Coste de los protocolos de seguridad en redes MANET*

Helena Rifà-Pous, Joan Vila-Canals, Jordi Herrera-Joancomartí

Estudios de Informática, Multimedia y Telecomunicaciones

Universitat Oberta de Catalunya

Rbla. del Poble Nou, 156

08018 Barcelona

{hrifa,jvilacan,jherreraj}@uoc.edu

Resumen

Los mecanismos de seguridad son uno de los requisitos fundamentales para el buen funcionamiento de los protocolos de redes ad hoc móviles. En este artículo se analizan los problemas de seguridad de los protocolos de encaminamiento básicos, se describen las soluciones de seguridad existentes, y se hace un estudio del coste computacional y energético que supone para el sistema la inclusión de mecanismos de seguridad.

1. Introducción

La proliferación de terminales móviles en el mercado ha hecho surgir nuevas formas de comunicación basadas en la creación de redes formadas por dispositivos de usuarios que se agrupan de forma esporádica. Este tipo de redes reciben el nombre de redes móviles ad hoc (MANET) [2], y están tomando especial importancia por ser unas redes que no precisan de infraestructura dedicada, son rápidas de desplegar, pueden proporcionar acceso a la información en contextos y entornos aislados y/o conflictivos, y su coste es reducido.

La transmisión de datos en las redes MANET se realiza a través de los propios terminales finales de los usuarios que forman parte de la red, que actúan como encaminadores de los paquetes. Por ello es necesario que los nodos colaboren y realicen las funciones de soporte permitiendo que el rango de comunicación de cada usuario se extienda más allá del alcance de sus radiaciones electromagnéticas.

En comunidades de usuarios heterogéneas la cooperación voluntaria de todos los nodos no es asumible y por lo tanto, son necesarios mecanismos de seguridad que permitan gestionar el proceso colaborativo y proteger al sistema de ataques maliciosos que intentan sacar provecho de la red sin invertir nada a cambio. Aunque la seguridad es uno de los aspectos fundamentales para el funcionamiento de los protocolos de encaminamiento en redes ad hoc, el hecho que en estos entornos se utilicen dispositivos con unos recursos limitados y con poca autonomía de acción, ha llevado a que los mecanismos de seguridad no sean priorizados a la hora de diseñar los protocolos por suponer un coste elevado y una carga para el sistema.

En el presente artículo presentamos un estudio de los costes temporales y energéticos de los protocolos de encaminamiento en redes ad hoc y evaluamos su viabilidad. El resto del artículo está organizado como sigue: en la sección 2 describimos los requisitos de los protocolos de descubrimiento de rutas y hacemos un repaso de los protocolos seguros más relevantes. La sección 3 detalla la metodología de análisis y el funcionamiento de los protocolos estudiados. En la sección 4 se describen las pruebas realizadas para obtener el coste temporal y energético de diferentes algoritmos criptográficos y se exponen los resultados obtenidos. La sección 5 analiza el coste de tres protoco-

*Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología con el proyecto SEG2004-04352-C04-04 PROPRIETAS-WIRELESS.

los de encaminamiento y los compara con los costes del resto del sistema. Finalmente, en la sección 6 se resumen las conclusiones sobre el efecto que tienen en el coste del sistema los mecanismos de seguridad en los protocolos de red.

2. Encaminamiento en redes ad hoc

En una red ad hoc genérica, los nodos no tienen comunicación directa con todos los demás nodos de la red. La transmisión de paquetes se hace a través de encaminamientos *multihop*, es decir, los paquetes son reenviados a través de múltiples nodos intermedios que hacen de enlace entre emisor y receptor. Los protocolos de encaminamiento son los encargados de descubrir y mantener las tablas de rutas entre dos nodos cualquiera de la red. La información que se intercambian los nodos para construir la visión virtual de la topología de red tiene que ir protegida para evitar que se planifiquen falsas rutas que impidan la entrega de paquetes a los destinatarios a los que van dirigidos, y para asegurar una colaboración justa y uniforme de todos los usuarios. Además, se intenta que no haya revelación de datos personales de cada uno de los participantes de la red, aunque el conocimiento de la localización en la que se encuentra un usuario es, por la naturaleza del protocolo, casi inevitable.

