Integración Segura de MANETs, desplegadas en zonas de recursos limitados, a Redes de Infraestructura

Sergio H. Rocabado Moreno[1],Daniel Arias Figueroa[1], Ernesto Sánchez[1] Javier Díaz[2]
[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada (UNSa)
[2]L.IN.T.I. – Laboratorio de Investigación en Nuevas Tecnologías Informáticas (UNLP)
[1]srocabad@cidia.unsa.edu.ar, [1]daaf@cidia.unsa.edu.ar, [1]esanchez@cidia.unsa.edu.ar, [2]jdiaz@unlp.edu.ar

Resumen. Las características de las redes móviles ad hoc (MANET – Mobile Ad hoc NETwork) la convierten en una tecnología ideal, para ser utilizada en zonas remotas donde la cobertura de la red celular es limitada y la electricidad es un recurso escaso.
En este trabajo realizamos el estudio de un caso de integración de una MANET, desplegada en una zona remota y de recursos limitados, a una red de infraestructura. Se efectuaron pruebas de comunicación sobre canales "seguros" y "no seguros" con la finalidad de medir el consumo de recursos (ancho de banda y energía) en los nodos de la red ad hoc. Los resultados obtenidos permiten determinar el consumo adicional de recursos introducido por el uso de protocolos seguros.

Palabras Clave: MANET, Seguridad, Energía, IPSec, Bluetooth, GPRS.

1 Introducción

Una red móvil ad-hoc o MANET (del inglés Mobile Ad-hoc Networks) [4] es una colección de nodos inalámbricos móviles que se comunican de manera espontánea y autoorganizada constituyendo una red temporal sin la ayuda de ninguna infraestructura preestablecida (como puntos de acceso WiFi o torres de estaciones base celulares con antenas 2G, 3G o 4G) ni administración centralizada.

Una de las principales ventajas de una MANET es la posibilidad de integrarla a una red de infraestructura con diferentes fines, entre otros podemos mencionar el acceso a Internet y a sistemas de información de una organización desde un dispositivo móvil [11].

En este trabajo realizamos el estudio de un caso de integración de una MANET, desplegada en una zona remota y de recursos limitados, a la red de infraestructura de una organización (Intranet). Dicha integración se realizo a través de la red celular, considerando los siguientes inconvenientes y limitaciones:

- La energía en la zona de despliegue es escasa, lo que dificulta la capacidad de recarga de los dispositivos que forman parte de la MANET.

- Las redes celulares en zonas remotas no brindan servicios de tercera (3G) o cuarta generación (4G), solo se dispone de tecnología 2G (GSM/GPRS) que proporciona un ancho de banda limitado y variable.
- La mayor parte de los dispositivos móviles utilizados en zonas remotas son equipos baratos y de características básicas, que incorporan tecnologías como Bluetooth y 2G en lugar de WiFi y 3G.
- Las MANETs y las redes celulares utilizan un medio compartido (aire) para transmitir los datos y se encuentran expuestas a "ataques" o accesos no autorizados. Se requiere entonces la implementación de canales de comunicación "seguros" entre los nodos de la red ad hoc y los equipos de la red de infraestructura.
- La implementación de niveles de seguridad elevados implica un incremento del consumo de ancho de banda y de la energía en los nodos móviles [17]. Ambos recursos son limitados en zonas remotas, por lo que se hace necesario elegir un nivel de seguridad que no comprometa los recursos disponibles para el normal funcionamiento de la MANET.

En [10], articulo presentado en CACIC 2011, montamos un escenario de pruebas *indoor* sin considerar condiciones externas (distancia, interferencias, entre otros). Continuando con esta línea de investigación, esta vez trabajamos sobre un escenario *outdoor* afectado por factores externos, que disminuyen el rendimiento e incrementan el consumo de recursos en los nodos de la red ad hoc.

El escenario que utilizamos para realizar el estudio, conecta a la MANET remota con un servidor de la red de infraestructura a través de la red celular (GPRS). Sobre este realizamos pruebas extremo a extremo (nodo móvil a servidor), por canales de comunicación no seguros y seguros (IPSec), con la finalidad de determinar el consumo de ancho de banda y energía en los dispositivos móviles. Los resultados obtenidos permiten establecer el consumo adicional de recursos provocado por el uso de protocolos seguros.

