligeras para ser

desplegadas en distintos lugares y ser reposicionadas rápidamente y los componentes de la unidad AAA se puede ubicar en posiciones protegidas, por ejemplo en RADAR en una zona de bosque o el SAMOC en un barranco.

Figura 118. Estación Base WiMAX

Figura 119. Detalle de CPE WiMAX en el SAMOC

La red desplegada y configurada durante las pruebas soporta las necesidades de intercambio de información de los sistemas de mando y control en uso por la unidad AAA (COAAAS y SIMACET_FFT). La arquitectura de comunicaciones WiMAX propuesta y validada durante esta prueba proporciona soporte para los siguientes flujos de datos:

- Detección, exploración y seguimiento de objetivos del radar, esta es la información más crítica, debido a las restricciones temporales y de precisión. La información debe llegar en tiempo real al SAMOC.
- Video en streaming desde los sensores opto-electrónicos. La transmisión de video en entornos tácticos es aún en tema bajo investigación. Las redes WiMAX son capaces de soportar transmisiones de video, información de mucho valor en una unidad AAA. La red permitió la transmisión de video desde los sensores hacia el servidor de video (SARF), localizado en el SAMOC, en un topología de estrella, para la posterior transmisión de video bajo demanda en tiempo real de flujos específicos hacia los terminales FFT localizados en los vehículos de la unidad, así como a cualquier puesto de mando retrasado que lo requiriese utilizando un enlace backhaul para este propósito.
- VoIP, actualmente las comunicaciones de voz dentro de la unidad se utilizan radios VHF PR4Gv3, el uso de VoIP sobre la red WiMAX permite la reducción de equipos y utilizar una sola red para transportar toda la información necesaria. Para la prueba se utiliza una centralita de Asterix, con un soft-phone integrado en cada vehículo.
- Intercambio de datos FFT, el cual requiere muy poco ancho de banda dado que ha sido diseñado para funcionar sobre radios de poco ancho de banda como VHF o HF. Tal como se ha comentado previamente el FFT se encarga de distribuir información relativa a posicionamiento de vehículos, alarmas, amenazas, objetos y mensajes de texto corto. El cliente FFT también permite la posibilidad de reproducir video en tiempo real o bajo demanda. Esta característica es interesante cuando un miembro de la unidad necesita acceder a los flujos de video de los sensores opto-electrónicos recibidos en el SAMOC.

Adicionalmente, el puesto de mando de nivel Brigada tiene un enlace directo a la red WiMAX de la unidad AAA para recibir información de cualquier nodo C2I desplegado. La información del COAAAS, FFT y flujos de video en el SAMOC se utiliza para alimentar el sistema C2IS SIMACET.

La configuración de terminales, seguridad, direccionamiento y flujos de información de la red WiMAX se realizó con la herramienta WIMTAC, desarrollada durante la fase de investigación de la presente tesis.

La clasificación de los flujos de información en la clase de servicio adecuado en la red WiMAX garantizan los niveles de QoS y QoE aceptables para los usuarios finales. A continuación se detallan la asignación de clases de servicio (definidas en el estándar IEEE 802.16) utilizadas durante la prueba:

- La flujo de Radar se mapeo a la clase de servicio rtPS, con prioridad máxima y 10Mbps garantizados tanto en el uplink como en el downlink.
- El flujo de video se mapeo a la clase de servicio rtPS con menor prioridad y un ancho de banda garantizado de 1Mbps para cada sensor opto-electrónico conectado a la red.
- El flujo de VoIP, se mapeo a la clase de servicio UGS (Unsolicited Grant Service) con un retardo mínimo y con un jitter garantizado de 256Kpbs por cliente en el uplink.
- El flujo de FFT se mapeo a la clase nrtPS (non real time Polling service) con un 1Mbps por cliente WiMAX.
- Adicionalmente, todos los flujos en downlink, se mapearon a la clase BE (Best Effort) a excepción del flujo del radar debido a la criticidad del sistema

Los recursos que proporciona la red WiMAX son mayores que los que ofrecen las radios de combate tradicionales, sin embargo, son limitados. De hecho, una de las principales características de WIMAX es que proporciona mecanismos para gestionar de forma adecuada los recursos para optimizar el desempeño global de la red. El uso de parámetros de configuración adecuados para cada servicio garantiza que la unidad AAA obtenga el mejor desempeño posible con la red WiMAX y que mejore la operatividad en el despliegue de la unidad. WiMTAC ha sido diseñado específicamente para uso táctico de WiMAX con el objetivo de facilitar la configuración correcta de parámetros y obtener al máximo desempeño técnico y la máxima operatividad táctica.

Durante las pruebas de campo, el primer punto a probar era la configuración de la red WiMAX, se utilizaron los parámetros en la Tabla 17, los cuales fueron configurados a través de WiMTAC. Los parámetros de la red WiMAX que afectaron directamente el desempeño del sistema fueron los siguientes:

- Scheduling Type: Durante la prueba se utiliza UGS para el flujo de VOIP dado que requiere una tasa de trasmisión de datos constante, rtPS para los flujos que requieran poco retardo y jitter como el radar y la distribución de vídeo desde los sensores opto-electrónicos y nrtPS para el tráfico FFT el cual puede tolerar retardos.
- Scheduling Polling Period y Traffic Priority: estos parámetros están relacionas con el parámetro anterior y especifican una cuantificación de la prioridad asignada a cada flujo, los más críticos tienen una mayor prioridad.
- Maximum Sustained Rate: Es la tasa máxima de transmisión asignada a un servicio de acuerdo a sus requisitos de ancho de banda. En la pruebas de campo con la unidad AAA, la tasa más alta fue asignada al radar y la más baja al servicio de VoIP.
- Minimum Reserved Rate: Es el ancho de banda mínimo garantizado para cada servicio, el más alto fue asignado al radar y el más bajo al servicio de VoIP.
- Tolerated Jitter: Cuantifica la tolerancia del servicio al jitter debido a los cambios en la carga de red. VoIP tiene un valor de 0 y el radar es el siguiente jitter más bajo debido a la naturaleza de la información y los requisitos de procesamiento en el SAMOC. El video y el FFT se configuraron con tasas más tolerantes al jitter.
- Maximum Latency: Cuantifica el retardo máximo entre el emisor y el receptor del flujo de información. El vídeo y la VoIP son más sensibles a la latencia y el radar y el FFT menos.

	Video	Radar	VoIP	FFT
Scheduling Type:	**rtPS**	**rtPS**	**UGS**	**nrtPS**
Scheduling Polling Period	70	90	30	90
Traffic Priority	5	4	7	6
Max. Sustained Rate	5 Mbps	10 Mbps	200 Kbps	1 Mbps
Min. Reserved Rate	2 Mbps	5 Mbps	200 Kbps	500 Kbps
Tolerated Jitter	100 ms	50 ms	0	100 ms
Max. Latency	150 ms	200 ms	150 ms	200 ms

Tabla 17. Parámetros de QoS utilizados en la red WiMAX durante las pruebas

La Figura 120, muestra la distribución de las unidades de AAA durante la prueba de campo, vista en una captura de pantalla de SIMACET-FFT. El puesto de mando de nivel Brigada también tenía una conexión WiMAX y estaba localizado a 20Km de la estación y no se ve en la captura de pantalla.

Figura 120. Captura de FFT con el detalle del despliegue de las unidades AAA

Después de la prueba de campo, los miembros de la unidad de AAA llenaron un cuestionario compuesto de 50 preguntas para medir la QoE. Las preguntas estaban relacionas con las ventajas operativas de utilizar WiMAX y la usabilidad de WIMTAC como herramienta táctica que pudiese mejorar el despliegue, gestión y configuración de una red WiMAX y de la unidad AAA. La Tabla 18 resume las respuesta más relevantes proporcionadas por lo usuarios (10 en total) desde teniente coronel a sargento, con valores de 0 a 5.

Pregunta	Valoración
El despliegue y la configuración de la red WiMAX (BS y CPE) fue lo suficientemente rápido	4.6
La operativa de la unidad se mantuvo al menos al mismo nivel que cuando se utilizan los medios de comunicación habituales	5
Las trazas de radar no sufrieron ningún retardo durante las pruebas	5
Los servicios integrados sobre WiMAX fueron de utilidad para la operativa de la unidad	4.3
Valoración del servicio de streaming de video	4.8
Valoración del servicio de VoIP	4.2
Valoración del servicio FFT	4.7
Valoración de WiMTAC como herramienta táctica para las unidades AAA	4.5
Los procedimientos operativos de la unidad y el desempeño pueden ser mejorados con el uso de WiMAX	4.6

Tabla 18. Validación QoE realizada por el personal militar implicado en las pruebas

Los resultados de los cuestionarios fueron positivos, dos de las preguntas obtuvieron una valoración máxima de 5. Primero, los procedimientos operativos de la unidad fueron los mismos

que si se utilizasen los medios de comunicación habituales, es decir, el utilizar WiMAX no produjo una reducción en la capacidad de operación de la unidad. Esta pregunta, tuvo una respuesta razonable debido al mayor ancho de banda que proporciona la red WiMAX en comparación con los medios en uso actualmente. También se evaluaba, si el uso de esta tecnología inalámbrica supondría una sobrecarga operativa para la unidad, los cual evidentemente resulto negativo.

