B-MAC Y OTROS PROTOCOLOS DE ACCESO AL MEDIO

PLANTEAMIENTOS PREVIOS

Uno de los problemas principales actualmente en redes de sensores es que existen multitud de protocolos y subsistemas para solucionar temas puntuales (véase Figura 1), que hacen amplias suposiciones sobre el resto del sistema y sobre cómo interactúan todas sus partes.

Hay trabajos de un mismo grupo de investigación que integran distintos componentes en sus diseños para trabajar juntos, pero que son incapaces de interactuar con los trabajos propuestos por otros grupos de investigación.

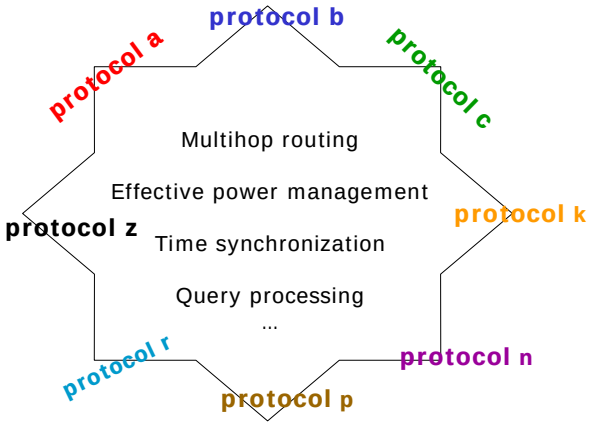

Figura 1. Problema de incompatibilidad de protocolos.

Como ya ocurrió con las redes cableadas, esta incompatibilidad inherente entre protocolos y sistemas reduce la interacción posible entre grupos de investigación e impide el progreso.

Se han construido grandes y complejos sistemas, pero los servicios resultantes, interfaces y protocolos son incompatibles unos con otros. Uno de los principales problemas actuales en redes de sensores es la falta de una *arquitectura de red* de sensores global. Esta arquitectura podría identificar los servicios esenciales y sus relaciones conceptuales, el conjunto de interfaces a esos servicios y, finalmente, los protocolos que incluyan formatos de paquete, comunicación y estado de las máquinas. Por tanto, sería el marco de referencia para tratar problemas como gestión de la topología, descubrimiento de vecinos, routing, naming, etc.

Según las Universidad de Berkeley el tema fundamental será definir un componente funcional que represente un servicio común, que permita una amplia variedad de usos y una implementación por debajo, es lo que han llamado SP, *The Sensor-net Protocol* [30].

NUEVAS ARQUITECTURAS PARA REDES DE SENSORES

Los estándares que hasta ahora han resuelto los problemas derivados de la comunicación en redes cableadas, no parecen solventar adecuadamente los problemas que surgen cuando entra en juego la comunicación en un medio inalámbrico. Características como multidifusión y ruido presente en el medio, llevan a pensar que las soluciones adoptadas para redes cableadas no serán adecuadas en este nuevo escenario.

Movilidad, alta probabilidad de pérdida de enlace, baterías limitadas y bajos recursos computacionales suponen nuevos retos, y por tanto una nueva perspectiva de afrontar el reto de la comunicación en un medio inalámbrico.

Además las nuevas características del medio, permiten nuevos tipos de conexiones ad-hoc, más allá de las soluciones basadas en infraestructura, es decir, más allá de una red controlada por un punto de acceso. Las redes de sensores inalámbricas, suponen un primer reto al respecto: cientos o miles de nodos, desplegados al azar y que se organizan de manera autónoma para implementar una solución a un problema concreto, además, carentes de una infraestructura previa y con la barrera de recursos energéticos limitados. Este tipo de soluciones, necesita de una nueva visión de la arquitectura de red tradicional.

Existen diversas propuestas actualmente. Una de las más importantes es la presentada por la Universidad de Berkeley [30], referencia más importante en el trabajo que se va a desarrollar. En ella aparece una nueva forma de trabajar, denominada metodología Cross-Layer,

La propuesta de la Universidad de Berkeley se puede ver en la siguiente figura (véase Figura 2). En ella se hace una descomposición en capas en la que aparece SP como servicio unificador que sirve de puente entre protocolos y aplicaciones superiores y la capa de enlace y física por debajo. La diversidad de funcionalidad de las capas inferiores supone todo un reto para la definición y diseño de SP, que aún está en desarrollo. Además de los servicios de las capas superiores e inferiores de SP, la arquitectura tiene servicios cross-layer, que son los que aparecen a la izquierda de la Figura 2. Estos servicios cross-layer incluyen la gestión del consumo, sincronización y

descubrimiento de vecinos, entre otros. Estos servicios se definen cross-layer porque van a usar el espectro completo de capas de la arquitectura y no solo una en particular.

Como las redes de sensores van a tratar nuevos dominios de aplicación es inevitable que surjan también nuevos servicios.