2. Tecnologías de soporte para la formación de MANETs

Existen 4 estándares que permiten realizar comunicaciones inalámbricas de corto alcance que se pueden utilizar para la formación de redes móviles ad hoc: Bluetooth (IEEE 802.15.1), Ultra-wideband (UWB, IEEE 802.15.3), ZigBee (IEEE 802.15.4) y WiFi (IEEE 802.11).

Elegimos la tecnología Bluetooth para realizar el despliegue de MANETs, en zonas de recursos limitados, por las siguientes razones:

- Bluetooth utiliza un radio de corto alcance que ha sido optimizado para el ahorro de energía y operación adecuada de la batería [12].
- El consumo de energía de Bluetooth es inferior al de UWB y WiFi. En [14] se presenta un estudio comparativo entre diferentes tecnologías inalámbricas, entre

los resultados de este estudio se observa que el consumo de energía en mili watts de UWB y WiFi es hasta 4 veces superior al consumo de Bluetooth.

- Su bajo precio y reducido tamaño [13], posibilitan que la mayor parte de los dispositivos móviles que se consiguen en el mercado tengan incorporada la interfaz Bluetooth (WiFi y UWB encarecen el dispositivo).
- No se requieren componentes de infraestructura. Una red WiFi requiere la instalación y configuración de componentes (Ej: Puntos de acceso) que requieren energía para funcionar.
- Facilidad y rapidez de despliegue.

2.1 Bluetooth (IEEE 802.15.1)

Bluetooth es una tecnología [11] para radio enlaces diseñada para que una amplia variedad de periféricos y dispositivos móviles como netbooks, tablets, teléfonos celulares y PDAs (Personal Digital Assistants) puedan establecer comunicación e intercambiar información entre sí a través de enlaces de corto alcance (10 a 100mts).

Bluetooth fue diseñada para eliminar el uso de cables entre dispositivos, y luego se comenzó a utilizar para la creación de redes personales PAN (Personal Área Network). Una PAN es una red formada por una gran variedad de dispositivos que se comunican entre sí mediante cables o a través del medio inalámbrico a cortas distancias [12].

Posteriormente el estándar IEEE 802.15.1 [4] presenta una WPAN (Wíreless Personal Área Networks) que utiliza tecnología inalámbrica Bluetooth, y soporta dos tipos de topologías: *piconet* y *scatternet.*

La mas sencilla es la *piconet* que consiste en una WPAN formada por un dispositivo *Bluetooth* que actúa como maestro comunicado con hasta 7 dispositivos *Bluetooth* que actúan como esclavos, cualquier dispositivo puede ser maestro pero teniendo en cuenta que solo debe existir uno por *piconet.*

La *Scatternet* se forma a partir de de la superposición de varias *piconet,* un dispositivo puede ser esclavo de una *piconet* a la vez que es maestro de otra, o puede ser esclavo de varias *piconet.*

2.2 IP sobre Bluetooth

El perfil PAN (Personal Area Networking) [2] de bluetooth, proporciona el transporte de datagramas IPv4 mediante el protocolo BNEP (Bluetooth Network Encapsulation Protocol) [3].

El escenario de uso más habitual del protocolo BNEP es el denominado NAP (Network Access Point), en el cual uno de los dispositivos actúa como puente para conectar los nodos de una piconet a una red IP.

Para realizar transporte de datos IP el protocolo BNEP reemplaza la cabecera Ethernet (típica de las conexiones LAN cableadas) por su propia cabecera, de forma que la cabecera BNEP y el payload de Ethernet serán encapsulados en una PDU de L2CAP. En [10] se describe con detalle el proceso de encapsulamiento y el overhead introducido.

3. Tecnologías de soporte para la integración de MANETs a redes de infraestructura.

Existen 4 tecnologías que permiten integrar una MANET remota a una red de infraestructura, estas son: 2G (GSM), 2.5G (GPRS), 3G (UMTS, HSDPA y HSUPA) y 4G (LTE).

Los factores más importantes a considerar a la hora de elegir una de las tecnologías son: Cobertura en la zona de despliegue de la MANET, consumo de energía y velocidad de transmisión de datos.

En [15] y [16] se presentan estudios relacionados con el consumo de energía en diferentes tecnologías de celulares, los resultados muestran que GPRS consume entre un 40% y 70% menos energía comparado con UMTS.