En segundo lugar, el principal servicio de la unidad de AAA, es la traza del radar, ya que está alimenta la herramienta de mando y control (COAAAS) y no dejo de funcionar y no hubo retardos en la transmisión durante las pruebas. Este era el flujo más crítico en este caso de uso de la red WiMAX.

En relación al resto de preguntas, la valoración fue positiva, es de destacar el servicio de transmisión de vídeo desde los sensores opto-electrónicos. Al momento de las pruebas, no se utilizaba ningún sensor de video en la unidad de AAA, lo cual supuso una experiencia muy positiva. El uso de video en la unidad de AAA era imposible debido al uso de radio VHF con muy poco ancho de banda para conectar al SAMOC con el FDC. Al momento de las pruebas, no existía una doctrina de uso de este tipo de sensores, por lo tanto las respuestas relacionadas a las preguntas relativas a la transmisión de video reflejan la opinión personal de los individuos. También hubo una alta valoración del FFT como sistema, el cual está perfectamente integrado con la herramienta de distribución de video y también con el uso de WiMTAC como herramienta táctica para configurar la red WiMAX.

5.4.2 Conclusiones sobre la validación de la arquitectura en el escenario 3.

Existe una necesidad de una red WMAN dentro del puesto de mando de una unidad militar táctica, principalmente cuando las necesidades de ancho de banda aumentan (Ej.: distribución de vídeo). WiMAX proporciona una reducción en el tiempo de despliegue, así como, un incremento significativo en ancho de banda y desempeño lo cual proporciona la capacidad de introducir nuevos servicios.

Se han presentado las pruebas de campo llevadas a cabo en la unidad de AAA, utilizando WiMAX como medio de comunicación, para medir la QoE en el despliegue y la inclusión de nuevos sensores y servicios (VoIP y Video). La evaluación del desempeño de la arquitectura propuesta fue exitosa y la QoE percibida por los usuarios se validó por medio de un cuestionario. La unidad se integró por medio del sistema SIMACET-FFT, utilizando la red WiMAX para distribuir los datos.

El resultado de la prueba de campo has sido que WiMAX puede proporcionar comunicaciones dentro de una unidad sustituyendo todos los cables y otros medios de comunicación inalámbrica, con un incremento en rango de cobertura, ancho de banda y tiempo de despliegue. Debido al soporte de IP en WiMAX, es posible soportar mecanismos específicos de COMSEC, siendo entonces esta tecnología un candidato COTS para proporcionar soporte WMAN a nivel de batallón u otras unidades tácticas en el campo de batalla. El sistema fue valorado subjetivamente y la respuesta de los usuarios fue altamente positiva.

6 Conclusiones y trabajo futuro

En el presente punto se detallan, de manera concisa, las principales conclusiones de la presente tesis doctoral y se apuntan las posibles líneas de continuación de la misma.

6.1 Conclusiones

Durante el transcurso de la presente tesis doctoral se han ido cumpliendo todos y cada uno de los objetivos que se habían propuesto al comienzo de esta investigación

En este apartado de conclusiones finales, se va a describir como se han ido alcanzando los objetivos prioritarios de esta investigación, fijados al comienzo de la misma, así como las lecciones que se pueden extraer de la consecución de estos objetivos y los posibles beneficios que esta investigación puede aportar.

Los objetivos prioritarios de la presente tesis, que se han cumplido durante el desarrollo de la misma son los siguientes:

Se ha realizado un exhaustivo y profundo análisis del estado del arte acerca de las arquitecturas de comunicaciones inalámbricas en sistemas de mando y control, desde sus comienzos hasta las últimas propuestas. Este trabajo ha conducido a la evaluación y estudio de los distintos modelos teóricos y aproximaciones a las comunicaciones tácticas para sistema mando y control, particularizando en los conceptos y líneas de investigación más novedosos surgidos a partir de los trabajos promovidos y auspiciados por el Command and Control Research Programme (CCRP) del departamento de defensa estadounidense (DoD, Department of Defense). Además se han investigado, estudiado y evaluado las distintas arquitecturas y aproximaciones existentes en el área de comunicaciones inalámbricas para sistemas C4ISR de pequeña unidad, área a la que se circunscribe la presente tesis. Por otra parte, al ser los sistemas C4ISR complejos elementos que integran múltiples módulos tecnológicos, se ha llevado a cabo un profundo y extenso estado del arte los componentes tecnológicos de las arquitecturas de comunicaciones de sistemas C4ISR. Para ello, se han realizado completos estados del arte en las áreas de arquitectura y frameworks de sistemas C4ISR, sistemas de comunicaciones tácticos, arquitecturas cross-layer, redes cognitivas, enrutamiento en redes tácticas, modelos de Calidad de Servicio (QoS) y sistemas de gestión.

Con todo ese conocimiento adquirido se ha propuesto una arquitectura de comunicaciones para sistemas de mando y control de pequeñas unidades que constituye la principal aportación científica de la presente tesis. Dicha arquitectura se ha descompuesto en tres planos un plano de red, un plano de software y un plano de gestión cross-layer como módulos constituyentes fundamentales.

Para poder certificar la validez de la arquitectura de comunicaciones propuesta se ha diseñado, desarrollado e implementado, siguiendo los principios y especificaciones de la misma y se ha probado dentro del sistema de mando y control de pequeña unidad llamada SIMACOP desarrollado dentro del grupo de investigación de forma paralela. La arquitectura de comunicaciones se ha probado exitosamente sobre distintos medios de transmisión tanto militares (HF, VHF, Satélites militares) como civiles (satélites comerciales, mesh, wifi, WiMAX). La arquitectura de comunicaciones propuesta ha permitido utilizar indistintamente y de manera transparente al usuario cualquiera de los principales medios radio tácticos disponibles, tanto civiles como militares. Debido a las limitaciones de los entornos tácticos, se han desarrollado esquemas de réplica que permiten una eficiente diseminación de la información en tiempo útil en entornos tan adversos como los tácticos. Una vez validad la arquitectura de comunicaciones desarrollada se ha incluido dentro la solución vehicular de seguimiento de fuerzas propias (FFT) que es la que

actualmente utiliza el Ejército de Tierra español. Por otra parte, la inclusión de flujos multimedia ha sido una destacada aportación en el ámbito de la integración de sensores de la arquitectura propuesta.

Las implementaciones desarrolladas han sido validadas en múltiples demostraciones, maniobras militares, ejercicios y pruebas de validación de organismos nacionales e internacionales. Al ser validadas sus implementaciones consideramos que se valida de forma evidente y en consecuencia la arquitectura de comunicaciones propuesta, contribución principal de la presente tesis. En particular, las implementaciones desarrolladas han sido probadas y evaluadas en los ejercicios Coalition Warrior Interoperability Demonstration (CWID) de la OTAN, tanto nacionales como internacionales, en las demostración de un proyecto europeo de investigación del sexto programa marco, en demostraciones y ejercicios para el Regimiento de Trasmisiones 21(RT-21), Brigada de Transmisiones (BRITRANS), Unidad Militar de Emergencias (UME), Regimiento de Caballería Ligera no. 8 Lusitania (RCL-8). En el ámbito civil, ha sido validada por el Consorcio Provincial de Bomberos, Guardia Civil, protección civil y Organizaciones No Gubernamentales (ONG). De manera internacional también ha sido validada por organismos de atención de emergencias en Colombia como la Dirección Nacional de Prevención y Atención de Riegos (DPAE). Por otra parte una de las implementaciones ha sido exhaustivamente evaluada por parte del organismo JCISAT del Ejército de Tierra pruebas que han conducido a su adquisición por el mismo, compra que nos parece una validación evidente del sistema implementado y, por lo tanto, de la arquitectura propuesta.

Diversas aportaciones de la tesis han contribuido en gran medida a la participación del Grupo de Sistemas de Tiempo Real Distribuido en los proyectos europeos: PASR-MARIUS (Mobile Autonomous Reactive Information system for Urgency Situations), PASR-CITRINE (Common Intelligence and Traceability for Rescues and IdentificatioN opErations), IST-DYVINE (DYnamic VIsual NEtworks) y WOLF (Wireless Robust Link for Urban Force Operations), éste último de la Agencia Europea de Defensa (EDA).

