Editore
Telecom Italia S.p.A.

Direttore responsabile
Michela Billotti

Direttore tecnico
Roberto Saracco

Comitato di direzione
Alessandro Bastoni, Francesco Cardamone, Gianfranco Ciccarella, Oscar Cicchetti, Sandro Dionisi, Stefano Nocentini, Fulvio Parente, Cesare Sironi, Luca Tomassini

Segreteria di redazione
Carla Dulach

Contatti
Via di Val Cannuta, 250 - 00166 Roma
tel. 0636885308
notiziario.redazione@telecomitalia.it

Progetto grafico e impaginazione
Marco Nebiolo

Stampa
Tipografia Facciotti
Vicolo Pian Due Torri, 74 - 00146 Roma

Registrazione
Periodico iscritto al n. 00322/92 del Registro della Stampa presso il Tribunale di Roma in data 20/05/1992

ISSN 2038-1921

Il Notiziario Tecnico è disponibile anche online: ***www.telecomitalia.it*** (Canale Innovazione)

Chiuso in tipografia - 06 aprile 2010

In copertina scatto artistico di ***Giuseppe La Barbera***
"El Caminito": via del quartiere Boca di Buenos Aires

Carta ecologica riciclata
Fedrigoni Symbol Freelife Satin
Prodotto realizzato impiegando carta certificata FSC Mixed Sources COC-000010.
Prodotto realizzato impiegando carta con marchio europeo di qualità ecologica Ecolabel - Rif. N° IT/011/04.

NOTIZIARIO TECNICO
TELECOM ITALIA

Anno19 NumeroUNO Dicembre2010

Guardare oltre

L'immagine della copertina di questo numero, frutto della partecipazione al nostro concorso del collega Giuseppe La Barbara che ha fatto questo scatto nella strada "El Caminito" di Buenos Aires, è l'emblema della nostra posizione editoriale: "guardare oltre". Per seguire, raccontare, vivere l'innovazione non si può di certo rimanere "con le finestre chiuse", ma è essenziale tenerle ben spalancate, magari per meglio sporgersi nell'osservare cosa succeda intorno a noi.

Il Notiziario tecnico, da sempre riflesso del "nuovo" di Telecom Italia, su questo numero presenta le tecnologie di neuromarketing, che, partendo dall'analisi celebrare e dai sensori biometrici, hanno come obiettivo la valutazione delle risposte sensomotorie, cognitive ed emotive delle persone agli stimoli di marketing; il tutto come ipotizzabile miglioramento dei servizi offerti ai nostri clienti.

Il tema dello "shopping", basato però sul m-payment, è anche oggetto dell'articolo sulla sperimentazione in corso tra Telecom Italia e la Miroglio Fashion, che permette ai clienti degli outlet "Vestebene Factory Store" di raccogliere i punti fedeltà attraverso il telefono cellulare dotato di tecnologia radio a corto raggio NFC (Near Field Communication), visualizzarne il saldo direttamente sul display e riceverne i bonus via sms.

Il tema delle NFC è anche oggetto di una scheda tutorial; da questo numero infatti la Redazione ha scelto di presentare un approfondimento, scritto in modo semplice e divulgativo, per spiegare brevemente anche "ai non addetti ai lavori" le caratteristiche di una data tecnologia.

Sempre del ciclo "innovazione" fanno parte altri due articoli: uno dedicato all'evoluzione delle reti, l'altro al *quantum computing*.

Nel dettaglio il primo presenta una rassegna di alcune aree di evoluzione tecnologica attese entro il 2020, che avranno un impatto specifico sull'evoluzione delle reti di telecomunicazioni, sia sotto il profilo di stimolo alla domanda di connettività e alla sua tipologia, sia sotto quello di abilitazione a nuove architetture di connessione.

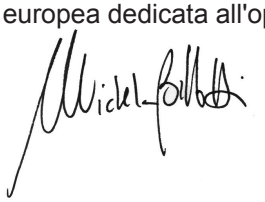
Il secondo scritto, invece, illustra lo stato dell'arte del *Quantum Information Science* (QIS), interessante per la realizzazione di reti fotoniche crittografate su lunghe distanze.

Il tema della "sicurezza" è il perno su cui verte il contributo dedicato all'utilizzo dei Barcode bidimensionali (2D Barcode), che per la loro estrema semplicità di utilizzo, unita all'evoluzione tecnologia dei terminali mobili, possano far insorgere insospettabili problemi di sicurezza, a cui è necessario porre rimedio.

L'impegno alla sostenibilità ambientale, per cui Telecom Italia ha di recente ricevuto anche illustri riconoscimenti, si concretizza, invece, nell'articolo dedicato all'innovazione tecnologica dei sistemi di scavo (tecniche *no-dig*), il che rappresenta una buona via sostenibile per lo sviluppo infrastrutturale del nostro Paese.

Completa questo numero la sintesi della conferenza europea dedicata all'open source.