La figura 1 ilustra el incremento de las velocidades de transferencia en las diferentes tecnologías, desde las redes GSM (9 kbit/s) hasta las redes 4G (1 Gbit/s). Note que las tecnologías HSDPA, HSUPA y LTE utilizan diferentes velocidades para el enlace descendente (DL - downlink) y para el ascendente (UL – uplink).

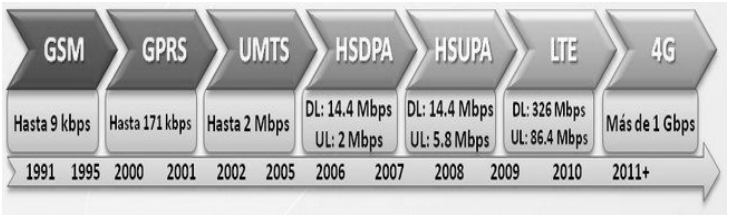

Figura 1. Velocidad de transferencia en las distintas tecnologías celulares.

Para integrar la MANET desplegada en zona remota elegimos la tecnología GPRS (en lugar de UMTS o HDPSA), fundamentamos esta elección en las siguientes razones:

- El consumo de energía es menor en los dispositivos móviles que utilizan GPRS, en comparación con los que utilizan UMTS o HDPSA – Esto se debe a lo siguiente:
  - El numero de estaciones base compatibles con los estándares UMTS/HDPSA es limitado en zonas alejadas, por este motivo los dispositivos móviles 3G deben conectarse a antenas situadas a grandes distancias y utilizan mayor potencia para transmitir los datos.
  - Las velocidades de transferencia alcanzables por los estándares 3G y 4G requieren de modulaciones más complejas, las cuales necesitan de muchos cálculos adicionales y obligan a un mayor uso de CPU a los dispositivos y, por lo tanto, a un mayor consumo de energía.
- Disponibilidad de la tecnología GSM/GPRS en zonas remotas - La tecnología 3G(UMTS o HSDPA) generalmente se encuentra en zonas con gran concentración de usuarios y su implementación en zonas alejadas implica un importante recambio tecnológico por parte de las compañías de celulares.

- La mayor parte de los dispositivos utilizados en zonas remotas solo soportan GSM/GPRS - Esto se debe a que el costo de un dispositivo 2G/3G es muy superior al de un dispositivo 2G, y su adquisición no se justifica en zonas alejadas donde solo se dispone de redes 2G y la tecnología 3G es muy limitada o directamente no existe.
- Velocidad de transferencia – Si bien la velocidad máxima de transferencia que soporta la red GPRS (hasta 171Kbit/s) es pequeña en comparación a UMTS, es suficiente para establecer una conexión con la red de infraestructura.

3.1 GPRS

GPRS (General Packet Radio Service) es una extensión de la tecnología GSM que permite aprovechar la infraestructura de GSM para brindar mejores servicios de transmisión de datos a las aplicaciones. A diferencia de GSM que utilizaba conmutación de circuitos, GPRS utiliza conmutación de paquetes para la transmisión de datos (packet-oriented).

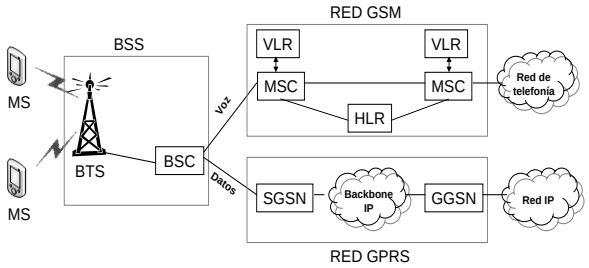

Figura 2. Arquitectura de una red GSM/GPRS [6].

En la figura 2 se ilustra la arquitectura de la red GSM/GPRS, la red GRPS es la encargada de gestionar las comunicaciones de datos y esta formada por los nodos SGSN y GGSN interconectados a través de un backbone IP. El SGSN (Serving GPRS Support Node) se encarga de la entrega de paquetes desde y hacia las estaciones móviles que se encuentran en su área de servicio. El GGSN (Gateway GPRS Support Node) interconecta el backbone de la red GPRS y las PDNs (Packet Data Networks) externas, actúa como un router entre la red GPRS y una red de datos externa (Internet, intranet, etc).

