Università degli Studi di Padova
Facoltà di Ingegneria

UNIVERSITÀ DEGLI STUDI DI PADOVA
FACOLTÀ DI INGEGNERIA

—

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

—

TESI DI LAUREA TRIENNALE IN INGEGNERIA
DELL'INFORMAZIONE

INTERNET OF THINGS E TECNOLOGIA RFID

RELATORE: CH.MO PROF. MICHELE ROSSI

LAUREANDO: **ENRICO TOIGO**

ANNO ACCADEMICO 2012-2013

Abstract

Internet Of Things è un nuovo paradigma tecnologico, ancora in fase di sviluppo. Questa locuzione fa riferimento a un insieme di oggetti, di diverso tipo, che interagiscono tra loro, e allo stesso tempo, sono connessi a questa rete globale; tutto questo grazie alla tecnologia *wireless*. In questo elaborato verrà trattato sia il tema dell'*Internet Of Things* e sia quello delle tecnologie che hanno permesso e ne stanno permettendo la sua diffusione come WSN, RFID e NFC, verranno infine descritti alcuni utilizzi dell'IOT all'interno della vita reale.

Indice

Indice iii

Introduzione 1

1 Internet Of Things 5
- 1.1 Quadro generale . . . 5
- 1.2 WSN . . . 8
- 1.3 Internet Of Things: architettura del protocollo . . . 10

2 Tecnologia RFID 15
- 2.1 Introduzione . . . 15
- 2.2 Gli standard RFID . . . 17
  - 2.2.1 Standard EPC . . . 18
- 2.3 Architettura RFID . . . 20

3 Tecnologia NFC 21
- 3.1 Quadro generale . . . 21
- 3.2 Architettura NFC . . . 23

4 Sicurezza 27

5 Conclusioni 31

Glossario 38

Bibliografia 41

Elenco delle figure

1 Il web 3.0: estensione del web 2.0 2

1.1 Rappresentazione schematica dell'Internet Of Things 7
1.2 Architettura del protocollo IOT 11
1.3 Rappresentazione schematica di un sistema M2M 13

2.1 Codice EPC 18
2.2 Suddivisione frequenze e standard RFID 18
2.3 Architettura del sistema RFID 20

3.1 Classificazione dei *tag* NFC, secondo NFC Forum 23
3.2 Architettura NFC secondo NFC Forum 24
3.3 Previsione dell'integrazione della tecnologia NFC negli *smartphone* 25

ELENCO DELLE FIGURE

Introduzione

Con lo sviluppo sempre più rapido delle varie tecnologie di comunicazione si sta avendo un continuo aumento di dispositivi che possono accedere alla rete ed interagire con essa.

Quando si fa riferimento a una rete globale di oggetti intelligenti di ogni tipo come computer, tv, vestiti... che interagiscono tra loro attraverso protocolli internet, non si fa altro che definire l'**Internet Of Things (IOT)**. L'IOT presenta una grande eterogeneità di dispositivi che si differenziano per funzionalità, tecnologia e ambito di utilizzo. Uno strumento importante per lo sviluppo dell'IOT è il web 3.0 o web semantico.

Già da qualche anno si sta concretizzando il concetto di web 3.0[1]. Il web 3.0 si basa sull'unione del web 2.0 (figura 1) — in cui gli utenti possono, a differenza del web 1.0 o web statico, interagire condividendo con altri utenti contenuti da loro stessi creati — con il web semantico, ovvero un web in cui ciascuna risorsa è descritta utilizzando XML e è messa poi in relazione con altre risorse attraverso dei link che possono specificare anche il tipo di legame, per esempio un documento può essere collegato al suo autore attraverso un link con etichetta "creato da". Rispetto al web 2.0 ciascuna risorsa e ciascun link sono identificati attraverso l'aggiunta di proprietà che permettono di dare una maggior quantità di informazione all'uomo, ma soprattutto alle macchine [3, 11].

[1]Questo termine fu coniato da Jeffrey Zeldman nell'articolo "Critical of Web 2.0 and associated technologies such as Ajax"

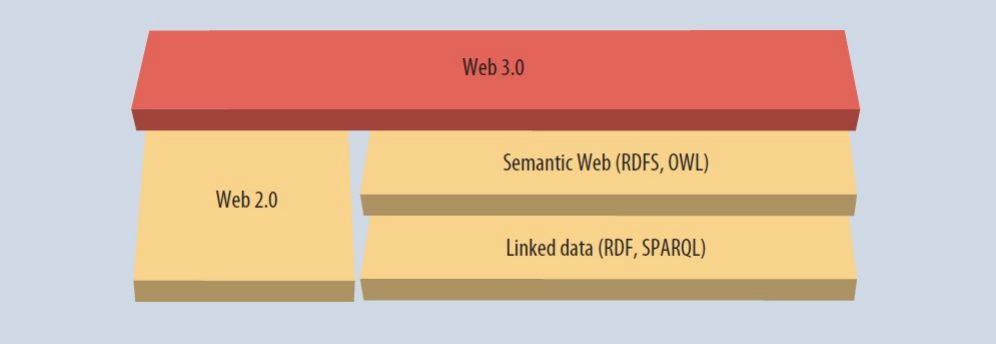

Figura 1: Il web 3.0 si basa sia sul web 2.0 sia sul web semantico e sia su linguaggi come RDF e SPARQL che permettono di individuare, unire e mettere in relazione tra loro le informazioni all'interno del web

Nel web 2.0 le varie applicazioni non sono in grado di contestualizzare l'informazione che manipolano, l'obiettivo del web 3.0 è appunto quello di permettere alle applicazioni di capire e interpretare ciò che stanno gestendo in base al contesto in cui sono. Ciò che il web semantico descrive è detto risorsa, essa viene rappresentata utilizzando sia il legame che c'è tra le varie risorse sia utilizzando le proprietà della risorsa stessa come dimensioni, colore, affidabilità... I linguaggi cardine del web semantico sono:

- **Resource Description Framework (RDF)**: è il linguaggio utilizzato per rappresentare metadati all'interno del Word Wide Web in modo *machine-oriented* cioè orientato verso una comunicazione *Machine-To-Machine* (M2M). La codifica dell'informazione avviene attraverso l'utilizzo dell'*Uniform Resource Identifier* (URI) che permette di individuare in modo univoco, attraverso una stringa, la risorsa da descrivere. L'informazione è descritta attraverso RDF utilizzando tre *statements* :
  - *soggetto*: identifica la risorsa
  - *predicato*: identifica la caratteristica del soggetto/risorsa
  - *oggetto*: identifica il valore della proprietà [7]
- **Ontology Web Language (OWL)**: è un linguaggio ontologico. Esso si basa sulla rappresentazione dell'informazione attraverso l'utilizzo del significato dei vari termini e del legame che c'è tra essi [9].

- **SPARQL Protocol and RDF Query Language (SPARQL)**: è un linguaggio *query* che permette, attraverso delle interrogazioni, di individuare i dati in formato RDF presenti all'interno del web, il quale viene considerato come un database [10].

A differenza del web 2.0 in cui c'era una comunicazione "Human-to-Human" nel web 3.0 la comunicazione è più estesa perché include anche quella *Human-To-Machine* e quella *Machine-To-Machine*. Ultimamente molti progetti stanno nascendo orientati verso una ricerca e creazione di standard o applicazioni nel campo dell'Internet Of Things, per esempio il progetto *ebbits* (Enabling business-based Internet of Things and Services)[1] orientato verso l'ambito del business, con lo scopo di permettere alle aziende di integrare in modo semantico l'IOT nei processi aziendali e di sostenere l'interoperabilità tra applicazioni commerciali. Altri progetti sono *IoT@Work*[2] — rivolto allo sviluppo di tecnologie con lo scopo di adattare i processi produttivi delle imprese in modo rapido e agevole ai nuovi processi e modelli di mercato — *IOT-A*[3] — un progetto con lo scopo di creare un modello di architettura di riferimento per l'interoperabilità di sistemi IOT, partendo dalla definizione di un insieme di concetti base, tra questi la scalabilità, e utilizzando un approccio top-down per sviluppare protocolli, interfacce e algoritmi — *Casagras 2*[4] — un progetto che si basa sullo studio delle varie caratteristiche della tecnologia RFID implementata in IOT.

L'**obiettivo** di questa tesi è quello di descrivere in cosa consiste l'IOT, le tecnologie più importanti che stanno permettendo a questo nuovo concetto di diffondersi, in ordine di importanza sono: WSN, RFID, NFC e infine verranno proposti alcuni esempi di applicazioni pratiche in cui sono utilizzate le tecnologie sopra citate.

