UNIVERSITE DE RENNES 1

Zigbee
IEEE 802.15.4

Bernard Cousin

Zigbee présentation

- C'est quoi ?
  - Un ensemble de protocoles de communications de haut niveau
    - Utilisant des transmission radio à faible consommation,
    - Pour une transmission de données à faible débit (250 Kbit/s)
    - Sur une faible étendue (WPAN)

    => basé sur la norme IEEE 802.15.4 ("Low-Rate Wireless Personal Area Network (LR-WPAN) standard")
- Ca sert à quoi
  - Pour rendre un service de contrôle à distance …d'un équipement électrique… ou autre.

Plan

- Présentation de Zigbee
- Zigbee et les autres
- Domaines d'application de Zigbee
- Fonctionnement de Zigbee

Bibliographie

- Protocols and architectures for wireless sensor networks.
  by H. Karl, A. Willig. Wiley, 2005.
- ZigBee Resource Guide
  A Webcom Publication, 2011
- ZigBee Wireless Networking
  by Drew Gislason. Newnes Publications, 2008
- ZigBee Wireless Networks and Transceivers
  by Shahin Farahani. Newnes Publications, 2008
- Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4
  by Jose A. Gutierrez, Edgar H. Callaway, and Raymond L. Barrett. IEEE Press, 2003
- Wireless Sensor Networks: Architectures and Protocols
  by Edgar H. Callaway. CRC Press 2004.

Présentation de Zigbee

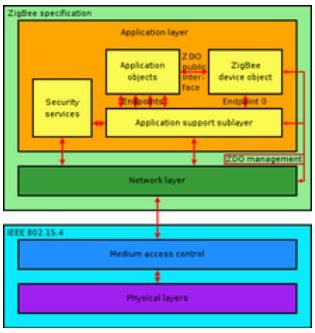
- Zigbee :
  - Proposé en 1998
  - Normalisé en mai 2003, puis 2006
  - À bas coût : 1$
    - Diffusion large
  - À basse consommation
    - Longue durée de vie
  - Communication dans un réseau
    - Augmentation de l'étendue

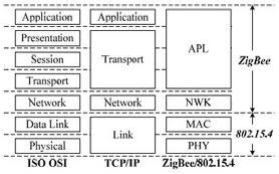
Caractéristiques de ZigBee

- Low data throughput: 250 Kbit/s
- Protocol stack: 32 KBytes
- Number of nodes: 2^{64}
- Range: 1 – 100 m
- Topologie :
  - Étoile, arborescente, maillée
- Bande fréquentielle : "ISM band"
  - Europe 868 MHz; USA + Australie : 915 MHz; Monde : 2.4 GHz
- Délai de réveil : 30 ms (Bluetooth : 3 s)

Architecture Zigbee

- Basé sur IEEE 802.15.4
  - Couche Physique
  - Couche MAC
- Composants de Zigbee:
  - Network layer
  - Application support layer (APS)
  - Zigbee device object (ZDO)
  - Application's manufacturer objects
- ZDO :
  - Gestion de l'équipement
  - Gestion du réseau
  - Decouverte
  - Sécurité





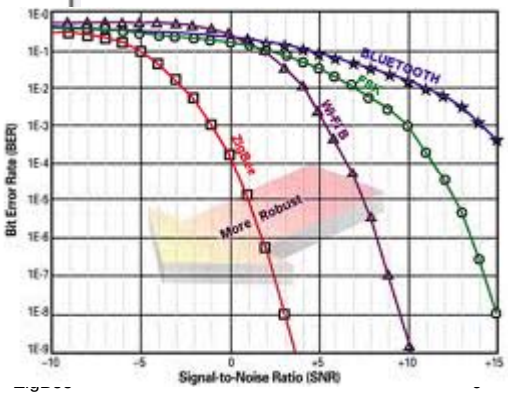
Zigbee Pro

- In 2007, ZigBee Pro
  - multicasting,
  - many-to-one routing,
  - high security with Symmetric-Key Key Exchange (SKKE)

Comparaison Zigbee et les autres

- Débit / Etendue

- SNR / BER



ZigBee versus Bluetooth or Wifi

	Protocole ZigBee	Bluetooth	Wifi
IEEE	802.15.4	802.15.1	802.11a/b/g
Besoin mémoire	4-32 Kb	250 Kb	1 Mb+
Autonomie avec pile	Années	Jours	Heures
Nombre de nœuds	65 000+	7	32
Vitesse de transfert	250 Kb/s	1 Mb/s	11-54-108 Mb/s
Portéé	100m	10-100m	300m