3.2 IP sobre GPRS

La red GPRS utiliza el protocolo GTP (GPRS Tunneling Protocol) para transportar los datagramas IP del usuario entre los nodos de soporte de GPRS (GSN), por debajo de él los protocolos estándares TCP o UDP se encargan de transportar los paquetes por la red (Figura 3). Resumiendo, en el Backbone del GPRS tenemos una

arquitectura de transporte: IP usuario – sobre GTP – sobre UDP/TCP- sobre IP backbone.

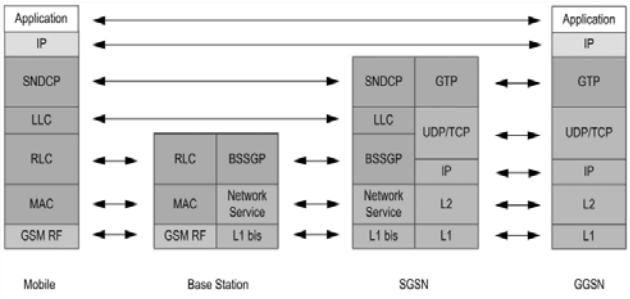

Figura 3. Modelo de capas de GPRS [6]

4. Escenario de pruebas

En la figura 4 se observa una representación gráfica del escenario montado para realizar las pruebas, en el mismo se interconecta una MANET a una INTRANET utilizando la red GSM/GPRS, los dispositivos móviles de la MANET acceden a la red GPRS a través de uno de los nodos que actúa como punto de acceso a la red GPRS (Gateway Bluetooth/GPRS).

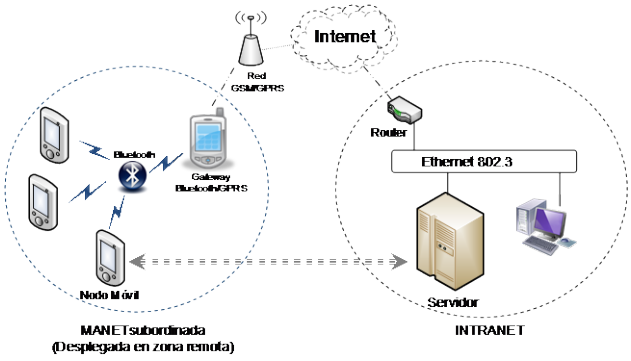

Figura 4. Escenario de pruebas

La conexión de los dispositivos móviles al punto de acceso a la red (NAP - Network Access Point) se realizó utilizando el perfil PAN (Personal Área Network) [12] del estándar Bluetooth [11].

El punto de acceso a la red se configuro sobre uno de los nodos de la MANET utilizando la aplicación "Android Wifi Tether" [19], esta aplicación utiliza el Framework netfilter e iptables [21] para implementar un puente entre la PAN bluetooth y la red GSM/GPRS.

El envío de un datagrama IP desde el nodo móvil hasta el servidor de la intranet, se realiza de la siguiente manera:

1 – El nodo móvil envía el datagrama IP, encapsulado en BNEP, al punto de acceso a la red (NAP).
2 – El NAP transmite el datagrama al SGSN de la red GPRS, desde donde viaja al GGSN encapsulado en GTP.
3 - El GGSN re-envía el datagrama a Internet, por donde viaja hasta llegar al router frontera de la red destino.
4 –El router frontera de la red destino encamina el datagrama hacia el servidor, encapsulado en una trama ethernet.

4.1 Equipamiento utilizado

En la tabla 1 se muestra la configuración de los dispositivo móviles que se utilizaron para realizar las pruebas.

	Nodo Gateway	Nodo móvil remoto
Marca y modelo	Motorola ATRIX	Motorola Milestone 2
SO	Android OS, v2.3 (Gingerbread)	Android OS, v2.2 (Froyo)
CPU	Dual-core 1 GHz Cortex-A9	1 GHz Cortex-A8
GPU	ULP GeForce	PowerVR SGX530
Chipset	Nvidia Tegra 2 AP20H	TI OMAP 3630
RAM	1 GByte	512 Mbytes
2G Network	GSM 850 / 900 / 1800 / 1900	GSM 850 / 900 / 1800 / 1900
Bluetooth	v 2.1	v 2.1
Batería	Lí-po (lithium polymer) 1930 mAh, 3.7 v.	Lí-po (lithium polymer) 1400 mAh, 3.7 v.

Tabla 1. Configuración de los dispositivos móviles ad hoc.