Con **WSN** si intende una rete costituita da sensori, non necessariamente disposti in una posizione predeterminata nell'ambiente reale, con lo scopo di effettuare *sensing*, elaborazione dati (se il sensore ha le risorse per farlo) e interazioni con

[1] http://www.ebbits-project.eu
[2] https://www.iot-at-work.eu/
[3] http://www.iot-a.eu/public/
[4] http://www.iot-casagras.org

altri sensori. I nodi che compongono questa rete sono caratterizzati dal fatto di avere risorse limitate in termini di capacità di calcolo, memoria e approvvigionamento energetico.
Le reti di sensori vengono utilizzate in vari campi come per esempio quello militare, della sicurezza, quello medico...
La tecnologia **RFID** era stata inizialmente studiata per applicazioni correlate all'identificazione degli oggetti fisici attraverso l'invio di un ID su richiesta di un *reader*. I componenti principali di questa tecnologia sono i *tag*, i *reader* e un sistema informatico di *back-end*. Un utilizzo di questa tecnologia si ha nei siti di stoccaggio per il tracciamento delle merci in transito oppure per la localizzazione del bestiame e degli animali selvatici...
Per quanto riguarda la tecnologia **NFC** si può dire che sfrutta la tecnologia RFID per permettere ai vari dispositivi, posti a piccole distanze l'uno dall'altro, di comunicare. Generalmente uno dei due dispositivi è un telefono cellulare. Gli utilizzi primari di NFC sono: condivisione di informazioni attraverso la connessione con altri dispositivi elettronici, accesso a contenuto digitale e transazioni *contactless*.

Struttura della tesi:

- nel capitolo 1 verrà trattato il tema dell'IOT andando a spiegare in cosa consiste e analizzando l'architettura proposta nell'ambito del progetto IOT-A, per poi andare a spiegare cosa sono le reti di sensori (WSN) e perché esse sono importanti per la diffusione dell'IOT.

- nel capitolo 2 verrà trattata la tecnologia RFID, descrivendone le caratteristiche principali e gli standard su cui si basa.

- il capitolo 3 descrive una tecnologia derivante dall'RFID: la tecnologia NFC. Questo tipo di tecnologia si sta diffondendo sempre più, soprattutto integrata negli *smartphone*, utile a rendere più veloci le operazioni di *ticketing*, pagamento, acquisizione di informazioni da poster, confezioni, abiti...

- il capitolo 4 è una discussione su alcuni attacchi informatici che possono interessare un sistema IOT e le eventuali tecniche che si possono adattare per evitarli.

1

Internet Of Things

L'obiettivo di questo capitolo è quello di definire quali sono gli "attori" di una rete di oggetti e le tecnologie che stanno rendendo possibile la sua realizzazione. Quando si parla di internet delle cose si fa riferimento a qualsiasi tipo di oggetto intelligente, quindi si può parlare di un computer, di un sensore, ma anche di un'automobile o di una forbice... Tutti questi oggetti possono comunicare (in tutta la tesi quando si parla di comunicazione, collegamenti o interazioni tra nodi si fa riferimento alla tecnologia *wireless*) tra loro grazie alla presenza di chip all'interno di essi. Ecco quindi che si può pensare non più a una rete limitata a dispositivi come computer, cellulari, tablet, ma a una rete globale in cui, in qualsiasi momento, ogni oggetto è connesso, indipendentemente dal luogo in cui si trova.

1.1 Quadro generale

In questo capitolo viene descritto in cosa consiste l'Internet Of Things, il cui sviluppo è dovuto soprattutto alla tecnologia *wireless*. Successivamente verrà trattata la tecnologia WSN, di notevole importanza per lo sviluppo e diffusione dell'IOT, e infine si descriverà l'architettura del protocollo IOT proposto nell'ambito del progetto europeo IOT-A.
Con Internet Of Things si intende una rete di oggetti interconnessi, individuati in modo univoco, che posso comunicare tra loro — comunicazione *Machine to Machine* (M2M) — o interagire con il mondo reale — comunicazione *Machine to*

Human (M2H). L'IOT permette di avere un collegamento tra il mondo virtuale e quello reale. Il termine *Internet Of Things* fa riferimento o ad un insieme di dispositivi che interagiscono tra loro e con l'ambiente circostante, o al *web of things* cioè un insieme servizi web a cui possono accedere i vari dispositivi connessi.
Un'altra interpretazione, del significato, è quella semantica — concetto sul quale si basa anche il web 3.0 — in cui si fa riferimento a un sistema in cui viene gestita, dai dispositivi, un'informazione contestualizzata.
I dispositivi che fanno parte della rete di oggetti sono chiamati *smart objects* o *smart things*, che a differenza dei normali dispositivi possiedono la capacità di poter interagire all'interno del sistema di comunicazione in cui sono inseriti: hanno quindi un ruolo attivo. Essi possono essere individuati attraverso le seguenti caratteristiche:

- Sono degli oggetti veri e propri caratterizzati da costo, forma, peso...
- Hanno risorse limitate in termini di capacità computazionale, memoria, approvvigionamento energetico e *routing*.
- Sono identificati in modo univoco da un ID (codice alfanumerico), possono individuare vari dispositivi nella rete e essere individuati, e inoltre a essi è associato anche un nome che permette all'uomo di riconoscerlo.
- Posso essere influenzati e influenzare la realtà che li circonda come per esempio gli attuatori (robot, motori elettrici, pistoni idraulici...) [5]

Grazie allo sviluppo che sta avendo la tecnologia *wireless* e agli studi sull'IOT la comunicazione "*anywhere, anytime by anything*" non è più considerata una vera e propria utopia, infatti sempre più dispositivi, in qualsiasi momento, anche senza ricevere degli input da parte di una persona, possono accedere alla rete e interagire con i vari dispositivi connessi (Figura 1.1) [14].

Figura 1.1: Rappresentazione schematica dell'Internet Of Things

La concretizzazione del significato dell'IOT è resa possibile grazie a tecnologie abilitanti come **Wireless Sensor Networks - WSN** utilizzate soprattutto per operazioni di *sensing*. I nodi di una WSN sono dei sensori, disposti all'interno di un ambiente, con lo scopo di rilevare determinati dati, inviarli per esempio a un sensore con capacità di elaborazione detto *sink*, affinché essi vengano elaborati. La WSN può essere utilizzata in varie applicazioni militari, mediche, di monitoraggio ambientale...

Per quanto riguarda le tecnologie abilitanti per l'IOT è da considerare anche l'**RFID (Radio Frequency IDentification)** inizialmente utilizzata per il solo processo di identificazione, e ultimamente anche per minime operazioni di *sensing*. Un sistema RFID è costituito da *tag*, i *reader* e un sistema informatico di *back-end* che permette di associare a ogni ID, l'oggetto fisico corrispondente e eventuali altre informazioni connesse a esso.

Un utilizzo di questa tecnologia si ha nei siti di stoccaggio per il tracciamento delle merci in transito, oppure per la localizzazione del bestiame e degli animali selvatici, per il controllo degli accessi attraverso l'utilizzo di biglietti, *ski pass*...

Un'altra tecnologia da tenere in considerazione è la **Near Field Communication (NFC)** che si sviluppa a partire dai sistemi RFID. La differenza sostanziale consiste nella distanza di comunicazione tra i dispositivi, essa è molto piccola e si aggira attorno ai 10 cm. NFC è usata per condividere informazioni tra i vari dispositivi, per accedere a contenuti digitali presenti per esempio in poster abilitati alla comunicazione NFC e per effettuare operazioni di *ticketing*.
L'eterogeneità di dispositivi e di applicazioni, in un sistema IOT, rende necessaria la presenza di un software detto **Middleware** che fa da "collante" tra i dispositivi e le applicazioni presenti in essi. Alcuni *Middleware* si basano, per quanto riguarda l'architettura, su **SOA (Service Oriented Architecture)** come per esempio il *Middleware*, ancora in fase di sviluppo, realizzato all'interno del progetto europeo HYDRA[1]: *LinkSmart Middleware* [5].

1.2 WSN

Una rete di sensori consiste di un numero più o meno elevato di piccoli sensori a basso costo, bassa potenza e con la possibilità di eseguire varie funzioni nei limiti delle loro caratteristiche computazionali e di memoria. Questi sensori, all'interno della rete, sono chiamati nodi e il loro compito principale è quello di raccogliere dati dall'ambiente in cui essi sono inseriti. La rete di sensori è una rete dinamica che riesce a supportare anche un incremento del numero di sensori connessi oppure anche una diminuzione degli stessi dovuta a dei guasti; inoltre la topologia di questa rete, oltre a variare spesso, dipende anche dall'utilizzo che se ne fa. La WSN è una rete ad-hoc con alcune limitazioni dovute sia al tipo di comunicazione usata sia ai sensori impiegati. La progettazione di WSN dipende da alcuni fattori quali:

- *Tolleranza ai guasti*: è la capacità di mantenere le funzionalità della WSN senza interruzioni dovute ai guasti, spesso frequenti, dei nodi. L'affidabilità $R_k(t)$ è definita utilizzando una variabile aleatoria di Poisson, che indica la probabilità di non avere un guasto in un intervallo di tempo compreso tra 0 e t, con λ_k il tasso di guasto del sensore k, e è uguale a $R_k(t) = e^{-\lambda_k t}$

[1] http://www.hydramiddleware.eu

- *Scalabilità*: è la capacità della rete di poter gestire un aumento del numero di sensori connessi, spesso è utilizzata anche la densità di sensori all'interno del raggio di trasmissione di ciascun nodo in una data regione X. La densità è ottenuta dalla seguente formula $\mu(R) = \frac{N\pi R^2}{X}$ dove R indica il range del raggio di trasmissione dei nodi e N il numero di dispositivi nella regione X.

- *Costi di produzione*: il costo di ciascun sensore è di fondamentale importanza per il costo totale delle reti. L'obiettivo è quello di utilizzare sensori a basso costo, che dipende soprattutto dalle funzionalità dei sensori stessi.

