

Technologies Émergentes en ISI

Chapitre 3 : Technologies Sans fils

F.Z. Filali

Octobre 23, 2017



1 Partie 1 : RFID

- Définitions
- Architecture
- Protocoles
- Applications
- Problèmes

2 Partie 2 : WSN

- Concepts de base
- Architecture
- Communication et protocoles

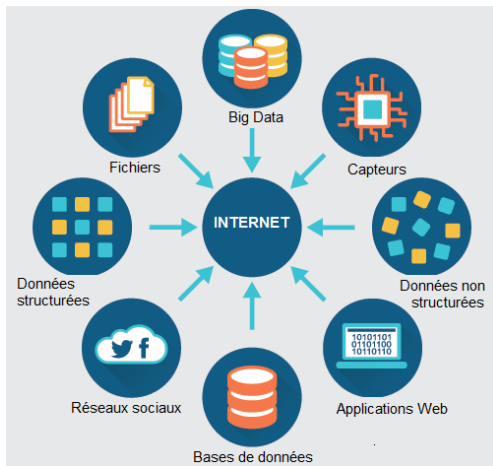
- Problèmes
- Zigbee : IEEE 802.15.4
- Applications

3 Partie 3 : IoT

- Introduction
- Définitions
- Acteurs
- Interactions et connections
- Architecture
- Composants
- Technologies



Introduction



Partie 1

Technologies RFID



Définitions

- Radio Frequency IDentification : Identification par radio fréquence.
- Une technologie Automatisée d'IDentification et de Collecte de données (AIDC).
- Il permet aux entreprises particulièrement de capturer et de suivre des données sans fil à l'aide d'ondes radio.





Architecture

Un système RFID contient trois composants majeurs :

- Tag
- Lecteur
- Système Backend (base de données)

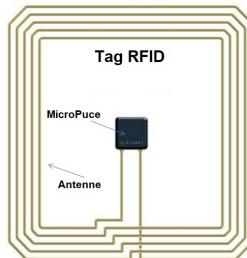




Architecture : Tag ou étiquette

Trois composants :

- Antenne : Transmettre et réceptionner des ondes radio (collecter de l'énergie).
- Circuit intégré (micropuce) : Transmettre les IDs.
- Carte (PCB) : Maintenir les composants ensemble.





Architecture : Tag ou étiquette

Types :

① Passive

- NFC, Aucune alimentation , peu coûteux et petits.
- La plage de lecture est très courte : jusqu'à 10 m.
- Technique de rétro diffusion pour envoyer les données au lecteur.

② Active

- Alimentation fournit avec l'étiquette (embarquée) : pile, batterie.
- Plage de lecture plus étendue : 100 m ou plus, plus chers et plus gros.
- Autonome et envoie leurs identifiants à un débit régulier (entre 1 et 15 sec).

③ Semi-passive / Semi-active

- Plage de lecture longue : jusqu'à 100 m.
- Énergie fournit à bord : Semi passive → pour alimenter les circuits.
Semi-active → pour la transmission de données.



Architecture : Lecteur RFID

- Lecteur RFID peut être sous deux formes :
 - Lecteur RFID fixe : installé de manière fixe.
Exemple : caisse des supermarchés, RFID en bibliothèque, contrôle d'accès aux zones ... ;
 - Lecteur RFID portable : flasher portatif qui permet de lire les étiquettes manuellement.
Exemple : terminal portable, smartphone, authentification de véhicule. . .





Architecture : Lecteur RFID

- Le lecteur RFID fonctionne de la manière suivante :
 - il transmet à travers des ondes-radio l'énergie au tag RFID,
 - il transmet des requêtes d'informations aux étiquettes RFID situées dans son champ magnétique,
 - il réceptionne les réponses et les transmet aux applications concernées.
- La communication entre le lecteur RFID et l'étiquette est possible grâce à chaque antenne RFID intégrée dans chacun des 2 composants.
- Types : lecture seule, lecture/écriture.

Architecture : Système Backend

- Le lecteur RFID sert d'intermédiaire entre les tags et les systèmes backend.
- Une fois qu'un système backend reçoit des données transmises par un lecteur RFID, le système exécute une application en fonction des données qu'il a reçu.

Question

Quelles sont les différences entre le RFID et le Code Barre ?



