# Evaluación de una solución cross-layer para el ahorro de energía en mecanismos de seguridad sobre redes 802.11

Antonio Urbano Fullana[1], Josep Lluís Ferrer Gomila[2],
M. Francisca Hinarejos Campos[3], Magdalena Payeras Capellà[4] y Llorenç Huguet Rotger[5]
Universitat Illes Balears, Dept. Matemáticas e Informática,
Ctra. Valldemossa, Km 7,5. 07120, Palma
E-mail: antonio.urbano@uib.es[1] jlferrer@uib.es[2] xisca.hinarejos@uib.es[3]
mpayeras@uib.es[4] l.huguet@uib.es[5]

***Resumen*—El uso de dispositivos móviles que requieren conectividad inalámbrica se está generalizando por lo que es necesario disponer de redes inalámbricas eficientes que apliquen mecanismos de seguridad con un coste energético bajo. Lograr que estos dispositivos tengan un consumo de energía bajo es actualmente uno de los principales problemas de las redes inalámbricas. La energía consumida por operaciones de cálculo y por la comunicación intensa de los protocolos de seguridad inalámbricos utilizados para proporcionar privacidad, integridad y autenticidad, depende de la longitud de los datos transferidos y del nivel de seguridad de la sesión. En artículos anteriores hemos propuesto una solución de seguridad cross-layer, a la que llamaremos CL-WSec, para mejorar el consumo de energía de la batería en redes inalámbricas. CL-WSec permite que el terminal móvil y el punto de acceso puedan establecer, de manera eficiente, sesiones seguras extremo a extremo. En este artículo realizamos el análisis de esta solución y a partir de simulaciones demostramos que la aplicación de la solución CL-WSec proporciona una mejora del rendimiento frente a soluciones de seguridad que no aplican cross-layer, especialmente para longitudes de paquete elevadas.**

## I. Introducción

Las aplicaciones tradicionales en redes cableadas están siendo complementadas con servicios basados en la movilidad de los usuarios. Estos usuarios requieren conectividad y acceso a los recursos desde cualquier ubicación en la que se encuentren. Las redes de área local 802.11 [1] son un ejemplo donde se utilizan dispositivos inalámbricos para el acceso a redes y servicios, y en particular a Internet. Los dispositivos móviles que operan en redes inalámbricas están limitados por los recursos internos disponibles. En este sentido destacamos el tiempo de proceso y la capacidad de la batería. El tiempo de proceso relaciona las operaciones que un terminal es capaz de realizar en un intervalo de tiempo y que condiciona el tiempo de respuesta. La capacidad de la batería es un recurso crítico porque cuando esta se agota el terminal deja de funcionar.

En [17], [18] y [19] hemos estudiado el aumento del tiempo de respuesta y del consumo de energía en aquellos dispositivos inalámbricos que aplican mecanismos de seguridad que garantizan la autenticación, privacidad e integridad de la informacion. En estos artículos se analiza la redundancia de cifrado en entornos que, por sus características, aplican mecanismos de seguridad en diferentes capas, y se presenta una propuesta de ahorro de energía que se obtiene al reducir el número de octetos cifrados. La propuesta se fundamenta en la implementación de un algoritmo, basado en el diseño Cross-Layer [11], que permite que un terminal inalámbrico, que aplica una política con varios mecanismos de seguridad con cifrado de la información, reduzca el consumo de energía aplicando el criterio de que un campo que debe ser cifrado por el servicio de seguridad de capa lo será si no ha sido cifrado en capas superiores, o es un campo introducido por el protocolo de capa y que se cifra en el protocolo original.

**Contribución.** En este artículo mostraremos mediante simulaciones el aumento del tiempo de vida de la batería estimado al aplicar el algoritmo de reducción de cifrado basado en el diseño Cross-Layer, que llamaremos CL-WSec, a diferentes escenarios con diferentes políticas de seguridad y variando la tasa de transferencia. Los resultados obtenidos muestran que el ahorro de energía de la batería es mayor para longitudes de paquete elevadas y tasas de transmisión bajas.

**Organización.** Este artículo se organiza como sigue. En la sección II describimos el trabajo realizado anteriormente y que utilizamos en este artículo para el análisis del rendimiento de los mecanismos de seguridad y la aplicación de los mismos en redes inalámbricas cuando implementan la propuesta CL-WSec. En la sección III describimos los escenarios y las políticas de seguridad utilizados para el análisis del rendimiento. En la sección IV describimos el proceso realizado en las simulaciones para cuantificar el consumo de energía debida a los mecanismos de seguridad aplicados en las diferentes políticas, a partir de la solución CL-WSec. Los resultados obtenidos se muestran en la sección IV y las conclusiones y el trabajo futuro se presentan en la sección V.