- *Sicurezza*: è necessario considerare che un canale *wireless* è aperto a chiunque. Utilizzando un dispositivo sincronizzato sulla stessa frequenza di trasmissione, di due o più dispositivi, ognuno può monitorare o partecipare alla comunicazione oppure effettuare un attacco informatico. In una WSN, a causa delle limitate risorse dei sensori non è possibile implementare dei complessi algoritmi di sicurezza senza andare a peggiorare la *performance* della rete stessa. Spesso si utilizzano algoritmi ottimizzati che non vadano a richiedere una grande quantità di risorse ai sensori e che allo stesso tempo non influenzino notevolmente le prestazioni dell'intera rete. Alcuni requisiti minimi che possono essere implementati sono la criptazione dei dati e la richiesta di autenticazione per accedere alla WSN (queste procedure verranno descritte nel capitolo 4).

- *Limitazioni hardware*: ciascun nodo deve consumare una bassa quantità di energia — spesso i sensori vengono progettati in modo da poter ricavare energia da fonti esterne come per esempio il sole — operare in regioni a alta densità e adattarsi all'ambiente.

- *Topologia della rete di sensori*: a causa di un elevato numero di sensori presenti nella rete, il quale non è statico bensì dinamico, fa si, che anche la struttura della rete cambi frequentemente.

- *Ambiente*: i sensori devono adattarsi a ambienti che vanno dal fondale dell'oceano a ambienti con alte temperature, oppure in ambienti estremamente rumorosi...

- *Mezzi di comunicazione*: la tecnologia *wireless* offre varie possibilità per effettuare una comunicazione per esempio utilizzando onde radio o raggi infrarossi o ancora sistemi laser. Un'opzione, per quanto riguarda l'utilizzo di comunicazioni con onde radio, è l'utilizzo delle bande *Industrial Scentific and Medical (ISM)*. I vantaggi principali introdotti sono: l'assenza di cablaggio, permettendo quindi di posizionare i sensori anche in luoghi difficili da raggiungere con esso oppure in ambiti dove l'aggiunta di uno o più cavi più risultare problematico. Le ISM sono utilizzate sia da WSN, ma anche da comunicazioni Wi-Fi (un particolare tipo di comunicazione *wireless* basata sullo standard IEEE 802.11), sono libere da licenza, hanno un grande spettro di allocazione e sono disponibili in tutto il mondo. Sono anche presenti alcuni svantaggi come: limitazione in potenza, interferenze dovute alle applicazioni già esistenti e sovraffollamento delle bande. Un altro tipo di comunicazione, in una rete di sensori, è quella a raggi infrarossi che hanno il vantaggio di essere robusti all'interferenza dei dispositivi elettrici, sono sistemi poco costosi e *license-free*. Lo svantaggio principale è che per comunicare richiedono la cosiddetta *line-of-sight*. I sistemi laser hanno una velocità molto elevata e vengono utilizzati per connettere dispositivi molto vicini tra loro. Lo svantaggio principale consiste nell'essere sensibili alle condizioni esterne e alle vibrazioni.

- *Consumo di energia*: i sensori utilizzati hanno una limitata sorgente di energia, per esempio una batteria, e questo limita la prestazioni dell'intera rete, ecco perché più risultare utile progettare i sensori con pannelli fotovoltaici o altri tipi di tecnologia in modo che essi siano indipendente per quanto riguarda l'approvvigionamento energetico [13].

1.3 Internet Of Things: architettura del protocollo

Spesso le soluzioni proposte, in ambito IOT, per connettere i vari oggetti assieme non tengono in considerazione aspetti riguardanti l'interoperabilità, la privacy e la sicurezza. Uno degli obiettivi del progetto europeo IOT-A, già citato in precedenza, è quello di creare un modello di architettura di riferimento per l'in-

teroperabilità dei sistemi IOT, in modo poi da potere sviluppare dei protocolli di standardizzazione e interfacce tenendo in considerazione anche fattori come la *privacy* e la sicurezza. L'approccio utilizzato è quello top-down partendo attraverso la definizione dei blocchi fondamentali riguardanti l'IOT per poi andare a analizzare ciascun blocco nello specifico.

Un esempio di modello generale per descrivere l'architettura del protocollo IOT è quello di definire dei blocchi riguardanti la sicurezza e altri che implementano funzioni come la *raccolta dell'informazione* dall'ambiente circostante, la *consegna dell'informazione* (utilizzando per esempio una WSN), *l'elaborazione dei dati* che consiste anche nel filtrare dati di poco interesse. L'architettura proposta dal progetto sopra citato è in Figura 1.2.

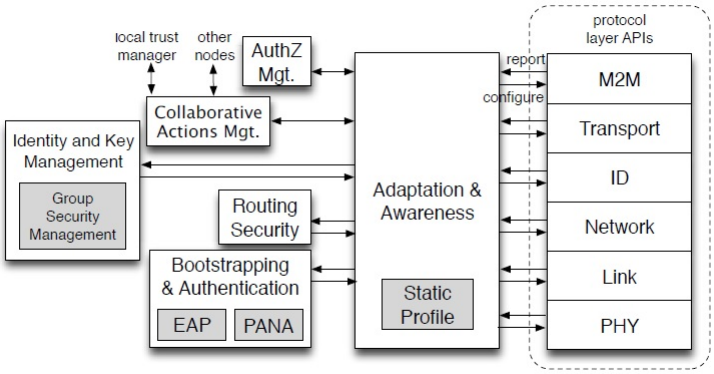

Figura 1.2: Architettura del protocollo IOT: la parte di destra gestisce la connessione dei dispositivi alla rete, la ricezione e la spedizione di pacchetti e esegue controllo d'errore e di congestione. La parte di sinistra gestisce la sicurezza e la crittografia della comunicazione

Nella figura 1.2 i blocchi che costituiscono l'architettura sono:

- *Machine-to-Machine (M2M)*: permette la comunicazione tra dispositivi di differenti reti o attraverso un linguaggio comune oppure attraverso la *traduzione* dell'informazione scambiata tra i dispositivi. Una possibile soluzione è quella di utilizzare un *proxy*. Inoltre grazie all'utilizzo di algoritmi decisionali è possibile dare una risposta a un possibile fenomeno fisico, in tempo reale, basandosi sui dati raccolti dai dispositivi ottenuti attraverso

il monitoraggio dell'ambiente in cui sono stati collocati. Nella figura 1.3 è rappresentato un esempio di una comunicazione M2M tra un dispositivo mobile e un computer, da notare il ruolo del *back-end server* che permette a due reti differenti — internet (rete *unconstrained*) e WSN (rete *constarined*) — di poter comunicare, questo grazie anche a un *proxy* che mette in relazione i due linguaggi utilizzati dalle diverse reti.

- *Transport (TRA)*: questo livello permette di garantire, tra sorgente e destinatario, una certo livello di prestazione in termini di consegna e affidabilità.

- *Identification(ID)*: questo livello permette di migliorare la sicurezza in quanto ha la funzionalità di individuare un nodo, sia per quanto riguarda la posizione all'interno della rete sia il tipo di dispositivo grazie all'ID del nodo stesso evitando così di autenticare nodi malevoli all'interno della rete.

- *Network (NET)*: gestisce l'indirizzamento dei nodi e l'instradamento dei pacchetti.

- *Link Layer (Link)*: questo livello gestisce l'accesso al mezzo trasmissivo e inoltre implementa un controllo dell'errore sul mezzo che connette tra loro due nodi.

- *Physical Layer (PHY)*: si occupa della trasmissione del segnale nel mezzo trasmissivo, quindi implementa modulazione, demodulazione e codifica di canale.

- *Bootstrapping and Authentication*: gestisce l'autenticazione dei nodi che vengono a aggiungersi nella rete. I protocolli utilizzati per quest'operazione sono: *Protocol for Carrying Authentication for Network Access (PANA)*, attraverso un server di autenticazione, oppure per garantire una maggiore operabilità è usato *Extensible Authentication Protocol (EAP)*.

- *Static Profile*: rappresenta le caratteristiche attraverso di endpoint per quanto riguarda le risorse di cui dispone in termini di dimensioni della memoria, di potenza di elaborazione, di ID. . . e delle impostazioni di sicurezza che intende utilizzare o che necessita dalla rete.

- *Collaborative Actions Management*: è utilizzato quando un nodo non riesce a eseguire un compito troppo impegnativo dal punto di vista computazionale. Quando viene richiesto l'aiuto di questo modulo viene stabilita una connessione criptata con il nodo in difficoltà.

- *Identity and Key Management*: fornisce una comunicazione sicura tra endpoint. Inoltre permette la comunicazione tra due nodi attraverso il protocollo AKE (Authenicated Key Exchange) che si basa su uno scambio di chiavi di sessione in modo che soltanto i due nodi coinvolti siano in grado di decriptare le informazioni che si scambiano.

- *Adaptation and Awarness*: questo blocco è responsabile della configurazione dello stack protocollare del nodo e della raccolta di informazioni riguardo il suo stato corrente.

- *Group Security Management*: questo blocco fa rispettare la sicurezza, in comunicazioni *multicast* o *broadcast*.

- *Routing Security*: è responsabile dell'implementazione di soluzioni con l'obiettivo di ridurre i cosiddetti *routing attacks*.