Para conseguir los objetivos de seguridad propuestos existen dos alternativas de acción distintas:

1. **Prevención.** Este tipo de soluciones están diseñadas para impedir que los nodos maliciosos realicen ataques, y en caso que lo intenten, sean frustrados. Los mecanismos de seguridad en los que se basan son la autenticación de nodos, la protección de la integridad de la información de encaminamiento que viaja por la red y la confidencialidad de los datos privados.

2. **Detección y reacción.** Estos sistemas actúan en caso que un nodo haya infringido el protocolo, consiguiendo saltar los mecanismos preventivos establecidos. Las técnicas de detección se fundamentan en el control y la monitorización de los nodos que forman la red. Por otro lado, los mecanismos de reacción definen como se debe gestionar la publicación de las intrusiones detectadas y diseñan protocolos de reputación para evitar que los nodos maliciosos queden impunes a sus acciones.

Las dos técnicas no son excluyentes sino complementarias, y por lo tanto, en el diseño de los protocolos siempre se tiene en cuenta el enlace y el traspase de información de unos mecanismos a otros.

En este artículo nos centraremos en sistemas de prevención. Los sistemas preventivos intentan evitar ataques utilizando técnicas de clave simétrica, asimétrica o cadenas de hash. La criptografía de clave simétrica tiene la ventaja que tiene un coste computacional muy bajo y es eficiente. Por otro lado, la gestión de claves es complicada, y más si el sistema es abierto y dinámico. La criptografía de clave asimétrica requiere más recursos computacionales, pero la gestión de claves es más sencilla. Finalmente, las técnicas basadas en cadenas de hash son muy rápidas y ligeras, pero por si solas no pueden ofrecer todos los servicios de seguridad requeridos y se tienen que complementar con mecanismos basados en clave pública o privada.

Los protocolos de clave simétrica para redes ad hoc más resaltables son SAR (Secure aware Ad hoc Routing protocol) [15] y SRP (Secure routing protocol for mobile ad hoc networks) [12]. SAR introduce la idea de utilizar una métrica para la búsqueda de caminos de transmisión basada en niveles de seguridad. Los usuarios están asociados a unos niveles de seguridad y cada nivel comparte una clave secreta. Sólo los nodos que comparten la clave de nivel pueden procesar y reenviarse mensajes entre ellos. El inconveniente de este protocolo es la dificultad de gestionar y operar con estos niveles de seguridad, que ofrecen muy poca flexibilidad. Por otro lado, el protocolo SRP se basa en la creación de asociaciones de seguridad (SA) para cada pareja de usuarios que se quieren comunicar. Aunque el protocolo se basa en algoritmos de clave simétrica eficientes, el hecho que cada subgrupo de dos usuarios de

una red deban compartir una clave diferente es muy costoso y difícil de gestionar.

Otras propuestas destacables por su voluntad de ser muy ligeras son las basadas principalmente en algoritmos de hash. Los protocolos SEAD (Secure Efficient Ad hoc Distance vector routing protocol) [8] y ARIADNE [9] utilizan cadenas de hash para prevenir que los nodos intermedios de una ruta modifiquen los datos de encaminamiento sensibles. De todas formas, es necesario que el emisor del mensaje sea autenticado y eso se puede hacer mediante unas claves simétricas pre-establecidas (que no siempre existen) o utilizando el protocolo TESLA (Time Efficient Stream Loss tolerant Authentication), que aunque robusto, introduce retardos en el sistema y requiere la sincronización temporal de todos los nodos participantes, cosa que es difícil de asegurar.