## II. Trabajo relacionado.

El trabajo presentado en este artículo se basa en el análisis previo realizado en [17], [18] y [19] donde comprobamos que la aplicación de mecanismos de cifrado penaliza el rendimiento del dispositivo que los aplica y, en particular, penaliza el consumo de energía. En esos artículos se propone una solución para eliminar la multiplicidad de cifrado en los campos que son cifrados por más de un mecanismo de seguridad y, con ello, reducir el número

| Requisitos de seguridad. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Capa | Protocolo | Campo | P0 | P1 | P2 | P3 | P4 |
| APLICACIÓN | HTTP | CABECERA HTTP<br>DATOS HTTP | –<br>– | SSL-RC4-SHA | SSL-RC4-SHA | IPSEC-3DES-SHA | SSL-RC4-SHA |
| TRANSPORTE | SSL | CABECERA SSL<br>SSL HASH | –<br>– | WEP128<br>SSL-RC4-SHA | IPSEC-3DES-SHA<br>SSL-RC4-SHA | IPSEC-3DES-SHA | IPSEC-3DES-SHA<br>SSL-RC4-SHA |
| | TCP | CABECERA TCP | – | WEP128 | IPSEC-3DES-SHA | IPSEC-3DES-SHA | IPSEC-3DES-SHA |
| RED | IP | CABECERA IP | – | WEP128 | IPSEC-3DES-SHA | IPSEC-3DES-SHA | IPSEC-3DES-SHA |
| | IPSEC | NUEVA CABECERA IP<br>CABECERA ESP<br>ESP TRAILER<br>ESP AUTH | –<br>–<br>–<br>– | –<br>–<br>–<br>– | IPSEC-3DES-SHA | IPSEC-3DES-SHA | IPSEC-3DES-SHA |
| MAC | LLC | CABECERA LLC | – | WEP128 | – | WEP128 | WEP128 |
| | WEP | MIC | – | WEP128 | – | WEP128 | WEP128 |

Tabla I: Mecanismos de seguridad CL aplicados en cada campo con la solución CL-WSec.

total de octetos cifrados en cada política de seguridad. El criterio aplicado es que un campo que debe ser cifrado por el servicio de seguridad de capa lo será si no ha sido cifrado en capas superiores, o es un campo introducido por el protocolo de capa y que se cifra en el protocolo original. Este criterio permite mantener la seguridad en capas superiores y elimina las operaciones de cifrado en capas inferiores.

En [18] definíamos los términos mecanismo de seguridad original y mecanismo de seguridad CL a los mecanismos de seguridad de capa que aplica el cifrado de datos original y al mecanismo de seguridad de capa que implementa la solución CL-WSec propuesta, respectivamente. La solución CL-WSec permite reducir el número de octetos cifrados en aquellas políticas que aplican más de un mecanismo de seguridad. La tabla I describe los mecanismos de seguridad que se aplicarán, en cada política, a los campos de cada protocolo al implementar la solución CL-WSec. En la tabla II se detalla una comparativa del número de octetos cifrados por los mecanismos de seguridad original con el número de octetos cifrados por los mecanismos de seguridad CL, a partir de una longitud de datos de aplicación igual a L octetos. En esta tabla se observa que al aplicar la solución CL-WSec a cada política, la primera capa, en sentido descendente, que aplica seguridad, cifrará los datos de aplicación (L octetos) y las capas inferiores cifrarán una longitud fija de octetos que, en cada política, depende del número de octetos correspondientes a cabeceras de protocolos y mecanismos de seguridad utilizados.

| Políticas de seguridad | | | | | |
|---|---|---|---|---|---|
| | | Número de octetos cifrados en cada capa y política. | | | |
| Política | Número Octetos | SSL | IPSec | MAC | TOTAL |
| P1 | Cifrado original | L+16 | – | L+73 | 2L+89 |
| | Cifrado CL-WSec | L+16 | – | 57 | L+73 |
| P2 | Cifrado original | L+16 | L+65 | – | 2L+81 |
| | Cifrado CL-WSec | L+16 | 49 | – | L+65 |
| P3 | Cifrado original | – | L+44 | L+104 | 2L+148 |
| | Cifrado CL-WSec | – | L+44 | 60 | L+104 |
| P4 | Cifrado original | L+16 | L+65 | L+125 | 3L+206 |
| | Cifrado CL-WSec | L+16 | 49 | 60 | L+125 |

Tabla II: Octetos cifrados antes y después de aplicar CL para cada capa y política.

La idea de reducir el consumo de energía al modificar el cifrado de la información ha sido estudiado en [15]. Los autores presentan un algoritmo adaptativo que se basa en que, cada capa aplica el mecanismo de seguridad que menos energía consume en función del tipo de paquete y de la longitud de los datos, pero siguen manteniendo la multiplicidad de cifrado. Los datos referentes al consumo de energía de diferentes algoritmos de cifrado utilizados en las simulaciones han sido obtenidos a partir de estudios realizados por otros autores. En [7] y [13] se indican los resultados de consumo de energía de diferentes algoritmos de cifrado utilizados en IPSec. En [16] los autores analizan el rendimiento y consumo de energía del algoritmo de cifrado RC4 (utilizado en SSL y WEP) en función de la frecuencia de la CPU. En [13] y [14] los autores cuantifican el consumo de energía cuando se cifra la información con el algoritmo RC4.