Réponse



Caractéristiques	Code Barre 1D	Code Barre 2D	RFID
Capacité (nb de caractères)	1 à 40	5 à 3000	Quelques caractères à plusieurs ko
Visibilité de l'étiquette	Obligatoire	Obligatoire	Non obligatoire
Lecture	Oui	Oui	Oui
Ecriture	Non	Non	Non
Distance de lecture	0 à 5 m	15 à 100 cm	1 à 100 m
Coût	faible	faible	cher



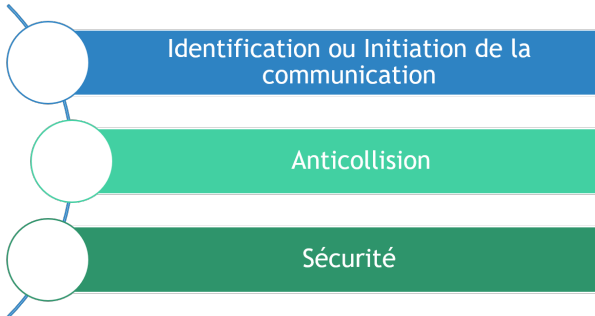
Protocoles

- ISO, EPCglobal : standardisation et normalisation.
- Un protocole de communication dans le cas de la RFID est une façon d'organiser la conversation entre les étiquettes et un lecteur afin de s'assurer que l'information est effectivement transférée. Il définit :
 - Interface d'accès : type de modulation du signal, type de signal envoyé par l'étiquette, vitesse de transmission...
 - Moyen du contrôle d'accès : qui communique? quand? Comment les collisions entre les tags sont gérées?
 - Définitions de données: type de données associé à une étiquette, leur interprétation...



Protocoles

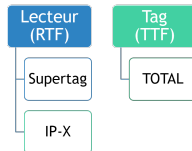
Problématiques et défis pour définir les protocoles :





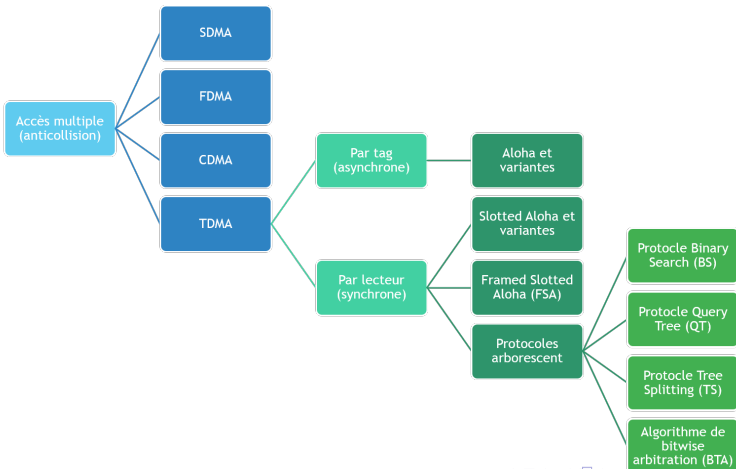
Protocoles : 1. Identification

- Problème : qui parle en premier ?
- Solution :
 - Le lecteur initie la comm. (RTF, Reader Talk First) :
 - Détecter une grande quantité d'étiquettes dans un temps acceptable;
 - Interroger un groupe de tag seulement.
 - L'étiquette initie la comm. (TTF, Tag Talk First) :
 - Plus performant : peu de collision.
 - Mise en place simple.
 - Identification lente.
- Exemples : Supertag (TTF), IP-X (variante de supertag), TOTAL (Tag Only Talks After Listening : RTF).