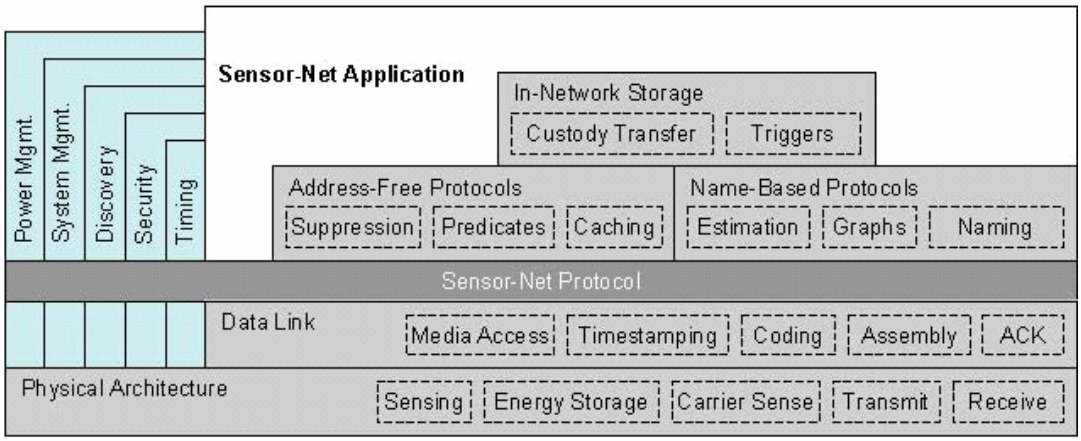

Figura 2. Nueva propuesta de arquitectura

Mientras no se disponga de baterías que doten a los motes de autonomía prolongada, los esfuerzos se centraran en exprimir al máximo los anteriores planos para conseguir una reducción de consumo.

Actualmente el objetivo del ahorro de energía supone el eje principal en la investigación con protocolos de control de acceso al medio (MAC) que suponen una de las responsabilidades de la capa de enlace de datos. A lo largo del presente proyecto se estudiará detalladamente la influencia de los protocolos de control de acceso en el consumo energético de la red. Pero el reto no es sólo el conseguir ahorro de energía sino de adaptarse a un medio de comunicación inalámbrico inherentemente dinámico. La radio es uno de los dispositivos del nodo que más consumo realiza y los algoritmos MAC son los responsables de su uso, por ello centraremos nuestro estudio en algoritmos que incluyan la gestión de la misma.

FUNCIONES DE LA CAPA MAC

La subcapa MAC, perteneciente a la capa de enlace de datos, se encarga del control de acceso al medio y responsable de transmitir los paquetes. También lleva las labores de validar las tramas que recibe, comprobar errores en la transmisión y confirmar la recepción de tramas al emisor.

Otras funciones menos relevantes para nuestro estudio, pero también importantes son, la fragmentación de paquetes, control de flujo, tasa de transmisión y funciones relacionadas con la gestión de la batería. En resumen se encarga de controlar un medio de comunicación compartido por una serie de dispositivos que se comunican a través de él [19].

Las restricciones de las redes de sensores, especialmente el ahorro de energía, influyen directamente en el diseño de los protocolos de control de acceso al medio (MAC).

Estos protocolos se pueden agrupar en dos clases básicas, lo protocolos basados en slots o ranurados y los basados en muestreo. En los protocolos ranurados, los nodos dividen el tiempo en intervalos discretos (ranuras de tiempo o slots), y los planifican dependiendo de si la radio está en modo recepción, modo transmisión o apagada. Sincronizar los slots con los vecinos permite que los nodos enciendan la radio solamente cuando sea necesario, con lo que se reduce considerablemente el *idle listening*, o escucha ociosa. Estos protocolos a menudo son estáticos; después de que se planifique un determinado horario o sincronización para los slots, un nodo solo puede comunicarse con otros nodos dentro del mismo periodo de slots previamente establecido. Los periodos cortos de comunicación pueden conducir a un aumento de la contención, y los costes de la sincronización y mantenimiento penalizan el consumo energético y el ancho de banda. Los protocolos ranurados incluyen los protocolos TDMA[20], IEEE 802.15.4 [21], S-MAC [22], T-MAC [23] y TRAMA [24], entre otros.

La segunda clase de protocolos son los basados en muestreo. En lugar de coordinar las ranuras de tiempo, los nodos despiertan periódicamente en busca de actividad en el canal de radio, si la detectan, comienzan a recibir los datos. Dependiendo de la capa física, esta detección se puede basar en el nivel de energía del canal o en la detección de portadora. El muestreo periódico del canal permite que un nodo ahorre energía manteniendo su radio apagada la mayor parte del tiempo. En contraste con los protocolos ranurados, los protocolos de muestreo son muy flexibles: un nodo puede comunicarse con otro cualquiera dentro del alcance de la radio. Pero la flexibilidad tiene un coste. Mientras que los protocolos ranurados envían los paquetes de datos regularmente, en muestreo hay que enviar mensajes largos y costosos para despertar a un vecino. Dentro de los protocolos basados en muestreo están: Aloha[31] , B-MAC [26], WiseMAC [25], transceiver de Chipcon CC2500 [28], y la plataforma mica de Berkeley [29].

