Internet of Things

Javier Romero Schmidt

javier.romeros@alumnos.usm.cl

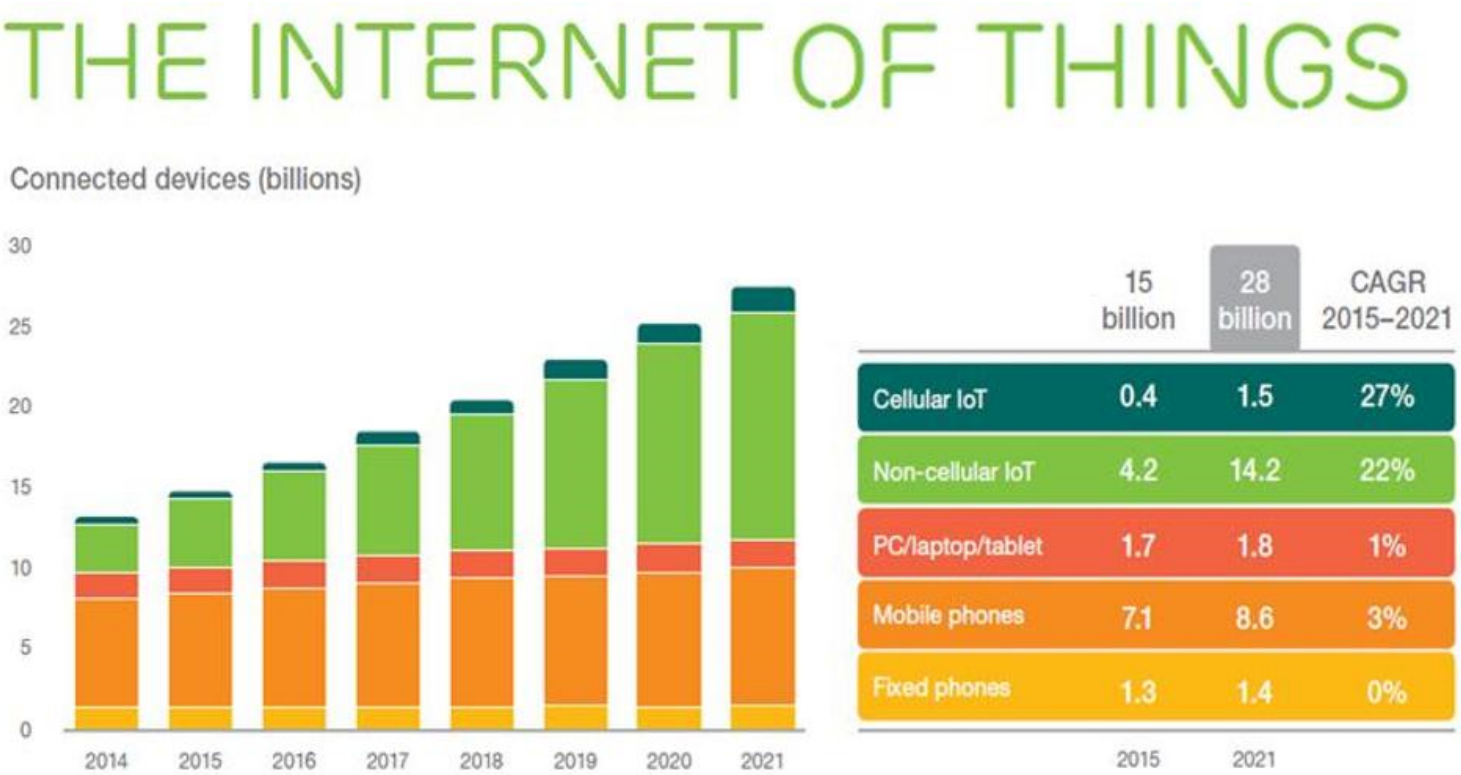
Departamento de Electrónica
Universidad Técnica Federico Santa María