Brand Name	Wi-Fi [IEEE802.15.11b]	Bluetooth	ZigBee [IEEE802.15.4]
Battery Life	Several hours	Several days	Several years
Maximum Network Capacity	32nodes	7nodes	64000nodes
Communication Distance	100m	10m	>30m
Communication Speed	11Mbps	1Mbps	250Kbps
Security Method	SSID	64bit, 128bit	32,64,128 bit AES
Applications	Wireless LAN	Wireless speech	Remote control Measurement, Control

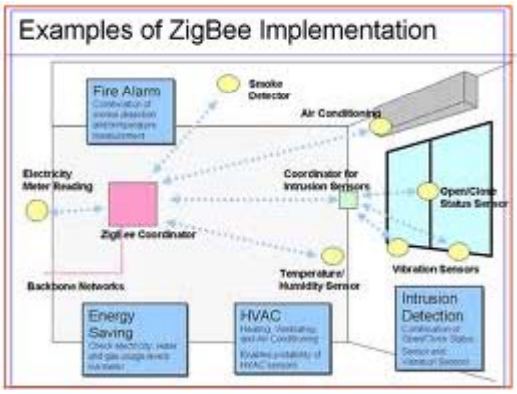
10

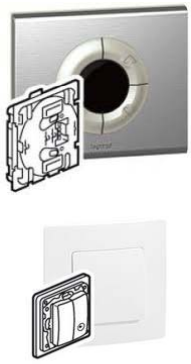
Domaines d'application

- ZigBee Home Automation
- ZigBee Smart Energy 1.0 => 2.0
- ZigBee Telecommunication Services
- ZigBee Health Care
- ZigBee RF4CE (Radio Frequency for Consumer Electronics)- Remote Control
- ZigBee Building Automation
- ZigBee Retail Services
- Zigbee Input Devices
- Zigbee 3D Sync

Domaines d'application

Un domaine d'application





"Zigbee Smart Energy"

- Un exemple d'application : Zigbee Smart Energy"
  - "IP-based protocol"
- Ses fonctionnalités :
  - Contrôle et notification de l'utilisation de l'énergie et de l'eau
  - Téléchargement de la configuration et du "firmware"
  - Services pré-payés
  - Information de l'usager et système de messagerie
  - Contrôle du système de rechargement des batteries des véhicules électriques
  - Gestion des profils (d'usager, applicatif, etc.)

Les types d'équipement ZigBee

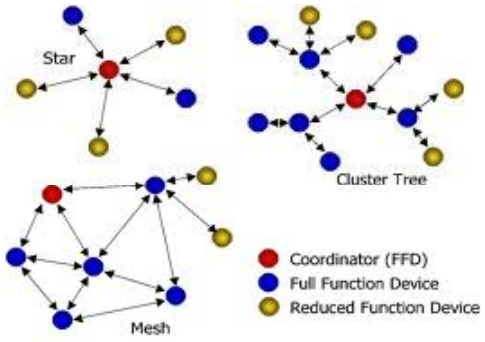
- Le coordinateur ZigBee (ZC) :
  - Un et un seul
  - Tiers de confiance
  - Racine du réseau et passerelle vers les autres réseaux
  - Alimentation permanente
- Le routeur ZigBee (ZR) :
  - Equipement intermédiaire
  - Qui route les paquets au sein du réseau
  - Alimentation permanente
- L'équipement terminal Zigbee (ZED)
  - Ne communique qu'avec un routeur ou le coordinateur
  - Endormi la plupart du temps

Exemple

- Lampe et son interrupteur
  - La lampe est alimentée : Zigbee router ou coordinateur
  - L'interrupteur est réveillé très rarement : un équipement terminal Zigbee

Les types d'équipement ZigBee

- Le coordinateur ZigBee (ZC) :
- Le routeur ZigBee (ZR) :
- L'équipement terminal Zigbee (ZED)



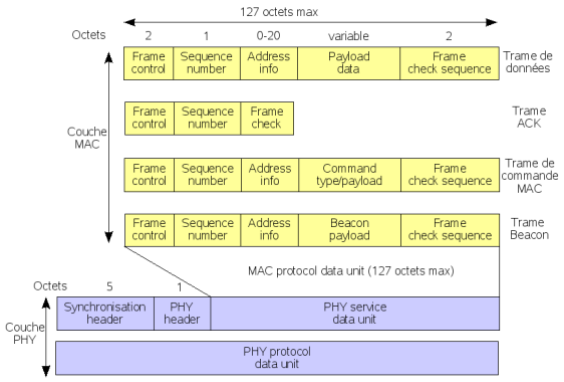
Les protocoles Zigbee

- Protocole de routage
  - Ad-hoc On-demand Distance Vector (AODV)
    => Réseau ad-hoc à faible débit
- Compatible avec les réseaux avec ou sans "beacon"
- CSMA/CA
  - Sauf pour les "beacons", les acquittements, les "Guaranteed Time Slots" (GTS)