Debido a las dificultades de desplegar protocolos de clave simétrica y protocolos basados en cadenas de hash, han ido surgiendo diferentes propuestas de protocolos más sencillos de gestionar basados en algoritmos de clave pública. Uno de los primeros fue ARAN (Authenticated Routing for Ad hoc Networks routing protocol) [14], que se fundamenta en el uso de firmas digitales para controlar qué nodos forman parte de la ruta entre dos usuarios. El protocolo SADSR (Security Aware Adaptive Dynamic Source Routing Protocol) [6] es similar a SAR en el hecho que usa el nivel de confianza como métrica para establecer las rutas de envío, pero no utiliza criptografía de clave simétrica sino firmas digitales para controlar que los nodos intermedios sean los correctos. Los protocolos SAODV (Secure Ad hoc On-demand Distance Vector Protocol)[7] y SEDYMO (Secure Dynamic MANET On-demand Routing Protocol) [13] combinan el uso de mecanismos de firma digital y cadenas de hash con el objetivo de ser más ligeros que los anteriores. Finalmente, el protocolo SRDP (Secure Route Discovery Protocol) [10], que combina criptografía simétrica, asimétrica y cadenas de hash, introduce la noción de autenticación retrasada para aligerar la carga del protocolo y que sea un poco más rápido (aunque el coste energético sea el mismo). La integridad de las rutas es verificada en los mensajes de respuesta del protocolo, no durante la fase de emisión de descubrimiento de rutas.

Por su flexibilidad y robustez, los protocolos de encaminamiento basados en clave asimétrica son los que mejor se adaptan al entorno de las redes ad hoc. Las críticas a este tipo de protocolos son debidas a su coste, pero la carga total que suponen para el sistema tiene que ser comparada en el marco de un entorno real en el que se pueda estudiar si los retardos que introducen y el coste energético son asumibles o no por los terminales finales.

3. Metodología y protocolos analizados

3.1. Metodología

En una red formada por terminales móviles, con unos recursos limitados y con una topología de red dinámica, no es fácil mantener actualizadas las tablas de encaminamiento. Existen dos estrategias básicas para el diseño de protocolos de encaminamiento: los protocolos reactivos, que empiezan a construir la tabla de encaminamiento para un nodo y a calcular el camino a un cierto destino cuando un usuario tiene la necesidad de transmitir un mensaje, y los protocolos proactivos, que mantienen permanentemente unas rutas de enlace entre todos los nodos para que cuando alguien quiera retransmitir algo pueda hacerlo al instante. Aunque los primeros inducen un retardo cuando se inicia la comunicación entre dos nodos, en general son los preferidos porque no malbaratan recursos para establecer rutas que no se van a usar.

A continuación detallamos las operaciones involucradas para poder realizar el envío de mensajes entre dos usuarios de una red ad hoc, basándonos en el uso de protocolos de encaminamiento reactivos y con mecanismos de seguridad de clave asimétrica.

1. **Gestión de claves.** Fase que comprende la generación de claves, certificados y gestión de los vínculos de confianza.

2. **Descubrimiento de rutas.** Un nodo

emisor quiere enviar un mensaje a un receptor con una ubicación desconocida. Se desencadena un mecanismo para establecer un camino entre los dos nodos. En esta fase es importante la autenticación de los usuarios que formaran parte de una ruta, y garantizar la integridad de los datos.

3. **Transmisión de datos.** El nodo emisor y receptor se comunican mediante la ruta establecida en la fase de descubrimiento de rutas. Son necesarios servicios de autenticidad, integridad y confidencialidad de los mensajes.

En la sección 4 se analiza el coste de los algoritmos de seguridad involucrados en cada una de las fases de una comunicación en una red ad hoc para unos protocolos determinados.

3.2. Protocolos analizados

Se han analizado tres protocolos de encaminamiento seguros, reactivos, y basados en mecanismos de clave asimétrica: ARAN, SAODV y SEDYMO.

ARAN y SAODV son extensiones del protocolo AODV [5]. ARAN es un protocolo pesado que requiere que tanto los mensajes de descubrimiento de rutas como las respuestas a estos mensajes vayan firmados por todos los nodos de la ruta y que éstos tengan que validar dos de las firmas del mensaje antes de procesar la información. Es un protocolo robusto, aunque puede sufrir ataques de tipo *selfish* debido a que la métrica que usa para escoger una ruta está basada en el tiempo de transmisión, y esa variable no está protegida.