Los principales protocolos de cada una de las categorías se detallaran en la siguiente sección.

PROTOCOLOS EXISTENTES

Protocolo ranurado IEEE802.15.4

El protocolo IEEE802.15.4 se considera estándar desde el 2003 y surge por la necesidad de tener un protocolo estándar de bajo consumo y bajo ancho de banda para redes de sensores. Establece dos topologías de red, la topología tipo estrella y la topología *"Peer-to-Peer"*(véase Figura 3). La topología que se utilice depende de la aplicación en la que se va a utilizar la red de sensores. En aplicaciones como periféricos e interfaces de PC, se pueden utilizar conexiones tipo estrella, mientras que en aplicaciones para la monitorización de terrenos que despliegan la red por un área de terreno considerable se implementa una red Peer-to-Peer para salvar los problemas de cobertura. Desde el punto de vista de la topología cuenta con tres tipos de nodos, RFD, FFD y el controlador de red (ver Figura 3). Cada uno con funciones especificas en función de la topología de red.

Dependiendo de la aplicación y de la topología los nodos serán de un tipo u otro:

- ***Topología en estrella:*** Hay un nodo único FFD que recibe el nombre de *PAN coordinator* que entre sus tareas se tiene la coordinación el acceso al medio.

- ***Topología peer to peer:*** Todos sus nodos suelen ser FFD, ya que todos tienen la misma prioridad de acceso al medio, y aunque existe un *PAN coordinator*, éste no tiene las mismas funciones relevantes. Se corresponde con arquitecturas de red en malla o Ad–Hoc.

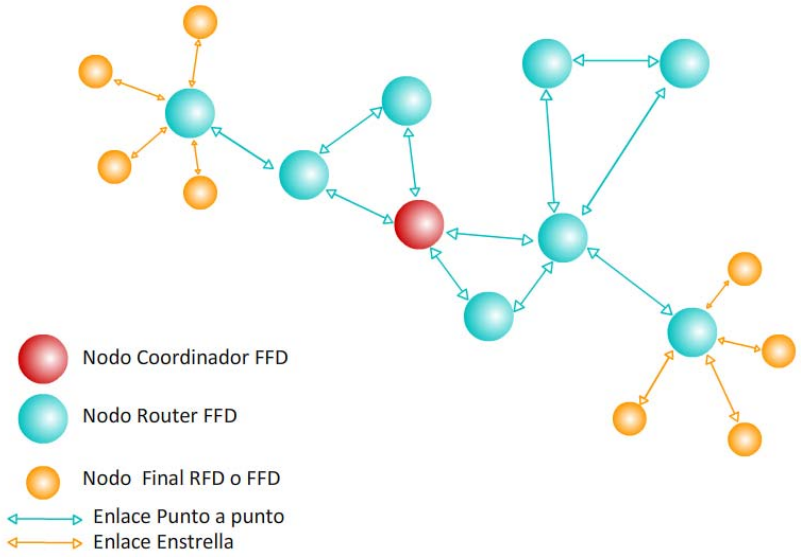

Figura 0. Tipos de nodos y topologías posibles en el estándar 802.15.4

El IEEE 802.15.4 establece 3 clases de funcionamiento, utilizando *beacons*, no utilizándolos y utilizando *beacons* con un tiempo de acceso garantizado (GTS). El utilizar un modo u otro de operación lo establecerá la topología y la aplicación a la que se va a dedicar la red.

- **IEEE 802.15.4 con *beacons.***

El mecanismo de utilización de *beacons*, consiste en que un determinado nodo, mandará unas señales, balizas, de manera periódica, marcando una serie de divisiones de tiempo entre dos *beacons***,** los slots. En concreto, se establecen 16 slots. Los nodos que quieran transmitir lo hacen en uno de estos slots. La señal, indica a un nodo que puede transmitir, si no tiene nada para trasmitir se apaga. En el caso de transmitir, espera un periodo de contención aleatorio, de varios slots. Tras ese periodo, si el canal está libre, el nodo retransmitirá alineado con el siguiente slot de tiempo. La sincronización permite que varios nodos puedan transmitir al mismo tiempo, reduciendo las colisiones, intentos de retransmisión, etc.

El PAN *coordinator* se encarga de transmitir *beacons* cada cierto tiempo, entre *beacon* y *beacon* se establece una supertrama compuesta de 16 slots , slots de *backoff.* Al periodo que acupán los 15 slots libres que hay entre *beacons* se les llama

CAP (*Contention Access Period*), en ellos los dispositivos pueden transmitir de forma coordinada (ver Figura 4).