- *Authorization Management (AuthZ Mgt.)*: gestisce l'accesso in entrata e in uscita ai sevizi andando a controllare i certificati di accesso e gli utenti autenticati senza l'utilizzo di certificato [17].

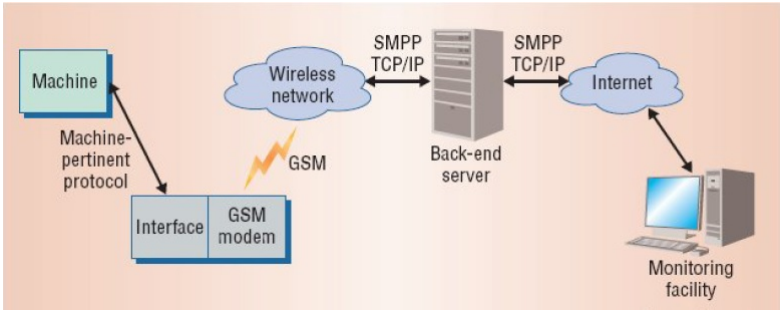

Figura 1.3: Rappresentazione schematica di un sistema M2M

Alcuni elementi da tenere in considerazione per quanto riguarda l'IOT:

- *Eterogeneità dei dispositivi*: quindi è necessario sviluppare un'architettura tale da poter gestire una comunicazione con elementi differenti.
- *Scalabilità*: il sistema è dinamico quindi è necessario considerare un possibile aumento(diminuzione) del numero di dispositivi connessi, delle dimensioni dell'ID identificativo, del numero di interconnessioni, del numero di servizi.
- *Ubiquità dei dati scambiati attraverso comunicazione wireless*: l'utilizzo della comunicazione tramite mezzo *wireless* permette ai dispositivi intelligenti di poter interagire, nella rete, con altri dispositivi.
- *Ottimizzazione del consumo di energia*: questo punto è dovuto alle limitazioni imposte dai dispositivi e per questo è necessario sviluppare e integrare in essi sistemi per l'accumulo di energia da fonti presenti nell'ambiente.
- *Localizzazione*: è possibile localizzare attraverso un ID i dispositivi collegati alla rete e quindi tracciarne le varie attività e spostamenti.
- *Gestione automatica dei dispositivi*: a causa di un numero elevato di dispositivi intelligenti è necessario che essi riescano a gestirsi in modo automatico (per esempio nel caso di piccoli guasti) così da rendere minimi gli interventi da parte dell'uomo.
- *Interoperabilità semantica*: è la capacità dei dispositivi di poter comunicare tra loro scambiandosi informazioni utili, filtrando quindi dati incoerenti o poco significativi.
- *Sicurezza e privacy*: a causa della forte relazione dell'IOT con il mondo reale è necessario che le comunicazioni siano sicure e venga preservata la *privacy* in quanto possono essere scambiati dati sensibili [5].

2

Tecnologia RFID

L'obiettivo di questo capitolo è quello di mettere a conoscenza il lettore di quanto sia importante la tecnologia RFID, andando a descrivere quali sono i dispositivi necessari per permettere questo genere di comunicazione e i protocolli caratterizzanti. Verrà infine effettuato un breve cenno sull'architettura RFID.

2.1 Introduzione

Una connessione onnipresente tra mondo reale e mondo virtuale, concetto che spesso viene associato a IOT, è resa possibile grazie a tecnologie di comunicazione *wireless* a bassa potenza; la tecnologia *wireless* è nota da decenni, ma doveva essere integrata in dispositivi di piccole dimensioni e non dotati di una fonte di energia a lunga durata, questo ha reso necessario lo studio di una nuova tecnica che si adattasse alle limitazioni imposte da questi oggetti.
In un primo momento, per quanto riguarda l'**identificazione** degli oggetti, venivano usati i codici a barre. Il principale svantaggio di questa tecnica è che la lettura richiede una *line-of-sight*, e inoltre, se il codice si usura, è molto difficile riuscire ad acquisire i dati con il lettore ed è necessario l'intervento umano.
Successivamente prese piede la tecnologia **Radio Frequency IDentification (RFID)**, che per quanto riguarda l'ambito dell'identificazione è la più diffusa. Inizialmente la RFID era utilizzata per il solo processo di identificazione, solo ultimamente questo sistema permette anche minime operazioni di *sensing*.
L'utilizzo di un sistema RFID si ha nei siti di stoccaggio per il tracciamento delle

merci in transito, oppure per la localizzazione del bestiame e degli animali selvatici, per il controllo degli accessi attraverso l'utilizzo di biglietti, *ski pass*...
I vantaggi della tecnologia RFID sono: maggiore quantità di dati immagazzinati nei *tag* rispetto ai dati immagazzinati nei codici a barre, tracciamento degli oggetti che integrano RFID, modifica delle informazioni presenti nei *tag*, non è richiesta una lettura *line-of-sight* e possono essere supportate più letture contemporanee, inoltre i *tag* si usurano molto meno rispetto ai codici a barre. Per quanto riguarda gli svantaggi della tecnologia RFID c'è da tenere in considerazione il fattore *privacy*; questo a causa dei molti dati immagazzinati e in circolazione, ma anche perché i *tag* sono facilmente tracciabili, inoltre non è possibile un utilizzo di tecniche di crittografia potenti a causa delle limitazioni imposte dai chip utilizzati all'interno dei *tag*.

Un sistema RFID è costituito da un *tag*, da un lettore e da un sistema informatico che permette di identificare l'oggetto a cui è associato un preciso e unico ID. Il *tag*, che è identificato da un ID codificato secondo un particolare standard, è costituito da un chip, un'antenna e dall'involucro esterno. I *tag* possono essere classificati in

- *Attivi*: hanno una batteria interna che permette di avere una maggiore velocità di trasferimento dei dati, ma allo stesso tempo ne limita il ciclo di vita. Le dimensioni di questi *tag* sono maggiori dei *tag passivi*, così come il loro costo. Possono iniziare la comunicazione.

- *Passivi*: non dispongono di una batteria interna, però riescono a ricavare l'energia di cui necessitano dal *reader*. Sono di piccole dimensioni e a basso costo.

- *Semipassivi*: dispongono di una batteria interna che alimenta il chip, ma non il trasmettitore. Non iniziano mai una comunicazione a causa della bassa quantità di energia di cui dispongono. Se interrogati dal *reader* si attivano e gli rispondono; generalmente il *tag* è spento.

- *Semiattivi*: dispongono di una batteria propria, però generalmente i *tag* sono disattivati e l'attivazione avviene tramite sollecitazione da parte del *reader*.

Un *reader* è quel dispositivo che permette di acquisire le informazioni dal *tag*. Il range di lettura dipende dalla frequenza utilizzata e dal tipo di *tag* [16].

Gli standard principali, utilizzati per codificare l'ID, sono quelli introdotti dall'*Auto-ID Center*, una partnership, fondata nel 1999, tra quasi 100 aziende conosciute in tutto il mondo, e sette università leader nella ricerca e quelli dell'*International Organization for Standardization (ISO)*. Prima di effettuare un confronto tra gli standard definiti dalle due organizzazioni è bene definire alcuni range di frequenza a cui essi fanno riferimento:

- *Low Frequency (LF)* range tra 30 kHz e 300 kHz. I *tag* che utilizzano queste frequenze sono molto piccoli e la distanza dal reader, per essere letti, è di circa un centimetro.
- *High Frequency (HF)* range tra 3 MHz e 30 MHz. Il range di lettura è individuato sulle decine di centimetri.
- *Ultra High Frequency (UHF)* range tra 300 MHz e 3 GHz. Consumo di potenza e range di lettura più alti.
- *Microonde* frequenze maggiori di 3GHz. Per quanto riguarda la dimensione dei dispositivi è più piccola quanto più elevata è la frequenza. Utilizzate per le lettura in velocità per esempio nei pedaggi, oppure per il tracciamento delle rotte delle navi... [4]

2.2 Gli standard RFID

Alcuni standard introdotti dall'organizzazione ISO sono:

- *ISO 14443 e 15693*: contiene le informazioni per garantire l'interoperabilità di dispositivi nelle frequenza 13.56 MHz e inoltre il metodo di registrazione dei dati e il loro utilizzo. **Near Field Communication (NFC)** si basa sullo standard ISO 14443.
- *ISO 18000*: contiene le informazioni, riguardanti i protocolli di comunicazione, usate per l'identificazione. Inoltre specifica come ottenere l'interoperabilità e la compatibilità di oggetti alle frequenze 135KHz, 13.56 MHz, 860-930 MHz e 2.45 GHz.

- *EPC (Electronic Product Code)*: è uno standard utilizzato per UHF, si basa su una codifica dell'ID di 64, 96 o 128 bit, in base al chip utilizzato.

2.2.1 Standard EPC

Per quanto riguarda la codifica dell'ID, nello standard EPC, i bit vengono suddivisi in 4 parti (considerando una codifica a 96 bit, figura 2.1):

1. *Intestazione 8 bit*: identifica la versione, il tipo, la struttura, la lunghezza della codifica.
2. *EPC Manager 28 bit*: identifica il produttore dell'oggetto.
3. *Object Class 24 bit*: memorizza tipo e categoria del prodotto.
4. *Serial Number 36 bit*: identifica in modo univoco il prodotto.