En cuanto a las mejoras y ventajas, que las investigaciones realizadas en la presente tesis, pueden aportar en el campo de arquitecturas de comunicaciones para sistemas de mando y control de pequeña unidad, podríamos enumerar las siguientes:

- La propuesta de una arquitectura de comunicaciones cross-layer, cognitiva para sistemas de mando y control de pequeñas unidades flexible, que permite la integración de tecnologías de comunicaciones heterogéneas en la arquitectura de red, la inclusión masiva de sensores y redes de sensores y la inclusión de flujos multimedia para mejorar la Common Operational Picture (COP) de los oficiales al mando de una operación al permitirles, “ver con sus propios ojos”, lo que está ocurriendo en un punto concreto del teatro de operaciones. Además, la arquitectura propuesta permite visualizar dichos flujos en cualquier punto de la red, aplicando el concepto teórico de 'sensor-to-the-net'.
- El desarrollo e inclusión de mecanismos de réplica robustos y eficientes que permitan que todos los sistemas de mando y control implicados en una operación compartan la información en ‘tiempo útil’ y puedan disponer de la misma visión del teatro de operaciones pese a las condiciones adversas de los entornos tácticos.
- La elevada valoración por parte de los usuarios finales de los sistemas desarrollados como elementos que aportaban una mejora considerable en su desempeño a la hora de cumplir las misiones asignadas, tal y como se ha visto en el capítulo 5 de validación.
- El hecho de que uno de los sistemas desarrollados para validar las propuestas teóricas de la presente tesis esté en uso por el Ejército de Tierra español nos parece una de las principales aportaciones a la sociedad del presente trabajo.

La investigación realizada en la presente tesis ha generado las siguientes publicaciones:

- Tactical Use of WiMAX-based networks for anti-aircraft artillery units. IEEE Military Communications Conference, 2011 - MILCOM 2011; ISBN: 978-1-4673-0079-7.
- Video Distribution Framework for Tactical Operations. IEEE Military Communications Conference, 2011 - MILCOM 2011; ISBN: 978-1-4673-0079-7.
- Video sensors integration in a C2I system. Military Communications Conference, 2009. MILCOM 2009. IEEE; ISBN: 978-1-4244-5238-5.
- SIMACET-FFT: Spanish Army friendly force tracking system. Military Communications Conference, 2009. MILCOM 2009. IEEE; ISBN: 978-1-4244-5238-5.
- SIMACOP: Small Units Management C4ISR System. IEEE International Conference on Multimedia and Expo, 2007 – ICME 2007; ISBN: 1-4244-1016-9.

También ha generado la participación en los siguientes congresos especializados en temáticas de Mando y Control:

- Video Integration in Friendly Force Tracking systems: SIMACOP-FFT, a field experience. 14th International Command and Control Research and Technology Symposium ICCRTS 2009:“C2 and Agility”.
- Flexible Command and Control Architecture to Achieve Agility. 14th International Command and Control Research and Technology Symposium ICCRTS 2009:“C2 and Agility”.

6.2 Trabajo futuro

Esta tesis se enmarca dentro de la línea de investigación de mando y control en el grupo de Sistemas de Tiempo Real Distribuido de la UPV que ya ha dado lugar a otras tesis relativas a modelos de datos en entornos tácticos [Car07] y a arquitecturas de sistemas C4ISR de pequeña unidad [Pér09] y en breve dará lugar a otras más. En el ámbito concreto de las arquitecturas de comunicaciones inalámbricas para sistemas C4ISR, objeto de esta tesis, se está trabajando ya y/o se prevén como puntos en los que ahondar la tarea de investigación y desarrollo los siguientes:

Tomando como referencia la aproximación de diseño cross-layer y agnóstica del medio de transmisión de la arquitectura de comunicaciones propuesta en esta tesis, la cual estaba centrada exclusivamente en la capa de aplicación para un sistema C4ISR se puede extrapolar para crear un router táctico o gestor de comunicaciones software cuyo objetivo final sea que cualquier aplicación de usuario utilice la Red Radio de Combate de forma transparente como si de una red IP convencional se tratara.

Otra línea de trabajo es la de proponer, diseñar e implementar un modelo de referencia de arquitectura abierta para entornos tácticos, el enfoque a seguir sería definir un modelo similar al OSI (pero sin los inconvenientes de este último) que defina las capas de la pila como entidades con Interface Control Documents (ICDs) bien definidos entre ellos.

El modelo OSI no se aplica directamente a las redes tácticas por muchas razones entre ellos los requisitos de seguridad exigidos. La literatura está llena de críticas al modelo OSI y similares, incluyendo el modelo TCP/IP. Aunque el modelo TCP/IP es ahora la tecnología dominante y es previsible que lo siga siendo durante un tiempo indefinido. Técnicas como la señalización cross-layer, la fusión de las capas en la pila de protocolos (especialmente capas 2 y 3), las compensaciones entre la codificación de red, y la fiabilidad de la capa de transporte, son el camino hacia un rendimiento más óptimo de comunicaciones inalámbricas tanto comerciales como tácticas basadas en el modelo IP. Uno de los problemas conocidos con el modelo OSI es la cantidad de

bits de cabecera transmitidos a través de los medios de comunicación física en comparación con los bits de información. Puesto que cada capa funciona de forma independiente con sus propias cabeceras, la relación de datos de cabecera sobre datos de información puede ser muy alta. Por otra parte, debido a la naturaleza poco fiable de enlaces inalámbricos tácticos, los paquetes de redundancia de control de errores de codificación tales como la codificación de red puede disminuir aún más los recursos de ancho de banda disponible para el tráfico de usuario.

Por lo tanto se hace necesario un modelo táctico de arquitectura abierta. Una verdadera arquitectura abierta basada en radios SDR o CR significaría diferentes fabricantes que producen las diferentes capas de la pila de protocolos, como la capa de IP sin cifrado, IP cifrado, o capas de radio que cumplen con estándar dado. Se podría utilizar capa IP sin cifrado del proveedor X y la capa IP sin cifrado del proveedor Y, y las dos capas se comunicarían sin problemas, ya sea en la misma forma de onda o en diferentes formas de onda. Ambas capas IP sin cifrado tendrán capacidad táctica por encima de lo que tiene la capa IP comercial.

Cumplir con una forma de arquitectura abierta es esencial para la evolución de las comunicaciones y redes inalámbricas tácticas. Esto haría un buen uso de las tecnologías comerciales existentes al conseguir la mayor cantidad de funcionalidades en manos de los combatientes con coste reducido. El reto aquí es crear un modelo de arquitectura abierta que no cree ninguna vulnerabilidad o ponga en peligro la seguridad.

Vale la pena señalar que la línea divisoria entre las redes y comunicaciones inalámbricas táctica y comercial se desdibuja en algunas áreas. Los investigadores en ambos campos reconocen el valor de la señalización cross-layer, la gestión cognitiva del espectro, radios cognitivas, la codificación de la red, y así sucesivamente. Sin embargo, las necesidades de seguridad de las comunicaciones inalámbricas tácticas siempre darán lugar a una desviación inevitable. La distinción no debería negar la necesidad de una arquitectura abierta.

En definitiva, el objetivo principal de este modelo de referencia para entornos tácticos sería que los desarrolladores de tecnología se centren en una sola capa de la pila de protocolos, con base en los ICD definidos, para eliminar la necesidad de técnicas propietarias. En lugar de tener que diferentes implementaciones de la capa IP en diferentes radios (lo que hace que la interoperabilidad una pesadilla), los ICD definidos asegurarían la comunicación entre diferentes tecnologías, y al mismo tiempo cumplirían con las restricciones de seguridad adaptándose a la dinámica de las redes tácticas. De esta manera se podrá proporcionar al combatiente o al *first responder* aplicaciones valiosas y con excelentes capacidades de comunicaciones, permitiendo al mismo tiempo que lo integradores de radio y de plataformas adquieran capas de la pila de protocolo de diferentes desarrolladores a bajo costo.

7 Bibliografía

[Abe98]. Abeni, Buttazzo "Integrating multimedia applications in hard real-time systems" In Proceedings of the Real-Time Systems Symposium, pp. 3-13, 1998. (1998).

[ADAMO]. ADAMO: Advanced disaster architecture with mobility optimizations. Web: https://projects.ibbt.beladamo/. Enero 2007. (s.f.).

[Aga00]. S. Agarwal, A. Ahuja, J. P. Singh, R. Shorey. "Route-Lifetime Assessment¬ Based Routing (RAER) Protocol for Mobile Ad Roe Networks". Proceedings of IEEE ICC 2000, vol. 3, pp. 1697-1701. Junio 2000. (2000).

[AGA05]. Elements de départ AGATE et Origine, "Manuel de reference AGATE V3", Diciembre 2005. (2005).