La mejora del rendimiento en políticas que implementan varios mecanismos de seguridad ha sido estudiado en [3] y [4]. En estos artículos se presentan 5 escenarios, 3 de ellos considerando “roaming", y 12 políticas de seguridad. Estas políticas se contruyen como combinación de los protocolos de seguridad TLS, IPSec y WEP, más la política en la que no se aplica ningún mecanismo de seguridad. Una vez planteados los escenarios y mecanismos de seguridad aplicados, se asignan pesos a cada uno de los servicios de seguridad ofrecidos en cada capa y se calcula el nivel de seguridad ofrecido por cada política. Establecido el nivel de seguridad, los autores analizan el rendimiento desde el punto de vista del tiempo de autenticación y del número de octetos introducido por los mecanismos de seguridad. Con estos datos, obtienen un valor de rendimiento para cada política de seguridad. Hay que indicar que en este artículo no se analiza el efecto sobre el consumo de energía en un dispositivo inalámbrico y que en [4] se indica el estudio de la seguridad Cross-Layer, pero que el artículo no hace ninguna referencia a una comunicación inter-capas tal y como propone el diseño Cross-Layer [11].

Los resultados que presentaremos en este artículo se han obtenido al simular diferentes escenarios que aplican el algoritmo CL-WSec, en los que uno o más nodos, que actuarán como terminales inalámbricos, se conectarán a un nodo, que actuará como punto de acceso. En esta comunicación se realizará un intercambio de información con unos parámetros determinados. Con el objeto de caracterizar el tráfico generado analizamos el estudio de otros autores sobre las características del tráfico en redes 802.11. En [9] se caracteriza el tipo de tráfico producido en el acceso a Internet en un entorno residencial cuando se utiliza una red inalámbrica. Por otra parte, existen proveedores que utilizan redes 802.11 para proporcionar acceso público a Internet en emplazamientos de especial interés (por ejemplo en aeropuertos) y que han sido analizados en [6] y [12]. Estas redes 802.11 operan en modo infraestructura en las que un punto de acceso realiza las tareas de gestión y control. En [5] se analiza el tráfico generado en una organización cuando los usuarios acceden a través de una red inalámbrica. En este estudio se ha caracterizado la tasa de tráfico en función del número y ubicación de los puntos de acceso, del número de usuarios, del día y hora, etc. Las aplicaciones multimedia y en

particular el uso de aplicaciones tipo Skype [2] generan una elevada tasa de transmisión. En la página web de Skype [2], se indican las tasas de transmisión recomendadas para diferentes usos de Skype. El análisis en entornos reales de la tasa de transmisión y de las características del tráfico generado por Skype ha sido estudiado en [8] y [10].

## III. Escenarios, políticas de seguridad y velocidad de transferencia.

En este artículo simularemos 5 posibles escenarios donde un punto de acceso da servicio a 1, 2, 5, 10 o 20 nodos inalámbricos. Acotaremos las posibilidades en cuanto a los mecanismos de seguridad aplicados en cada escenario, definiendo 5 políticas de seguridad diferentes (P0 a P4) que un terminal inalámbrico puede implementar. Estas políticas se implementan en la pila de protocolos TCP/IP y el estándar IEEE 802.11. Definiremos la política P0 como aquella que no implementa ningún mecanismo de seguridad. En la política P1 se implementa el protocolo de seguridad SSL, a nivel de transporte y el protocolo WEP a nivel MAC. En la política P2 se implementará el protocolo de seguridad SSL, a nivel de transporte, y el protocolo IPSec a nivel IP. La Política P3 implementa el protocolo IPSec a nivel IP, y el protocolo WEP a nivel de enlace. La política P4 implementará el protocolo de seguridad SSL, a nivel de transporte, el protocolo IPSec a nivel IP y el protocolo WEP a nivel MAC. Los parámetros utilizados en las simulaciones realizadas en este artículo referente al tipo de tráfico, la tasa de transferencia y la longitud de los paquetes de los usuarios inalámbricos, han sido definidos a partir de los resultados presentados en los artículos y experimentos citados en la sección II. Según estos resultados, las tasas de transferencia utilizadas en las simulaciones serán 100 Kbps, 500 Kbps y 1500 Kbps, y la longitud de los paquetes utilizado será 100, 500 y 1500 octetos.

En este artículo escogemos, para su análisis, los algoritmos para el cifrado y autenticación de la infomación a nivel de transporte SSL-RC4-SHA (SSL con los algoritmos RC4 y SHA1 para cifrado e integridad respectivamente). A nivel IP escogemos los mecanismos de seguridad IPSEC-3DES-SHA (IPSec ESP con 3DES y SHA1 como algoritmos de cifrado e integridad respectivamente). A nivel MAC el mecanismo elegido es WEP que implementa el cifrado mediante el algoritmo RC4 con clave de 128 bits y lo denotaremos como WEP128.