Buona lettura!



sommario

sommario

Neuromarketing: tecnologie e applicazioni

INNOVAZIONE

Gianluca Zaffiro

Il **neuromarketing** è un recente e innovativo campo di studi basato sulle **neuroscienze** e sul marketing, che ha come obiettivo la valutazione delle risposte sensomotorie, cognitive ed emotive dei soggetti agli stimoli di marketing. Attraverso l'applicazione di tecnologie di **analisi cerebrale** e **sensori biometrici**, il neuromarketing si propone di capire, a livello neurale e fisiologico, i motivi che spingono i soggetti ad optare per una determinata scelta piuttosto che un'altra. Ciò consente di fornire alle aziende uno strumento in più, da affiancare alle indagini di marketing tradizionali, per creare prodotti, servizi e campagne di marketing efficaci. Le potenzialità di tali studi sembrano dimostrate dall'interesse che il neuromarketing ha suscitato in diverse importanti società del calibro di **Google**, **Microsoft** e **Coca-Cola**, le quali vi hanno già ricorso concretamente in più occasioni. Per quanto riguarda gli Operatori di telecomunicazioni, è ipotizzabile che il neuromarketing contribuirà al **miglioramento dei servizi** offerti ai clienti, in particolare nello studio dell'usabilità dei dispositivi e della fruibilità dei servizi. Inoltre un approccio basato sull'analisi neurofisiologica potrebbe costituire una base per un innovativo sistema di tagging e raccomandazione di contenuti multimediali.

1 Introduzione

Il termine neuromarketing fu coniato nel 2002 da Ale Smidts, professore di analisi di mercato della Rotterdam School of Management e la prima conferenza sull'argomento fu organizzata nel 2004 al Baylor College of Medicine di Houston.

1.1 *Neuromarketing: che cos'è?*

Il neuromarketing è una nuova branca del mar-keting. I ricercatori utilizzano tecnologie come l'ElettroEncefaloGrafia (EEG) per misu-rare l'atti-vità elettrica relativa a ogni area del cervello, la functional Magnetic Resonance Ima-

ging (fMRI) per misurare l'ossigenazione del sangue nelle varie regioni del cervello correlata all'attività neu-ronale, sensori per misurare le variazioni di una variabile fisiologica (battito cardiaco, frequenza respiratoria, risposta galvanica della pelle), e/o sistemi di rilevamento del puntamento dello sguardo (eye-tracking) e dell'espressione facciale, per capire i motivi che spingono i soggetti ad optare per una determinata scelta, e quale parte del cervello è correlata con tale scelta.

I primi esperimenti di utilizzo della fMRI applicata al marketing risalgono alla fine degli anni '90 e furono opera di Gerald Zaltman della Harvard Business School.

1.2 *Neuromarketing vs marketing tradizionale*

Per decenni le imprese hanno utilizzato gli strumenti tradizionali di ricerca di mercato nel tentativo di determinare il motivo per cui i clienti preferiscono un prodotto rispetto a un altro: sono stati utilizzati questionari, interviste individuali con domande aperte e focus group di potenziali acquirenti. Tali tecniche, però, possono essere coadiuvate nel valutare meglio le preferenze dei consumatori, tenendo in conto che una risposta verbale alla classica domanda "Ti piace questo prodotto? Perché?" può essere influenzata da un **bias cognitivo**, cioè da una tendenza a far prevalere fattori cognitivi anche inconsci e pregressi su altri elementi sensoriali e percettivi, fenomeno studiato dalle scienze cognitive e dalla psicologia sociale. Un esempio emblematico di studio del bias cognitivo risale al 2004, anno in cui Read Montague usò la **fMRI** per comprendere meglio i motivi per cui la Coca-Cola venisse tradizionalmente preferita alla Pepsi. Read Montague è un neuroscienziato americano, titolare di una cattedra al Baylor College of Medicine di Houston, in Texas, e direttore del Laboratorio di Human Neuroimaging del medesimo College. Egli dimostrò che il vantaggio di Coca-Cola su Pepsi non era legato direttamente al sapore (infatti la Pepsi otteneva pari risultati nei *blind test*), ma piuttosto alla campagna pubblicitaria a lungo termine di Coca-Cola, la quale era riuscita a generare un messaggio culturale che influenzava aree del cervello legate alle preferenze personali.

Uno studio di neuromarketing, analizzando le reazioni dei soggetti a livello cerebrale e fisiologico, può complementare quanto emerge dalle ricerche di marketing più tradizionali, **discernendo ad esempio il bias cognitivo dalle percezioni consce o inconsce indipendenti da esso** e ovviando a una possibile non perfetta descrizione verbale elaborata dai soggetti riguardo a ciò che provano. Martin Lindstrom, esperto di neuromarketing, presidente dell'azienda Buyology Inc. e autore del libro omonimo [1], ne argomenta l'utilità, spiegando quanto sia importante capire come i messaggi di marketing vengano percepiti dai soggetti a livello pre-cognitivo, dato che l'85% del comportamento è guidato dal subconscio. Il neuromarketing, in conclusione, **aiuta a creare prodotti, servizi e campagne di marketing più efficaci, tenendo conto anche dell'impatto sui soggetti a livello inconscio [1], [2], senza escludere di poter sfruttare costruttivamente eventuali bias cognitivi che emergano durante i test**. Per esempio, un ricercatore di mercato può utilizzare tecniche di neuromarketing per capire se e come il consumatore reagisce da un punto di vista fisiologico ad un particolare colore di una confezione, al suono che si produce nel caso in cui la scatola del prodotto venga agitata, oppure all'idea di avere qualcosa che le altre persone non hanno.

2 Che cosa interessa misurare?

Il neuromarketing è basato sul legame tra **dati neurofisiologici misurabili e parametri utilizzabili come metrica per valutare stati d'animo** (parametri legati, ad esempio, al livello di coinvolgimento e di affaticamento del soggetto). I parametri principali derivano, come spiegato di seguito, dagli studi riguardanti le **emozioni** e il

cognitive load, studi che costituiscono quindi una base teorica generale per lo sviluppo e l'applicazione del neuromarketing.