[Ahn00]. C.W. Ahn, C.G. Kang, Y.Z. Cho, "Soft reservation multiple access with priority assignment (SRMA/PA): a novel MAC protocol for QoS-guaranteed integrated services in mobile ad hoc networks", En Proceedings of the IEEE VTC, vol. 2, pp. 942-947, 2000. (2000).

[Alb00]. D.S Alberts, J.J Garstka, F.P Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", Publicación del US Department of Defense Command and Control Research Program (CCRP), segunda edición revisada, Febrero de 2000. (2000).

[Alb03]. D.S. Alberts, R.E 1-layes, "Power to the edge", Publicación del US Department of Defense Command and Control Research Program (CCRP), 2003. (2003).

[Alb06]. D.S. Alberts, R.E Hayes, "Understanding Command and Control", Publicación del US Department of Defense Command and Control Research Program (CCRP), 2006. (2006).

[Alb99]. D.S. Alberts, J.J. Garstka, F.P. Stein, "Network Centric Warfare", Publicación del US Department of Defense Command.and Control Research Program (CCRP). (1999).

[ARE]. http://www.cdt.luth.se/projects/arena/. (s.f.).

[ARS]. AUSA Background Brief, "Army Space Support as a Critica! Enabler of Joint Operations", Institute of Land Warfare Publication, no. 97, Diciembre 2003. (s.f.).

[ATU]. "Arquitectura Técnica Unificada versión 1.0.2" Inspección General CIS, Ministerio de Defensa de España, 2007. (s.f.).

[Aud90]. N. C Audsley, "Deadline monotonic scheduling", Department of Computer Science white paper, University of York, 1990. (1990).

[Bai10]. Y. Bai, W. Du, C. Shen, Y. Zhou, B. Chen. "Emergency Communication System by Heterogeneous Wireless Networking". IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), pp. 488-492, . (2010).

[Bak89]. M. Baker, W. Beamish, M. Turner, "The use of MIL-STD-188-141A in HF data networks", Military Communications Conference (MILCOM'89), vol.1, pp. 75-79, . (1989).

[Bal93]. A. Ballardie, P. Francis, J. Crowcroft. "Core-Based Trees (CBT): An Architecture for Scalable Multicast Routing". Proceedings of ACM SIGCOMM 1993, pp. 85-95. Septiembre. (1993).

[Bal99]. R.O. Baldwin, N.J. Davis IV, S.F. Midkiff, "A real-time Medium Access Control protocol for ad hoc wireless local area networks", Mobile Comput. Commun. Rev. 3 (2), pp. 20-27. (1999).

[BAT]. www.battle-technology.com/this_issue04d.html. (s.f.).

[BATS]. http://www.batswireless.com/pdf/ship-to-shipFinal.pdf. (s.f.).

[Ben01]. M. Benveniste, G. Chesson, M. Hoeben, A. Singla, H. Teunissen, M. Wentink, "EDCF Proposed Draft Text", IEEE Working Document 802.11-01/12 1r1, Marzo. (2001).

[Ber07]. Berioli, M., Courville, N., Werner, M. "Emergency Communications over Satellite: the WISECOM Approach". 16th IST Mobile and Wireless Communications Summit, pp. 1-5. (2007).

[BFS]. http.//www.difesa.it/NR/rdonlyres/9422B093-9646-41D2-B6FA-ABB4A6018960/0/latrasformazionenetcentrica.pdf. (s.f.).

[BIO]. http://www.rusi.org/downloads/assets/Hon_Battlefield_Management_Systems.pdf. (s.f.).

[Bla05]. C. Blais, M.R Hieb, K. Galvin, "Coalition Battle Management Language (C-BML) Study Group Report." Paper 05F-S1W-041, Fall Simulation Interoperability Workshop, Orlando, Florida, Septiembre . (2005).

[Bla95]. Black, Uyless. Network Management Standards. Ed. McGraw-Hill, Inc. (1995).

[Bom98]. E. Bommaiah, M. Liu, A. McAuley, R. Talpade. "AMRoute: Ad HocMulticast Routing Protocol". Internet draft (work in progress), draft-talpade-manet-amroute-00.txt. Agosto . (1998).

[Bre03]. T. Brevick, "Network Centric Warfare - Norwegian Challenges", Canadian Forces Research Project CSC29. (2003).

[Bry05]. J. Brynielsson, M. Engblom, R. Franzen, J. Nordh, L. Voigt "Enhanced Situation Awareness using Random Particles", 10th International Command and Control Research and Technology Symposium (ICCRTS'05), Washington D.C, USA . (2005).

[But93]. G.C. Buttazzo, J.A. Stankovic, "RED: A Robust Earliest Deadline Scheduling Algorithm", En Proceedings of 3rd International Workshop on Responsive Computing Systems. (1993).

[But97]. G. C Buttazzo "Hard Real-time Computing Systems Predictable Scheduling Algorithms and Applications", Kluwer Academie Publishers. (1997).

[C1a90]. Raymond K. Clark "Scheduling Dependent Real-Time Activities", Ph.D. Thesis, CMUCS-90-155, School of Computer Science, Carnegie Mellon University. (1990).

[C2C-CC]. CAR 2 CAR Communication Consortiurn. Web: http://www.car-to-car.org/ . (s.f.).

[C4107]. http://jitc.fhu.disa.mil/. (s.f.).

[C4197]. C4ISR Architectures Working Group (AWG) "C4ISR Architecture Framework Version 2.0" Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Washington D.C, Diciembre . (1997).

[Cap03]. D. Caprioni, A. Russo, Small Unit Operations Situation Awareness System (SUO-SAS) RadioArchitecture And System Field Testing Results, IEEE MILCOM, Monterey (CA), Oct. . (2003).

[Car01]. S. Carey, M. Kleiner, M.R Hieb, R. Brown, "Standardizing Battle Management Language - A Vital Move Towards the Army Transformation." Paper 01F-SIW-067, Fall Simulation Interoperability Workshop, Orlando, Florida, USA, Septiembre . (2001).

[Car06]. M. Carvalho et al., "A Cross-Layer Communications Framework for Tactical Environments". Proceedings - IEEE Military Communications Conference MILCOM. Octubre . (2006).

[Car07] Carvajal Rodrigo, FJ. Adaptación de modelos de datos tácticos de sistemas de información para mando y control a la gestión de emergencias [Tesis doctoral]. Universitat Politècnica de València. doi:10.4995/Thesis/10251/1960. (2007).

[CEC]. http://www.fas.org/man/dod-101/sys/ship/weaps/cec.htm. (s.f.).

[Cha09]. Chakchai S. -In., Jain R., Tamimi A. K. Scheduling in IEEE 802.16e mobile WiMAX networks: key issues and a survey. IEEE Journal on Selected Areas in Communications, pp. 156-171. (2009).

[CHE97]. HEN T.-W., TSAI y GERLA M., "QoS routing performance in multihop multimedia, wireless networks". IEEE 6th International Conference on Universal Personal Communications Record, 1997. Conference Record., 1997, vol. 2, pp. 557¬-561 vol.2. (1997).

[Chi97]. C. C. Chiang, H. K. Wu, W. Liu, M. Gerla. "Routing in Clustered Multi-Hop Mobile Wireless Networks with Fading Channel". Proceedings of IEEE SICON 1997, pp. 197-211, Abril. (1997).

[Chi98]. C. C. Chiang, M. Gerla, L. Zhang. "Forwarding Group Multicasting Protocol for Multi-Hop, Mobile Wireless Networks". ACM/Baltzer Journal of Cluster Computing: Special Issue on Mobile Computing, vol. 1, no. 2, pp. 187-196. (1998).

[Cho04]. Chou, Joey, et al. "MAC and PHY MIB for WirelessMAN and WirelessHUMAN BS and SS". IEEE C802.16mgt-04/04r1, Julio 7. (2004).

[Cla01]. T. H. Clausen, G. Hansen, L. Christensen, G. Behrmann. "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation". Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001, Septiembre . (2001).

[Cla08]. T. Clancy, N. Goergen, "Security in Cognitive Radio Networks:Threats and Mitigation". - Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008, pp. 1-8. (2008).

[CVIS]. CVIS: Cooperative Vehicle-Infrastructure Systems.Web: http://www.cvisproject.org/. (s.f.).

[CWI]. www.cwid.js.mil/public/CWID07CoalitionPartners.pdf. (s.f.).

[Das02]. S. K. Das, B. S. Manoj, C. SivaRam Murthy. "A Dynamic Core-Based Multicast Routing Protocol for Ad Hoc Wireless Networks". Proceedings of ACM MOBIHOC 2002, pp. 24-35, Junio 2000. (2000).