## IV. Análisis del tiempo de vida de la batería.

En esta sección describimos el proceso realizado para cuantificar el ahorro en el consumo de energía y el aumento del tiempo de vida de la batería de un terminal inalámbrico, que hemos supuesto es una PDA iPAQ H3670, al aplicar la solución CL-WSec propuesta. Los resultados que presentamos se han obtenido analizando, mediante simulaciones, el comportamiento de un nodo (Nodo 1) que pertenece a una red inalámbrica. Estas simulaciones se han configurado a partir de los escenarios, políticas de seguridad, tasas de transferencia y longitud de los paquetes de datos descritos en la sección III.

Las simulaciones se han divido en dos fases. En una primera fase se utiliza el simulador ns2 y su modelo de energía para analizar, en cada escenario, el comportamiento de un nodo (Nodo 1) configurado con los valores de CBR y longitud de segmento TCP deseados. El resto de nodos adoptarán valores aleatorios. Para cada una de las simulaciones realizadas con ns2 obtenemos datos del consumo de energía de una PDA iPAQ H3670 cuando aplica la política P0 (ningún mecanismo de seguridad). En una segunda fase, a partir de los resultados obtenidos con ns2, calculamos el consumo de energía en las políticas restantes (P1, P2, P3 y P4) cuando implementan los mecanismos de seguridad originales y cuando aplican la solución CL-WSec. A partir de las líneas de eventos, que forman los ficheros con los resultados de las simulaciones realizadas en la primera fase con ns2, contabilizamos la energía consumida en operaciones de cifrado y descifrado. De las líneas de eventos extraemos los valores necesarios para el consumo de energía debido a operaciones de cifrado y descifrado aplicando los siguientes criterios:

1. La energía utilizada en operaciones de cifrado y descifrado se calculará para cada capa a partir de la longitud del campo de datos de aplicación. En la tabla II hemos establecido la relación entre el número de octetos cifrados en cada capa y política a partir de la longitud del campo de datos de aplicación (L), cuando aplicamos los mecanismos de seguridad originales y cuando se aplica la solución CL-WSec. Aplicando estos valores y conociendo el consumo de energía utilizado por cada mecanismo de seguridad para cifrar o descifrar un octeto, podemos calcular la energía consumida en operaciones de cifrado y descifrado en cada política.
2. Suponemos que en la retransmisión de una trama en el caso de pérdida de información, no se vuelve a cifrar la información ya que la trama permanece almacenada en un buffer interno en el nodo emisor.
3. La energía utilizada para operaciones de cifrado y descifrado es la suma de la energía necesaria para el “key setup"más la energía utilizada por cada mecanismo para cifrar los octetos de datos y los campos de los protocolos de capa.

Para cuantificar el consumo de energía debido a operaciones de cifrado y descifrado en cada una de las políticas supuestas, debemos conocer el coste en términos de energía consumida por octeto cifrado para cada mecanismo de seguridad aplicado. Estos valores se han obtenido utilizando los resultados presentados por diversos autores y que hemos descrito en la sección II. El consumo de energía en una PDA iPAQ H3670 cuando implementa el algoritmo de cifrado RC4 se estudia en [13], de donde se extrae (ver figura 5 de [13]) que el consumo por octeto para cifrar y descifrar mediante este algoritmo equivale a 3.93 uJ/octeto. El consumo de energía en esta PDA debido al cifrado en IPSec se analiza en [7] y [13], donde se extrae que el consumo debido al cifrado 3DES es de 6,04 uJ/octeto (ver figura 5 de [13]).

### *IV-A. Resultados.*

A continuación presentamos los resultados de ahorro de energía obtenidos mediante las simulaciones realizadas y

que hemos apuntado en la sección anterior. Estos resultados se dividen en dos grupos. El primer grupo de resultados está representado en las figuras 1 a 6 junto a la tabla III. Los resultados indicados en este primer grupo corresponden a los tiempos de vida obtenidos en un nodo (nodo 1) que pertenece a una red inalámbrica al variar la longitud del segmento TCP, el número de nodos de la red y la tasa de transferencia. El segundo grupo de resultados está representado en las figuras 7 a 11 que muestran el incremento del tiempo de vida de la batería, en este nodo 1, obtenidos al aplicar la solución CL-WSec para redes con 1, 2, 5, 10 y 20 nodos.