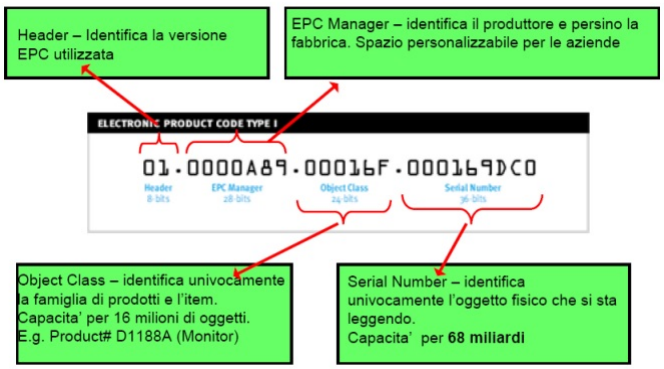

Figura 2.1: Codice EPC

Lo standard EPC è preferibile rispetto all'ISO 18000-6 tipo C in quanto permette di ottenere più identificativi in minor tempo, rendendo quindi molto pochi gli errori commessi. La suddivisione degli standard utilizzati, in base al range di frequenze è descritta in figura 2.2.

	LF	HF	UHF	Microwave
Freq. Range	125 - 134KHz	13.56 MHz	866 - 915MHz	2.45 - 5.8 GHz
Existing standards	11784/85, 14223	18000-3.1, 15693,14443 A, B, and C	EPC C0, C1, C1G2, 18000-6	18000-4

Figura 2.2: Suddivisione frequenze e standard RFID

Esistono varie versioni dello standard EPC:

- *Classe 0*: utilizzato da *tag* passivi, essi quando passano attraverso il campo generato dall'antenna del *reader* segnalano solo la loro presenza. Utilizzano le UHF. I dati sono scritti durante il processo di fabbricazione e non possono essere ulteriormente modificati.

- *Classe 1 Gen1*: utilizzato da *tag* passivi, essi quando passano attraverso il campo generato dall'antenna del *reader* segnalano solo la loro presenza. Utilizzano HF - UHF. Le memorie dei *tag* sono **write-one, read-many (WORM)**

- *Classe 1 Gen2*: sono utilizzati da *tag* passivi. Questa classe è stata realizzata con lo scopo di creare un unico standard globale in modo da renderlo conforme allo standard ISO. Le frequenze utilizzate sono le UHF. Le memorie dei *tag* sono WORM.

- *Classe 2*: lo usano i *tag* passivi, semipassivi e attivi, con frequenze UHF. Le memorie dei dispositivi sono riscrivibili e oltre alle proprietà della classe 1 è presente la proprietà di crittografia, autenticazione in lettura, di riutilizzo delle caratteristiche, può essere presente una fonte di energia per alimentare il *tag* e eventuali sensori presenti in esso.

- *Classe 3*: lo usano i *tag* semi-passivi o attivi con sensori. Quando il *reader* legge il *tag* riceve anche i dati riguardanti le grandezze misurate. Le memorie dei *tag* sono *read* e *write*.

- *Classe 4*: lo usano i *tag* attivi. Grazie alla presenza della batteria possono comunicare senza essere attivati dal *reader*. Le memorie dei *tag* sono *read* e *write*.

- *Classe 5*: lo usano i *tag* attivi. I *tag* che utilizzano questa classe di EPC hanno le stesse caratteristiche di quelli che utilizzano la classe 4, inoltre è implementata la possibilità di comunicare con *tag* passivi [16].

2.3 Architettura RFID

Un sistema RFID può essere schematizzato come in Figura 2.3. I *tag* vengono interrogati dal *reader* che invia un'enorme quantità di dati a un *Middleware* o *Savant*, esso ha il compito di filtrare, eventualmente contare e aggregare i vari dati per poi inviarli al servizio **Object Name Server (ONS)**. Il *Middleware* è costituito da due interfacce: *interfaccia reader* che permette la cooperazione tra tutti i *reader* connessi al software, e *l'interfaccia applicazione* che permette la comunicazione con le interfacce esterne. Il ruolo del servizio ONS è quello di o associare a ogni codice EPC le informazioni annesse al *tag*, o fornire l'IP del server che le contiene in formato *PML (Physical Markup Language)*. Il linguaggio PML si basa sul linguaggio XML, ed è utilizzato per descrivere le informazioni (locazione, caratteristiche dell'oggetto, tracciamento) del *tag* associate a un preciso EPC [2, 16].

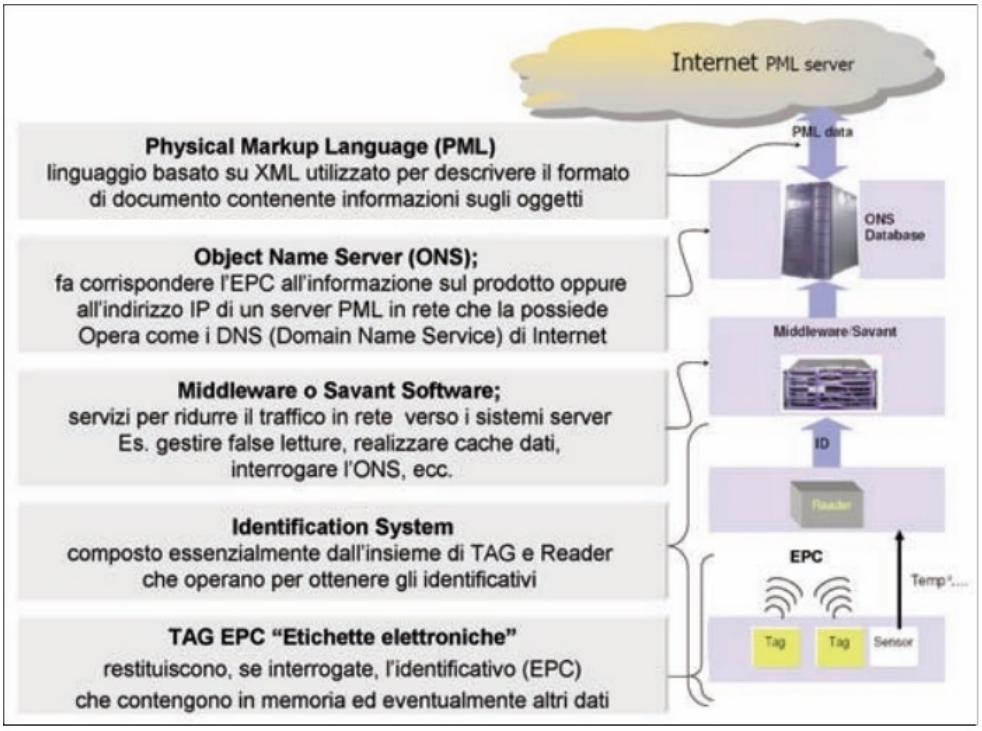

Figura 2.3: Architettura del sistema RFID

3

Tecnologia NFC

In questo capitolo verrà analizzata la comunicazione NFC, che deriva dalla tecnologia RFID. Verranno messe in luce le differenze rispetto all'RFID e descritte le caratteristiche della tecnologia NFC, inoltre verrà illustrata l'architettura NFC proposta da una delle più importanti organizzazioni *no-profit* (NFC Forum).

3.1 Quadro generale

La tecnologia *wireless* **Near Field Communication (NFC)** è un'evoluzione della tecnologia RFID, in cui, a differenza di quest'ultima, non c'è né distinzione tra *reader* e *tag* né distinzione tra dispositivi attivi passivi, ed è utilizzata la sola frequenza operativa di 13.56 MHz. Le altre caratteristiche della comunicazione NFC sono:

- distanza operativa al massimo di 10 cm
- *bitrate* con velocità massima di 424 Kbit/s

L'utilizzo di questa tecnologia è soprattutto per operazioni di *ticketing*, pagamenti sicuri, collegamenti *peer-to-peer* e per effettuare collegamenti con altri oggetti dotati di chip integrato NFC come per esempio stampanti, poster, televisioni... [16, 18]
La tecnologia NFC può essere per esempio utilizzata per attivare automaticamente il GPS sul proprio cellulare ogni volta che si sale in macchina, oppure per

attivare, sempre in modo automatico, la modalità *mute* quando si entra in camera da letto oppure se c'è una locandina, equipaggiata con chip NFC, di un film appena uscito al cinema è possibile avvicinare il proprio dispositivo (cellulare, tablet,...) a essa e scaricare così il trailer del film.
Il ruolo della *Near Field Communication* è quello di rendere la comunicazione, tra i due dispositivi, sicura.
Rispetto alla tecnologia RFID in NFC i dispositivi possono operare in modalità passiva, fornendo le informazioni richieste al *reader*, senza però avviare una comunicazione — i dispositivi passivi non dispongono di una fonte di energia propria; questa è una comunicazione tipo attivo-passivo o *read/write* — in modalità attiva, in cui i due dispositivi si scambiano tra loro i dati — comunicazione tipo attivo-attivo o *peer-to-peer* — oppure in modalità *Emulation Card* dove il dispositivo appare ai *reader* come un *ticket* o una *card*, permettendo operazioni di pagamento sicuro o di *ticketing*. Nella modalità *peer-to-peer* se deve essere inviata una grande quantità di dati è possibile utilizzare una connessione secondaria con un alto *rate* utilizzando differenti standard come per esempio *Bluetooth o WiFi* [18]. In una comunicazione NFC i *tag* sono classificati in:

- *Initiator*: è il dispositivo che ha inviato la richiesta.