[Das02]. S. K. Das, B. S. Manoj, C. SivaRam Murthy. "Weight-Based Multicast Routing Protocol for Ad Hoc Wireless Networks". Proceedings of IEEE GLOBECOM 2002, vol. 1, pp. 17-21. Noviembre. (2002).

[Dee96]. S. Deering, D. L. Estrin, D. Farinacci, V. Jacobson, C. G. Liu, L. Mei. "The PIM Architecture for Wide-Area Multicast Routing''. IEEE/ACM Transactions on Networking, vol. 4, no. 2, pp. 153-162. Abril . (1996).

[Den99]. D.J. Deng, R.S. Chang, "A priority scheme for IEEE 802.11 DCF access method", IEICE Trans. Commun.1E82-B (1), pp. 96-102. (1999).

[Dev01]. V. Devarapalli, A. A. Selcuk, D. Sidhu. ''MZR: A Multicast Protocol for Mobile Ad Hoc Networks". Internet draft (work in progress), draft-vijay-manet-mzr¬01.txt. Julio . (2001).

[Din98]. E.H. Dinan, B. Jabbari, Spreading codes for direct sequence CDMA and wide band CDMA cellular networks, IEEE Commun. Mag., Septiembre. (1998).

[Don05]. Donahoo Michael, Steckler, Brian. "Emergency mobile Wireless Networks Flyaway Communications (FLAC) with WIMAX 802.16 technology". Proceedings - IEEE Military Communications Conference MILCOM. . (2005).

[Dub97]. R. Dube, C. D. Rais, K. Y. Wang, S. K. Tripathi. "Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks". IEEE Personal Communications Magazine, pp. 36-45, Febrero . (1997).

[Dud04]. Dudzinski, K., Bozier, M. "Extension of wmanlfMib for Improved Manageability of 802.16d". IEEE c802.16f-04/03. Octubre 28. (2004).

[Elastix]. Open Source Unified Comunications Server: http://www.elastix.org. (s.f.).

[ELB]. http://www.eurosatory.mod.gov.il/pdfs/SOD_Elbit.pdf. (s.f.).

[Est04]. M. Esteve, "Sistemas y Protocolos de Tiempo Real", Material docente de la asignatura de doctorado, Universidad Politécnica de Valencia. (2004).

[Est06]. M. Esteve "C2 en la era de la información", Primeras Jornadas de Mando y Control, Universidad Politécnica de Valencia, Diciembre. (2006).

[FBC]. http://www.fas.org/man/dod-101/sys/land/fbcb2.htm. (s.f.).

[FCC06]. "Report and Recommendations to the Federal Communications Commission". lndependent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (included as Append ix B in FCC 06-83 regarding EB Docket No. 06- 119). Junio 12. (2006).

[FCS]. https://www.fcs.army.mil/. (s.f.).

[FEL]. Commandement de la Doctrine et de l'Enseignement Militaire Superieure "FELIN: Fantassin á Équipements et Liaisons Integres" Ministerio Francés de Defensa, http://www.cdes.terre.defense.gouv.fr/sitefr/materiels/CC/felin.htm. (s.f.).

[FEOS]. Filin S. A., Moiseev S. N., Kondakov M. S. Fast and Efficient QoS-Guaranteed Adaptive Transmission Algorithm in the Mobile WiMAX System. IEEE Transactions on Vehicular Technology, pp. 3477-3487. 2008. (s.f.).

[FFW]. Intp://nsrdec.riatick.armymil/about/techprog/index.htm. (s.f.).

[FIS]. http://www.defense-update.com/products/f/fist.html. (s.f.).

[Fla10]. http://www.nps.edu/About/News/NPS-Hastily-Formed-Networks-Research-Group-Responds-to-Haiti-Earthquake.html. (2010).

[Flo93]. S. Floyd, V. Jacobson, "Random Early Detection (RED) gateways for Congestion Avoidance", IEEE/ACM Transactions on Networking 1 (4): 397-41K. (1993).

[FOT05]. "Implementation of Network Centric Warfare", Force Transformation Research Program. (2005).

[Fuj05]. T. Fujiwara, T. Watanabe. "An Ad Hoc Networking Scheme in Hybrid Networks for Emergency Communications". Ad Hoc Networks, vol.3, no.5, pp.607- 620. (2005).

[Ful97]. C. L. Fullmer y J. J. Garcia-Luna-Aceves, "Solutions to Hidden Terminal Problems in Wireless Networks", Proceedings of ACM SIGCOMM 1997, pp. 39-49. Septiembre . (1997).

[GA008]. "Defense Acquisitions: 2009 review of future combat system is critical to prograrn's direction", United States Government Accountability Office (GAO) report, Abril . (2008).

[Gag96]. V.K. Garg, J.E. Wilkes, Wireless and Personal Communications Systems, Prentice Hall, Upper Saddle River, NJ. (1996).

[Gar09]. Garroppo R. G., Giordano S., lacono D., Cignoni A., Falzarano M. "Experimental Analysis of a WiMAX-Satellite Network for Emergency Management in Sea Areas". 2009 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks . (2009).

[Gar99]. J. J. Garcia-Luna-Aceves, E. L. Madruga. "The Core-Assisted Mesh Protocol". IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1380-1994. Agosto . (1999).

[GCC]. www.sap.corn/industries/defense-security/pdf/CS_Coalition_Warrior_Demonstration.pdf. (s.f.).

[GeoBIPS]. GeoBIPS: Geographical broadband integration for public services. Web: https://projects.ibbt be/geobips/. Diciembre, 2006. (s.f.).

[Ger97]. M. Gerla, C.R Lin, "MACA/PR: An asynchronous multimedia multihop wireless network", En Proceedings of the IEEE INFOCOM, Marzo . (1997).

[Ger98]. M. Gerla, T. W. Chen. "Global State Routing: A New Routing Scheme for Ad Hoc Wireless Networks". Proceedings of IEEE ICC 1998, pp. 171-175. Junio . (1998).

[Gon91]. M. Gonzalez-Harbour, L. Sha, "An Application-Level Implementation of the Sporadic Server", Carnegie Mellon University Software Engineering Institute (SEI), Technical Report CMU/SEI-91-TR-026. (1991).

[Gou77]. M.G. Gouda, Y. Han, E.D. Jensen, W.D. Johnson, R.Y. Kain, "Distributed Data Processing Technology", Vol. IV, "Applications of DDP Technology to BMD: Architectures and Algorithms", Honeywell Systems and Research Center, Minneapolis, USA. (1977).

[Gra07]. M. de Graaf, H. v.-D. (2007). *"Easy Wireless: Broadband ad-hoc networking for emergency services". The Sixth Annual Mediterranean Ad Hoc networking Workshop, Corfu, Grecia. Junio 12-15.*

[GRO99]. GROUPLW., IEEE Std . 802.11-1999, Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std. 802.11, 1999, Reference number ISO/IEC 8802-11:1999(E). (1999).

[Haa97]. Z. J. Haas, "The Routing Algorithm for the Reconfigurable WirelessNetworks". Proceedings of ICUPC 1997, vol. 2, pp. 562-566. Octubre . (1997).

[Hal04]. J. Hallberg, S. Svensson, A. Ostmark, P. Lindgren, K. Synnes, and J. Delsing "Enriched Media-Experiénce of Sport Events", En Proceedings of the sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2004), Diciembre . (2004).

[Hei97]. Heilbronner S., Wies R. "Managing PC Networks". IEEE Communications Magazine. Octubre . (1997).

[HNW]. http://www.govcomm.harris.com/solutions/products/000056.asp. (s.f.).

[Hon97]. Hong J. et al. "Web-Based Intranet Services and Network Management". IEEE Communications Magazine. Octubre . (1997).

[Hos04]. Hos E., Visser N, "Quality of Service for Wireless Networks", Junio . (2004).

[Huh98]. M. Huhns, M. Singh, Cognitive Agents, IEEE: Internet Computing, 87-89. (1998).

[ICIS]. ICIS: Interactive collaborative information systems. Web: http://www.icis.decis.nl. Programa BSIK, 2003. (s.f.).

[IDZ]. http://www.bundeswehr.de/redaktionen/bwde/bwdebase.nsf/CurrentBaseLink/N264HUBT969MMISDE. (s.f.).

[IEEE802.16-2004]. IEEE Standard for Local and Metropolitan Area Networks, Air Interface for Fixed Broadband Wireless Access Systems, Octubre. (2004).

[IEEE802.16e]. IEEE Standard for Local and Metropolitan Area Networks, A. I. (2006). *Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, Febrero 2006.*

[IEEE802.16m]. IEEE 802.16m-08/003r7. The IEEE 802.16m System Description Document. . (2009).

[IMP] www.eads.com/1024/es/businetidefence/des/army/c3i_systems/Impact/impact.html. (s.f.).

[ITU] International Communications Union: http://www.itu.int/ITU-T. (s.f.).