Las figuras 1 a 3, representan los tiempos de vida de la batería obtenidos para un nodo 1 que opera en una red inalámbrica sin ningún otro nodo y que intercambia información con el punto de acceso con longitudes del segmento TCP de 100, 500 y 1500 octetos respectivamente. Los resultados obtenidos indican que el tiempo de vida es mayor para valores de CBR bajos y valores altos del segmento TCP. A medida que aumenta el CBR el tiempo de vida de la batería se reduce hasta un valor límite inferior. Para valores de CBR altos y valores bajos de la longitud del segmento TCP, el terminal necesita enviar un número mayor de tramas por lo que se envía más información adicional debida a cabeceras. Al aumentar la longitud del segmento TCP y aumentar la tasa CBR, se envía la misma información con menos tramas y en menos tiempo. También debemos considerar que en una red con un nodo las únicas colisiones que se producen son entre el terminal inalámbrico y el punto de acceso por lo que el número de retransmisiones es muy bajo y no afecta a los resultados obtenido.

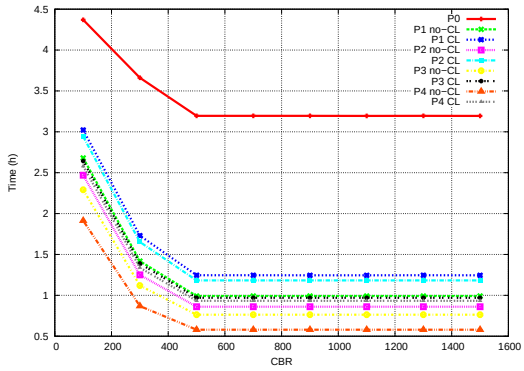


Figura 1: Tiempo de vida de la batería en una red con 1 nodo. Longitud del segmento TCP de 100 Octetos.

Las figuras 4 a 6 representan los tiempos de vida de la batería de un nodo que opera en una red inalámbrica formada por 2 nodos y que intercambia información con el punto de acceso con longitudes del segmento TCP de 100, 500 y 1500 octetos respectivamente. En estas gráficas observamos que el comportamiento es parecido al obtenido en una red con un único nodo. El tiempo de vida es mayor para valores de CBR bajos y valores altos de la longitud del segmento TCP. A medida que aumenta el CBR el tiempo de vida de la batería decrece hasta un valor límite inferior. En estas gráficas observamos como la pendiente de la curva

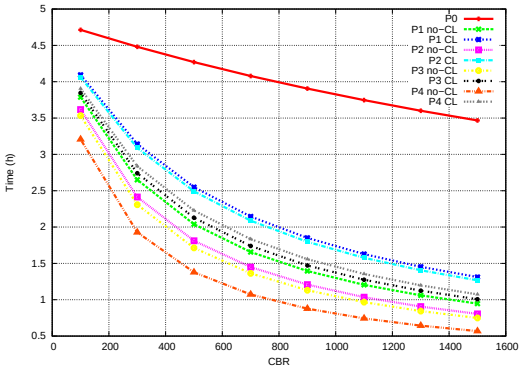


Figura 2: Tiempo de vida de la batería en una red con 1 nodo. Longitud del segmento TCP de 500 Octetos.

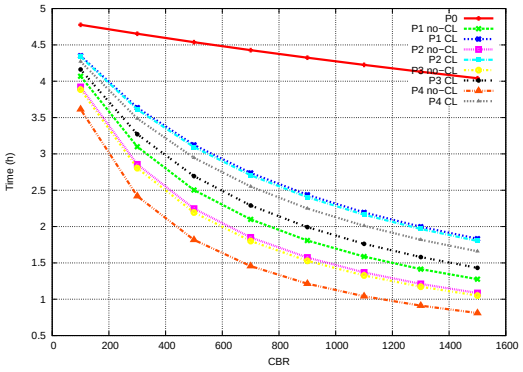


Figura 3: Tiempo de vida de la batería en una red con 1 nodo. Longitud del segmento TCP de 1500 Octetos.

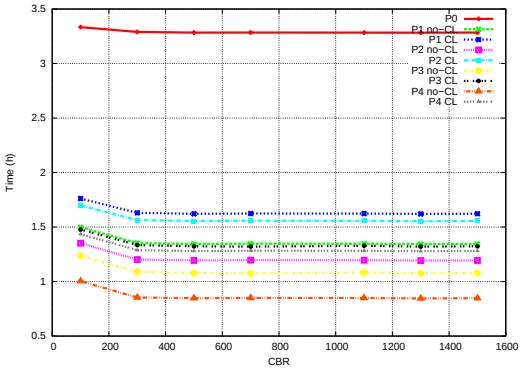


Figura 4: Tiempo de vida de la batería en una red con 2 nodos. Longitud del segmento TCP de 100 Octetos.