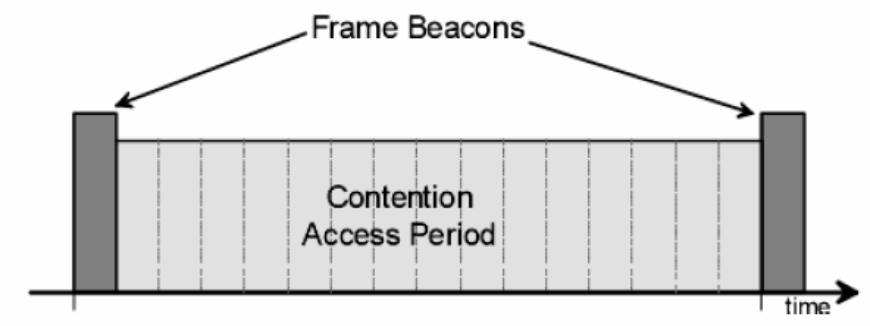

Figura 1. Modo con beacons. Con período de contención para el acceso.

En este caso, como mecanismo de acceso al medio utilizamos CSMA-CA ranurado en donde las ranuras de backoff están alineadas con el comienzo de un *beacon*. Cada vez que un dispositivo desea transmitir, primero tiene que alinearse con el siguiente slot de backoff y entonces tiene que esperar un número aleatorio de ranuras de backoff. Si el canal está libre, en el siguiente slot comenzaría a transmitir. Si el canal está ocupado, dejara pasar otro número aleatorio de ranuras de backoff. Los únicos paquetes que no están sometidos a CSMA-CA son los ACK's y los *beacons*.

- **IEEE 802.15.4 sin *beacons*.**

Aquí el mecanismo de acceso al medio es CSMA-CA no ranurado, esto implica que los dispositivos transmiten en el momento que es necesario sin esperar ningún *beacon* de ningún *PAN coordinator*. Su mecanismo de funcionamiento es el siguiente: cada vez que un dispositivo quiere transmitir, espera un tiempo aleatorio, si encuentra el canal libre espera un tiempo de backoff, pasado este tiempo intenta transmitir. Si el canal siguiera ocupado después del periodo de backoff volverá a esperar otro periodo aleatorio de tiempo y otro de backoff.

- **IEEE 802.15.4 con *beacons* y GTS.**

Esta tercera modalidad pretende proporcionar una latencia mínima para dispositivos que necesiten tener este parámetro garantizado, los GTS (*Guaranted Time Slot*). Se definen la trama de *beacon* y se sitúan dentro del periodo de libre contención (Contention Free Period, CFP). Este espacio es reservado para que en caso de haber mucho tráfico, ciertos dispositivos tengan siempre prioridad de utilizarlo para lograr así una mínima latencia (véase Figura 5).

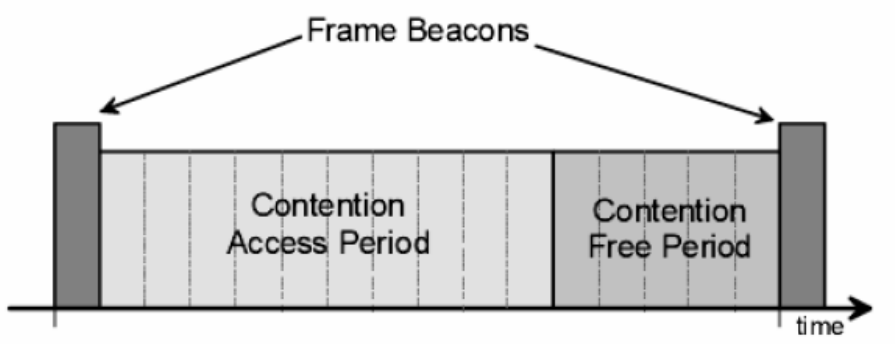

Figura 2 Modo beacons y zona exclusiva para GTS (los CFP).

El coordinador se encarga de la organización de los nodos de la red. Los nodos RFD's se asocian a un coordinador en las dos topologías. Los nodos FFD's pueden asociarse y comunicarse con otros coordinadores pero los nodos no pueden asociarse a nodos no coordinadores o RFD's. Cada vez que un coordinador se despierta, pone en marcha el mecanismo de *beacons y* envía una señal de red o *beacon*. Este *beacon* informa a los nodos sobre cuánto tiempo va a estar despierto, duración del *superframe* (véase Figura 6), y cuando va a volver a mandar otro *beacon*, duración del *beacon*. De esta manera, IEEE 802.15.4 establece tres posibilidades de acceso al medio, el mecanismo de señalizaciones (*beacons*) para el establecimiento de topologías en estrella, un mecanismo CSMA/CA para las topologías punto a punto y, para conseguir que ciertos nodos tengan prioridad, un mecanismo de contención que asegura un periodo de tiempo para estos dispositivos.