2.1 *Parametri neurofisiologici derivanti dalle teorie dell'emozione*

Riguardo alle emozioni, in psicofisiologia sono state elaborate diverse teorie da cui emergono alcuni concetti che possono essere utilizzati nel neuromarketing attribuendo loro una connotazione matematico/quantitativa. Il primo di questi concetti è l'***arousal***, cioè il **grado di attivazione** di un individuo in un determinato momento. Il fisiologo americano Walter Cannon nel 1932 caratterizzò **le emozioni attraverso l'intensità dell'attivazione**, connessa ad un insieme di modificazioni biologiche: lo stimolo emotigeno produce uno stato di attivazione che prepara l'organismo alla lotta o alla fuga (*fight or flight*), attraverso impulsi nervosi che vengono inviati dalla struttura cerebrale denominata talamo al sistema nervoso simpatico, producendo reazioni fisiologiche, e alla corteccia, producendo una percezione dell'emozione.

Stanley Schachter e Jerome Singer, psicologi statunitensi, dimostrarono poi nel 1962 l'assenza di differenze a livello pre-cognitivo tra due emozioni fondamentali come rabbia ed euforia. Partendo da quest'idea si sono sviluppate le **Teorie cognitive dell'emozione**, in cui le emozioni vengono considerate come stati di personalità vissuti con diversi livelli di intensità, ma anche attraverso l'attribuzione ad essi di una **valenza** positiva o negativa da parte del soggetto a livello cognitivo. La valenza è il secondo parametro che viene spesso considerato nelle applicazioni di neuromarketing.

Con lo sviluppo delle **neuroscienze** è stato successivamente possibile conoscere più approfonditamente struttura, funzione, sviluppo, biochimica, fisiologia, farmacologia e patologia del sistema nervoso centrale e del periferico. Nel neuromarketing sono rilevanti gli studi compiuti sull'**amigdala**, regione cerebrale ritenuta in grado di elaborare in maniera complessa l'esperienza emotiva di uno stimolo ed inviare messaggi che procurano le risposte di attivazione dell'organismo. Sapere attraverso una scansione cerebrale se la regione cerebrale in cui è collocata l'amigdala è attivata fornisce informazioni importanti riguardo al coinvolgimento di un individuo in un evento.

2.2 *Cognitive load*

Cognitive load [3] è un termine riferito al **carico di lavoro cerebrale necessario per l'esecuzione di un compito**, o, in altre parole, alla **difficoltà che un individuo deve superare per eseguire un compito, per imparare qualcosa**, o **per utilizzare uno strumento**. Il cognitive load è un altro parametro utilizzabile negli studi di neuromarketing e dipende da diversi fattori. Per esempio, le persone imparano più facilmente se possono costruire sulla base di nozioni già note, cioè utilizzando uno schema, mentre è più difficile imparare se il tempo a disposizione per l'apprendimento è minore.

3 Tecnologie di misura

Lo stato d'animo dei soggetti si può valutare a partire da misure di dati neurali, fisiologici e comportamentali (puntamento dello sguardo ed espressioni facciali). Sovente si impiegano congiuntamente più tecnologie per misurare diverse tipologie di dati ed ottenere così analisi più accurate. Le tecnologie di raccolta dati derivano in gran parte dal campo medico, sono **standardizzate** o comunque già consolidate. L'aggregazione dei dati e il loro utilizzo specifico in applicazioni relative al neuromarketing, invece, solitamente sono basati su **tecnologie proprietarie** delle aziende, in diversi casi **brevettate** o in attesa di brevetto. EmSense e NeuroFocus sono le aziende che hanno conseguito o avanzato richiesta per la maggior parte dei brevetti in ambito neuromarketing (in totale circa 40 fra patents e applications).

3.1 *Tecnologie per analisi neurale*

Si è già detto che per quanto riguarda l'analisi neurale (monitoraggio dell'attività cerebrale), vengono impiegati principalmente l'EEG (Elettro-EncefaloGramma) e la fMRI (risonanza magnetica funzionale).

1) **EEG**: l'EEG [4] misura l'**andamento temporale dell'attività elettrica del cervello** attraverso elettrodi posizionati sullo scalpo in numero variabile, a seconda delle misure che si intendono effettuare. Gli elettrodi sono posizionati in punti precisi, seguendo uno standard denominato 10-20 (*figura 1*). Le tracce risultanti dall'elettroencefalogramma sono la somma dei potenziali post-sinaptici (attività elettrica alle giunzioni sinaptiche tra i neuroni, laddove il segnale chimico viene convertito in elettrico) che originano differenze di potenziale dell'ordine dei 10-100 μV tra regioni diverse del cervello (con riferimento al potenziale misurato sul lobo di un orecchio). L'EEG fornisce in prima battuta misure nel dominio del tempo, da cui, tramite data processing, è possibile estrarre informazioni nel dominio della frequenza, per studiare l'attività corrispondente alle bande di frequenza che compongono l'attività cerebrale:
   1 **Onde Alfa**: frequenze da 8 ai 12 Hz;
   2 **Onde Beta**: frequenze da 14 ai 40 Hz;
   3 **Onde Delta**: frequenze da 0,5 a 4 Hz;
   4 **Onde Theta**: frequenze da 5 agli 8 Hz;
   5 **Onde Gamma**: frequenze da 30 ai 42 Hz.

