Integración Segura de MANETs con Limitaciones de Energía a Redes de Infraestructura

Sergio H. Rocabado Moreno[1], Javier Díaz[2], Daniel Arias Figueroa[1], Ernesto Sánchez[1]
[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, [2]jdiaz@unlp.edu.ar, [1]daaf@cidia.unsa.edu.ar,
[1]esanchez@cidia.unsa.edu.ar

Resumen. La seguridad y el consumo de energía son factores importantes para el éxito de la integración de MANETs a redes de infraestructura. La "seguridad", porque las MANETs utilizan un medio compartido (aire) para transmitir los datos y se encuentran expuestas a posibles "ataques" y/o accesos no autorizados, y el consumo de energía porque algunos o todos los dispositivos móviles de la MANET son alimentados por baterías con energía limitada y por ello se hace necesario optimizar la conservación de energía.
En este trabajo realizamos el estudio de un caso de integración de una MANET a una red de infraestructura buscando un equilibrio entre seguridad y consumo de energía. Los resultados de las mediciones nos permiten determinar el consumo adicional de energía generado por el uso de protocolos seguros.

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

1 Introducción

Como sabemos, las redes inalámbricas existentes WLAN (Wi-Fi), WMAN(Wi-Max) y WWAN (GPRS/3G) requieren la presencia de determinados elementos fijos que controlan las comunicaciones entre los nodos de la red o delimitan el rango de cobertura asociado a la misma (estaciones base en redes de telefonía, puntos de acceso para Wi-fi o Wi-Max, etc). Las Redes Móviles Ad Hoc (o MANETs, del ingles Mobile Adhoc NETworks) son un tipo de redes inalámbricas llevadas al extremo: no es necesaria ninguna infraestructura previa para comunicarse a través de la red. Los equipos o nodos que forman parte de ella (Notebooks, PDAs, Celulares) se organizan por si mismos para ayudarse los unos a los otros en el proceso de transportar paquetes de datos entre un origen y un destino. Por tanto las MANET dan un paso más en cuanto a movilidad (todos los nodos de la red pueden ser móviles) y flexibilidad (no se requiere inversión en infraestructura, y además se minimiza la gestión de la red pues se auto-organiza ella misma).

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.

Las características intrínsecas de este tipo de redes (incluyendo autoconfiguración, ausencia de infraestructura, movilidad de los nodos, topología dinámica ancho de banda limitado, falta de seguridad, conservación de energía, entorno imprevisible, entre otras), plantean exigencias que deben resolverse antes de realizar la integración.

El presente trabajo se enfoca en los aspectos de seguridad y conservación de energía:

- Seguridad porque las redes móviles utilizan un medio compartido (aire) para transmitir los datos y se encuentran expuestas a "ataques" o accesos no autorizados, y por esta razón se hace necesario utilizar protocolos de seguridad que permitan una integración "segura" de los dispositivos móviles a la red de infraestructura, garantizando el cumplimiento de los siguientes aspectos de seguridad: Confidencialidad, integridad, autenticación, no repudio.

- Conservación de Energía porque los dispositivos móviles que conforman la MANET tienen capacidad limitada de energía y pocas posibilidades para recarga de baterías cuando se encuentran en itinerancia, por lo tanto se debe optimizar el consumo de energía.

Ambos aspectos son importantes y están directamente relacionados, se debe tener en cuenta que la implementación de un protocolo de seguridad implica un consumo de energía adicional por tres motivos: 1) se incrementa el uso de CPU y memoria para realizar cálculos, 2) se generan encabezados adicionales (overhead) que deben ser transmitidos y 3) se intercambian mensajes para el establecimiento de un canal seguro.

Por otro parte, la implementación de niveles de seguridad elevados implica un aumento en el consumo de energía en los nodos móviles y reduce drásticamente el tiempo de vida de la red, por esta razón se hace necesario establecer un compromiso entre seguridad y consumo de energía.