Los equipos fueron especialmente preparados para minimizar el consumo de batería, se procedió entonces a: desinstalar las aplicaciones no indispensables para su funcionamiento, deshabilitar el acceso a redes 3G y WiFi, activar el modo “solo 2G” para acceso a la red, deshabilitar dispositivos de hardware no utilizados en las pruebas y habilitar el modo de bajo consumo.

4.2 Pruebas y mediciones realizadas

Se realizaron transferencias de 1 Mbyte de datos (Carga útil o *Payload*) entre un nodo móvil de la MANET y el servidor de la red de infraestructura.

El tráfico de datos se generó utilizando el protocolo ICMP, primero sobre un canal no seguro y luego sobre un canal seguro, el aseguramiento del canal se implemento utilizando el protocolo IPSEC [7] en modo transporte (extremo a extremo), combinando los siguientes parámetros:

Servicios: AH autenticación [9], ESP autenticación y encriptación [8]
Intercambio de claves: Modo Agresivo – PSK.
Autenticación: HMAC-SHA-1 y HMAC-MD5.

Cifrado: DES, 3DES, AES.

Para una descripción mas amplia de los parámetros IPSEC utilizados, se puede consultar [10], donde realizamos pruebas similares sobre un escenario de menor complejidad.

Las mediciones de consumo de energía en el nodo móvil remoto se realizaron con la aplicación PowerTutor [19], esta herramienta permite estimar la energía consumida en tiempo real y por proceso utilizando el modelo de consumo de energía descrito en [18].

Debido a los factores aleatorios y al ancho de banda variable de la red GPRS [6], las pruebas se ejecutaron durante varios días consecutivos y en diferentes horarios, los resultados presentados en la siguiente sección se obtuvieron promediando los valores obtenidos.

5. Resultados

En la figura 5 presentamos un gráfico comparativo de consumo entre las diferentes pruebas realizadas, incluyendo un canal no seguro y un canal seguro configurado utilizando diferentes opciones de IPSec.

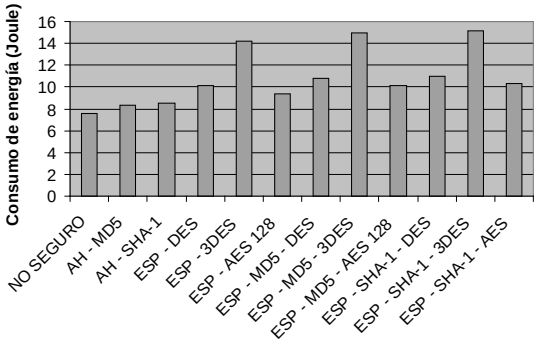

Fig. 5. Energía consumida para transferir 1 Mbyte de datos.

En la figura 6 se muestra la distribución de consumo energía para dos configuraciones IPSec que garantizan autenticación y confidencialidad.

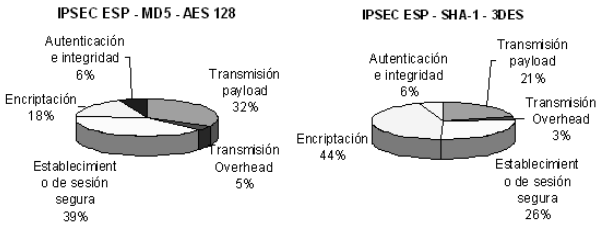

Fig. 6. Distribución del consumo de energía para ESP-MD5- AES y ESP–SHA-1-3DES

6. Conclusiones y trabajos futuros

La seguridad implica un consumo adicional de recursos que puede variar dependiendo de los algoritmos que se elijan para el establecimiento de un canal seguro, en el grafico comparativo de la figura 5 se visualiza que la opción que tiene el nivel mas elevado de seguridad (ESP – SHA-1 – 3DES) es la que mayor energía consume, duplicando el consumo de un canal no seguro. La elección de un nivel de seguridad en los nodos ad hoc dependerá de las posibilidades de recarga que existan en la zona de despliegue de la MANET.

Se observa que la diferencia de consumo que existe entre los algoritmos de autenticación es baja con respecto a la diferencia que existe entre los algoritmos de encriptación.

Se evidencian diferencias importantes en la distribución del consumo de energía al utilizar diferentes algoritmos de autenticación y encriptación.

Respecto a la energía consumida para el establecimiento de sesión segura IPsec, si bien el porcentaje en la distribución de consumo (figura 6) podría parecer importante, se debe tener en cuenta que este consumo se realiza una sola vez antes de comenzar la transmisión de la carga útil de datos.