[ITU06]. http://www.itu.int/ITU-D/asp/Events/ITU-ESCAP-BangkokDec2006/. (2006).

[Iwa99]. A. Iwata, C. C. Chiang, G. Pei, M. Gerla, T. W. Chen. "Scalable Routing Strategies for Ad Hoc Wireless Networks". IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369-1379. Agosto . (1999).

[Jan09]. H.C. Jang, YN. Lien, T.C. Tsai. "Rescue Information System for Earthquake. Disasters based on MANET Emergency Communication Platform". Proceedings of the IWCMC 2009, pp. 623-627, Junio . (2009).

[JCO]. https://www.cwid.js.mil/public/CWID08FR/htmlfiles/168int.html. (s.f.).

[Ji00]. L. Ji, M. S. Corson. "Differential Destination Multicast (DDM) Specification". Internet draft (work in progress), draft-ietf-manet-ddm-00.txt. Julio . (2000).

[JIDM]. http://www.opengroup.org/external/jidm/. (s.f.).

[Joa99]. M. Joa-Ng, I. T. Lu. "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks". IEEE Journal on Selected Arcas in Communications, vol. 17, no. 8, pp. 1415-1425. Agosto . (1999).

[Joh96]. D. B. Johnson, D. A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks". Mobile Computing, Kluwer Academie Publishers, vol. 353, pp. 153-181. (1996).

[JOV]. http://www.dtic.mil/jy2010/jvpub.html. (s.f.).

[Ju02]. Ju, H. C. (2002). *"An Embedded Web Server Architecture for XML-based Network Management". Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS 2002), pp.1-14. Florencia, Italia. Abril .*

[Kat05]. http://faculty.nps.edu/dl/HFN/index.htm. (s.f.).

[Kat07]. S. Kato, N. Yamasaki "Feedback-Controlled Server for Scheduling Aperiodic Tasks", International Journal of Computer, Information, and Systems Science, and Engineering. (2007).

[Kid10]. D. Kidston, L. Li. "Management through cross-layer design in mobile tactical networks". IEEE Network Operations and Management Symposium - NOMS 2010, pp. 890-893. Abril . (2010).

[Kim11]. Kim, K., Choi, Y.-j., Lee, S.-h., Hanzo, L., Chung-Min, Y., Lee, S.-w., y otros. (2011). *erformance comparison of various VoIP codecs in wireless environments, Ubiquitous Information Management and Communication: Proceedings of the 5th International Conference, (ICUIMC '11), pp.1-10.*

[Kle07]. M. Kleiner et al "Geospatial Battle Management Language: Bridging GIS, C2 and simulations" ESRI users conference . (2007).

[Ko98]. Y. Ko, N. H. Vaidya. "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks". Proceedings of ACM MOBICOM 1998, pp. 66-75. Octubre. (1998).

[Ko99]. Y. B. Ko, N. H. Vaidya. "Geocasting in Mobile Ad Hoc Networks: Location¬Based Multicast Algorithms". Proceedings of IEEE WMCSA 1999, pp. 101-110. Febrero . (1999).

[Kru07]. K. Kruger, M. F. (2007). *"Battle Management Language: Military Communication with Simulated Forces" In Improving M&S Interoperability, Reuse and Efficiency in Support of Current and Future Forces", Meeting Proceedings RTO-MP-MSG-056, Paper 5, pp. 5-1 — 5-10,.* Neuilly-sur-Seine, Francia.

[KUM06]. Kumar S., Raghavan V. "Medium access control protocols for ad hoc wireless networks: a survey". Ad hoc Networks, vol.•4, no. 3, pp. 326-358. Mayo . (2006).

[Lag92]. P. Lagarde, S:G di Pasquate, "The PR4G VHF ECCM system: extensive tactical communications for the battlefield", IEEE Military Communications Conference (MILCOM92), vol. 2, pp. 662-666, Octubre . (1992).

[LAN]. http://www.defence.gov.au/dmo/lsd/land125/index.cfm. (s.f.).

[Lee00]. S. Lee, C. K.-5. (2000). *LEE S. -B., Al-IN G. -S. , ZHANG X. y CAPBELL A.T. "INSIGNIA: an IP-based Quality of Service framework for mobile ad hoc networks". J. Parallel Distrib. Comput., vol. 60, no. 4,pp. 374-406.*

[Lee99]. S. J. Lee, M. Gerla, C. C. Chiang. "On-Demand Multicast Routing Protocol". Proceedings of IEEE WCNC 1999, pp. 1298-1302. Septiembre . (1999).

[Leh89]. J. Lehoczky L. Sha, Y. Ding, "The rate monotonic scheduling algorithm: exact characterization and average case behavior", IEEE Real-Time Systems Symposium, pp. 166-17. (1989).

[Lin96]. C.-H. Lin, "A multihop adaptive mobile multimedia network: architecture and protocols'', Tesis doctoral, Universidad de California Los Angeles (UCLA). (1996).

[Lin97]. C.R. Lin, M. Gerla, "Adaptive clustering for mobile wireless networks", IEEE Journal Sel. A. Commun. 15 (7), pp.1265-1275. (1997).

[Lin99]. LIN C.R. y Lnr J. S., "QoS routing in ad hoc wireless networks". IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1426-1438. (1999).

[Liu73]. C.L Liu, J.W Layland "Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment" Journal of the ACM, volume 20, issue 1, pp. 46-61. (1973).

[Mah06]. P. Mahonen, M. Petrova, J. Riihijarvi, M. Wellens, "Cognitive Wireless Networks: Your Network Just Became a Teenager", Proc. IEEE INFOCOM 2006. (2006).

[Mai95]. L. Maillet, C. Fraboul, "Scheduling complex real-time tasks in an embedded distributed system," ecrts, pp.62, 7th Euromicro Workshop on Real-Time Systems (EUROMICRO-RTS'95). (1995).

[Maj07]. S. Majid, K. Ahmed. "Cross-layer framework for post-disaster communications". IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, pp. 725-728. . (2007).

[Man01]. B. S. Manoj, R. Ananthapadmanabha, C. Siva Ram Murthy. "Link Life-Based Routing Protocol for Ad Hoc Wireless Networks". Proceedings of IEEE ICCCN 2001, pp. 573-576. Octubre . (2001).

[MAR]. http://www.mss.mil.se/taktik/article.php?id=9500. (s.f.).

[Mar91]. N. Marley, GSM and PCN Systems and Equipment, JRC Conference, Harrogate. (1991).

[Mar99]. Martin-Flatin, J.P., "Push vs. Pul! in Web-based Network Management". Proceedings of IFIP/IEEE International Symposium of Integrated Management (IM '99). Boston, MA. Mayo . (1999).

[Mck90]. P.E McKenney, ". f.-7. (s.f.). *1990.*

[Men04]. Menten, L. "Experiences in the Application of XML for Device Management". IEEE Communications Magazine. Julio. (2004).

[MES]. https://edge.arubanetworks.com/article/p-ieee-802-11-working-group-responsible-development-and-evolution-ieee-std-802-11-2007-commo. (s.f.).

[MESA]. Proyecto MESA, Mobility for Emergency and Safety Applications - Statement of Requirements, Version 3.3.1, Marzo . (2008).

[MIL-STD-187-721C]. MIL-STD-187-721C, "Planning and Guidance Standard for Automated Control Applique for HF Radio", Noviembre 1994. (s.f.).

[MIL-STD-188-110B]. MIL-STD- 188-110B, "Interoperability and Performance Standards for Data Modems", U.S. Army Information Systems Engineering Command, Abril de 2000. (s.f.).

[MIL-STD-188-141B]. MIL-STD-188-141B Change Notice 1, "Interoperability and Performance Standards for Medium and High Frequency Radio Equipment", U.S. Army Information Systems Engineering Command, 2001. (s.f.).

[MODa]. http://www.modaf.org.uk/. (s.f.).

[Mor04]. R. Morley, J. Kobsar, "Battle Command on the Move", Command and Control Research and Technology Symposium (CCRTS'04), San Diego, California, USA. (2004).

[Mou08]. A.V. Moura, C. d. (2008). *"Heuristics and Constraint Programming Hybridizations for a Real Pipeline Planning and Scheduling Problem", pp.455-462, En proceedings de 11th IEEE International Conference on Computational Science and Engineering,.*

[Mou92]. M. Mouly, M.-B. Pautet, The GSM System for Mobile Communications, Palaiseau, France. (1992).

[Moy94]. J. Moy. "Multicast Routing Extensions for OSPF". Communications of the ACM, vol. 37, no. 8, pp. 61-66. Agosto . (1994).

[Mur96]. S. Murthy,J. J. Garcia-Luna-Aceves. "An Efficient Routing Protocol for Wireless Networks". ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, vol. 1, no. 2, pp. 183-197, Octubre . (1996).