En este contexto nos propusimos estudiar el funcionamiento de protocolos de seguridad sobre un escenario de pruebas y analizar el impacto, de cada una de sus funcionalidades, en el consumo de energía de los nodos móviles

El escenario de pruebas que utilizamos integra una MANET a una LAN (infraestructura), sobre el mismo realizamos pruebas extremo a extremo (nodo móvil a nodo fijo) para determinar el consumo adicional de energía provocado por la segurización del canal de comunicaciones.

2. TCP/IP sobre bluetooth

Con el fin de garantizar la interoperatividad entre los dispositivos Bluetooth de distintos fabricantes, la especificación Bluetooth define un conjunto de perfiles. Cada uno de los perfiles definidos en [1] representa un posible escenario de uso en el que dos o más dispositivos dotados con tecnología Bluetooth deben interactuar para proporcionar al usuario un determinado Servicio.

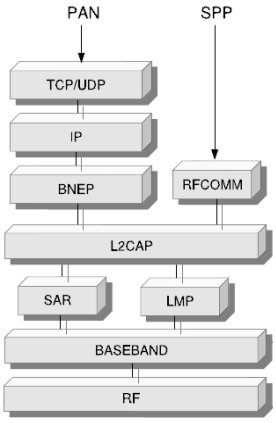

Fig. 1. Arquitectura de protocolos Bluetooth.

En la figura 1 se muestran los dos perfiles para transporte de datos: El perfil SPP (Serial Port Profile) permite emular una comunicación serial RS232 y utiliza para ello el protocolo RFCOMM, el perfil PAN (Personal Area Networking) [2] permite el transporte de datos TCP/IP sobre L2CAP utilizando el protocolo BNEP (Bluetooth Network Encapsulation Protocol) [3].

BNEP proporciona 3 tipos de escenarios PAN: PANU, GN y NAP.

- PANU (Personal Area Network User). En este escenario se realiza una conexión punto a punto entre dos nodos.
- GN (Group Ad Hoc Network). Permite a dispositivos Bluetooth crear, de forma cooperativa, redes inalámbricas ad hoc prescindiendo del uso de hardware o infraestructura adicional de interconexión de red.
- NAP (Network Address Protocol). Un punto de acceso a red es una unidad que integra una o más radios Bluetooth y que actúa como un bridge, proxy o router entre una red Bluetooth y otra red de diferente tecnología (10BASE-T, GSM, etc).

2.1 Overhead Bluetooth

Para realizar transporte de datos TCP/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 datos de L2CAP (figura 2). A la información transportada por la trama Ethernet se añadirían un total de 15 bytes correspondientes a la cabecera BNEP y se reservan 176 para una posible cabecera extendida.

Cabe señalar que el protocolo BNEP no ha de realizar fragmentación de las tramas que entrega al nivel L2CAP para su transmisión, debido a que la especificación [3]:

- Fija el valor mínimo de la MTU de L2CAP para BNEP en 1691 bytes, según la expresión siguiente:

Payload (1500 bytes)+ cabecera BNEP (15 bytes) + posible cabecera extendida (176 bytes) = 1691 bytes

- Establece que el máximo payload que aceptará BNEP del nivel superior tiene que ser igual al valor de la MTU de L2CAP (valor mínimo: 1691), menos 191 bytes reservados para cabeceras BNEP (Figura 2).

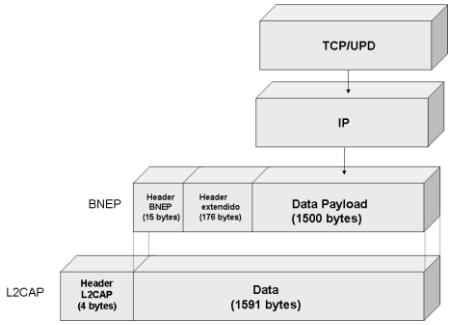

Fig. 2. TCP/IP sobre Bluetooth.