Comparando los resultados obtenidos en el escenario *indoor* propuesto en [10] con los resultados del escenario *outdoor*, concluimos que en este último los nodos tienen un consumo mayor (entre un 20% y 30%) de energía.

Para continuar con esta línea de investigación tenemos previsto:

- Incorporar Bluetooth 3.0 en lugar de la versión 2.1.
- Realizar pruebas sobre canales seguros (IPSec) entre el Gateway Bluetooth/GPRS y el servidor de la red de infraestructura, en lugar de los canales extremo a extremo (nodo - servidor).
- Efectuar mediciones de otros parámetros en los nodos de la red ad hoc: Latencia, troughput, utilización de la CPU.
- Incorporar compresión al protocolo IPSEC.
- Realizar pruebas utilizando otros protocolos de seguridad (SSL, TLS).
- Utilizar herramientas de simulación para modelar el comportamiento aleatorio de la red GPRS.

Referencias

1. Bluetooth Special Interest Group: “Bluetooth Profiles Specification Version 1.1”, en Specification of the Bluetooth System, tomo 2, Febrero 2001.
2. Bluetooth Special Interest Group: “Personal Area Networking Profile”, Junio 2001.
3. Bluetooth Special Interest Group: “Bluetooth Network Encapsulation Protocol (BNEP) Especification”, Junio 2001.
4. IEEE 802.15 WPAN Task Group 1, http://www.ieee802.org/15/pub/TG1.html.
5. IETF MANET Active Work Group, http://tools.ietf.org/wg/manet.
6. ETSI EN 301 344, Digital cellular telecommunications system, General Packet Radio Service (GPRS), Service description, V7.4.1, 2000.

7. S. Kent. BBN Corp. R. Atkinson. Home Network: “Security Architecture for the Internet Protocol”, RFC 2401. Nov. 1998.
8. S. Kent. BBN Corp. R. Atkinson. Home Network: “IP Encapsulating Security Payload (ESP)”, Network Working Group. RFC 2406 Category: Standards Track. Nov. 1998.
9. S. Kent, R. Atkinson: "IP Authentication Header", RFC 2402. Nov. 1998.
10. Sergio H. Rocabado Moreno, Javier Díaz, Ernesto Sánchez y Daniel Arias Figueroa. Integración Segura de MANETs con Limitaciones de Energía a Redes de Infraestructura. CACIC 2011. La Plata, Nov. 2011.
11. Carlos de Morais Cordeiro and Dharma Prakash Agrawal. Integrating MANETs, WLANs, and Cellular Networks. En su: Ad Hoc and Sensor Networks - Theory and Applications. 2nd Ed. Singapore: World Scientific Publishing, 2011. pp. 587-620. ISBN: 978-9814338899.
12. Carlos de Morais Cordeiro and Dharma Prakash Agrawal. Wireless PANs. En su: Ad Hoc and Sensor Networks - Theory and Applications. 2nd Ed. Singapore: World Scientific Publishing, 2011. pp. 196-258. ISBN: 978-9814338899.
13. Per Johansson. “Bluetooth – an Enabler for Personal Area Networking”. Ericsson Research. IEEE Network, 2001.
14. Jin-Shyan Lee, Yu-Wei Su and Chung-Chou Shen. “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”. The 33rd Annual Conference of the IEEE Industrial Electronics Society, Nov. 2007. pp. 46-51.
15. Niranjan Balasubramanian, Aruna Balasubramanian and Arun Venkataramani. Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications. 9th ACM SIGCOMM conference on Internet measurement conference, Nov. 2009. pp. 280-293. ISBN: 978-1-60558-771-4.
16. Gian Paolo Perrucciy,Frank H.P. Fitzeky and Giovanni Sassoy. On the Impact of 2G and 3G Network Usage for Mobile Phones’ Battery Life. European Wireless 2009. pp. 255-259.
17. P. Ni, Z. Li: “Energy cost analysis of IPSec on handheld devices”, Elsevier (2004).
18. L. Zhang, B. Tiwana , Z. Qian: “Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones”, ACM, 2010.
19. “Wi-fi Tether”, página oficial: http://code.google.com/p/android-wifi-tether.
20. “PowerTutor", página oficial: http://powertutor.org.
21. The Netfilter Project, página oficial: http://www.netfilter.org.