SAODV sólo requiere que el nodo origen firme los mensajes y que esta firma sea validada por todos los nodos de la ruta. Por otro lado, utiliza cadenas de hash para mantener la integridad de los datos modificados por los nodos intermedios. Este protocolo es más ligero que el anterior pero es vulnerable a ataques de impersonación, ya que los nodos intermedios pueden ser suplantados.

Finalmente, el protocolo SEDYMO es una extensión del protocolo DYMO [4], que a su vez, está basado en AODV. SEDYMO utiliza los mismos principios que SAODV pero corrige la vulnerabilidad de este último requiriendo la firma de los mensajes de encaminamiento por todos los nodos intermedios de una ruta. SEDYMO opera siguiendo un modelo de acumulación de rutas, es decir, que un proceso de descubrimiento de ruta crea tablas de encaminamiento completas no sólo para los nodos emisor y receptor, sino para todos los nodos intermedios. En este sentido, SEDYMO es muy eficiente y óptimo para redes en las que hay diferentes pares de comunicación.

Se ha escogido ARAN y SAODV para hacer la comparación porque son los dos protocolos más conocidos de este tipo. SEDYMO resuelve los problemas de SAODV pero puede ser más pesado. En la sección 5 se estudia el gasto particular de estos tres protocolos.

4. Costes de los algoritmos critográficos

Las pruebas se han hecho con una PDA modelo Compaq iPAQ H3970, con un procesador Intel XScale PXA250 a $400MHz$ y con $64MB$ de memoria SDRAM y 48MB de FlashROM. El sistema operativo que utiliza es la distribución Familiar[1] de Linux, en concreto la versión 0.8.4 que lleva un kernel 2.4.19. Hemos conectado la PDA a un PC a través del puerto serie, y el manejo y la monitorización de la PDA se realizan desde este puerto.

El PC utilizado es un DELL-DCNE con procesador Intel a $2,8GHz$ y una memoria RAM de $512MB$. El sistema operativo que usa es la distribución Ubuntu Edgy Eft de Linux, con un kernel 2.6.17. Se utiliza la aplicación *Minicom* para la conexión con la iPAQ.

Las pruebas sobre el coste de ciertas operaciones criptográficas se han hecho implementando pequeñas aplicaciones de test utilizando las librerías de seguridad OpenSSL [3].

4.1. Coste Temporal

El coste temporal de los algoritmos criptográficos se ha obtenido mediante la implementación de monitores temporales en las aplicaciones de test. Se ha usado la función de siste-

ma *times()* para controlar el tiempo de CPU gastado por cada proceso.

En primer lugar se ha analizado el tiempo expedido por un terminal cliente en la fase de gestión de claves, es decir, en la generación de pares de claves asimétricas. Se han hecho pruebas para el algoritmo RSA con dimensiones de claves de 512 y 1024 bits (ver Cuadro 1). Se han utilizado claves pequeñas porque son las únicas que tiene sentido ir renovando con una periodicidad elevada. Uno de los beneficios del uso de certificados de corta duración es que evita tener que gestionar listas de certificados revocados (CRLs).

Algoritmo	**Tiempo (ms)**
RSA-512	424
RSA-1024	1983

Cuadro 1: Tiempo para la generación de claves RSA

El coste temporal para la generación de claves es elevado, pero como es un proceso asíncrono y puede realizarse previamente a la adhesión a una red ad hoc, no es crítico que su duración supere el segundo.

En la fase de descubrimiento de rutas, los algoritmos critpográficos utilizados para proteger la autenticidad e integridad de los paquetes son las cadenas de hash y las firmas digitales.

Los algoritmos de hash son los algoritmos menos complejos de todos, y por lo tanto, intuitivamente son los que deben tener un menor coste temporal y energético. Esto se confirma en los resultados del Cuadro 2. También observamos que la validación de firmas digitales es mucho más rápida que la generación. Ello es debido a que se han utilizado pares de claves cuyo exponente público es 3.