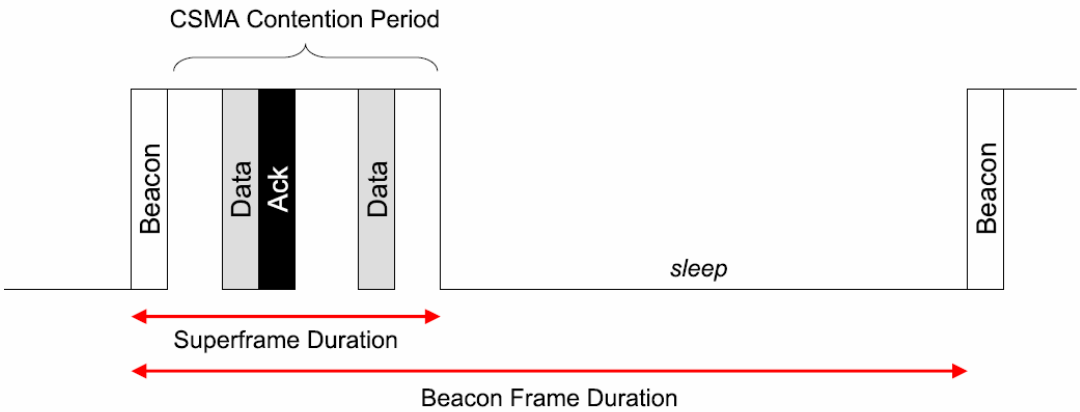

Figura 6. En 802.15.4 un Superframe consiste en un mensaje MAC beacon seguido de un período CSMA de contención para otro tráfico.

Al recibir el *beacon* del coordinador, los demás nodos pueden sincronizarse con el coordinador y realizar las peticiones para asociarse. Después de la notificación del coordinador de que se ha producido la asociación, los nodos asociados pueden enviar

datos al coordinador después de *beacon*. Los coordinadores envían la información a los nodos asociados dentro de los mensajes de *beacon*. Los nodos pueden solicitar datos al coordinador que enviará en mensajes de datos. Para comunicaciones de baja latencia o periódicas, los nodos pueden solicitar una ranura de tiempo garantizada (GTS) al coordinador. Cuando el coordinador envía el *beacon,* indica qué slots después del *beacon* están libres de contención y los asigna a los nodos que lo han solicitado. El coordinador es el único responsable de administrar y asignar el GTS.

En el caso de la topología *peer-to-peer*, los nodos FFD's tienen que escuchar los *beacon* de los otros nodos para comunicarse con ellos. Estos nodos deben mantener algún tipo de sincronización, pero el cómo se hace está más allá del alcance del estándar 802.15.4 [21].

En el estándar 802.15.4 se definen qué operaciones o responsabilidades tiene tanto la capa física PHY como la capa MAC. La capa PHY es responsable de encender y apagar el transceiver, detectar la energía en el canal, calcular la calidad del enlace, seleccionar los canales, detección de canal limpio *clear channel assessment* (CCA) y transmitir y recibir los paquetes a través del medio físico. El estándar especifica como frecuencias base de transmisión 2.4GHz, 916MHz, y 868MHz. Detecta el enlace indicando su estado a través de los indicadores de calidad del enlace y de detección de energía. Por ejemplo, mediante el detector de energía se puede saber si un canal esta libre, el detector de calidad del enlace se puede utilizar para seleccionar el siguiente salto cuando se enrutan paquetes. Por ésto, es importante que estas métricas estén accesibles para capas superiores de la arquitectura de red, para en función de estos parámetros optimizar su funcionamiento.

A nivel MAC se proporcionan las primitivas necesarias para establecer las dos topologías que definen el estándar, estrella y *peer-to-peer*. Estas incluyen la asociación, la desasociación, envió de *becons*, y los mecanismos del GTS. También proporciona los comandos para garantizar la transferencia de datos directa entre dos nodos, mediante el uso de ACK´s y primitivas para poder implementar a nivel de aplicación mecanismos de seguridad.

Protocolo ranurado S-MAC

Los diseñadores de S-MAC, tenían como pregunta clave ante su desarrollo, si sería necesario mantener la radio a la escucha durante todo el tiempo.

La mayoría de protocolos de control de acceso diseñados para hacer frente al medio radioeléctrico suponen una serie de tramas de control que arbitren el acceso. Ahora bien, en un medio ad-hoc, con innumerables posibilidades de variación en la infraestructura de la red original, podemos saturar el medio con este tipo de tramas de control. Además, se incrementa la probabilidad de tener que procesar paquetes que no estaban destinados al nodo que permanece a la escucha. Esto supone dos fuentes más de consumo de energía que nos hacen avanzar en dirección contraria al objetivo buscado.

El protocolo S-MAC (Sensor Medium Access Control) [27] es similar al 802.15.4 salvo algunas diferencias notables en sus mecanismos. S-MAC está basado en un esquema RTS-CTS de bajo consumo de energía para redes de sensores. S-MAC periódicamente duerme, despierta, escucha el canal, y después vuelve a dormir, utilizando lo que se conoce como *duty cycle*. Se diseño para funcionar como una "caja negra", ya que no dispone de ninguna interfaz, primitiva o funcionalidad que permita alterar el *duty cycle* o sus parámetros. A cambio de esto, encaminamiento, organización, sincronización y servicios de fragmentación de paquetes forman parte del protocolo. Todos estos servicios están disponibles para los protocolos de red.