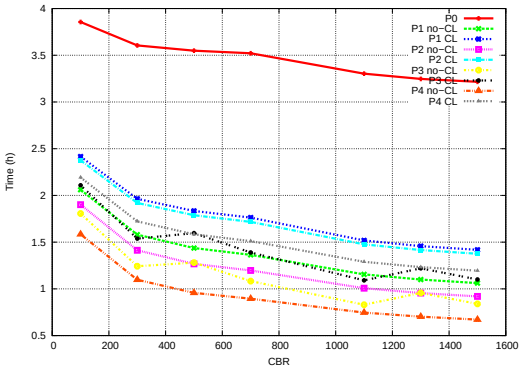


Figura 5: Tiempo de vida de la batería en una red con 2 nodos. Longitud del segmento TCP de 500 Octetos.

que representa el tiempo de vida de la batería es decreciente pero se suaviza respecto a una red con un nodo.

| Tiempo de vida medio de la batería en el nodo 1 (h) (Protocolo TCP). | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Red con 5 nodos | | | Red con 10 nodos | | | Red con 20 nodos | | |
| | Longitud TCP | | | Longitud TCP | | | Longituid TCP | | |
| Policy | 100 octetos | 500 octetos | 1500 octetos | 100 octetos | 500 octetos | 1500 octetos | 100 octetos | 500 octetos | 1500 octetos |
| P0 | 3.358 | 3.268 | 3.156 | 3.3908 | 3.2974 | 3.1791 | 3.416 | 3.324 | 3.208 |
| P1 no CL | 1.957 | 1.618 | 1.366 | 2.445 | 2.1175 | 1.8249 | 2.8245 | 2.754 | 2.321 |
| P1 CL | 2.223 | 1.994 | 1.786 | 2.6476 | 2.4384 | 2.2207 | 2.956 | 2.7937 | 2.615 |
| P2 no CL | 1.804 | 1.454 | 1.211 | 2.321 | 1.9640 | 1.6639 | 2.7413 | 2.462 | 2.190 |
| P2 CL | 2.17 | 1.96 | 1.769 | 2.610 | 2.4104 | 2.207 | 2.932 | 2.778 | 2.606 |
| P3 no CL | 1.69 | 1.297 | 1.856 | 2.2285 | 1.9123 | 1.641 | 2.677 | 2.423 | 2.17 |
| P3 CL | 1.951 | 1.703 | 1.497 | 2.4447 | 2.1991 | 1.957 | 2.825 | 2.632 | 2.426 |
| P4 no CL | 1.423 | 1.152 | 0.973 | 1.9861 | 1.662 | 1.398 | 2.498 | 2.217 | 1.951 |
| P4 CL | 1.929 | 1.803 | 1.685 | 2.4331 | 2.2933 | 2.1416 | 2.817 | 2.697 | 2.56 |

Tabla III: Tiempo de vida medio de la batería.

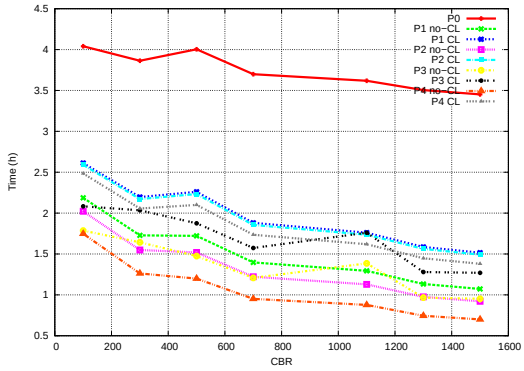


Figura 6: Tiempo de vida de la batería en una red con 2 nodos. Longitud del segmento TCP de 1500 Octetos.

En las simulaciones realizadas en redes inalámbricas con 5 nodos o más, podemos considerar que los tiempos de vida e incrementos del tiempo de vida de la batería obtenidos cuando aplicamos la solución CL son constantes y los indicamos en la tabla III. Esto ocurre en todas las políticas simuladas. La varianza máxima obtenida en estos resultados es de 0.009 h para una red con 5 nodos, 0.00033 h para una red con 10 nodos y 2.99E-05 h para una red con 20 nodos.

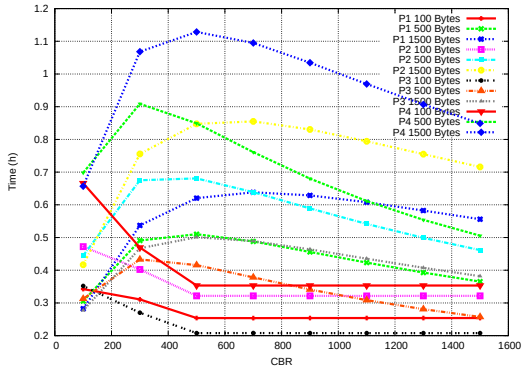


Figura 7: Incremento del tiempo de vida de la batería en una red con 1 nodo.

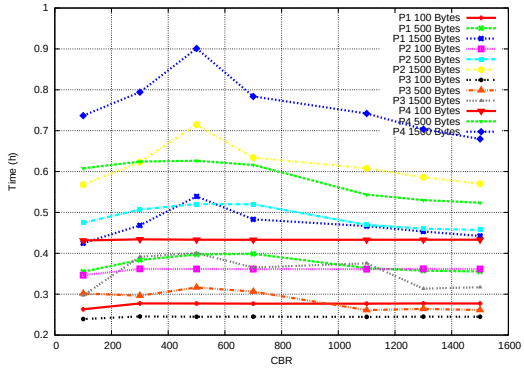


Figura 8: Incremento del tiempo de vida de la batería en una red con 2 nodos.