Les protocoles Zigbee

- Sans "beacon" l'équipement Zigbee reste constamment actif. Dans ce cas :
  - Le récepteur des routeurs est constamment actif
  - Accès au canal : CSLA/CA sans "slot"
- Avec "beacon"
  - Les routeurs transmettent périodiquement un "beacon" pour confirmer leur présence. Ils peuvent s'endormir entre deux "beacons".
  - "Beacon intervals" :
    - 15.36 milliseconds to 251.65824 seconds at 250 kbit/s,
    - 24 milliseconds to 393.216 seconds at 40 kbit/s
    - 48 milliseconds to 786.432 seconds at 20 kbit/s.

Trame Zigbee



Canaux IEEE 802.15.4

- 4 GHz : 16 canaux ZigBee de 5 MHz chacun jusqu'à 250 kbit/s,
- 915 MHz jusqu'à 40 kbit/s,
- 868 MHz jusqu'à 20 kbit/s.

- Le débit réél obtenu dépend surtout des entêtes et des délais.

Codage Zigbee

- IEEE 802.15.4 radio :
  - Codage DSSS ("direct-sequence spread spectrum")
  - "Binary phase-shift keying" (BPSK) pour les bandes des 868 Mhz et 915 MHz
    - 1 bit par symbole
  - "Offset quadrature phase-shift keying" (OQPSK) pour la bande 2,4 GHz
    - 4 bits par symbole
  - Distance de transmission
    - Entre 10 and 75 mètres, et jusqu'à 1500 mètres pour Zigbee Pro,
  - L'"Output power" de la radio est de 0 dBm (1 mW).

Routage Zigbee

- AODV ("*Ad hoc On-Demand Vector Routing*")
  - Fonctionnement
    - Lorsqu'une source veut atteindre une destination,
    - Elle diffuse par inondation un "route request" jusqu'à atteindre la destination
    - Chaque routeur intermédiaire ne conserve que la meilleure route
    - La destination renvoie un "route reply" sur le chemin de moindre coût vers la source
    - Lors de la réception d'un "route reply" la source met à jour sa table de routage ("destination", "next hop" et "path cost")
  - Avantages/inconvénients
    - Réactif (peu de surcoût)
    - Délai lors de la découverte d'une route

Communication model

- "Application layer data service"
  - Un enchainement de primitives typiques:
    - request-confirm/indication-response
  - Les objets applicatifs Zigbee sont identifiés :
    - 1-240 (0 non-utilisé, 255 diffusion)
- Deux services existent:
  - Le service "key-value pair" (KVP) pour la configuration :
    - description, request et modification des attributs d'un objet
    - grace à un simple interface : primitives "get", "set" and event", certaine générant une "response".
    - "compressed XML" (ou "full XML")
  - Le service de messages
    - Capable de transporter sans trop de surcoût des données quelconques

Table de liaison

- Le coordinateur possède une table de liaison
  - Au niveau applicatif
  - La table de liaison ("binding table") contient pour chaque cluster un numéro (8 bits) et l'adresse de chacun des deux équipements source et destination
  - Le profil
    - Ensemble de messages et de protocoles d'échanges pour une famille d'applications
  - Le cluster
    - Numéro de cluster est unique dans un profil
  - L'attribut
    - Un élément d'un équipement Zigbee. Par exemple, un capteur particulier sur un équipement.

Les adressages de Zigbee

- Adressage direct
  - On connait l'adresse du destinataire
  - "Radio address" et "endpoint identifier"
- Adressage indirect
  - "address, endpoint, cluster, attribute"
  - Passage et traduction par le coordinateur
  - Certains équipements peuvent être très simples
- *"broadcast* "
  - Diffusion à tous les "endpoints" d'un équipement Zigbee
- "*group addressing"*
  - un groupe de "endpoints" appartenant à un ensemble d'équipements Zigbee

ZigBee Gateway

- It supports the following features:
  - Address core IP, either IPv4 or IPv6 connectivity
  - IP security domain
  - Configuration
  - IP RPC protocol definitions
  - Network Address and port Translation (NAT)/Firewall traversal
  - Incorporate IP best practices using Internet Engineering Task Force (IETF), W3C and other existing IP-based standards (SOAP, REST)
  - IP terminates at the Gateway