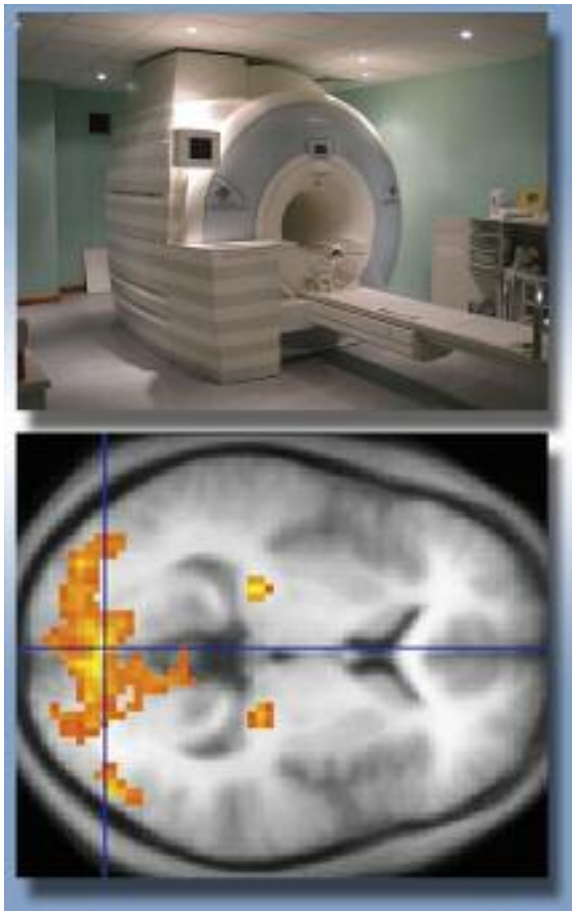
   Sono stati proposti diversi modi di aggregare le misure EEG al fine di estrarne informazioni utili; tali procedimenti applicati al neuromarketing sono solitamente proprietari e talvolta brevettati.
2) **fMRI**: L'acronimo fMRI è spesso usato come sinonimo di risonanza magnetica funzionale neurale, una delle tecnologie di neuroimaging funzionale di sviluppo più recente. La tecnica [5] si basa sulla visualizzazione della **risposta emodinamica, ovvero la variazione nel contenuto di ossigeno trasportato dall'emoglobina**, correlata all'attività neurale del cervello o del midollo spinale. È noto, infatti, che l'attività neurale causi variazioni del flusso sanguigno e dell'ossigenazione sanguigna nel cervello. Quando le cellule nervose sono at-

Figura 1 – Tracciati EEG dei diversi elettrodi

tive, consumano l'ossigeno trasportato dall'emoglobina. Effetto di questo consumo di ossigeno è un aumento del flusso sanguigno nelle regioni ove si verifica maggiore attività neurale, che avviene con un ritardo da 1 a 5 secondi circa. Tale risposta emodinamica raggiunge un picco in 4-5 secondi, prima di tornare a diminuire fino al livello iniziale: si hanno così, oltre che variazioni del flusso sanguigno cerebrale, anche modificazioni localizzate del volume sanguigno cerebrale e della concentrazione relativa di emoglobina ossigenata e non ossigenata (*figura 2*).

3) **MEG**: La MEG (**MagnetoEncefaloGrafia**) [6] misura **i campi magnetici prodotti dall'attività elettrica del cervello**. Tali campi magnetici sono estremamente deboli, tanto da richiedere di eseguire la MEG in stanze schermate da segnali magnetici. Questo, unito alla voluminosità della macchina, non rende la tecnica particolarmente adatta al neuromarketing, i cui test non dovrebbero allontanarsi troppo dal contesto in cui si verificherà realmente l'evento sotto studio. Nonostante ciò, l'azienda NeuroFocus ha incluso la MEG tra le tecnologie utilizzate in una delle proprie richieste di brevetto sul neuromarketing.

Figura 2 – Apparecchiatura fMRI e immagine di scansione



3.1.1 fMRI vs EEG: vantaggi e svantaggi delle due tecnologie

1) **Risoluzione spaziale e temporale delle misure**. La fMRI ha un'elevata risoluzione spaziale (da 3 a 6 mm), ma una risoluzione temporale grossolana (alcuni secondi) a causa delle proprietà fisiche del fenomeno misurato. L'EEG, misurando direttamente l'attività elettrica del cervello, ha una risoluzione temporale dell'ordine dei millisecondi, ma una risoluzione spaziale di alcuni centimetri, poiché si ottengono misure solo nelle posizioni corrispondenti agli elettrodi (a meno di ricorrere a tecniche EEG invasive, con sonde impiantate nelle microaree cerebrali di interesse).
2) **Difficoltà di gestione dell'apparecchiatura, costi e comfort per il soggetto**. L'EEG non richiede macchinari voluminosi e garantisce al soggetto un'esperienza relativamente confortevole, anche perché con l'atteso impiego di elettrodi *dry* non sarà più necessario applicare sullo scalpo gel conduttivi.
   I dispositivi di misura per l'EEG sono silenziosi, caratteristica importante per valutare le risposte dei soggetti a stimoli uditivi. L'EEG, inoltre, tollera relativamente bene movimenti da parte del soggetto, anche se in ogni caso essi producono artefatti nei tracciati che bisogna rimuovere con algoritmi di data processing.
   Allo stesso tempo, i costi dell'EEG non sono elevati ed è possibile, per un'azienda che esegue studi di neuromarketing, acquistare le apparecchiature, oppure sviluppare in proprio dispositivi che integrino elettrodi EEG. Per esempio, EmSense ha sviluppato e ha richie-

Figura 3 – A sinistra: set Biosemi per EEG; a destra il dispositivo EmBand™ di EmSense

sto un brevetto per la fascia elastica EmBand™ (*figura 3*) da indossare sulla fronte, che integra elettrodi EEG e sensori per misure di variabili biometriche.