El objetivo, tal y como se aclara en [3], es que los 1691 octetos, sumados a los 4 bytes de cabecera de L2CAP, puedan transportarse en cinco paquetes DH5 de 339 bytes cada uno.

3 IPSec

IPSec [4] es un estándar desarrollado por IETF para proveer extensiones de seguridad en el nivel de red del protocolo TCP/IP. IPSec permite definir un canal seguro entre el origen y el destino utilizando una asociación de seguridad (SA), sobre este canal se habilita el envió y recepción de paquetes (TCP, UDP, ICMP, entre otros) protegidos criptográficamente y sin necesidad de realizar ningún cambio en las aplicaciones.

IPSEC soporta dos tipos de servicios criptográficos:

1. ESP (Encapsulated Security Payload) [5]
2. AH (Authentication Header) [6].

ESP provee confidencialidad, autenticidad e integridad sobre los datos, en cambio AH solo garantiza la autenticidad e integridad.

El establecimiento de una conexión IPSec requiere dos fases: Fase 1 (ISAKMP SA) [7] y Fase 2 (IPSec SA) [8], ver tabla 1.

La fase 1 realiza una autenticación mutua entre las entidades que desean establecer un canal seguro y genera las claves de encriptación para la fase 2. Esta fase tiene 2 modos: Principal y Agresivo, la diferencia entre ambos está dada por la cantidad de mensajes que intercambian (tabla 1) y en la protección de la identidad del cliente que no está contemplada en el modo agresivo.

Tabla 1. Fases para el establecimiento de una conexión IPSec.

Fase	Intercambio de claves	Mensajes intercambiados
Fase 1	Modo principal	6
	Modo agresivo	3
Fase 2	Modo rápido	3

La fase 2 negocia el algoritmo de cifrado y autenticación para proteger futuras transacciones, tiene un solo modo: Rápido.

IPSEC utiliza Diffie Hellman (D-H) para el intercambio de claves y dispone de tres mecanismos de autenticación: 1) PSK (Pre-Shared Key), 2) Firma digital y 3) Clave pública.

Un código de autenticación MAC (Message autentication Code) es utilizado para autenticar los mensajes intercambiados después del establecimiento de la conexión, para generarlo se requiere la implementación de HMAC-SHA-1 [9] o HMAC-MD5 [10].

IPSEC soporta dos modos de conexión: 1. Modo túnel, normalmente utilizado para establecer canales seguros entre dos Gateways de comunicación y 2. Modo transporte, utilizado para establecer canales seguros extremo a extremo entre dos hosts.

Para garantizar la confidencialidad IPSEC permite configurar diferentes algoritmos de encriptación, en este trabajo utilizamos: AES, DES y 3DES. IPSec primero encripta los datos y luego crea el MAC para los datos encriptados, de forma que si una modificación ocurre durante la transacción, se detectara el fallo con solo verificar la MAC y sin necesidad de realizar el proceso de desencriptado [11].

IPSec implementa compresión a través de un protocolo llamado IPCOMP [12], soportando los siguientes algoritmos de compresión: DEFLATE, LZS y LZJH.

Elegimos IPSec para realizar las pruebas, sobre otros protocolos y arquitecturas de seguridad, por dos motivos:

- Es una arquitectura de seguridad que contempla gran parte de los mecanismos de seguridad ofrecidos por los diferentes protocolos y arquitecturas
- Es la arquitectura de seguridad que se utilizará en la próxima generación de redes IP, al encontrarse incluida en la versión 6 del protocolo IP (IPv6)

3.1 Overhead de IPSec

En la figura 3 se observan los encabezados agregados a un datagrama IP por los diferentes servicios de seguridad del protocolo IPSec en modo transporte:

- Orig IP hdr - Encabezado IP (20 bytes)
- TCP hdr- Encabezado TCP (20 bytes)
- AH hdr - Encabezado AH (24 bytes)
- ESP hdr + ESP trl - Encabezados ESP en modo confidencialidad (10 bytes)
- ESP hdr + ESP trl + ESP auth - Encabezados ESP en modo confidencialidad y autenticación (22 bytes)