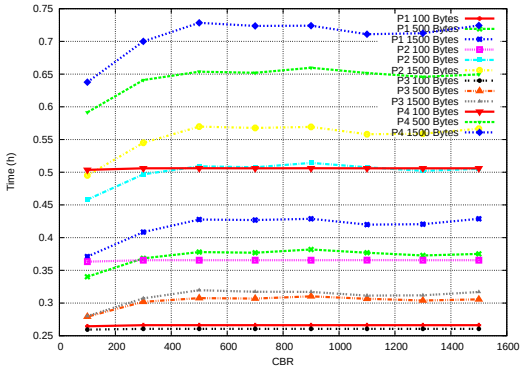


Figura 9: Incremento del tiempo de vida de la batería en una red con 5 nodos.

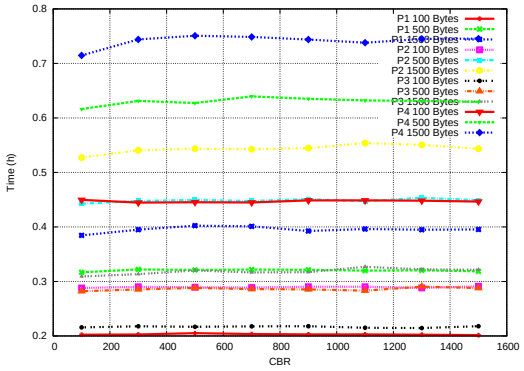


Figura 10: Incremento del tiempo de vida de la batería en una red con 10 nodos.

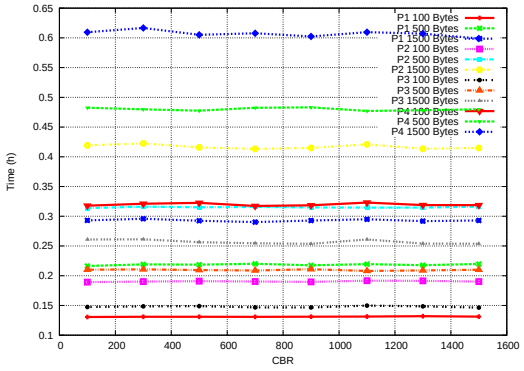


Figura 11: Incremento del tiempo de vida de la batería en una red con 20 nodos.

Si analizamos los resultados correspondientes al incremento del tiempo de vida de la batería obtenidos al aplicar la solución CL para redes con 1, 2, 5, 10 y 20 nodos obtenemos las figuras 7 a 11. En estas gráficas podemos observar que en una red inalámbrica con 1 nodo (figura 7), todas las políticas analizadas con una longitud del segmento TCP igual a 1500 octetos tienen un incremento máximo del

tiempo de vida de la batería para un valor del CBR igual a 500 Kbps. Si la longitud del segmento TCP es de 500 octetos, el valor máximo del incremento del tiempo de vida se produce para un valor del CBR igual a 300 Kbps y si la longitud del segmento TCP es de 100 octetos, el valor máximo se produce con un CBR igual a 100 Kbps (mínimo CBR simulado).

Los resultados obtenidos en una red inalámbrica con 2 nodos, indican que el valor máximo del incremento del tiempo de vida se obtiene para una longitud de segmento TCP de 1500 octetos cuando el valor del CBR está entre 500 y 700 Kbps. Para una longitud de segmento TCP de 500 octetos, el máximo incremento se obtiene, también, para un CBR de entre 500 y 700 Kbps. De los resultados obtenidos para una longitud de segmento TCP de 100 octetos, podemos considerar que el incremento del tiempo de vida es constante para cualquier valor de CBR.

En las simulaciones realizadas para una red inalámbrica con 5 nodos, los resultados obtenidos indican que el valor máximo del incremento del tiempo de vida se obtiene para una longitud de segmento TCP de 1500 octetos, cuando el CBR es 500 y 1500 Kbps. Para una longitud de segmento TCP de 500 octetos, el máximo incremento se obtiene con un CBR de 900 Kbps. Para una longitud de segmento TCP de 100 octetos, consideramos que el incremento del tiempo de vida es constante para cualquier valor de CBR. Los resultados obtenidos en las simulaciones realizadas para redes inalámbricas con 10 y 20 nodos (figuras 10 y 11), dan un valor constante para el tiempo de vida de la batería, al considerar diferentes valores del CBR y del segmento TCP.

De los resultados presentados extraemos la conclusión de que la política con la que se obtiene un mayor incremento del tiempo de vida es la política P4 y que este incremento es mayor cuanto mayor es el valor de la longitud de los datos de aplicación (L). Al aumentar el número de nodos de la red, para una longitud de datos L, podemos cosiderar que el valor del incremento del tiempo de vida es constante para cada política y no depende de la tasa de transferencia CBR utilizada.