L'apparecchiatura per la fMRI, al contrario, è molto costosa (circa $ 4.000.000 [1], [2]) e complessa da gestire, quindi generalmente ci si rivolge a centri specializzati, in cui una singola scansione può costare $ 3.000 – 4.000 [1], [2]. Durante una scansione fMRI il soggetto deve rimanere completamente immobile all'interno della macchina *(figura 2)*, con evidenti svantaggi. Questo fatto limita l'utilizzo della fMRI nel neuromarketing ad applicazioni in cui il soggetto possa effettivamente rimanere immobile, ad esempio la visualizzazione di immagini o filmati che vengono proiettati su uno schermo all'interno della macchina, con la possibilità di rispondere ai test tramite interazioni semplici come premere un pulsante.

3) **Regioni cerebrali analizzabili**. Con l'EEG si eseguono solamente misure sulla corteccia, e non è possibile analizzare risposte cerebrali nelle regioni del cervello situate più in profondità, come l'amigdala, la cui attività è importante nel neuromarketing. In questi casi bisogna usare la fMRI.

3.2 *Biosensori*

Congiuntamente o alternativamente alle tecniche di analisi neurale, nel neuromarketing si utilizzano quasi sempre **sensori biometrici** per monitorare parametri fisiologici degli individui. I vantaggi sono molteplici: da un lato la sensoristica ha **costi molto contenuti** e spesso le apparecchiature possono essere prodotte direttamente dalle aziende del neuromarketing, dall'altro **i parametri fisiologici sono variabili importanti nella valutazione delle reazioni degli individui**, per cui è fondamentale tenerne conto. I biosensori più impiegati nel neuromarketing monitorano il **battito cardiaco**, la **respirazione**, la conducibilità galvanica della pelle (**GSR**) e il puntamento dello sguardo, tramite sistemi di **eye-tracking**. Vengono inoltre utilizzati sensori per rilevare i **movimenti dei muscoli facciali** riconducibili a diverse espressioni del volto, anche se a questo proposito esistono studi riguardanti approcci software [7], il cui obiettivo è riuscire a ricavare l'espressione facciale partendo dalla rilevazione dalla posizione e dall'inclinazione relativa di elementi espressivi del viso. I sensori devono essere realizzati in modo da essere meno invasivi possibile, affinché siano confortevoli da utilizzare per i soggetti. Spesso sono integrati in fasce che vengono indossate in testa, su apparecchiature simili a occhiali, oppure, per esempio nel caso dell'azienda Innerscope, i sensori vengono integrati su indumenti progettati appositamente.

3.3 *Data processing*

Uno studio di neuromarketing rende necessario raccogliere e aggregare una grande quan-

tità e varietà di dati. I dati sono sempre affetti da rumore, per esempio nell'EEG i movimenti della testa o i battiti di ciglia causano artefatti nei tracciati relativi alle onde cerebrali. È necessario quindi adottare da un lato sistemi di filtraggio sui dati grezzi per renderli leggibili e significativi, e dall'altro metodi di raccolta e archiviazione efficienti per immagazzinare i dati e renderli consultabili in seguito. Almeno per le applicazioni di neuromarketing attuali, **spesso non è necessario fornire immediatamente i risultati**, e ciò rende possibile elaborare i dati in un secondo momento. In futuro è prevedibile che saranno sviluppate applicazioni in cui l'output sarà fornito in tempo reale. Per esempio si può pensare a un sistema di raccomandazione di contenuti multimediali, che utilizzi parametri neurofisiologici.

4 Misure neurofisiologiche e valutazione degli stati d'animo

Parametri neurofisiologici come arousal e valenza sono ricavabili e misurabili con varie metodologie, alcune delle quali sono presentate in questa sezione. Dall'aggregazione ed elaborazione dei suddetti parametri e dei dati neurofisiologici si ottengono valutazioni inerenti allo stato d'animo del soggetto, utilizzabili nel neuromarketing. L'intero processo si svolge solitamente attraverso i passaggi logici sintetizzati in *figura 4*.

4.1 *Misure neurofisiologiche dell'arousal*

L'arousal può essere valutato [8] utilizzando l'**EEG** e **parametri fisiologici** come la **GSR** e il **battito cardiaco**. Aumentando il livello di arousal, in genere, le onde cerebrali misurate dall'EEG aumentano in frequenza e diminuiscono in ampiezza, inoltre si osserva un aumento della GSR e della frequenza cardiaca.

4.2 *Asimmetria dell'attività cerebrale e valenza delle emozioni*

In letteratura scientifica si dimostra [9] che la **valenza** delle emozioni può essere valutata conoscendo l'**asimmetria** tra l'attività dei due emisferi cerebrali. L'azienda di neuromarketing EmSense ha richiesto un brevetto (WO/2008/108814) basato sull'associazione tra l'**asimmetria emisferica delle onde alfa e theta frontali e la valenza delle emozioni**. Il soggetto viene innanzitutto stimolato con un evento, quindi vengono misurati due segnali EEG, uno dalla regione frontale destra e uno dalla regione frontale sinistra. Il parametro di interesse viene poi ricavato attraverso diverse possibili relazioni matematiche da utilizzare a seconda del contesto.