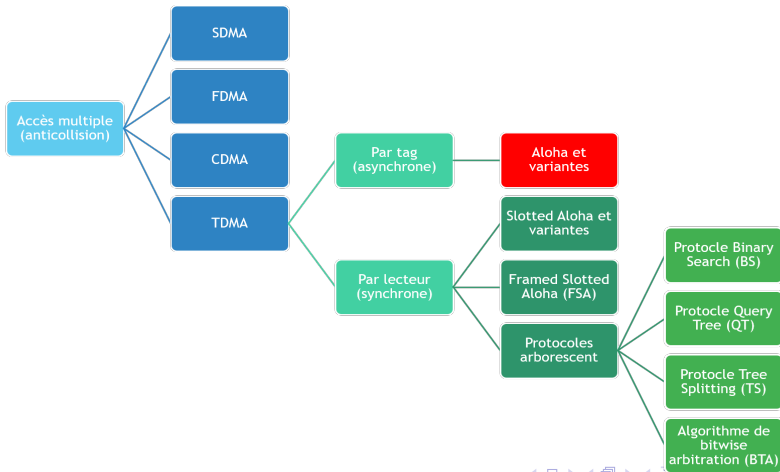


Protocoles : 2.Anti-collision



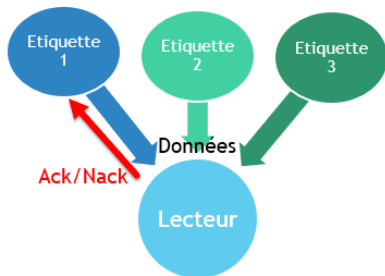


Protocoles : 2.Anti-collision - ALOHA





Protocoles : 2.Anti-collision - ALOHA

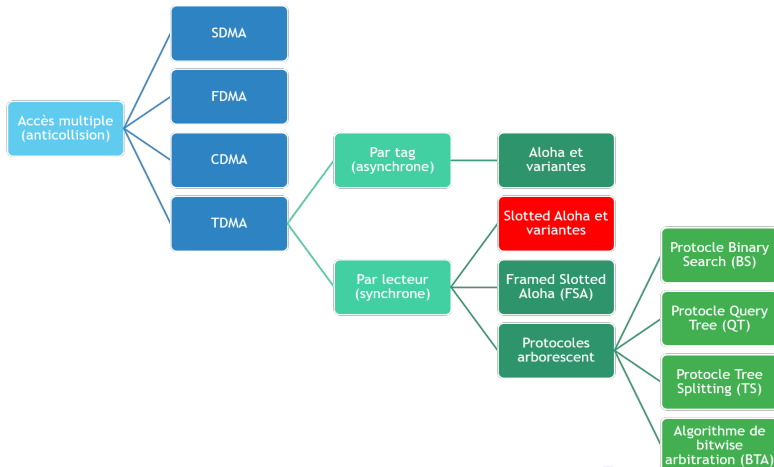


Algorithme :

- Le tag transmet immédiatement lorsqu'il a des données,
- Le tag attend une réponse ack/nack du lecteur,
- Si l'ack n'est pas reçu, le tag attend un temps aléatoire et retransmet les données.



Protocoles : 2.Anti-collision - Slotted ALOHA

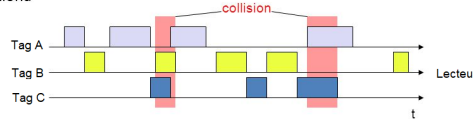




Protocoles : 2.Anti-collision - Slotted ALOHA

- Slotted : Time Slot (Tranche de temps).
- L'envoi doit toujours être fait lors du début d'une tranche de temps.
- Synchronisation des étiquettes se fait par le lecteur.