En la fase de transmisión de datos son necesarios, además de los algoritmos de hash y firma digital, algoritmos de cifrado simétrico y asimétrico que permitan garantizar la confidencialidad de los datos. Se han realizado pruebas de cifrado asimétrico para el intercambio de claves, obteniendo los resultados del Cuadro 3.

Algoritmo	**Tiempo (ms)**
SHA-1	$0,01$
Firma RSA-512	$11,74$
Validación RSA-512	$0,66$
Firma RSA-1024	$61,39$
Validación RSA-1024	$1,35$

Cuadro 2: Tiempo de los algoritmos de hash y clave asimétrica

Algoritmo	**Tiempo (ms)**
Cifrado RSA-512	$0,71$
Descifrado RSA-512	$11,84$
Cifrado RSA-1024	$1,41$
Descifrado RSA-1024	$61,23$

Cuadro 3: Tiempo de los algoritmos de cifrado de claves

Por otro lado, se han realizado pruebas de cifrado de mensajes con clave simétrica sobre ficheros de diferentes tamaños y los resultados los hemos descrito utilizando una ecuación lineal de la forma:

$$Tiempo = a.size + b$$

Es decir, existe una componente fija asociada a la carga del programa, y una componente incremental que es proporcional al tamaño del paquete en Kb. Los resultados experimentales confirman la precisión del modelo lineal y nos han permitido determinar los valores de los coeficientes lineales a y b para los diferentes algoritmos (ver Cuadro 4). Nótese que el protocolo más eficiente es AES con claves de 128 bits, que además ofrece un muy buen nivel de seguridad. Cifrar $1Kb$ de datos tarda unos $0,78ms$, y $1Mb$ cuesta $766,28ms$. Es por lo tanto un algoritmo apropiado tanto para cifrar datos confidenciales que pueden llevar los propios protocolos de encaminamiento, como flujos de información que se quieran transmitir dos usuarios.

4.2. Coste Energético

El coste energético de las diferentes operaciones se ha estimado a partir de los datos del estado de la bateria disponibles en

Algoritmo	Tiempo (ms)
DES	$1,27 + 1,03.s$
3DES	$3,44 + 2,63.s$
AES_128	$0,89 + 0,77.s$

Cuadro 4: Tiempo de los algoritmos de cifrado simétricos

`/proc/asic/battery`.

En primer lugar se han realizado pruebas sobre el coste de las funciones básicas de una PDA. Esto es, el gasto en *stand-by* con la pantalla inactiva y activa (ver Cuadro 5).

Estado	Potencia (mW)
Stand-by pant. inctv	375,87
Stand-by pant. actv	805,62
Consumo de pantalla	429,75

Cuadro 5: Coste básico de una PDA

El coste energético de los algoritmos involucrados en la fase de gestión de claves se detalla en el Cuadro 6. Aunque las operaciones de generación de claves asimétricas son costosas, sólo deben ejecutarse de forma muy puntal. Nótese además, que la generación de un par de claves RSA de 512 bits consume lo mismo que la pantalla de la PDA encendida durante medio segundo, por lo tanto, no es una operación crítica para la PDA.

Algoritmo	Energía (mJ)
RSA-512	213,65
RSA-1024	1205,51

Cuadro 6: Coste para la generación de claves RSA

El Cuadro 7 muestra los resultados de los algoritmos criptográficos utilizados en los protocolos de encaminamiento, ejecutados durante la fase del descubrimiento de rutas. El coste de los algoritmos sigue una ecuación lineal en función del tamaño del paquete s en Kb.