ZigBee Gateway

- Zigbee gateway provides:
  - Broad ZigBee/IP application support that can span all profile needs (neutral and generic)
  - Public profiles can use ZigBee Gateway to connect the ZigBee networks to IP networks
  - Private profiles can use standard gateway devices to connect private ZigBee network to remote applications
- Zigbee gateway is scalable, and extensible:
  - Layered standard enables both very low cost and very powerful Gateways
  - Framework that can be included within profiles as a basic device type or hybrid devices
  - Profile groups can incorporate and extend from the framework capitalizing on a rich set of base functionality and infrastructure definition
  - Gateway Framework extensions

ZigBee Gateway

- ZigBee Gateway defines a two-layered API :
  - A set of abstract (protocol independent) functions :
    - Support for complete Application Support Layer (APS), ZigBee Device Object (ZDO), and security services (SEC) commissioning both into and out of ZigBee networks
  - An extensible set of RPC protocols (i.e. bindings) specifying how to expose the API using a specific protocol. Release 1 of the Gateway specification features :
    - SOAP provides higher level web services oriented access to the Gateway API
    - REST provides a lightweight web-based API
    - GRIP is the protocol of choice for simplest ZigBee Gateway Devices, given its tiny footprint

SOAP

- SOAP is a standard
  - perform remote procedure calls through Hypertext Transport Protocol (HTTP)/Extensible Markup Language (XML) requests
- Syntax of requests is specified by an XML document (Web Services Description Language [WDSL])
  - Annex D of ZigBee Gateway specification
- Most popular development environments provide tools
  - generate stubs by “compiling” WSDL documents, actually turning remote into local calls
- Applications can concentrate on their business logic without having to deal with the complexities of network communications and data formatting, and achieve interoperability with no effort

REST

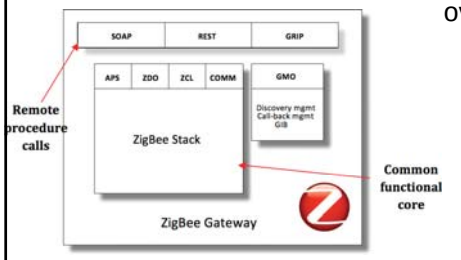
- REST, similar to SOAP
  - encodes remote invocation using HTTP/XML schema, but instead of just tunneling them through HTTP POST, it uses all the HTTP methods to access the API as a “resource repository”
- XML documents are much shorter and simpler, and in many cases the body does not even exist
- The footprint of both the Application and the ZigBee Gateway Device stack is very light
- Many operations can be performed using a Web browser

GRIP

- GRIP is a binary protocol
  - exchanges raw ZigBee stack structures on Transmission Control Protocol (TCP) connections
- Being a binary protocol, it features minimal bandwidth usage
- Basic API procedures
  - send and receive ZCL/APS/NWK packets
  - are implemented just by placing a TCP envelope, so the Gateway implementation could be a tiny layer on top of the ZigBee stack

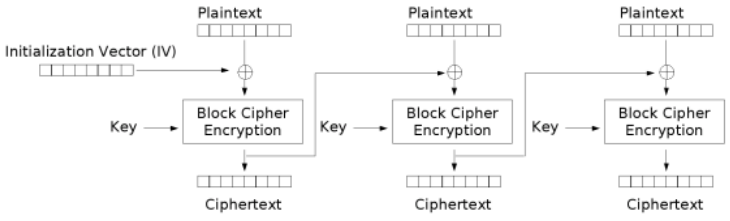
The two-tiered API

- The two-tiered API is matched by a two-layered functional architecture:
  - A northbound “interface” implementing at least one of the three bindings
  - A protocol-agnostic layer that implements each sub-segment of the overall API:
    - APS, ZDO, ZigBee Cluster Library (ZCL) and ZigBee Network Layer (COMM)
      - expose the different layers of the ZigBee stack
    - Gateway Management Object (GMO)
      - provides access to low-level ZigBee stack functions as well as high-level “macro” functions. These coarse-grained functions reduce complexity on optimized IP network traffic
    - ZigBee Gateway Device (ZGD) specification defines its own information base (GIB) and cluster to advertise the “Gateway service” to ZigBee nodes



La sécurité de Zigbee

- Cipher Block Chaining (CBC)
  - A technique for constructing a message authentication code from a block cipher
  - From IBM, 1976
  - Codage long car séquentiel
  - Technique de chiffrement anti-rejeu



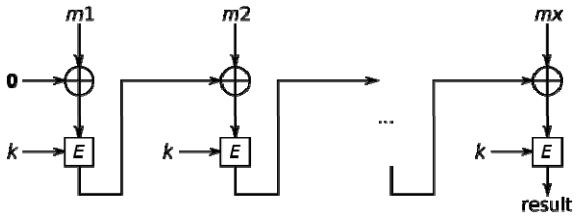
Cipher Block Chaining (CBC) mode encryption

La sécurité de Zigbee

- Chiffrement par blocs
  - AES 128 bits ("Advanced Encryption Standard"),
  - Algorithme de chiffrement symétrique.
    - "Rijndael" remporta en octobre 2000 le concours, lancé en 1997.