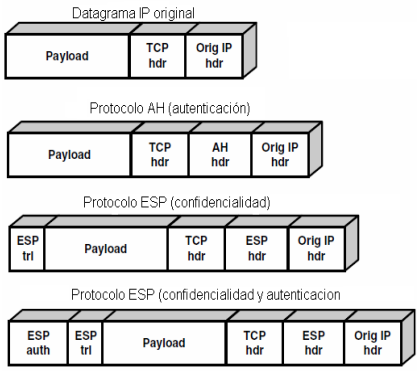

Fig. 3. Overhead de IPSec AH y ESP en modo transporte.

Un estudio detallado sobre la conformación de los campos que generan el overhead de IPSEC se puede encontrar en [13].

4. Pruebas realizadas

En la figura 4 se observa el escenario montado para realizar las pruebas, en el mismo se interconectan una MANET y una LAN, un dispositivo móvil de la MANET se comunica con el servidor de la red de infraestructura a través de un nodo que actúa como punto de acceso a la red de infraestructura (Gateway 802.15/802.3).

La conexión del nodo móvil al NAP (Network Access Point) se realizó utilizando el perfil PAN (Personal Area Network) [2] del estándar Bluetooth [1].

El punto de acceso a la red se implementó utilizando las características de enrutamiento de Linux y habilitando la pila de protocolos BlueZ [15], esta configuración fue posible gracias a que la habilitación de BNEP [3] en BlueZ da de alta en el sistema una interfaz virtual de red que se integra en el sistema de red de Linux. Elegimos BlueZ como pila Bluetooth, por ser una implementación gratuita y completa que ha sido adoptada por defecto e incorporada en el Kernel de Linux desde la versión 2.4.20.

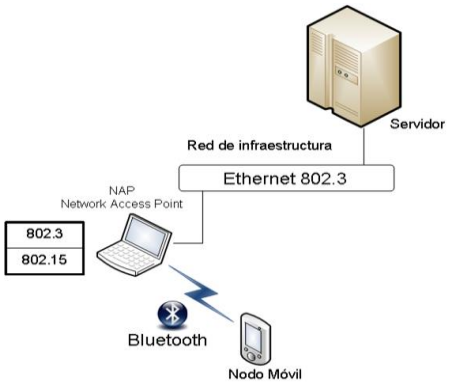

Fig. 4. Escenario de pruebas.

El tráfico de datos entre el nodo móvil y el servidor 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 en modo transporte (extremo a extremo), combinando los siguientes parámetros:

Servicios: AH autenticación, ESP autenticación, ESP autenticación y encriptación.
Intercambio de claves: Modo Agresivo – PSK.
Autenticación: HMAC-SHA-1 y HMAC-MD5.
Cifrado: DES, 3DES, AES.

La configuración del dispositivo móvil con el cual se realizaron las pruebas, es la siguiente:

Equipo:	Motorola MILESTONE 2
CPU:	1 GHz Cortex-A8
GPU:	PowerVR SGX530
Chipset:	TI OMAP3630
RAM:	512MB RAM.
SO:	Android OS, v2.2 (Froyo) en modo super usuario.
Bateria:	Lítio-íon, 1390 mAh, 3.7 v.

Este equipo fue especialmente preparado para minimizar el consumo de bateria, se procedió entonces a: desinstalar las aplicaciones no indispensables para su funcionamiento, deshabilitar dispositivos de hardware no utilizados en las pruebas y habilitar el modo de bajo consumo.

4.1 Medición del consumo de energía

Las mediciones de consumo de energía en el smartphone se realizaron con la aplicación PowerTutor [16], esta herramienta permite estimar la energía consumida en tiempo real y por proceso utilizando el modelo de consumo de energía descrito en [17]. Las pruebas se ejecutaron a distintos niveles de carga de batería (100%, 75%,50% y 25%) y los resultados presentados en este trabajo se obtuvieron promediando los valores obtenidos en las pruebas.