16 de noviembre de 2016

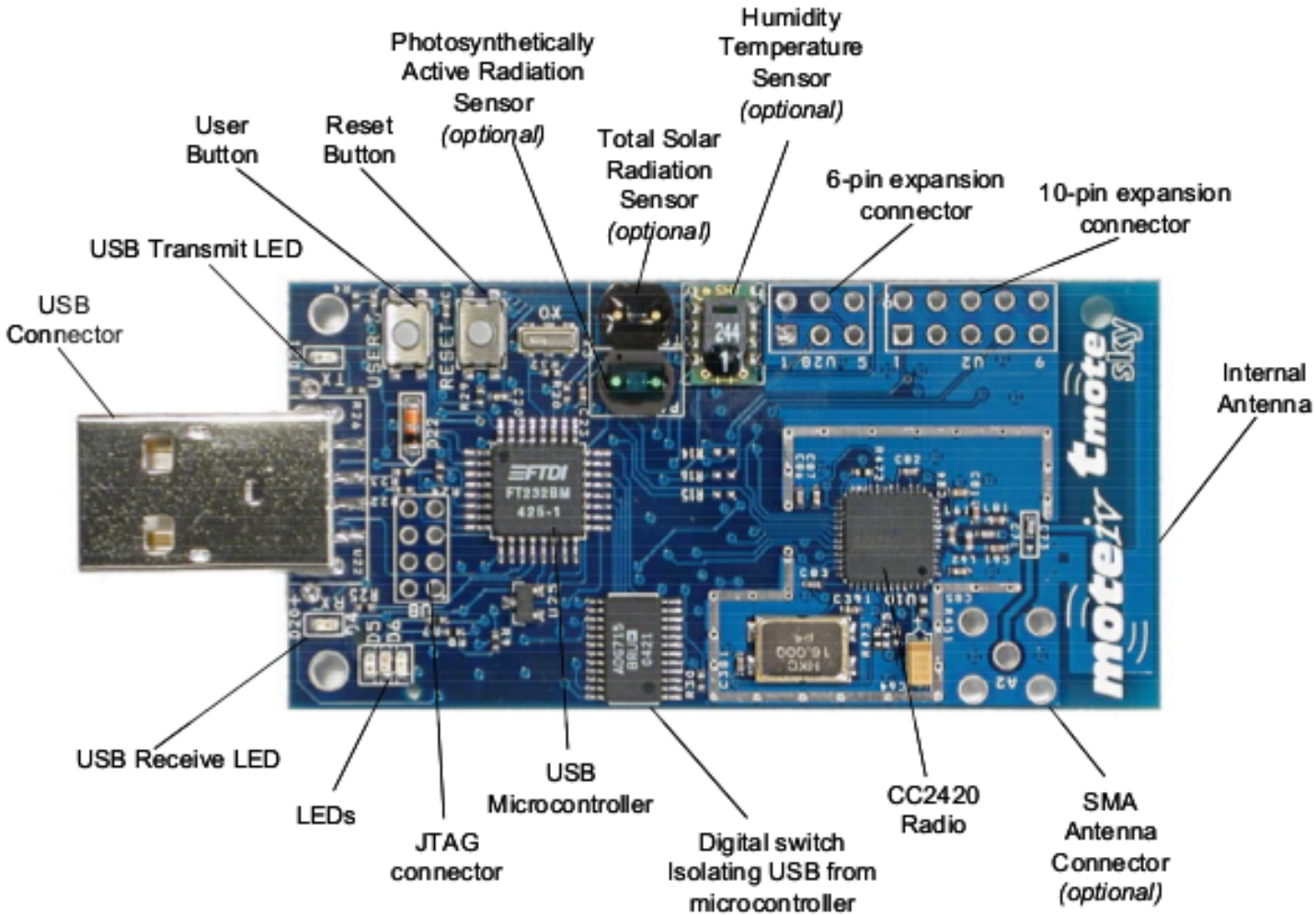
Tabla de Contenidos

Internet de las Cosas

Problema


THE INTERNET OF THINGS
Connected devices (billions)
30
25
20
15
10
5
0
2014
2015
2016
2017
2018
2019
2020
2021
15 billion
28 billion
CAGR 2015–2021
Cellular IoT 0.4 1.5 27%
Non-cellular IoT 4.2 14.2 22%
PC/laptop/tablet 1.7 1.8 1%
Mobile phones 7.1 8.6 3%
Fixed phones 1.3 1.4 0%
2015
2021