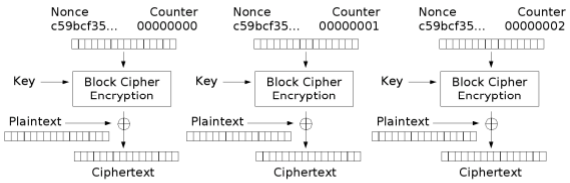
La sécurité de Zigbee

- Utilise "Cipher Block Chaining Message Authentication Code" (CBC-MAC)
  - a technique for constructing a message authentication code from a block cipher



La sécurité de Zigbee

- *"CTR mode" (CM);* ou "integer counter mode" *(ICM); ou* "segmented integer counter" *(SIC)*
  - constructing a message authentication code from a block cipher



Counter (CTR) mode encryption

Quelques équipements Zigbee

- Atmel ATmega128RFA1, AT86RF230/231
- Digi International XBee XB24CZ7PIS-004
- Ember EM250
- Freescale MC13224
- GreenPeak GP520-GP530-GP540
- Jennic JN5148
- RadioPulse MG2410 and MG2450/55
- Renesas uPD78F8056/57/58, M16C/6B3 and R8C/3MQ
- Sena Technologies Inc. : ProBee, ProBee-ZU/ProBee-ZS/ProBee-ZE
- STMicroelectronics STM32W
- Samsung Electro-Mechanics ZBS240
- Texas Instruments CC2530 and CC2520
- Microchip Zigbee MRF24J40MB

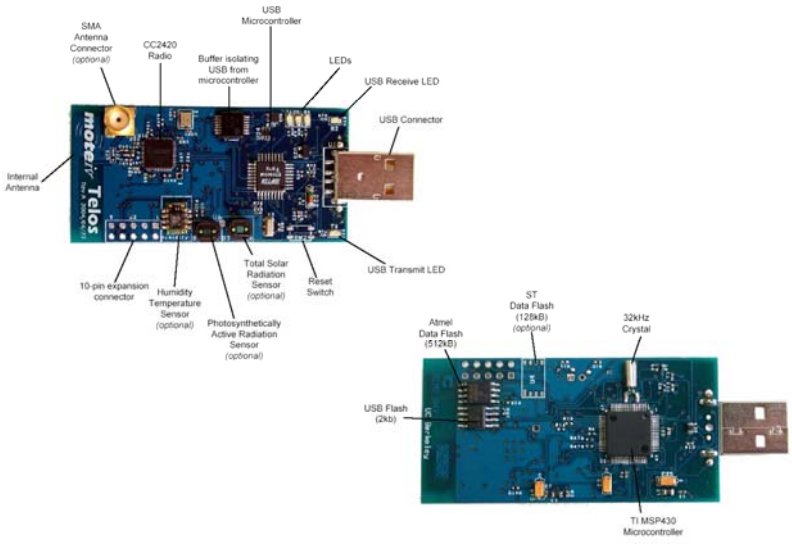
Telos Platform

Telos wireless platform
(revision A)

- Texas Instruments 16-bit MSP430F149 microcontroller (2KB RAM, 60KB ROM)
- Chipcon 2420, 250 kbit/s, 2.4 GHz, IEEE 802.15.4 compliant wireless transceiver with programmable output power
- Integrated onboard antenna with 50 m range indoors and 125 m range outdoors
- Integrated humidity, temperature, and light sensors

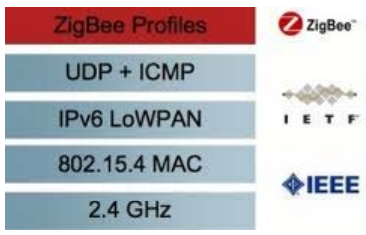
39

Telos Platform



40

Conclusion


ZigBee Profiles
UDP + ICMP
IPv6 LoWPAN
802.15.4 MAC
2.4 GHz
ZigBee
IETF
IEEE