## V. Trabajo futuro.

Como trabajo futuro queremos destacar la necesidad de complementar este artículo con el análisis del ahorro de energía estimado para aplicaciones que utilizan el protocolo UDP y el conjunto TCP/UDP.

## VI. Agradecimientos

Este trabajo ha sido parcialmente financiado por el MEC y FEDER bajo el proyecto ARES "Grupo de Investigación Avanzada en Seguridad y Privacidad de la Información"(Consolider - Ingenio CSD2007-004).

## Referencias

[1]IEEE Std 802.11-1997 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[2]Skype Web Site [Online]. *Available: http://www.skype.com*.

[3]Agarwal A. K. and Wang W. On the impact of quality of protection in wireless local area networks with ip mobility. *Mobile Netw Appl. Springer*, pages 93–110, Nov 2006.

[4]Agarwal A. K., Wang W. and McNair J. Y. An experimental study of cross-layer security protocols in public access wireless networks. *IEEE Globecom*, pages 1747–1751, 2005.

[5]Balazinska M and Castro P. Characterizing mobility and network usage in a corporate wireless local-area network. *MobiSys '03 Proceedings of the 1st International Conference on Mobile systems, applications and services*, pages 5–17, May 2003.

[6]Chen Na, J. K. Chen, T. S. Rappaport. Measured Traffic Statistics and Throughput of IEEE 802.11b Public WLAN Hotspots with three different applications. *IEEE Transactions on Wireless Communications*, 5(11):3296–3305, Aug. 2006.

[7]Da Costa Junior F., Gaspary L., Barbosa J., Cavalheiro G., Pfitscher1 L., and Ramos J.D.G. Evaluating the Impact on Data Reception and Energy Consumption of Mobile Devices using IPSec to securely access WiFi Networks. *Wireless Communications and Networking Conference (WCNC2005). News Orleans. LA, USA*, March 2005.

[8]De Cicco L., Mascolo S. and Palmisano V. . Skype Video Responsiveness to Bandwidth Variations. *ACM NOSSDAV '08 Proceedings of the 18th International Workshop on Network and Operating Systems Support for Digital Audio and Video*, May 2008.

[9]Florian Wamser, Rastin Pries, Dirk Staehle, Klaus Heck and Phuoc Tran-Gia. Traffic characterization of a residential wireless Internet access. *Telecommunication Systems.*, 48(1-2):5–17, May 2010.

[10]Jing Zhu. On Traffic Characteristics and User Experience of Skype Video Call. *In proceeding 2011 IEEE 19th International Workshop on Quality of Service (IWQoS)*, pages 1–3, June 2011.

[11]Kawadia V. and Kumar P.R. A cautionary perspective on cross-layer design. *IEEE Wireless Communications*, 12(1):3–11, 2005.

[12]M. Rodring, C. Reis, R. Mahajan, D. Wetherall and J. Zahorjan. Measurement-based Characterization of 802.11 in a Hotspot Setting. *SIGCOMM'05 Workshop*, pages 5–10, Aug. 2005.

[13]Potlapally N. R., Ravi S., Raghunathan A. and Jha N.K. A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols. *IEEE Transactions on Mobile Computing*, 5(2):128–143, Feb. 2003.

[14]Prasithsangaree P. and Krishnamurthy P. Analysis of Energy consumption of RC4 and AES Algorithm in Wireless LAN. *IEEE GLOBECOM 2003*, pages 1445–1449, 2003.

[15]Prasithsangaree P. and Krishnamurthy P. On a framework for energy-efficient security protocols in wireless networks. *Computer Communications, Elsevier Science*, 27(17):1716–1729, Nov. 2004.

[16]Rapuano S. and Zimeo E. Measurement of performance impact of SSL on IP data transmissions. *ScienceDirect Measurement*, 41:481–490, 2008.

[17]Urbano Fullana A., Ferrer Gomila J.L. and Payeras Capellá M. Mejoras del rendimiento con el diseño CrossLayer para los servicios de seguridad. *IX Jornadas de Ingenieria Telemática 2010 (JITEL)*, pages 206–213, 2010.

[18]Urbano Fullana A., Ferrer Gomila J.L. and Payeras Capellá M. Reducción de la redundancia de cifrado en redes basadas en TCP/IP y 802.11. *Reunión Espanola de Criptologia Seguridad de la Información (RECSI 2010)*, pages 265–270, 2010.

[19]Urbano Fullana A., Ferrer Gomila J.L., Payeras Capellá M., Hinarejos Campos F. y Huguet Rotger Ll. Cross-Layer secrecy design on TCP/IP and 802.11 for energy saving. *4th IFIP International Conference on New Technologies, Mobility and Security*, pages 1–5, 2011.