Problema


Photosynthetically Active Radiation Sensor (optional)
Humidity Temperature Sensor (optional)
User Button
Reset Button
Total Solar Radiation Sensor (optional)
6-pin expansion connector
10-pin expansion connector
USB Transmit LED
USB Connector
Internal Antenna
USB Receive LED
LEDs
JTAG connector
USB Microcontroller
Digital switch Isolating USB from microcontroller
CC2420 Radio
SMA Antenna Connector (optional)

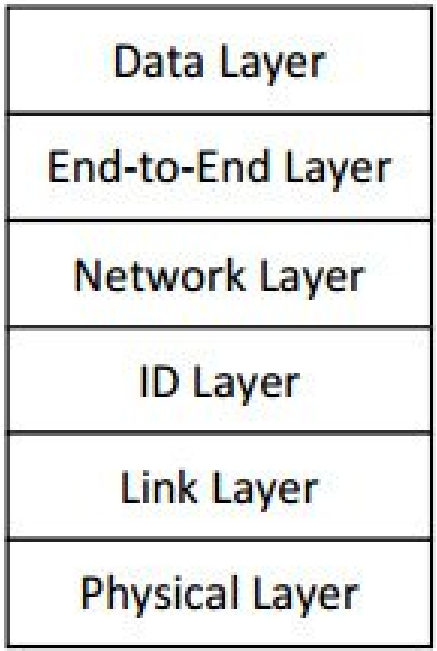
Necesidad

- Protocolo estándar de comunicación Ligero
- Que permita implementar seguridad
- Capacidad de configurar redes de gran cantidad de dispositivos

Protocolos de Comunicación

En la actualidad existen diversos protocolos destinados a IoT para las distintas capas de comunicación. Para la capa de aplicación existen protocolos como MQTT o CoAP.

Otros muy comunes son 6LoWPAN y RPL para capa de transporte.



Símil de modelo OSI para IoT

CoAP - Constrained Application Protocol

Definido en estándar IETF [RFC 7252][1], el cual tiene las siguientes características:

- Facilmente traducible a HTTP para integración con la Web
- Capacidad de multidifusión de mensajes
- Cabecera Pequeña
- Baja complejidad de análisis sintáctico
- Soporte de URI

Estructura de Paquete y Métodos

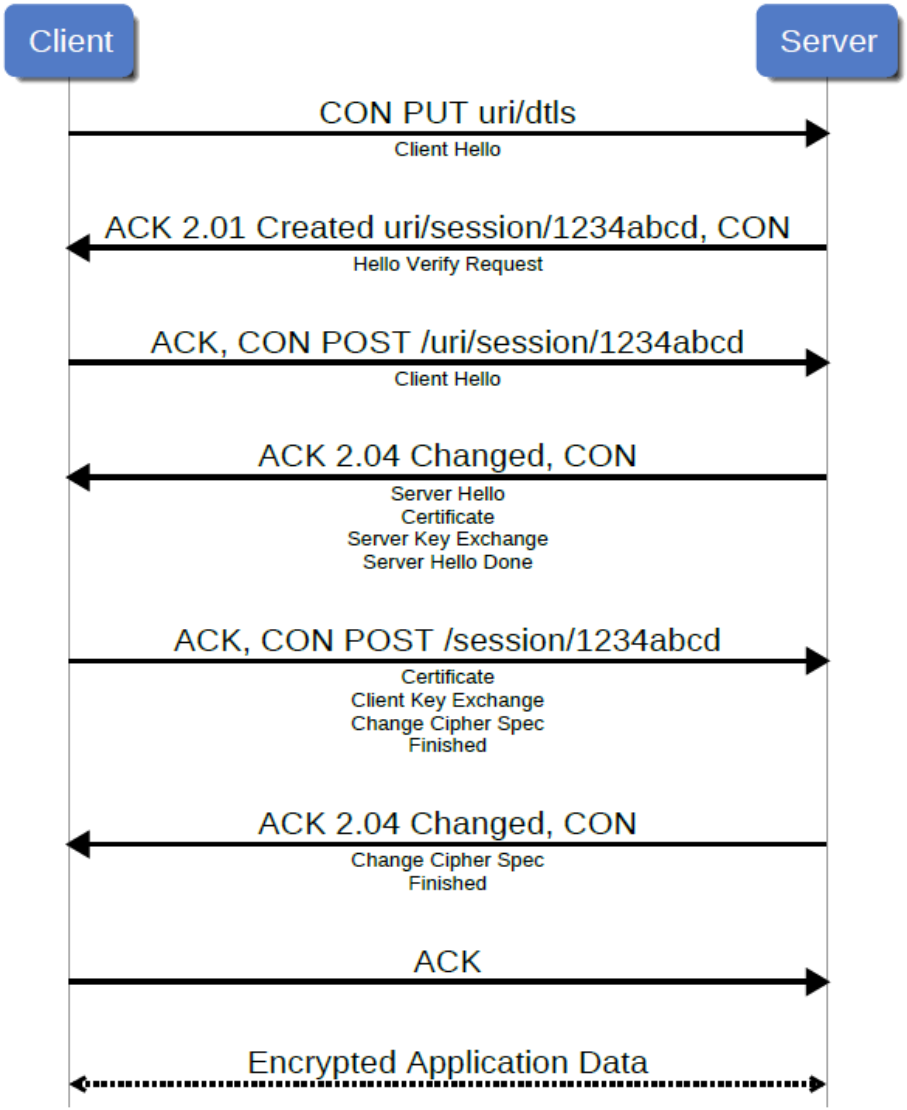
Ver	T	TKL	Code	Message ID
Token (if any, TKL bytes) ...				
Options (if any) ...				
1 1	1 1	1 1 1 1	Payload (if any) ...	