Aloha

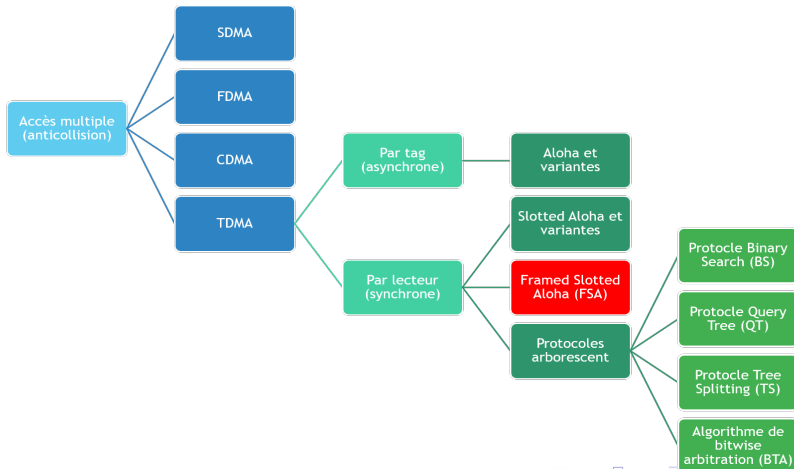


Slotted Aloha



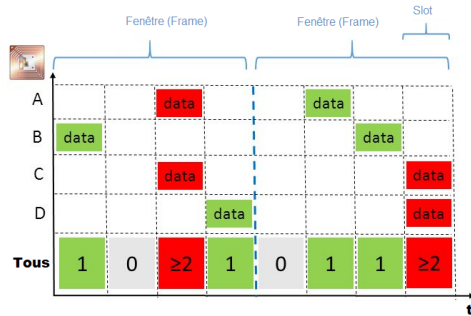


Protocoles : 2.Anti-collision - Framed Slotted ALOHA



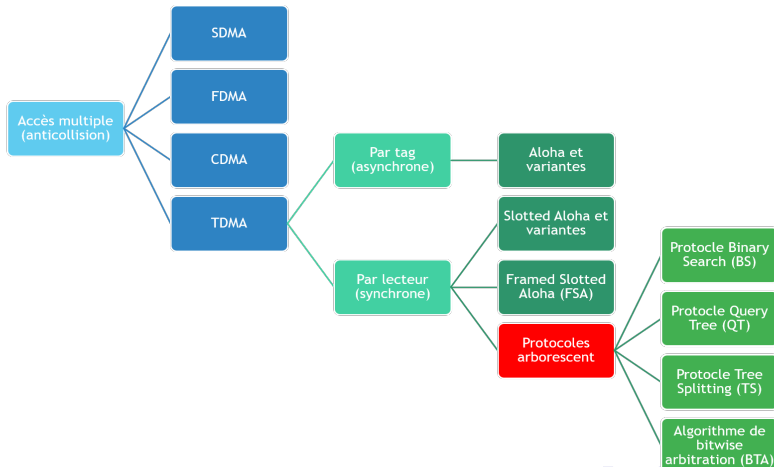
Protocoles : 2.Anti-collision - Framed Slotted ALOHA

- Utilisation de frame (fenêtre).
Taille Frame = nombre étiquettes.
- Le lecteur accepte les données si une seule étiquette répond, sinon collision.
- Autres algorithmes :
 - Dynamic Framed Slotted ALOHA (DFSA),
 - Advanced Framed Slotted ALOHA (AFSA),
 - Enhanced Framed Slotted ALOHA (EFSA).





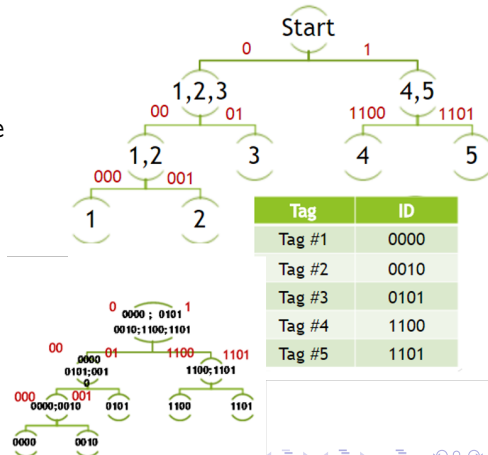
Protocoles : 2.Anti-collision - Protocoles arborescents





Protocoles : 2.Anti-collision - Protocoles arborescents

- Méthode déterministe.
- Consiste à résoudre le problème de collision.
- Plusieurs implémentations :
 - Binary Search
 - Query-Tree Algorithm
 - Tree Splitting
 - Bitwise arbitration
 - ...





Protocoles : 3.Sécurité

- Capacité de calcul, mémoire limitée, faible coût → vulnérable.
- Confidentialité :
 - Désactivation de l'étiquette.
 - Limiter l'accès : fonction de hashage sur le metaID → algorithme Weis.
 - Cryptographie minimale : collection de pseudonymes.
- Authentification :
 - Protection de l'accès au tag,
 - Protection de l'accès au système back-end.



Applications RFID

- 1ère utilisation (1970) → Surveillance électronique des articles.
- Industrie automobile,
- Vente au détail,
- Suivi et identification,
- Systèmes de paiement,
- Contrôle d'accès,
- ...



Problèmes et préoccupations en matière de RFID

- Inondation de données et filtrage de données envoyées;
- Standardisation globale ;
- Problèmes de sécurité ;
- Passeports.

Partie 2

Réseaux de capteurs sans fils (WSN)



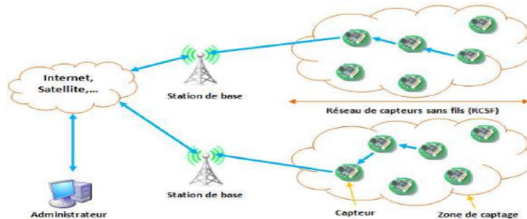
Concepts de base

- RCSF, Réseaux de capteurs sans fils (WSN, Wireless Sensors Networks)
- Réseau de capteurs auto-alimentés dotés de capacités de calcul et de communication sans fils.
- Autonomes, distribués spatialement pour surveiller les conditions physiques et environnementales.
- Le WSN est construit à partir de nœuds (quelques centaines à des milliers) connecté à des capteurs.