4.3 *Rapporto fra onde theta e alfa e coinvolgimento del soggetto (engagement)*

Uno stato mentale può essere valutato attraverso il rapporto fra le onde cerebrali theta e alfa, misurabile attraverso EEG. La letteratura scientifica presenta ad esempio metodi [10] per aumentare la capacità creativa degli individui, allenando i soggetti ad aumentare il rapporto fra le onde theta e le onde alfa attraverso un feedback uditivo conseguente alle misure EEG. Sempre EmSense ha avanzato alcune richieste di brevetto, basate

Figura 4 – Diagramma concettuale del procedimento per la valutazione degli stati d'animo

sull'utilizzo delle **onde theta (θ)** e **alfa (α)**, oltre al **battito cardiaco, per valutare il coinvolgimento (*engagement*) del soggetto**. L'**engagement** è associato al livello di attività dell'individuo, attività che non implichi però uno sforzo cognitivo. Generalmente, un battito cardiaco accelerato è indicativo di un livello di engagement più alto; un elevato livello di onde theta è indice di elevato impegno cognitivo, associato a un livello di engagement minore. Al contrario, un livello alto di onde alfa è indicativo di un'attività cognitiva più limitata e di maggiore engagement. La procedura di EmSense prevede di fornire uno stimolo mediatico (per esempio un filmato) che contenga un evento a un individuo e di applicare relazioni matematiche che coinvolgono grandezze misurate tramite EEG e frequenza cardiaca.

4.4 *Una modellizzazione degli stati d'animo*

Le possibilità di scelta e pesatura dei parametri neurofisiologici da impiegare nel neuromarketing sono molteplici. In generale si possono rappresentare gli stati d'animo attraverso un **sistema triassiale** (*figura 5*). In questo modello il primo asse riguarda l'**arousal** e il secondo asse è associato alla **valenza** delle emozioni. I due assi definiscono un piano che rappresenta il coinvolgimento (**engagement**) del soggetto. Questo modello a due dimensioni è spesso citato in letteratura scientifica, e fu adottato per la prima volta da Heller nel 1986. Il coinvolgimento può avere anche una componente cognitiva (legata ad esempio agli interessi della persona) che non implica sforzi cerebrali da parte del soggetto. La componente dell'attività cognitiva che caratterizza lo sforzo cerebrale, ad esempio nell'esecuzione di calcoli matematici, viene invece considerata in un terzo asse, associato al **cognitive load**.

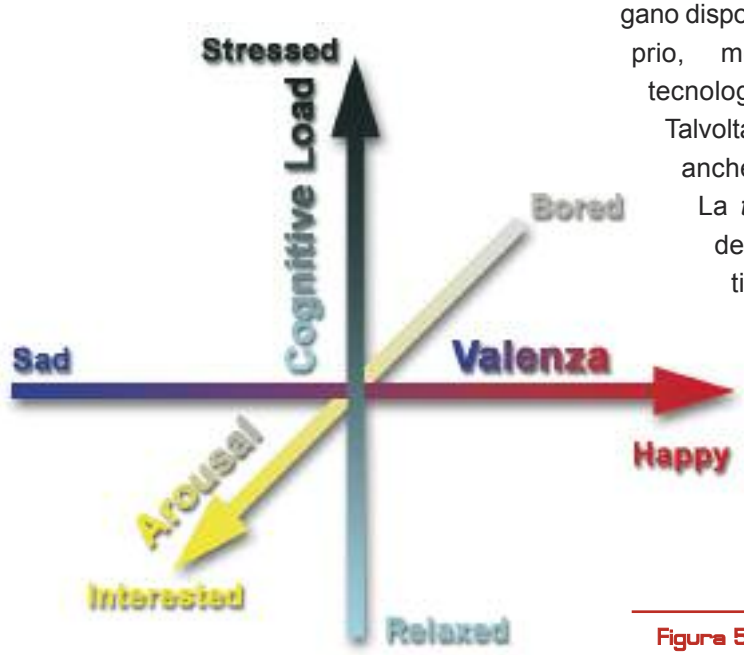


Figura 5 – Modello triassiale per la valutazione degli stati d'animo

5 Player del mercato e aree di applicazione

5.1 *Aziende che operano nel neuromarketing*

Allo stato attuale, la maggior parte delle aziende di neuromarketing sono **statunitensi** e di **recente fondazione**. Alcune aziende impiegano dispositivi (EEG e sensori) sviluppati in proprio, mentre altre utilizzano soluzioni tecnologiche prodotte da altre aziende. Talvolta le aziende di neuromarketing offrono anche servizi di marketing tradizionale. La *tabella 1* riassume le caratteristiche delle principali aziende di neuro marketing. Tra queste c'è l'italiana Map Brain Communication.

Azienda	Sedi	Anno Fondazione	Tecnologie	Prodotti/ Servizi offerti
Buyology Inc.	New York, NY	2008	EEG e fMRI	Soluzioni marketing per aziende basate sul ruolo del subconscio nel processo decisionale
EmSense	San Francisco, Monterey, Santa Monica, CA	2004	EEG + biosensori (dispositivo proprietario) + software proprietario	Neuromarketing applicato a pubblicità, disposizione prodotti in supermercati, pagine web, packaging e videogames
FKF	Headquarter a Washington DC, fMRI eseguite a Los Angeles, CA	2004	fMRI + parametri biomedici	Valutazione efficacia di pubblicità stampate o video; studio intensivo del brand e della pubblicità
Innerscope	Boston, MA	2006	Biosensori integrati in un indumento (sistema proprietario)	Misura dello stato emotivo e della reazione agli stimoli al fine di aiutare nelle decisioni di marketing
Lucid Systems	San Francisco, CA	2006	EEG + biosensori, utilizza tecnologia Biopac	Neuromarketing applicato a: farmaci senza prescrizione, online media, TV e film, packaging, cibi e bevande, videogiochi, software, politica
MindSign	San Diego, CA	2007	fMRI, eye-tracking	Neuromarketing applicato a: pubblicità, intrattenimento, software, e politica
NeuroFocus	Berkeley, CA	2005	EEG + biosensori	Neuromarketing per misura dell'efficacia di pubblicità, brand, prodotti, e analisi dei competitor
Neurosense	Oxford, U.K.	1997	fMRI, magnetoencefalografia (MEG)	Consulenza di neuromarketing, neuroimaging, test psicologici creati ad hoc
Map Brain Communication	Prato, Italia	2006	EEG, utilizza apparecchiatura Galileo Mizar 40 di EBNeuro	Analisi di pubblicità, consulenza di neuromarketing, marketing tradizionale e formazione della forza vendita