El periodo de actividad es fijo en S-MAC, 115ms, pero el periodo en el que duerme, es variable. La longitud del periodo de dormido dictamina el *duty cycle*. La red se divide en celdas, y cada nodo perteneciente a una celda intercambia información necesaria para la sincronización de sus envíos, los nodos que pertenecen a mas de una celda deben mantener la información de sincronización de ambas celdas.

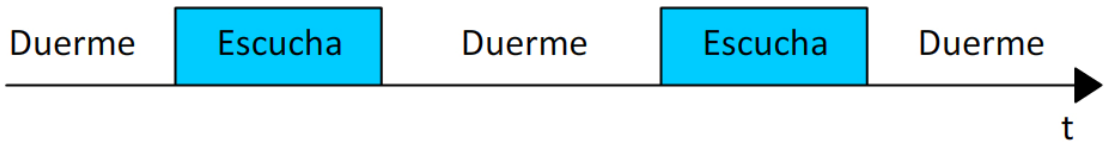

Figura 3. Períodos de escucha y dormido en SMAC.

T-MAC [25] es un protocolo que mejora el uso de la energía frente a S-MAC, usando un preámbulo muy corto para escuchar en el principio de cada período activo. Después de la sincronización del período activo, hay una ventana muy corta para enviar o recibir los paquetes RTS-CTS. Si no hay ninguna actividad en este período, el nodo vuelve al estado *sleep*. T-MAC con cargas de trabajo variables, utiliza un quinto de la energía de S-MAC.

En cargas de trabajo homogéneas, T-MAC y S-MAC se comportan igual. T-MAC sufre de los mismos problemas de la complejidad y del escalabilidad que S-MAC [30].

Protocolo de muestreo B-MAC

El reciente trabajo de Joseph Polastre [26] ha sacado a la luz un nuevo protocolo para la capa MAC en redes de sensores, nombrado como B-MAC (Berkeley Medium Access Control), capaz de reducir la denominada escucha ociosa o *idle listening*, tiempo que el nodo escucha el medio sin recibir transmisión alguna. B-MAC propone que cada nodo despierte periódicamente para comprobar la actividad en el canal, en caso de detección de actividad permanece a la escucha y en caso negativo vuelva a dormir (véase Figura 8), a dicho período se le ha denominado *wake-up* time. El tiempo entre periodos *wake-up* se fija mediante el denominado *check interval.* B-MAC define 8 *check intervals*, y cada uno de ellos se corresponde a un *listening mode* diferente.

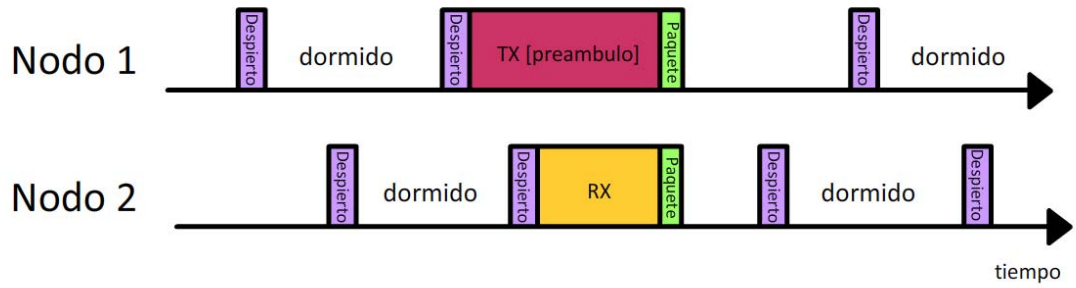

Figura 4. Estado de la radio en nodos usando B-MAC a lo largo del tiempo.

Para asegurar que todos los paquetes son recibidos, los paquetes se envían con un preámbulo cuya longitud de transmisión es superior al *check interval.* B-MAC define 8 tamaños de preámbulo, cada uno relacionado con un diferente modo de transmisión, lo que el protocolo denomina *transmit mode*.

Otra gran ventaja de B-MAC es su modularidad y flexibilidad, B-MAC proporciona interfaces accesibles a las capas superiores, con la finalidad que desde estas capas superiores se pueda fijar los modos de *listening* y *transmit,* ajustándose a las necesidades del momento. Su propio autor refleja que usando dichas interfaces, y realizando las modificaciones de modo oportunas atendiendo al estado instantáneo del nodo, se pueden llegar a conseguir grandes ahorros de energía en la red.

No entraremos más en detalle sobre este protocolo, como se ha realizado con los anteriores, ya que se le dedica el siguiente capítulo de esta memoria a su descripción, estudio de componentes e implementación, creyendo conveniente presentarlo aquí con esta breve descripción.

Protocolo de muestreo WISE-MAC

WiseMAC [33] es un protocolo propuesto por el instituto Suizo de Electrónica y Microtecnología (CSEM). Está orientado a redes de sensores basadas en infraestructura. Se ha realizado un nuevo diseño del sistema radio. El protocolo WiseMac está diseñado especialmente para funcionar con el sistema WiseNet del CSEM, que incorpora un *transceiver* de radio FSK, con dos bandas de trabajo 434 y 869 Mhz. El protocolo se basa en la idea de tener dos modos de comunicación: comunicaciones entre el nodo y la estación base y desde ésta a los nodos. Caracteriza los dos modos de comunicación para optimizarlos por separado.