Los resultados de los algoritmos de cifrado de clave asimétrica y simétrica utilizados en la fase de transmisión de datos se muestran en los Cuadros 8 y 9. Los algoritmos de clave

Algoritmo	Energía (mJ)
SHA-1	0,01
Firma RSA-512	6,24
Validación RSA-512	0,29
Firma RSA-1024	40,72
Validación RSA-1024	1,09

Cuadro 7: Coste de los algoritmos utilizados en los protoclos de encaminamiento

asimétrica son más pesados y sólo se utilizan para cifrar datos pequeños o claves de sesión (las pruebas se han realizado cifrando claves AES). Entre los criptosistemas simétricos, el más ligero es AES de 128 bits, con costes de centenas de μJ para cifrados de $1Kb$, y costes de $511,4mJ$ para archivos de $1Mb$.

Algoritmo	Energía (mJ)
Cifrado RSA-512	0,47
Descifrado RSA-512	8,84
Cifrado RSA-1024	0,76
Descifrado RSA-1024	43,68

Cuadro 8: Coste de los algoritmos de cifrados de claves

Algoritmo	Energía (mJ)
DES	$0,67.s$
3DES	$1,72.s$
AES_128	$0,50.s$

Cuadro 9: Coste de los algoritmos de cifrado simétricos

5. Coste de los protocolos de encaminamiento

En esta sección analizaremos el coste de los protocolos de encaminamiento ARAN, SAODV y SEDYMO, basándonos en los resultados de los costes de los algoritmos criptográficos presentados en la sección 4.

El Cuadro 10 muestra el número de operaciones criptográficas llevadas a cabo por el conjunto de nodos que forman parte de la ruta

de enlace entre un emisor y un receptor separados N saltos y con un contador del número máximo de saltos en la red igual a mhc.

Protocol	Sign.	Verif.	Hash
ARAN	$2(N-1)$	$2(2N-3)$	-
SAODV	2	$2(N-1)$	$2(\sum_{i=1}^{N}(mhc-i+1))$
SEDYMO	$2(N-1)$	$2(\sum_{i=1}^{N-1} i)$	$\sum_{i=1}^{N}(mhc-i+1)$

Cuadro 10: Número de operaciones criptográficas

Evaluamos los protocolos usando firmas digitales RSA con claves de 512 bits.

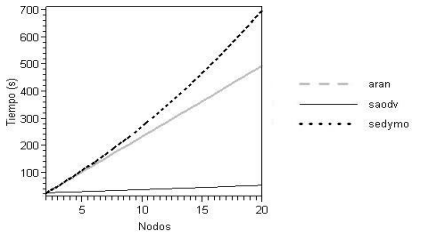

Figura 1: Retardos introducidos por los protocolos de encaminamiento

La Figura 1 muestra el retardo que introducen las operaciones criptográficas en el protocolo de descubrimiento de ruta, es decir, el tiempo que debe esperar el emisor antes de poder iniciar la transmisión de paquetes.

El protocolo que introduce más retardos es SEDYMO, ya que actúa de forma similar a un protocolo proactivo. Inicialmente se establecen muchas rutas con el consiguiente coste temporal, pero cuando alguno de los nodos involucrados en la ruta establecida quiera iniciar una nueva comunicación con alguien del grupo, el retardo será nulo. Los retardos de ARAN y SAODV son menores.

Para agilizar los protocolos en situaciones en que las redes son muy grandes se pueden utilizar técnicas de validación retrasada de firmas, como hace el protocolo SRDP. El problema de este tipo de soluciones es que puede llevar a que haya un gasto computacional mucho más elevado que en el anterior caso porque como la validación de los paquetes no se comprueba al instante y éstos se retransmiten tanto si son auténticos como no, un paquete falso puede llegar a muchos nodos y todos ellos, en su momento, tendrán que comprobar la autenticidad del mismo.

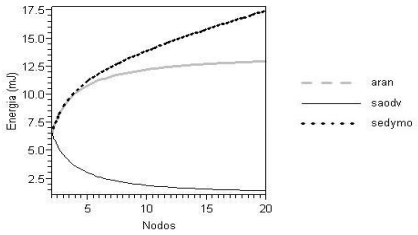

Figura 2: Coste energético de los protocolos de encaminamiento

La Figura 2 muestra los resultados del consumo medio de energía por nodo en el proceso de descubrimiento de una ruta entre 2 nodos cualquiera separados N saltos. El parámetro que indica el contador máximo de saltos (mhc) que puede haber en una ruta se ha fijado al propio diámetro de la red en cada caso, N. Los resultados muestran que el protocolo más ligero es SAODV, seguido de ARAN, y finalmente SEDYMO.