Tabella 1 – Aziende di neuromarketing

5.2 *Aree di applicazione*

Dall'analisi delle attività delle aziende sul mercato, sono stati enucleati i principali contesti di utilizzo del neuromarketing, elencati di seguito secondo l'interesse che potrebbero suscitare in un operatore di telecomunicazioni:

- **Pubblicità**: il neuromarketing è stato ampiamente utilizzato, anche da compagnie di rilievo, per misurare l'efficacia di pubblicità stampata o video (spot).
- **Multimedia Engagement**: è possibile valutare tramite tecniche di neuromarketing un trailer cinematografico o anche un intero lungometraggio. L'obiettivo è comprendere l'andamento nel tempo del livello di coinvolgimento del-

l'audience e individuare i punti di un film dove, ad esempio, vi sono livelli elevati di suspense o sorpresa negli spettatori. Un discorso simile vale anche per i programmi televisivi: il neuromarketing può aiutare a predirne il livello di successo. Molte delle richieste di brevetto avanzate dalle aziende di neuromarketing riguardano quest'area applicativa.

- **Ergonomia**: Il neuromarketing può essere utile per migliorare l'**ergonomia dei dispositivi di interfaccia** e, di conseguenza, la ***user experience***. In particolare si possono valutare il coinvolgimento dell'utente, il carico di lavoro cognitivo che è richiesto per imparare ad usare il dispositivo, la soddisfazione o lo stress generati dal suo utilizzo.
- **Videogiochi**: attraverso il neuromarketing si può valutare il **coinvolgimento** dei giocatori, identificare le *feature* più interessanti e ottimizzare i dettagli dei giochi. È possibile calibrare adeguatamente la difficoltà in modo che un gioco risulti stimolante, ma non eccessivamente difficile.
- **Packaging**: Il neuromarketing può essere impiegato per ottenere un **design delle confezioni** che attiri maggiormente l'attenzione, in modo che, ad esempio un cliente possa riconoscere il prodotto più facilmente su uno scaffale di un supermercato.
- **Product placement**: Studi di neuromarketing possono indicare il migliore **posizionamento del prodotto** sullo scaffale di un supermercato e la **collocazione ottimale della pubblicità** relativa ad un prodotto o ad un brand all'interno di una scena durante uno show televisivo.
- **Politica**: Si possono applicare tecniche di neuromarketing per compiere studi in ambito politico, per esempio misurando le reazioni degli elettori ai candidati durante comizi e discorsi.

CASE STUDIES DI NEUROMARKETING	
Pubblicità	**Coca-Cola** ha incaricato **EmSense** [11] di effettuare una ricerca con tecniche di neuromarketing per scegliere tra varie possibilità lo spot pubblicitario da mandare in onda durante il Superbowl; Per quanto riguarda la pubblicità su Internet, l'azienda **NeuroFocus**, in collaborazione con **MediaVest**, agenzia di marketing, ha utilizzato tecniche di neuromarketing [12] per conto di **Google** nel tentativo di trovare un modo per valorizzare Youtube, valutando l'impatto sugli utenti dell'introduzione degli *invideo ads*, banner pubblicitari sovrapposti ai video di Youtube.
Multimedia Engagement	**20th Century Fox** ha commissionato studi a **Innerscope** [13] per valutare trailer cinematografici per i film "*28 Weeks Later*" e "*Live Free or Die Hard*"; **NBC** ha commissionato studi a **Innerscope** [13] sulla percezione degli spettatori nel fast-forwarding durante la pubblicità; **Disney** [14] ha attrezzato in proprio un laboratorio per studiare l'efficacia della sua pubblicità online.
Ergonomia	**Microsoft** nel 2006 [15] ha utilizzato l'EEG per studiare la possibilità di riconoscere *task* svolti dall'utente utilizzando un elettroencefalografo a basso costo.
Gaming	**EmSense** ha condotto uno studio [16] sul genere di videogiochi "sparatutto in soggettiva" valutando in funzione del tempo i livelli di emozioni positive, di impegno cognitivo e dell'arousal dei giocatori durante la partita.
Politica	In un articolo [17] pubblicato da studiosi di diverse università americane in collaborazione con **FKF**, azienda di neuromarketing, vengono presentati i risultati di uno studio eseguito prima delle elezioni presidenziali del 2008, per osservare le risposte cerebrali di un gruppo di elettori sottoposti alla fMRI.