Por un lado, estarán las comunicaciones *downlink*, que son las que van de la estación base al nodo. Como principal característica tiene que los nodos escuchan el medio durante un tiempo aleatorio, y si el medio está ocupado esperan por si llegan paquetes para ellos o el medio se desocupa. La estación base al solicitar los datos, debe asegurarse de que el nodo esté en modo de recepción cuando quiera transmitir, por lo que añade un preámbulo a sus tramas que alarga la duración hasta igualarla al periodo de muestreo del nodo receptor. La clave está en reducir este periodo haciendo que la estación base conozca exactamente cuánto dura y por tanto cuándo ocurrirá el siguiente periodo de escucha.

La solución que plantea WiseMAC para las comunicaciones de nodo a estación base se basa en tener en cuenta que la energía en la estación base es ilimitada, por tanto puede escuchar el canal continuamente. El protocolo MAC que se utilizará no necesita de ningún esquema de *wake-up* (véase Figura 9). Hay que resolver el problema de los accesos múltiples a un medio compartido como es el canal de radio. Si las comunicaciones entre los nodos y la estación base provocan un nivel de trafico próximo a la máxima capacidad del medio, este problema se vuelve muy complejo. Sin embargo, si el nivel de tráfico es relativamente moderado, solo mediante CSMA [34] se puede acercar claramente al caso ideal, sin producir *idle listening*, *overhearing* y solamente algunas colisiones.

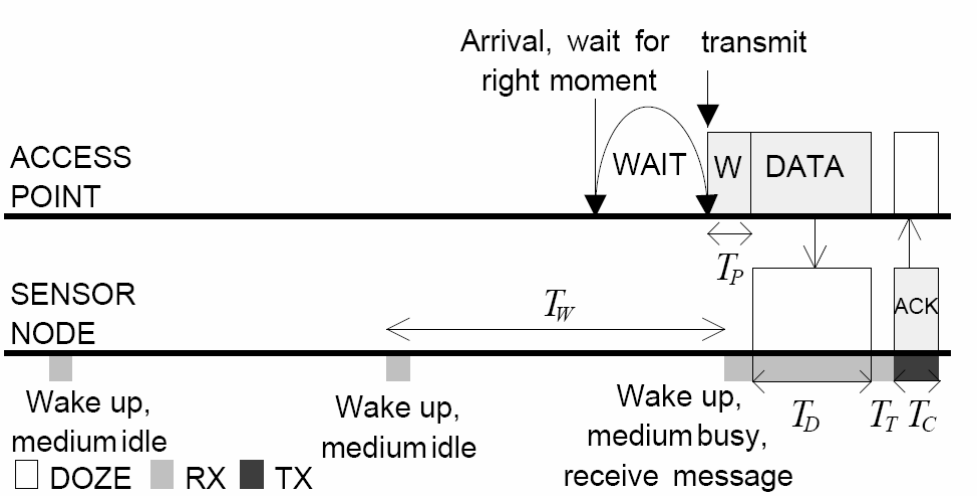

Figura 5 Técnica de mensajes wake-up en Wise-Mac

Para las comunicaciones entre la estación base y nodos el protocolo WiseMAC se basa en la técnica de muestreo del preámbulo [35]. Esta técnica consiste en el muestreo periódico del canal en busca de actividad. Cada uno de estos muestreos son relativamente cortos. Todos los nodos de la red muestrean el canal el mismo periodo de tiempo *Tw*. Si el canal está ocupado, el nodo continúa escuchando hasta que reciba un *frame* de datos, o hasta que el canal que libre. La estación base envía un preámbulo de *wake-up*, de tamaño igual al período de muestreo, delante de cada *frame* de datos para asegurar que el receptor está despierto cuando llega el paquete de datos. Esta técnica produce un consumo de energía muy bajo cuando los nodos encuentran el canal libre. La desventaja está en que los preámbulos de *wake-up* son largos, provocando limitaciones en el *throughput* y gastos indirectos de consumo de energía en la recepción. Los gastos indirectos en la recepción no solo afectan al nodo receptor, sino también al resto por culpa del *overhearing*.

La idea que introduce WiseMAC consiste en que la estación base aprenda con qué frecuencia cada nodo realiza sus muestreos del canal. Al conocer el horario de muestreo del nodo destino, la estación base envía la información justo en el momento que sabe que el nodo va a escuchar el canal y así puede utilizar un preámbulo de *wake-up* mínimo *Tp*. La estación base mantiene una tabla con todas las temporizaciones de muestreo de cada nodo. La tabla se construye con la base de la información sobre el tiempo que falta para el siguiente muestreo que envían los nodos en los paquetes de ACK.