Para determinar la energía consumida sobre un canal “no seguro”, medimos la energía utilizada para la transmisión de: el overhead bluetooth (inciso 2.1), el overhead IP e ICMP y la carga útil de datos (Payload). A partir de estas mediciones obtuvimos el consumo de energía por byte (µjoule/byte)

En el caso del canal seguro dividimos las mediciones en 3 partes:

- Energía consumida por el uso de CPU para la encriptación y autenticación de datos. Se implemento y ejecuto cada algoritmo en el smartphone utilizando texto plano elegido y sin realizar la transmisión de los datos. Métrica: µjoule por byte procesado.

- Energía consumida por la transmisión de: el overhead de bluetooth (inciso 2.1), el overhead de IPSec (inciso 3.1), el overhead IP e ICMP y la carga útil de datos (Payload). Métrica: μjoule por byte transmitido.

- Energía consumida durante el establecimiento de un canal seguro, incluye el intercambio de mensajes fase1 y fase 2 en modo agresivo de IPSEC (ver Tabla 1), este es un valor fijo que no depende de la cantidad de bytes procesados ni transmitidos.

5. Resultados

A continuación se presentan los resultados obtenidos en tres tablas que resumen cada aspecto estudiado:

Tabla 2. Energía consumida por los algoritmos de autenticación.

Algoritmo	Energía consumida (μJ/Byte)
MD5	0,62
SHA-1	0,81

Tabla 3. Energía consumida por los algoritmos de encriptación.

Algoritmo	Energía consumida (μJ/Byte)
DES	2,38
3DES	6,34
AES-128	1,71

Tabla 4. Energía consumida por el establecimiento de una sesión segura IPSec.

Algoritmo	Energía consumida (Joules)
Modo principal PSK	3,017
Modo agresivo PSK	2,815

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. Se observa 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.

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

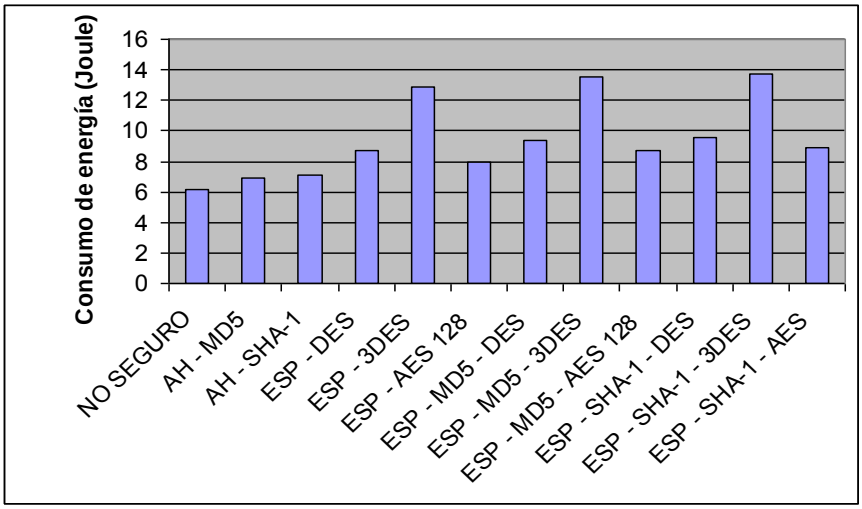

Fig. 5. Energía consumida para transferir 1 Mbyte de datos.