Tiene la capacidad de emplear métodos como GET, POST, PUT y DELETE. Además de tener un funcionamiento similar a HTTP, y aunque esté basado en UDP ocupa ACKs para emular TCP.

¿Pero se puede implentar seguridad en CoAP?

Es fundamental ofrecer seguridad en la comunicación de dispositivos de capacidades restringidas, esto es tener Confidencialidad, Integridad del mensaje y Autenticación.

La mayoría de autores proponen el uso de DTLS (Datagram Transport Layer Security), protocolo de capa de transporte sobre UDP para comunicación segura.[2][3][4]



La solución propuesta por Capossele et. al permite establecer una conexión segura sobre CoAP, la cual además permite utilizar menor cantidad de recursos que una solución DTLS estándar.

Protocol	ROM	RAM
CoAP + Blip	51410 B	6653 B
standard DTLS	10983 B	7380 B
DTLS over CoAP	8936 B	7144 B

Así con CoAP usando el protocolo DTLS para proveer seguridad se puede elegir entre:

- *NoSec*: Sin seguridad
- *RawPublicKey*: Seguridad con Clave Pública Cruda
- *PreSharedKey*: Seguridad con Clave Pre Compartida

Teniendo así URIs del tipo **coap://** y **coaps://** similar a HTTP seguro.

Contiki e Instant Contiki

Contiki[5] es un sistema operativo de código abierto diseñado para IoT. Tiene la capacidad de conectar a Internet dispositivos pequeños de bajo costo y poder, soportando diversos estándares de Internet.

Mientras que Instant Contiki, actualmente en su version 3.0, es un SO basado en Ubuntu. Diseñado para configurar y simular redes de IoT de manera más fácil.

Cooja

Cooja es una herramienta incluida en Instant Contiki que permite simular redes IoT con motes reales. En esta se pueden implementar todas las características del SO Contiki, ayudando a desarrolladores a probar sus códigos antes de implementar en Hardware real.

Referencias I

[1] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," Internet Requests for Comments, RFC Editor, RFC 7252, June 2014, http://www.rfc-editor.org/rfc/rfc7252.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7252.txt

[2] A. Capossele, V. Cervo, G. De Cicco, and C. Petrioli, "Security as a coap resource: an optimized dtls implementation for the iot," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 549–554.

[3] J. Park and N. Kang, "Lightweight secure communication for coap-enabled internet of things using delegated dtls handshake," in *2014 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2014, pp. 28–33.

Referencias II

[4] R. A. Rahman and B. Shah, "Security analysis of iot protocols: A focus in coap," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*. IEEE, 2016, pp. 1–7.

[5] "Contiki: The Open Source OS for the Internet of Things." [Online]. Available: http://contiki-os.org/

¡Gracias por su Atención!