La duración del preámbulo de *wake-up* se calcula de forma que se compense la diferencia entre el reloj del nodo y el de la estación base. Esta diferencia es proporcional al tiempo que ha pasado desde la última resincronización (es decir la última vez que se recibió un ACK del nodo).Teniendo en cuenta el valor μ que es la tolerancia del cristal

de cuarzo del oscilador que se utiliza en el reloj, l que es el intervalo entre comunicaciones, la duración del preámbulo de wake-up es:

$$TP = \min(4\mu l, TW)$$

Si nivel de tráfico es alto, el intervalo l entre comunicaciones es pequeño, y por tanto el preámbulo *wake-up* ($4\mu l$). Si el tráfico es bajo, el intervalo entre comunicaciones es grande en promedio, pero como máximo igual a TW. Esta característica es muy importante (véase figura 10) y hace que el protocolo WiseMAC se adapte al tráfico. Los gastos indirectos por paquete disminuyen con niveles altos de tráfico.

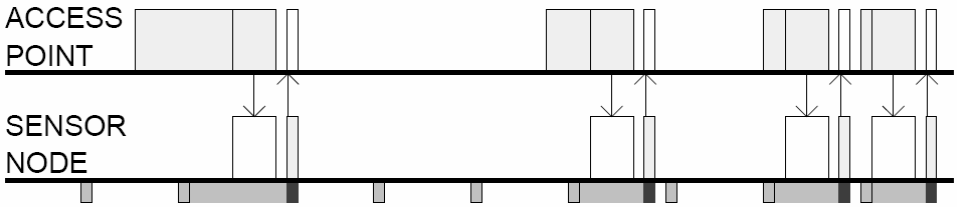

Figura 6 Adaptación de WiseMac al nivel de tráfico para evitar el *overhearing*.

El overhearing se atenúa cuando el tráfico es alto, gracias a las técnicas de muestreo de preámbulo y la minimización de la duración del preámbulo de *wake-up*. Como ya se ha comentado los nodos sensor no se sincronizan entre sí. Sus temporizaciones de muestreo son independientes. Con niveles de tráfico altos, la duración del preámbulo de *wake-up* es más pequeña que el período de muestreo y las transmisiones cortas pueden crear *overhearing*.

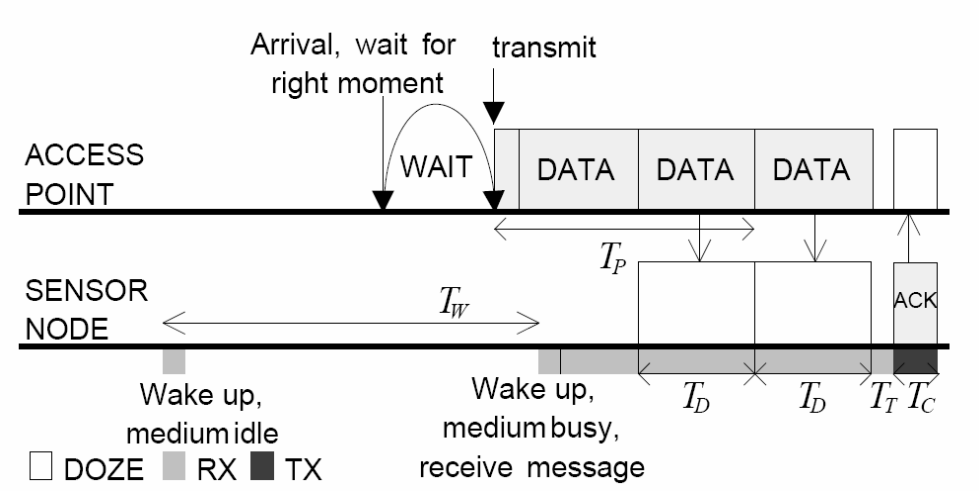

Figura 7 Repeticiones de los frames de datos cuando hay preámbulos muy largos.

Cuando el nivel de tráfico es bajo, la longitud del preámbulo de *wake-up* puede exceder la longitud del paquete de datos. En este caso, el preámbulo *wake-up* se compone de unos pocos bits de sincronización seguidos de varias repeticiones del *frame* de datos. Cuando un nodo encuentra el canal ocupado tiene que esperar a que le llegue un delimitador de *marco* que se envía al comienzo de cada *frame*. En la cabecera de cada *frame* de datos, el nodo puede comprobar si esos datos son para él o no. Si el destino es otro nodo, se duerme. Si el destinatario es él, recoge la información y envía un ACK de reconocimiento.

Una característica muy importante de WiseMAC, está inspirada en el protocolo IEEE 802.11 [36] y en IEEE 802.15.4 y es la presencia del bit *frame pending* en la cabecera de cada paquete de datos. Un nodo que reciba un paquete de datos con este bit continúa escuchando después de enviar el reconocimiento. El siguiente paquete lo envía la estación base después de que le llegue el ACK. Este esquema permite utilizar un intervalo de *wake-up* más grande que el intervalo medio entre llegadas para un determinado nodo. También minimiza el retraso en la cola de mensajes de la estación base cuando el nivel de tráfico se dispara. Finalmente, es interesante observar que no hay colisiones en WiseMAC para un canal de bajada, pues la estación base es la única que inicia las comunicaciones en este canal.