Concepts de base

- Un middleware WSN est une infrastructure logicielle qui regroupe le matériel du capteur, le système d'exploitation, les piles de réseau et les services d'application.
- Exemple : Détection d'incendie ou de catastrophe.





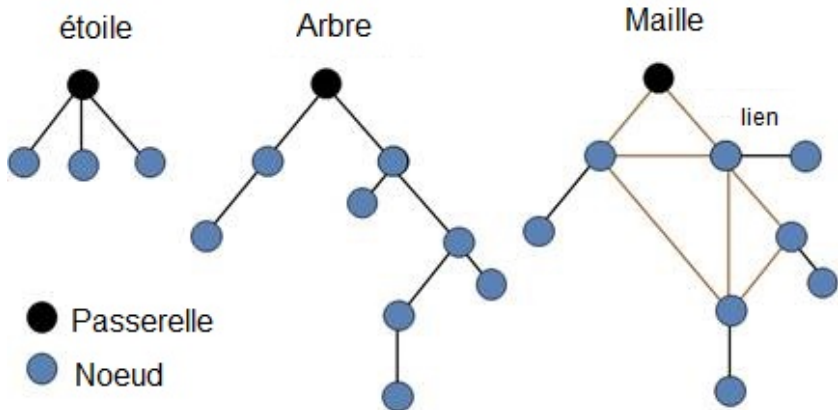
Concepts de base

Principales caractéristiques :

- Type de service,
- La qualité de service,
- Tolérance aux fautes,
- Durée de vie,
- Scalabilité,
- Maintenance,
- Programmation flexible.

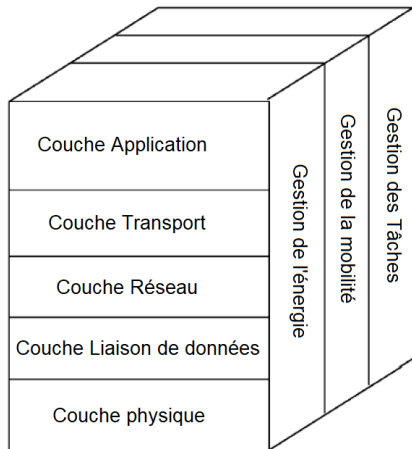


Architecture des Réseaux de capteurs





Communication et pile protocolaire





Problèmes et préoccupations

- Capacités fonctionnelles limitées,
- Énergie limitée,
- Scalabilité,
- Redondance,
- Manque d'identification globale,
- Stockage,
- Latence,
- Tolérance aux pannes.



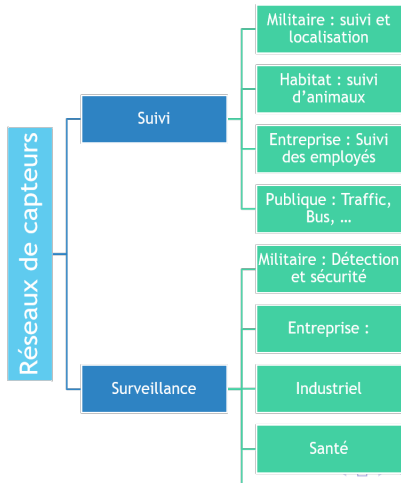
Zigbee : IEEE 802.15.4

- ZigBee : Le standard IEEE 802.15.4
- propose une norme pour les couches physique et liaison de données, orientée très faible consommation énergétique.
- La pile proposée par l'IEEE et la ZigBee qui a pour objectif de promouvoir une puce offrant un débit relativement faible (100Kbps environ) mais à un coût très bas, et une consommation électrique extrêmement réduite.





Applications

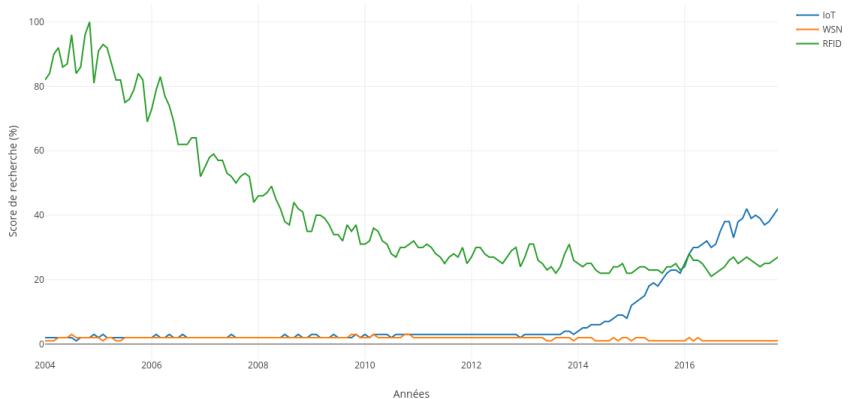


Partie 3

Internet of Things (IoT)