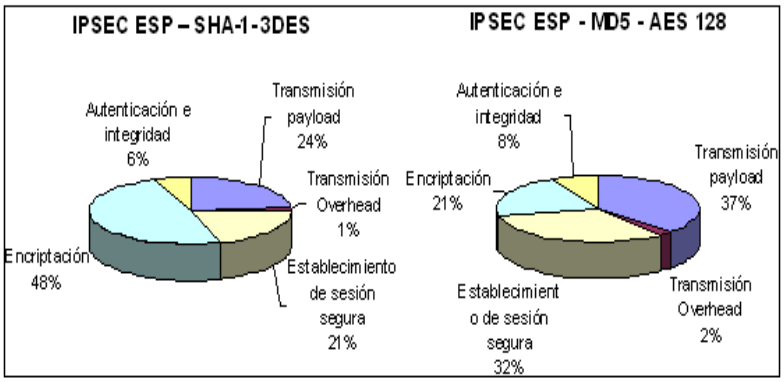

Fig. 6. Distribución del consumo de energía para ESP–SHA-1-3DES y ESP-MD5- AES

6. Conclusiones y trabajos futuros

La seguridad implica un consumo adicional de energía que puede variar dependiendo de los algoritmos que se elijan para el establecimiento de un canal seguro, la configuración de un nivel de seguridad para el dispositivo móvil dependerá de las posibilidades de recarga que existan cuando el dispositivo se encuentre en itinerancia.

Los resultados obtenidos en nuestros experimentos muestran 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.

Observamos el uso de 3DES como algoritmo de cifrado tiene un alto impacto en el consumo de energía, si reemplazamos 3DES por AES el consumo de energía se puede reducir casi en un 30%,

Por otro lado, en el caso de los algoritmos de autenticación e integridad observamos que la diferencia de consumo entre SHA-1 y MD5 es muy baja y no impacta de manera significativa en el consumo de energía.

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 la diferencia entre el modo principal y agresivo podría parecer importante (casi 10%), se debe tener en cuenta que este consumo se realiza una sola vez antes de comenzar la transmisión de la carga útil de datos.

Para continuar con esta línea de investigación tenemos previsto:

- Incorporar compresión al protocolo IPSEC.
- Realizar pruebas utilizando otros protocolos de seguridad (SSL, TLS)
- Realizar pruebas de campo fuera de laboratorio, en escenarios afectados por condiciones externas (distancia, interferencias, entre otras).
- Utilizar la red celular (GPRS) para la integración segura de MANETs a redes de infraestructura.

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. S. Kent. BBN Corp. R. Atkinson. Home Network: “Security Architecture for the Internet Protocol”, RFC 2401 (Nov. 1998).
5. S. Kent. BBN Corp. R. Atkinson. Home Network: “IP Encapsulating Security Payload (ESP)”, Network Working Group. RFC 2406 Category: Standards Track (Nov. 1998).
6. S. Kent, R. Atkinson: "IP Authentication Header", RFC 2402 (Nov. 1998).
7. D. Maughan, Schertler M., Schneider J. Turner: "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408 (Nov 1998).
8. D. Harkins, D. Carrel: "The Internet Key Exchange (IKE)", RFC 2409 (Nov 1998).
9. C. Madson, R. Glenn: "The Use of HMAC-SHA-96 within ESP and AH", RFC 2404 (Nov.1998).
10. C. Madson, R. Glenn: "The Use of HMAC-MD5-1-96 within ESP and AH", RFC 2403 (Nov. 1998).
11. Sheila Franke: “Demystifying the IPSec Puzzle”, Artech House Computer (2001).
12. A. Shacham, B. Monsour, R. Pereira, M. Thomas: “IP Payload Compression Protocol IPCOMP”, RFC 2393 (Dec 1998).
13. C. Xenakis, N. Laoutaris, L. Merakos, Ioannis Stavrakakis, “A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms” (2006).
14. P. Ni, Z. Li: “Energy cost analysis of IPSec on handheld devices”, Elsevier (2004).
15. “BlueZ”, página oficial del proyecto: http://www.bluez.org.
16. “PowerTutor", página oficial: http://powertutor.org.
17. L. Zhang, B. Tiwana , Z. Qian: “Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones”, ACM, (2010).