La diferencia en el coste de los diferentes protocolos de encaminamiento es notable y en cada caso se tendrá que analizar cuál es el protocolo que mejor se adapta a la situación en función del tipo de terminales que integren la red y el grado de robustez que se requiera dar. En redes grandes el protocolo SAODV es el más adecuado dado que no tiene un coste exponencial con el número de saltos que tiene una ruta. En redes en las que hay muchas comunicaciones bidireccionales dentro de un grupo, el mejor protocolo es SEDYMO, que permite establecer todas las tablas de rutas con una sola ejecución del protocolo.

En cualquier caso, dada la importancia que tienen para el buen funcionamiento de la red los protocolos con mecanismos de seguridad, y por la facilidad de manejo y gestión de los protocolos basados en criptografía de clave asimétrica, consideramos que la sobrecarga energética que introducen al sistema es soportable. El coste inducido tiene unos margenes muy inferiores al producido por otros servicios disponibles en las PDAs, como interfaz de usuario ($429,75mW$) o acceso a la red sin hilos

(en modo de espera, la red consume $741mW$, ver [11]).

6. Conclusiones

En el presente artículo hemos realizado pruebas que muestran que el coste introducido por los servicios de seguridad en los protocolos de encaminamiento para redes ad hoc es asequible para redes de pequeño y mediano tamaño (unos 20 nodos de diámetro). Para redes más grandes, los retardos temporales se pueden minimizar utilizando técnicas de validación retrasada, y los costes energéticos, usando protocolos que, aunque no sean robustos contra todos los ataques de seguridad, si ofrecen una buena protección y son eficientes, como SAODV. Finalmente, cabe destacar que son los módulos de interfaz de usuario y de red los que suponen el gasto energético principal de la PDA, no los costes computacionales.

Referencias

[1] "Familiar Project," http://familiar.handhelds.org.

[2] "Mobile Ad-hoc Networks (manet)," http://www.ietf.org/html.charters/manet-charter.html.

[3] "OpenSSL Project," http://www.openssl.org.

[4] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol," *IETF Internet Draft, v.06*, October 2006, (Work in Progress).

[5] E. C.Perkins and S.Das, "Ad hoc on demand distance vector (aodv) routing," IETF Experimental RFC, Tech. Rep. 3561, July 2003.

[6] S. Ghazizadeh, O. Ilghami, E. Sirin, and F. Yaman, "Security-aware adaptive dynamic source routing protocol," in *IEEE Conference on Local Computer Networks (LCN)*. Washington, DC, USA: IEEE Computer Society, 2002, p. 0751.

[7] M. Guerrero, "Securing ad hoc routing protocols," *IETF Internet Draft, v.06*, september 2006, (Work in Progress).

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. I, pp. 175–192, 2003.

[9] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *ACM Conference on Mobile Computing and Networking*, 2002.

[10] J.Kim and G. Tsudik, "Srdp: Securing route discovery in dsr." in *MobiQuitous*. IEEE Computer Society, 2005, pp. 247–260.

[11] L.Feeney and M.Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment," in *INFOCOM*, 2001, pp. 1548–1557.

[12] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *Commun. Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[13] H. Rifa-Pous and J. Herrera-Joancomarti, "Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol," in *Communication Networks and Services Research (CNSR)*. Los Alamitos, CA, USA: IEEE Computer Society, 2007, pp. 372–380.

[14] K. Sanzgiri, B. Dahilly, B.Ñ. Leviney, C. Shieldsz, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *International Conference on Network Protocols (ICNP)*, November 2002, pp. 78–87.

[15] S. Yi, P.Ñaldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *MobiHOC*, October 2001.