Introduction

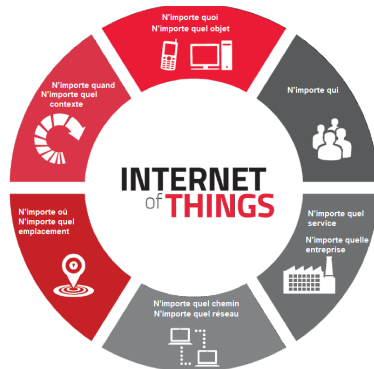
Tendances de recherche de Google Trends depuis 2004 pour les termes Internet of Things, Réseaux de capteurs sans fil WSN et RFID





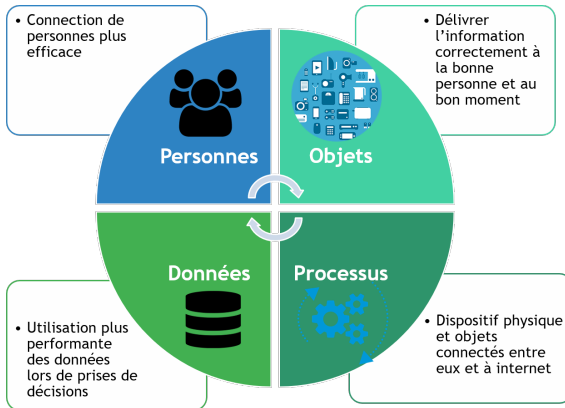
Définitions

- IoT permet de connecter n'importe:
 - Temps
 - Emplacement
 - Personne
 - Objet
 - Réseau
 - Service
- Le groupe RFID définit l'Internet des objets comme : Le réseau mondial d'objets interconnectés adressable uniquement par des protocoles de communication standard.



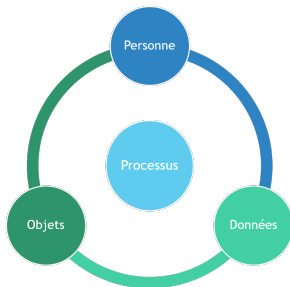


Les acteurs de l'IoT





Interactions et connections



Personne à
Personne (People-to-
People, P2P)



Machine à Personne
(Machine-to-
People, M2P)

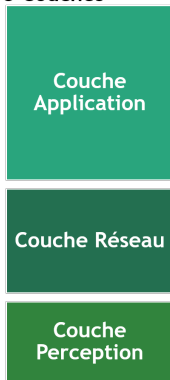


Machine à Machine
(Machine-to-
Machine, M2M)



Architecture de l'IoT

**Architecture
3 Couches**



**Architecture
Basée Intergiciel**



**Architecture
Basée SOA**

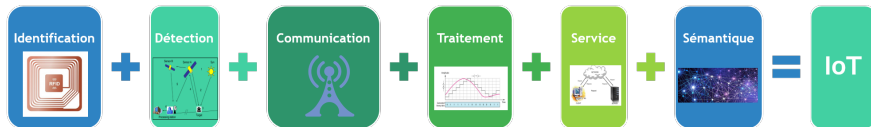


**Architecture
5 couches**





Composants de l'IoT





Technologies de l'IoT

Composant IoT	Identification		Détection	Communication	Traitement		Service	Sémantique
	Nommage	Adressage			Matériel	Logiciel		
Technologies	-EPC -uCode	-IPv4 -IPv6	-Capteurs intelligents -Dispositifs de détection portable -Capteurs embarqués -Actionneurs -Tag RFID	-RFID -NFC -UWB -Bluetooth -BLE -IEEE 802,15,4 -Z-Wave -WiFi -WiFiDirect -LTE-A	-Objets intelligents -Arduino -Phidgets -Intel Galilo -Raspberry Pi -Gadgeteer -BeagleBone -Smartphone	-OS (Contiki, TinyOS, LiteOS, RiotOS, Android) -Cloud (Nimbits, Hadoop, ...)	-Agrégation (smart Grid) -Collaboration (smart home) -Ubiquitaire (smart city)	-RDF -OWL -EXI

Questions ?