- *Target*: è il dispositivo che ha risposto alla richiesta dell'*Initiator*.

Un'altra classificazione dei *tag* è rappresentata in figura 3.1, i cui sono individuati 4 tipi di *tag* in base agli standard *ISO 14443 Type A*, *ISO 14443 Type B* e *ISO 18092* da parte di NFC Forum[1]. Gli standard sono riconosciuti da *ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), ETSI (European Telecommunications Standards Institute) e ECMA (European Computer Manufacturers Association)*. NFC Forum è una delle più importanti organizzazioni per lo sviluppo, la divulgazione, implementazione è la standardizzazione della tecnologia NFC, è un'organizzazione senza scopo di lucro, nata nel 2004, che vanta più di 190 aziende tra i suoi membri, tra esse Nokia, Sony, Google, Intel... [8]

[1] http://www.nfc-forum.org

	Standard	Capability	Memory	Data rate	Notes
Type 1	ISO14443A	Read Rewrite	96 bytes, expandable to 2 kbytes	106 kbit/s	Simple, cost effective and ideal for many NFC applications
Type 2	ISO14443A	Read Rewrite Read only	48 bytes, expandable to 2 Kbytes	106 kbit/s	
Type 3	ISO 18092 FeliCa	Read Rewrite	2 Kbytes	212 kbit/s	Higher cost, more complex applications
Type 4	ISO14443A and B	Read Rewrite Read only Configured at manufacture	32 kbytes	Between 106 kbit/s and 424 kbit/s	

Figura 3.1: Classificazione dei *tag* NFC, secondo NFC Forum

3.2 Architettura NFC

Nel 2006 NFC Forum ha divulgato la sua prima *release* dell'architettura NFC (Figura 3.2) che è orientata all'interoperabilità. Gli standard caratteristici di NFC sono:

- *ISO 14443 Type A/ Type B*: standard che regolano la tecnologia *proximity card*, essa fa riferimento a *card* che per essere lette non necessitano di essere inserite in un *rader*, ma possono operare a distanza (la distanza massima è inferiore ai 10 cm e la frequenza a cui lavorano è di 13.56 MHz). La differenza tra *Type A* e *Type B* riguarda i metodi utilizzati per la modulazione, la codifica dei bit e per quanto riguarda i protocolli anti-collisione. Questi standard regolano la modalità di comunicazione *read/write*.

- *ISO 18092*: descrive in modo equivalente il protocollo NFCIP-1 (NFC *Interface and Protocol*), e definisce le regole per la comunicazione *peer-to-peer*. Questo standard definisce il tipo di modulazione, la codifica, il formato dei dati, la velocità di trasferimento dei pacchetti e i metodi anti-collisione.

- *FeliCa*: è lo standard (non approvato dall'ISO) creato da Sony: è un'estensione del protocollo ISO 14443. Utilizzato soprattutto in sistemi di pagamento elettronico.

- *ISO 21481*: questo standard è equivalente al protocollo NFCIP-2 e ha il compito di definire le regole di *switch* tra gli standard ISO 14443, ISO 18092 e FeliCa. Il *Mode Switch* fa riferimento a questo standard [16, 18].

L'architettura è costituita dal livello fisico RF layer, il quale è definito dai vari protocolli descritti in precedenza, e sopra di esso si trovano il protocollo di *switch* e i vari protocolli di alto livello che comunicano con il livello applicazione.
I protocolli di alto livello sono:

- *LLCP (Logical Link Control Protocol)*: è un protocollo (di livello 2) progettato per supportare applicazioni con limitate richieste di traffico o per protocolli di rete come IP o protocolli di livello 5,7 come OBEX (OBject EXchange). LLCP migliora le funzionalità di base definite dallo standard ISO 18092 per le applicazioni *peer-to-peer*.

- *RTD (Record Type Definition) & NDEF (NFC Data Exchange Format)*: NDEF è uno standard per la definizione del formato dei dati scambiati dai *tag*. Ciascun messaggio viene suddiviso in record.
  RTD definisce la struttura dei record e il tipo di record, e quest'ultimo aspetto identifica il significato semantico del dato. RDT permette quindi di definire una struttura per l'identificazione del tipo di dato in un messaggio NDEF. I tipi di *tag* definiscono come i messaggi NDEF sono letti e come sono scritti dai dispositivi [1].

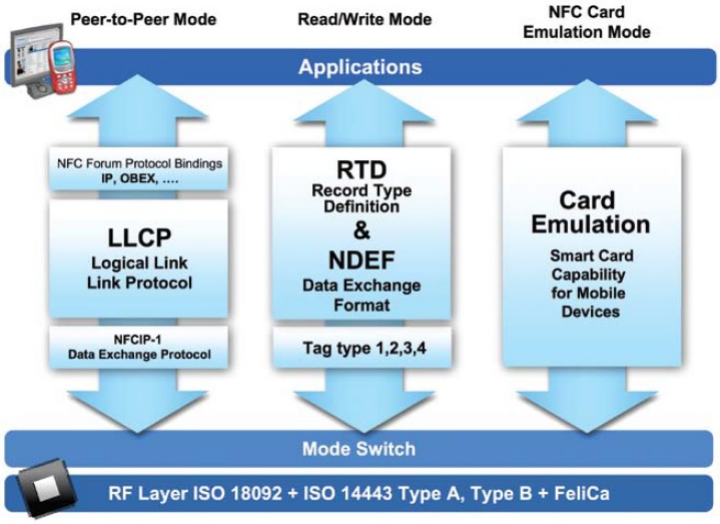

Figura 3.2: Architettura NFC secondo NFC Forum

Un esempio di utilizzo di questa architettura si ha quando con un cellulare si vuole effettuare un pagamento in un supermercato. Per prima cosa è necessario che le due parti (cellulare e dispositivo del supermercato) siano abilitate alla comunicazione NFC.
Per quanto riguarda la struttura del cellulare ci deve essere un modulo NFC che da una parte permette la comunicazione NFC — quindi gestisce il modo in cui avviene la comunicazione, formato dei dati e tipo dei record, e definisce le regole crittografiche — e dall'altra interagisce con la SIM, che può essere considerata come un piccolo conto in banca, per poter comunicare con il sistema di pagamento del supermercato. Quando lo *smartphone* è avvicinato alla *pay station* verrà richiesto un codice PIN e dopo il suo inserimento la transizione monetaria sarà eseguita.
La tecnologia NFC integrata negli *smartphone* sta avendo una crescita notevole, come si può vedere in figura 3.3, e i campi di utilizzo di questa comunicazione sono tra i più svariati: dal tracciamento delle merci, all'ambito medico oppure a quello dei sistemi antifurto...

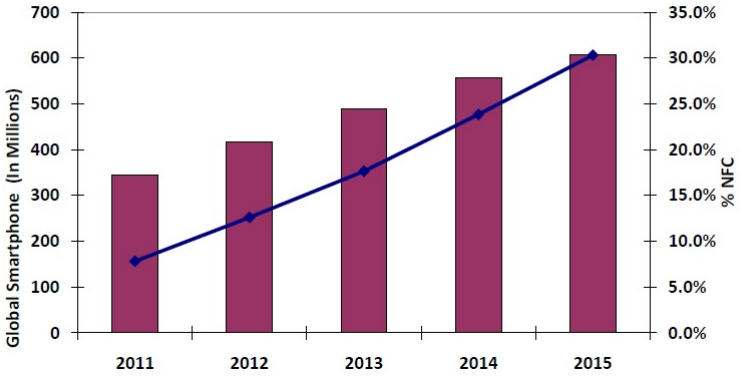

Figura 3.3: Previsione dell'integrazione della tecnologia NFC negli *smartphone*. [Fonte: Nokia]

4

Sicurezza

In questo capitolo verrà presentata una breve discussione sul tema della sicurezza che interessa un sistema IOT, ma anche le tecnologie a esso connesse: WSN, RFID, NFC. Si descriveranno alcuni attacchi informatici che possono essere compiuti seguiti poi da una discussione sulle possibili tecniche da adottare per evitarli.

Lo sviluppo di queste tecnologie WSN, RFID, NFC porta ad avere una grande quantità di dati disponibile su qualsiasi persona/oggetto presente nel mondo. Come conseguenza di questa enorme disponibilità di informazioni si ha la presenza di tentativi illeciti volti a carpire questi dati. Ad esempio i *tag* possono essere usati per localizzare gli spostamenti di una persona e capire quando non è in casa per effettuare il furto, oppure è possibile localizzare oggetti di valore, magari in transito da uno stabile a un altro, in modo da poter capire quando effettuare il colpo... Altri usi illegali potrebbero essere la modifica di dati all'interno dei *tag*, la sottrazione di dati sensibili per creare una profilazione di una persona o di un'azienda... I dispositivi che vogliono effettuare l'attacco approfittano del fatto che la comunicazione è *wireless* per effettuare azioni di *eavesdropping*, ma sfruttano anche l'assenza di algoritmi sofisticati e potenti per proteggere i dati a causa delle limitate risorse, dei nodi della rete, in termini di capacità di calcolo, memoria, approvvigionamento energetico... a disposizione dei sensori. I principali problemi legati alla sicurezza sono l'autenticazione — essa non sempre può essere utilizzata perché è necessario che i dispositivi scambino un determinato numero di messaggi con i server e non tutti i dispositivi hanno le capacità di farlo —

l'integrità dei dati — essa fa riferimento al trasferimento dei dati dalla sorgente al destinatario in modo sicuro, senza che essi vengano modificati lungo il tragitto — la confidenzialità, che fa riferimento al servizio per mantenere la segretezza di dati importanti inviati, utilizzando tecniche di criptazione.