[Nag87]. J. Nagle: "On packet switches with infinite storage." IEEE Transactions on Commumunications, 35(4):435-438, Abril . (1987).

[Nev08]. Neves P., Fontes F., Monteiro J., Sargento S., Bohnert T. M. Quality of service differentiation support in WiMAX networks. International Conference on Telecommunications (ICT) . (2008).

[OFW]. http://www.globalsecurity.org/military/systems/ground/ofw.htm. (s.f.).

[Owe96]. W.A Owens, "The emerging US system of systeins", Institute for National Strategic Studies white paper, Washigton DC, USA. (1996).

[Oza99], T. Ozaki, J. B. Kim, T. Suda. "Bandwidth Efficient Multicast Routing Protocol for Ad Hoc Networks". Proceedings of IEEE ICCCN 1999, pp. 10-17. Octubre . (1999).

[PAK]. www.defencetalk.com/forums/archive/index.php/t-2980.html. (s.f.).

[Par97]. V. D. Park, M. S. Corson. "A Highly Adaptive Distributed Routing Algorithrn for Mobile Wireless Networks". Proceedings of IEEE INFOCOM 1997, pp. 1405¬1413. Abril. (1997).

[Pav04]. Pavlou, G., Flegkas, P., Gooveris, S., Liotta, A. "On Management Technologies and the Potential of Web Services". University of Surrey. IEEE Communications Magazine. Julio . (2004).

[Pav98]. Pavlou, G., Aidarous, S., Plevyak, T. "OSI Systems Management, Internet SNMP and ODP/OMG CORBA as Technologies for Telecommunications Network Management". Telecommunications Network Management: Technologies and Implementations. IEEE Press. (1998).

[Pér09] Pérez Llopis, I. Arquitectura de un sistema C4ISR para pequeñas unidades [Tesis doctoral]. Universitat Politècnica de València. doi:10.4995/Thesis/10251/6067. (2009).

[Per94]. C. E. Perkins, P. Bhagwat. "Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers". Proceedings of ACM SIGCOMM 1994, pp. 234-244, Agosto. (1994).

[Per99]. C. E. Perkins, E. M. Royer. "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100, Febrero . (s.f.). 1999.

[POSX]. http://www.opengroup.org/. (s.f.).

[Pra04]. Pras, Aiko, Drevers, Thomas, van de Meent, Remco, Quartel, Dick. "Comparing the Performance of SNMP and Web Services-based Management". E-Transactions on Network and Service Management. . (2004).

[Pro09]. D.M. Protogerakis, D.A. Gramatke, "A System Architecture for a Telematic Support System in Emergency Medical Services", 3rd International Conference on Bioinforrnatics and Biornedical Engineering. ICBBE 2009, pp. 1-4. . (2009).

[Pul07]. Pullen, J. H. (2007). *"Joint Battle Management Language (JBML) — US Contribution to the Coalition Battle Management Language Product Development Group and the NATO MSG-048 Technical Activity." Paper 07E-SIW-029, European Simulation Interoperability Workshop, Genova, Italia.*

[Ras08]. N. Rashmi, "Secure Cognitive Networks", IEEE European Conference on Wireless Technology, EuWiT, p. 107-110. (2008).

[Rav05]. B.Ravindran, E.D Jensen, P.Li. "On Recent Advances in Time/Utility Function Real-Time Scheduling and Resource Management", Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC'05). (2005).

[RFC2003]. Perkins. "IP Encapsulation Within IP". Octubre . (1996).

[RFC2205]. "RFC 2205 Resource Reservation Protocol (RSVP) Version 1 Functional", Network Working Group of the Internet Engineering Task Force (IETF), Septiembre 1997. (s.f.).

[RFC2474]. "RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 headers", Network Working Group of the Internet Engineering Task Force (IETF), Diciembre 1998. (s.f.).

[RFC2475]. "RFC 2475 An Architecture for Differentiated Services", Network Working Group of the Internet Engineering Task Force (IETF), Diciembre 1998. (s.f.).

[RFC2597]. "RFC 2597 Assured Forwarding PHB Group", Internet Engineering Task Force (IETF), Junio 1999. (s.f.).

[RFC2598]. "RFC 3246 An Expedited Forwarding PHB (Per Hop Behavior)", Network Working Group of the Internet Engineering Task Force (IETF), Marzo 2002. (s.f.).

[RFC4118]. Yang, L., Zerfos, P., Sadot, E., "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)". Junio 2005. (s.f.).

[RFC4564]. Govindan, S., Cheng, H., Yao, Z.H., Zhou, W.H., Yang, L., "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)". Julio 2006 . (s.f.).

[RFC5415]. Calhoun, P., Montemurro, M., Stanley, D. "CAPWAP Protocol Specification". Marzo 2009. (s.f.).

[RFC5416]. Calhoun, P., Montemurro, M., Stanley, D. "CAPWAP Protocol Binding for IEEE 802.11". Marzo 2009. (s.f.).

[Ron06]. T. Rondeau, Bin Le, D. Maldonado, D. Scaperoth, C. Bostian, "Cognitive Radio Formulation and Implementation", IEEE Proc. CROWNCOM, Mykonos, Greece, pp. 1-10. (2006).

[Roy00]. E. M. Royer, C. E. Perkins. "Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing". Internet draft (work in progress), draft-ietf-manet-maodv-00.txt. Julio . (2000).

[Roy99]. E. M. Royer, C. E. Perkins. "Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol". Proceedings of ACM MOBICOM 1999, pp. 207-218. Agosto . (1999).

[SAFECOM]. Programa SAFECOM, "Statement of Requirements for Public Safety Wireless Communications & Interoperability", Department of Homeland Security, Version 1.2, Mayo 2007. (s.f.).

[SAFESPOT]. Web: http://www.safespot-eu.org/. (s.f.).

[SCA]. http://sca.jpeojtrs.mil/. (s.f.).

[Sco06]. C. Scordino, G. Lipari, "A Resource Reservation Algorithm for Power-Aware Scheduling of Periodic and Aperiodic Real-Time Tasks", IEEE Transactions on Computers, vol. 55, no. 12, pp. 1509-1522, Diciembre . (2006).

[Sha02]. M. Shafi, S. Ogose, T. Hattori (Eds.), Wireless Communication in the 2lst Century, Wiley-Interscience. (2002).

[SHARE]. SHARE: Mobile support for rescue forces, integrating multiple modes of interaction. IST 6° programa marco UE. Web: http://www.ist-share.org/. Diciembre 2007. (s.f.).

[She01]. S.-T. Sheu, "A bandwidth allocation sharing extension protocol for multimedia over IEEE 802.11 ad hoc wireless LANs", IEEE J. Sel. Areas Commun., pp. 2065¬ - 2080. (2001).

[Shi09]. Shi, Y., et al. "CAPWAP Protocol Binding MIB for IEEE 802.11". Disponible en: draft-ietf-capwap-802dot11-mib-04. Mayo 30. (2009).

[SIC]. http://www.nexor.com/press_releases/2008/interactive. (s.f.).

[Sim07]. O. Simeone, J. Gambini, Y. Bar-Ness , "Cooperation and cognitive radio", Proceedings of IEEE, International Conference on Communications (ICC), pp. 6511 - 6515, Junio. (2007).

[Sin98]. S. Singh, M. Woo, C. S. Raghavendra. "Power-Aware Routing in Mobile Ad Hoc Networks". Proceedings of ACM MOBICOM 1998, pp. 181-190. Octubre . (1998).

[SIV99]. SIVAKUMAR R., SINHA P. y BHARGHAVAN v., "CEDAR: a core-extraction distributed ad hoc routing algorithm". IEEE Journal on Selected Áreas in Communications, vol. 17, no. 8, pp. 1454 - 1465. . (1999).

[Skl97]. Sklar B., "Rayleigh Fading Channels in Mobile Digital Communication Systems. Pan I: Characterization", IEEE Communications Magazine, pp. 90-100, Julio . (1997).

[SLI03]. "Soldier-Level Integrated Communications Environment (SLICE) Soldier Radio Waveform (SRW) Functional Description Document (FDD)," v. 1.3, Nov. . (2003).

[SOB99]. SOBRINHO J. y KRISHNAKUMARA., "Quality-of-service in ad hoc carrier sense multiple access wireless networks". IEEE Journal on Selected Arcas in Communications, vol. 17, no. 8, pp. 1353-1368. (1999).

[Sri04]. Srikant, "The Mathematics of Internet Congestion Control", Boston, USA. (2004).

[Sri05]. Srivastava V., Motani M. "Cross-Layer Design: A Survey and the Road Ahead". IEEE Communication Magazine, vol.43, no. 12, pp. 112-19. . (2005).