Per proteggere i dati e evitare che azioni illecite vadano a buon fine alcune operazioni da compiere possono essere: l'utilizzo della crittografia per la creazione di un canale di comunicazione sicuro oppure la richiesta di PIN d'accesso per leggere, modificare e copiare i dati.
I principali attacchi che mettono in pericolo la sicurezza in una comunicazione *wireless* sono:

- *Eavesdropping*: questo fenomeno si presenta quando, per esempio, due dispositivi stanno comunicando tra loro e un terzo, in modalità di ascolto, si mette a intercettare i dati scambiati. Un fattore da tenere in considerazione è la distanza a cui deve essere posto il dispositivo che vuole effettuare l'attacco. La distanza dipende da fattori come: dimensioni, geometria dell'antenna del dispositivo attaccante, ambiente circostante, potenza utilizzata dall'emittente per trasmettere l'informazione, ma soprattutto dipende dalla tecnologia utilizzata per effettuare la comunicazione... Un aspetto da considerare è che il dispositivo attaccante non è necessario che riceva tutti i dati della comunicazione, ma può bastare anche una certa percentuale di essi per poter carpire i dati a lui interessati.
  Creando un canale sicuro è possibile evitare il fenomeno dell'*eavesdropping*. In un canale sicuro c'è lo scambio di chiavi di cifratura. In un primo momento i dati sono cifrati con una chiave A, poi vengono inviati al ricevitore che li decifra con una chiave B. Ci possono essere due tipi di algoritmi: simmetrici (quando le chiavi A e B sono identiche o in relazione reciproca) o asimmetrici (quando le chiavi A e B sono diverse o non sono in relazione reciproca).

- *Alterazione dei dati*: in questo caso il dispositivo che effettua l'attacco disturba la comunicazione, inviando dati che bloccano il canale oppure che creano confusione, in modo che il ricevitore non sia in grado di capire i dati inviati dal trasmettitore. Questo attacco può essere rilevato ascoltando

ciò che avviene nell'ambiente circostante, e analizzando le varie potenze di trasmissione infatti affinché questo attacco vada a buon fine è necessario utilizzare un'elevata potenza.

- *Modifica dei dati*: in questo caso il dispositivo che effettua l'attacco modifica i dati inviati in modo che vengano ricevuti dal ricevitore e considerati validi. Per effettuare questo genere di attacco è necessario conoscere la tecnica di modulazione e quella di decodifica. Per proteggersi da questo attacco si utilizza la tecnica del canale sicuro.

- *Inserimento di dati*: questo attacco è possibile se la risposta del ricevitore richiede un lungo tempo. Se è così, un *attaccker* può inserire un falso messaggio (considerato valido) prima della risposta del ricevitore. Per proteggere la comunicazione da questo attacco si può ridurre il tempo di attesa per la risposta, creare un canale sicuro oppure ascoltare il canale in modo da poter individuare l'eventuale attacco.

- *Attacco "man-in-the-middle"*: è un attacco in cui il dispositivo attaccante si posiziona in mezzo ai due dispositivi che stanno comunicando, fingendosi prima il trasmettitore e poi il ricevitore, oppure possono essere usati due dispositivi attaccanti con le funzioni di trasmettitore e di ricevitore. Ad esempio si può considerare che un nodo A voglia autenticare altri dispositivi nella rete e un dispositivo attaccante voglia rubare l'identità di un nodo B. L'elemento attaccante è costituito da due ricetrasmettitori, uno vicino ad A, chiamato B', e un secondo vicino a B chiamato A'. L'obiettivo dell'elemento attaccante è quello di far credere ad A che B' sia B, e a B che A' sia A.
  Il nodo B' trasmetterà il segnale ricevuto dal nodo A, al nodo A' che a sua volta lo trasmetterà al nodo B. Il nodo A risponderà, al segnale identificativo, inviando la sua identificazione. Il nodo A' riceverà la risposta del nodo A, che trasmetterà poi a B' il quale la invierà ad A. Sia il nodo A sia il nodo B non riusciranno a capire che i segnali ricevuti sono in realtà inviati da dispositivi attaccanti, in quanto essi replicano perfettamente il segnale captato. Dopo questa procedura il nodo A garantirà l'accesso al nodo B' avendolo scambiato per il nodo B.

Per proteggersi da questo attacco si può allestire un canale di comunicazione sicuro [6, 12, 16, 18, 19].

In questo capitolo è stata introdotta una breve discussione sulla sicurezza in un sistema IOT; una trattazione dettagliata del tema, che esula dall'obiettivo di questo elaborato, avrebbe richiesto molte più pagine di quante ne sono state dedicate in questa sede.

5

Conclusioni

In questo elaborato si è presentato il concetto di *Internet Of Things*, assieme a una tipologia di architettura, inoltre sono state descritte le tecnologie che hanno permesso un notevole sviluppo e diffusione come WSN,RFID e NFC. Infine è stata fatta una discussione concisa sul tema della sicurezza nei sistemi IOT.
Alcuni esempi di integrazione (o di futuro impiego) tra oggetti e tecnologie WSN, RFID e NFC sono:

- *Case intelligenti*: l'utilizzo della tecnologia IOT all'interno di edifici può migliorare i consumi di risorse come acqua, luce, gas... inoltre possono essere evitati incidenti domestici attraverso il monitoraggio dei vari oggetti. L'impiego dei sensori negli edifici serve anche a migliorare le condizioni di vita per esempio attraverso la regolazione automatica del riscaldamento, della luce... in base all'orario del giorno e delle condizioni atmosferiche.

- *Città intelligenti*: in questo caso l'utilizzo della tecnologia IOT è usato per migliorare situazioni di probabili congestioni dovute al traffico, ad esempio avvertendo gli automobilisti che si stanno dirigendo nella zona critica, oppure per dare indicazione della presenza di parcheggi liberi in quella zona, rilevare i livelli di inquinamento presenti nella città, immagazzinare energia solare in dispositivi presenti sulle strisce pedonali o sull'asfalto per poi alimentare i lampioni presenti a bordo strada, oppure ancora per segnalare eventuali contravvenzioni, presenza di incendi...

- *Sanità*: all'interno di questo ambito l'utilizzo di sensori è utile per rilevare dati riguardanti il paziente, utili per il medico, come: temperatura, pressio-

ne sanguigna, attività respiratoria, presenza di particolari disfunzionamenti, farmaci assunti in precedenza, allergie, intolleranze...
Un esempio di tecnologia NFC in questo settore si può avere nel pagamento del *ticket* allo sportello.

- *Sorveglianza*: l'utilizzo di sensori è utile per sorvegliare la propria abitazione, e in caso di pericolo, essi possono inviare un segnale d'allarme sia ai padroni sia alla stazione di polizia. Un altro utilizzo è quello di inviare un SMS al proprietario, non presente nell'abitazione, se un particolare oggetto (un vaso prezioso, un computer...), quando quest'ultimo viene spostato da una determinata area.

- *Sport*: i sensori sono spesso usati per indicare all'arbitro eventuali sviste nell'assegnazione dei punteggi, dati utili per gli allenatori...

- *Tracciamento*: in questo ambito sono inclusi i tracciamenti di merci per permettere di capire il percorso effettuato da quel tipo di oggetto, eventuali danni subiti, livello di umidità dell'ambiente in cui è presente l'oggetto...oppure per questioni di sicurezza è necessario monitorare il percorso effettuato da un determinato individuo [13–15].

Con la presenza di oggetti intelligenti negli edifici, nelle città, nella sanità... aumenta notevolmente la mole di dati disponibili in rete. Per assicurare la *privacy* delle persone è utile che alcuni dati, necessari temporaneamente, vengano poi eliminati dal sistema o vengano resi anonimi per evitare eventuali rischi. In una rete IOT è utile che ci sia un sistema di elaborazione centrale di tipo *cloud* in modo che altri dispositivi possano accedere a questo sistema e utilizzare le informazioni archiviate, senza dover ogni volta elaborare i dati raccolti per arrivare a un risultato già ottenuto.
Alcune interessanti sfide ancora aperte nell'ambito dell'IOT riguardano alcune caratteristiche dei sensori, che vengono dislocati nell'ambiente per monitorarlo, ad esempio essi devono avere un basso costo, possedere una struttura non complicata in modo da poterli riparare rapidamente e essere abilitati a approvvigionarsi l'energia necessaria per compiere le funzioni richieste. L'utilizzo di fonti energetiche rinnovabili, come ad esempio l'energia solare, è un interessante ambito di ricerca, questo perché permette ai sensori di avere maggiore autonomia e rendere

minimo l'intervento dell'uomo su di essi (viene evitato l'intervento per il cambio della batteria, quando questa se è esaurita).
Un'altra sfida è il miglioramento dell'affidabilità delle reti, sia dal punto di vista della sicurezza, della *privacy*, ma anche tecnologico e della scalabilità. Con l'aumento di dispositivi connessi alla rete è necessario studiare dei metodi di compressione dei dati (oppure metodi per fondere assieme delle informazioni simili e eliminare la ridondanza), in modo da evitare sia fenomeni di rallentamento dovuti all'incremento del traffico, sia periodi lunghi di trasmissione dei dati che provocando un dispendio di energia notevole dei vari dispositivi. Inoltre è necessario progettare algoritmi di instradamento adeguati e strutture tali da supportare l'aumento della quantità di dati e di dispositivi connessi. Per quanto riguarda la sicurezza è necessario definire dei metodi che permettano di salvaguardare la sicurezza in un sistema IOT attraverso l'utilizzo di un'identificazione preventiva e di protezione contro i vari attacchi informatici. Una sfida che riguarda la *privacy* è quella di migliorare gli standard, le metodologie e gli strumenti per la gestione dell'identità degli utenti e degli oggetti.
In un sistema IOT c'è però un problema che riguarda il livello di trasporto che ha il compito principale di garantire l'affidabilità *end-to-end* ed eseguire il controllo di congestione *end-to-end*. Nella rete internet il protocollo, al livello di trasporto, è il TCP (*Transmission Control Protocol*), esso però non è adeguato per un sistema IOT — è quindi necessario cercare di creare un protocollo che vada a sostituire il TCP nel caso di sistemi IOT — infatti:

1. Usando il protocollo TCP per ciascuna connessione deve essere avviata una **procedura di *setup***. Questa procedura in un sistema IOT non è necessaria perché vengono scambiate piccole quantità di dati (conseguentemente la durata della comunicazione è ridotta), mentre se si esegue questa procedura di *setup* gran parte della comunicazione è occupata da essa, inoltre i dati inviati in questa fase iniziale della comunicazione devono essere elaborati e trasmessi dai dispositivi che spesso hanno limitate risorse in termini di energia.

2. Il protocollo TCP esegue il **controllo di congestione** *end-to-end* e spesso la quantità di dati scambiati risulta molto piccola, risulta quindi essere un controllo superfluo oltre che svantaggioso per le prestazioni del sistema.

3. Il protocollo TCP richiede che siano presenti dei ***buffer* di memoria**, sia al trasmettitore che al ricevitore, in modo da poter immagazzinare i dati così in caso di trasmissione errata possono essere ritrasmessi. La gestione di questi *buffer* richiede risorse, in termini di energia, a dispositivi che ne hanno una disponibilità limitata o nulla [15].

Glossario

Broadcast tipo di trasmissione in cui un pacchetto inviato da un terminale verrà consegnato a tutti i dispositivi connessi alla rete., 13

Interoperabilità capacità di due o più sistemi, reti, mezzi, applicazioni o componenti, di scambiare informazioni tra loro e di essere poi in grado di utilizzarle., 3

IP È il protocollo attraverso il quale i dati vengono inviati da un computer all'altro in Internet. Ogni computer collegato a Internet ha almeno un IP-address che lo identifica univocamente., 19

ISO ente internazionale, con sede a Ginevra, che ha il compito di armonizzare le norme emanate dagli enti di normazione delle varie nazioni relativamente alle procedure tecniche e metrologiche; le direttive così stabilite internazionalmente sono dette norme ISO., 17

Metadato è un'informazione utilizzata per dare altre informazioni su altri dati., 2

Middleware generalmente si tratta di software con un ruolo di mediazione tra i dati e le informazioni elaborate a livello centrale e ciò che viene gestito direttamente a livello di interfaccia con l'utente., 7

Multicast tipo di trasmissione in cui un pacchetto inviato da un terminale verrà consegnato a un gruppo di dispositivi connessi alla rete., 13

OBEX protocollo utilizzato per comunicazioni *Bluetooth* o *Infrared*, esso ha il compito di gestire la sessione di comunicazione tra i dispositivi e di definire il *server* OBEX e il *client* OBEX per migliorare l'interoperabilità. Quando il *server* riceve un comando dal *client*, si crea una sessione in cui *server* e *client* interagiscono tra loro, 24

Ontologia è un'esplicita specificazione, sia del significato che del legame tra i vari concetti, di una concettualizzazione., 2

Proxy server in generale il proxy server è server situato tra una applicazione client e un server effettivo. Con lo scopo di migliorare le *perfomance* del sistema, filtrare le richieste di file, connessioni, pagine web o altre risorse disponibili in server differenti., 11

Rete ad-hoc è una rete che permette a più terminali di collegarsi tra loro senza l'utilizzo di un access point(AP)., 8

Rete constrained rete caratterizzata da un basso rate di trasferimento dati, < 1 Mbit/s, con presenza di alti livelli di latenza dovuti al basso rate della tecnologia del livello fisico e al periodico spegnimento dei nodi che costituiscono la rete per risparmiare energia, visto la limitata disponibilità della stessa., 11

Rete unconstrained rete caratterizzata da collegamenti a alta velocità, è la cosiddetta rete cablata. Le latenze sono dovute principalmente a possibili congestioni del traffico., 11

Routing è il processo che consiste nel selezionare un percorso in una rete attraverso il quale inviare i pacchetti., 6

Service Oriented Architecture (SOA) è un modello architetturale che si basa sulla cooperazione tra varie applicazioni (dette servizi) che risiedono su più computer differenti, presenti in una rete, con lo scopo di realizzare servizi più complessi., 7

URI (Uniform Resource Identifier) è una stringa di caratteri usata per identificare un nome o una risorsa web. Esso è costituito dall'unione dell'URL (Uniform Resource Locator) che permette di identificare una risorsa con un link e dell'URN (Uniform Resource Name) che permette di identificare una risorsa con il suo nome (ad esempio un codice identificativo)., 2

XML (eXtensible Markup Language) è un linguaggio che permette, attraverso delle annotazioni nel testo, di codificare il documento in modo che sia leggibile sia dall'uomo che dalle macchine., 1

Bibliografia

[1] NFC Forum Technical Specifications. URL: http://www.nfc-forum.org/specs/spec_list/.

[2] *Architecture design and performance evaluation of RFID object tracking systems*. 30 June 2007. URL: http://www.sciencedirect.com/science/article/pii/S0140366407001387.

[3] Navas Azeez. *Seminar report on "WEB 3.0"*. Retrieved: 10 August 2013. URL: http://www.seminarpaper.com/2011/12/seminar-report-on-web-30.html.

[4] Alessandro Ciasullo. "Un sistema di identificazione basato sulla tecnologia RFID". A.Y. 2005/2006. URL: http://www.rfid.fub.it/edizione_2/rfid_fondamenti_tecnologia_2.htm.

[5] Francesco De Pellegrini Daniele Miorandia Sabrina Sicari Imrich Chlamtac. *Internet of things: Vision, applications and research challenges*. Sept. 2012. URL: http://www.sciencedirect.com/science/article/pii/S1570870512000674.

BIBLIOGRAFIA

[6] E Haselsteiner, K Breitfuß. *Security in near field communication (NFC)*. 2006. URL: http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf.

[7] W3C Frank Manola Eric Miller. *RDF Primer*. 10 February 2004. URL: http://www.w3.org/TR/2004/REC-rdf-primer-20040210.

[8] *Getting Started With NFC*. Published online: 13 June 2013. URL: www.digikey.com/us/en/techzone/wireless/resources/articles/getting-started-with-nfc.html.

[9] W3C OWL Working Group. *OWL 2 Web Ontology Language Document Overview (Second Edition)*. 11 December 2012. URL: http://www.w3.org/TR/owl2-overview.

[10] W3C SPARQL Working Group. *SPARQL 1.1 Overview*. 8November 2012. URL: http://www.w3.org/TR/2012/PR-sparql11-overview-20121108.

[11] Jim Hendler. *Web 3.0 Emerging*. 20 January 2009. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4755170.

[12] Ian Poole. *NFC Near Field Communication Tutorial*. Retrieved: 28 August 2013. URL: http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php.

[13] Y. Sankarasubramaniam I.F. Akyildiz W. Su E. Cayirci. *Wireless sensor networks: a survey*. March 2002. URL: http://www.sciencedirect.com/science/article/pii/S1389128601003024.

[14] Slaven Marusic Jayavardhana Gubbi Rajkumar Buyya Marimuthu Palaniswami. *Internet of Things (IoT): A vision, architectural elements, and future directions*. Sept. 2013. URL: http://www.sciencedirect.com/science/article/pii/S0167739X13000241.

[15] Antonio Iera Luigi Atzori Giacomo Morabito. *The Internet of Things: A survey*. Oct. 2010. URL: http://www.sciencedirect.com/science/article/pii/S1389128610001568.

[16] Giuseppe Russo Paolo Talone. *RFID Fondamenti di una tecnologia silenziosamente pervasiva*. 2008. URL: http://www.rfid.fub.it/edizione_2/rfid_fondamenti_tecnologia_2.htm.

[17] Michele Rossi et al. *D3.6 - IoT Protocol Suite definition*. IOT-A. 11 June 2013.

[18] *The Keys to Truly Interoperable Communications*. 31 October 2007. URL: http://www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf.

[19] Yun Zhou, Yuguang Fang, Yanchao Zhang. *Securing wireless sensor networks: a survey*. 16 September 2008. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=%5C&arnumber=4625802.