[STA2014]. NATO Military Agency for Standardization, STANAG 2014: Formats for Orders and Designation of Timings, Locations, and Boundaries. Bruselas, BE, Edicion 9, 2000. (s.f.).

[STA2020]. NATO Military Agency for Standardization, STANAG 2020: Operational Situation Reports, OTAN, Febrero 1986. (s.f.).

[STA4285]. STANAG 4285, NATO Standardization Agreement, "Characteristics of 1200/2400/3600 bps Single Tone Modulators/Demodulators for HF Radio Links". (1990).

[STA4538]. STANAG 4538, NATO Standardization Agreement, "Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links". (s.f.).

[STA4539]. STANAG 4539, NATO Standardization Agreement, "Technical Standards for an HF Non-Hopping Waveform". (s.f.).

[STA5066]. STANAG 5066, NATO Standardization Agreement, "Profile for High Frequency (HF) Radio Data Communications". (1999).

[STA5255]. NATO Military Agency for Standardization, STANAG 5255: Joint Command Control Communications Information Exchange Data Modei (JC3IEDM), OTAN, Marzo 2009. (s.f.).

[STA5524]. Standard Agreement STANAG 5524 Ed.l "NATO C3 Technical Architecture", OTAN 2005. (s.f.).

[STA5527]. STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems, AC322(SC5)N(2006)0025 - Interim NFFI Standard for Interoperability of FTS, Diciembre 2006. (s.f.).

[Sta88]. J.A Stankovic, "Misconceptions About Real-Time Computing: A Serious Problem for Next-Generation Systems", IEEE Computer 21(10), pp.10-19, Octubre . (1988).

[Sti98]. D. Stiliadis, A. Varma, "Latency-rate servers: a general model for analysis of traffic scheduling algoritluns". IEEE/ACM Transactions on Networking 6 (5): 611-624. (1998).

[Str04]. Strauss, F., Klie, T. "Towards XML Oriented Internet Management". In Proceedings of the 8th IFIP/lEEE International Symposium Integrated Network Management, pp. 505-518. Colorado Springs, CO, USA. Marzo . (2003).

[Sys03]. Systematic Software Engineering A/S "IP Firefighter White Paper", Marzo . (2003).

[Tal08]. Talwalkar R. A., Ilyas M. Analysis of Quality of Service (QoS) in WiMAX networks. 16th IEEE International Conference on Networks (ICON). (2008).

[Tho00]. R. Thomas, R.A Beamer, P.K Sowell, "Civil application of DoD C4ISR architecture framework: a treasure department case study", 5th Internacional Command and Control Research and Technology Symposium (ICCRTS), Canberra, Australia. (2000).

[Tho05]. Ryan W. Thomas, Luiz A. DaSilva, Allen B. MacKenzie, "Cognitive Networks", Proc. IEEE DySPAN 2005, pp. 352-60. (2005).

[Tho98]. Thornpson J. "Web-based Enterprise Management Architecture". IEEE Communications Magazine. Marzo . (1998).

[TMB]. http://acd.itt.com/pdf/domestic/S-TBMS.pdf. (s.f.).

[Toh00]. C. K. Toh, G. Guichala, S. Bunchua. "ABAM: On-Demand Associativity¬ Based Multicast Routing for Ad Hoc Mobile Networks". Proceedings of IEEE VTC 2000, pp. 987-993. Septiembre . (2000).

[Toh97]. C. K. Toh. "Associativity-Based Routing for Ad Hoc Mobile Networks''. Wireless Personal Communications, vol. 4, no. 2, pp. 1-36. Marzo . (1997).

[TRITON]. http://sites.google.com/site/mingtuozhou/research/triton. (s.f.).

[TRO]. http://www.janes.com/articles/Janes-C41-Systems/TROP-Battlefield-Management-System-BMS-Poland.html. (s.f.).

[Tsa08]. K. Tsagkaris, A. Katidiotis, P. Demestichas, "Neural network-based learning schemes for cognitive radio systems", Computer Communications, v.31, n.14, p.3394¬-3404, Septiembre. (2008).

[Vid97]. R. Vidano, "SPEAKeasy II-an IPT approach to software programmable radio development", En IEEE MILCOM 97 Proceedings, Vol. 3, Issue , 2-5, pp. 1212¬1215, Noviembre . (1997).

[VMF]. MIL-STD-6017A (NOTICE 1), Department of Defense Interoperability Standard, "VARIABLE MESSAGE FORMAT (VMF) MESSAGE STANDARD", Noviembre 2006. (s.f.).

[Wai98]. D. Waitzman, C. Partridge, S. Deering. "Distance Vector Multicast Routing Protocol". Request For Comments 1075. Noviembre . (1988).

[Wel05]. B. J. Welch et al. "Supporting Demanding Hard-Real-Time Systems with STI", IEEE Transactions on Coniputers, Vol. 54, No. 10, p. 1188, Octubre . (2005).

[WIERD]. http://www.ist-weird.eu/documents.php?idfolder=60. (s.f.).

[Wil07]. C.Wilson, "Network Centric Operations: Background and Oversight Issues for Congress", Reporte del Congresional Research Service (CSR) para el congreso USA, abril . (2007).

[WINT]. http://peoc3t.monmouth.army.mil/wint/wint.html. (s.f.).

[Wir00]. T. Wirén, A. Mattson, B. Andersson "Info-Firefghter"5th International Command and Control Reseakch,and Technology Symposium (ICCRTS100), Canberra, Australia . (2000).

[Wis07]. J. Wiss, R. Gupta, "The WIN-T MF-TDMA Mesh Network Centric Waveform," Proc. IEEE MILCOM '07, Orlando, FL, Oct. 29-31. (2007).

[WMFT32-09]. Documento WiMAX Forum T32: The WiMAX Forum® Network Architecture Release 1.0 Version 4 - Stage 2: Architecture Tenets, Reference Model and Reference Points, Febrero . (2009).

[WMFT33-09]. Documento WiMAX Forum T33: The WiMAX Forum® Network Architecture - Release 1.0 Version 4 - Stage 3: Detailed Protocols and Procedures specifies protocol-level details, Febrero . (2009).

[WNW03]. "Wideband Networking Waveform (WNW) System Segment Specification," Boeing, spec. no. AJ01120, Feb. 12. (2003).

[Wu98]. C. W. Wu, Y. C. Tay, C. K. Toh. "Ad Hoc Multicast Routing Protocol Utilizing [ncreasing id-numberS (AMRIS) Functional Specification". Internet draft (work in progress), draft-ietf-manet-amris-spec-00.txt. Noviembre . (1998).

[XUE03]. XUE Q. y GANZ A., "Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks", Journal of Parallel and Distributed Computing, vol. 63, no. 2, pp. 154¬165, Febrero . (2003).

[Yan98]. S.Yan, H..0h, "A Modified Least-Laxity-First Scheduling Algorithm for Real-Time Tasks", En Proceedings of the 5th International Conference on Real-Time Computing Systems and Applications, pp. 31. (1998).

[Yar09]. A. Yarali, B. Ahsant, S. Rahman, "Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications". Second International Conference on Advances in Mesh Networks, Jun. 2009, pp. 143-149. . (2009).

[Yoo03]. Yoon, J.H., Ju, H.T., Hong, J.W. "Development of SNMP-XML Translator and Gateway for XML-based Integrated Network Management". International Journal of Network Management, Vol. 13, pp. 259-276. . (2003).

[You79]. W.R. Young, Advanced mobile phone services-Introduction, background and objectives, Bell Syst. Tech. J. 58 1-14. (1979).

[Yu05]. S. Yu, Y. Zhang, C. Song, K. Chen. "A security architecture for Mobile Ad Hoc Networks. Web: " http://blrc.edu.cn/blicweb/publication/ kc2.pdf. . (2005).

[Zha07]. Z. Zhang, X. Xie, "Intelligent Cognitive Radio: Research on Learning and Evaluation of CR Based on Neural Network", Proc. 5th International Conference on Information and Communications Technology (ICICT 2007), . (2007).

[Zho00]. H. Zhou, S. Singh. "Content-Based Multicast (CBM) in Ad Hoc Networks". Proceedings of ACM MOBIHOC 2000, pp. 51-60. Agosto . (2000).

[Zho09]. Zhou Ming-Tuo,Hiroshi Harada, Peng-Yong Kong and J aya Shankar Pathmasuntharam. "Wireless Mesh Networking for Maritime Intelligent Transportation Communication Systems". Nova Science Publishers. USA . (2009).

[ZHU02]. ZHU C. y CORSON M. "QoS routing for mobile ad hoc networks". INFOCOM2002. Twenty-First Annual Joint Conference of the IEEE Cornputer and Comrnunications Societies. Proceedings. IEEE, vol. 2, pp. 958-967, . (2002).