6 Considerazioni critiche

Il neuromarketing è soggetto a critiche di natura sia etica che scientifica. Dal punto di vista etico, le argomentazioni principali riguardano la possibilità che sia svolta un'opera di manipolazione sui consumatori, inducendoli all'acquisto di merci contro la loro volontà razionale. In particolare, è stato sottolineato [18], [19] come il **neuromarketing potrebbe essere utilizzato** da imprese produttrici di **tabacco**, **alcolici** o prodotti che potrebbero arrecare un **danno alla salute pubblica**, e inoltre potrebbe essere impiegato per **propaganda politica scorretta** o nella diffusione, soprattutto tra i giovani, di **valori di degrado**. A queste critiche risponde **Martin Lindstrom** [1], affermando che **tutto il marketing ha come obiettivo convincere i potenziali clienti ad acquistare**, e che sul marketing si basano tutti gli scambi commerciali. Il neuromarketing, secondo Lindstrom, permette di capire in anticipo quali prodotti siano destinati ad avere successo e di concentrare di conseguenza gli investimenti su tali prodotti, evitando sprechi da parte delle aziende, contribuendo anche alla riduzione del numero di messaggi pubblicitari inutili. In questo senso, deve essere inteso come **un campo di ricerca volto all'osservazione dei clienti** e non come qualcosa che possa interferire con le loro opinioni e sensazioni.

Il neuromarketing è criticato anche da un punto di vista scientifico. Alcuni neuroscienziati, infatti, invitano alla cautela, spiegando che **le conclusioni a cui si è giunti fino ad ora non sono ancora consolidate** e certamente non è possibile identificare un "***buying center***" cerebrale né capire in modo preciso la disposizione mentale di una persona ad acquistare semplicemente attraverso elettrodi e sensori biometrici. La **fMRI**, sebbene abbia permesso di fare molti progressi nella conoscenza del funzionamento del cervello, risulta tuttora difficile da utilizzare anche a fini diagnostici, ad esempio perché gli studi hanno una valenza statistica, e quindi potrebbero non riflettere i casi dei singoli individui. Analogamente non è detto che, per ogni area del cervello, l'attività sia imputabile esclusivamente a un determinato tipo di stimolo. Un esempio particolarmente legato al neuromarketing riguarda l'**amigdala**, considerato spesso un centro cerebrale che si attiva in caso di minaccia. Anche ammettendo ciò, non è tuttora dimostrabile che l'attività in questa regione cerebrale implichi necessariamente e univocamente che una persona si senta minacciata [20].

L'utilizzo del neuromarketing ha anche **limitazioni di tipo pratico**. Sebbene siano stati fatti molti progressi nel rendere le apparecchiature per le misurazioni neurofisiologiche il meno invasive possibile, allo stato attuale queste risultano ancora ingombranti e poco pratiche. Nel caso specifico della fMRI il soggetto è all'interno dell'apparecchiatura e deve rimanere quasi immobile, ma anche utilizzando l'EEG e i sensori biometrici, comunque, il soggetto deve solitamente indossare una cuffia, una fascia elastica o sensori sugli arti che ne limitano i movimenti.

7 Quali opportunità per Operatori di telecomunicazioni?

In un contesto di convergenza tecnologica e aumento delle capacità di rete, in cui gli Operatori, oltre a fornire la connettività, offrono comunemente **prodotti** e **servizi a valore aggiunto** e in cui crescono d'importanza le **relazioni tra gli Operatori** e i **Content Provider** per la fornitura di contenuti multimediali, il neuromarketing potrebbe fornire un aiuto per **migliorare in generale le offerte ai clienti**.

Il neuromarketing potrebbe contribuire naturalmente al rafforzamento del brand dell'Operatore e a costruire campagne di pubblicità più efficaci. Si potrebbe condurre per esempio un'indagine per verificare come e quanto sia radicata a livello inconscio nei clienti una percezione negativa legata a un'attività passata di monopolista. Altre applicazioni di neuromarketing, invece, interessano maggiormente attività tecnologiche e operative. Per esempio, nella progettazione e

implementazione di servizi e prodotti, sarebbe possibile introdurre nuovi strumenti di valutazione ergonomica e di usabilità. Inoltre il paradigma di offerta di contenuti multimediali potrebbe in futuro cambiare in funzione di un avanzamento della ricerca nelle neuroscienze.

7.1 *Usabilità dei prodotti e fruibilità dei servizi*

L'utilizzo di apparecchiature come EEG e sensori biometrici potrebbe permettere di acquisire misure di risposte neurali e fisiologiche per **valutare in un modo innovativo l'usabilità dei prodotti e la fruibilità dei servizi**. Per esempio, sulla scia dello studio effettuato da Microsoft [15], in futuro saranno probabilmente disponibili sistemi per **valutare il carico cognitivo necessario agli utenti per utilizzare un apparecchio** o la **difficoltà che incontrerebbe un utente nell'utilizzare un nuovo servizio** da introdurre sul mercato. Inoltre, anche quando l'usabilità dei prodotti sia già stata studiata ed ottimizzata in fase di progettazione in modo più "classico", il neuromarketing potrebbe comunque aiutare a **migliorare il livello di engagement della persona**, valutando ad esempio quanto un nuovo servizio "catturi" il cliente, cioè **quanto tenda a protrarsi l'utilizzo del servizio nel tempo**.

7.2 *Sistemi di tagging e raccomandazione*

È molto probabile che in futuro verranno sviluppate tecniche per **creare sistemi di tagging** innovativi per contenuti multimediali. I contenuti potrebbero così essere catalogati tramite etichette relative agli stati emotivi misurati durante test svolti a priori.

Inoltre, supponendo di utilizzare sensori EEG e biometrici per riconoscere lo stato emotivo di un utente, si potrebbero creare **sistemi di raccomandazione** dei contenuti basati da un lato sullo stato emotivo del cliente, e, dall'altro, sulle etichette associate ai contenuti dal sistema di tagging. Un problema non banale, in questo caso, sarebbe lo studio di un **modello che metta in relazione lo stato emotivo della persona/cliente con i contenuti da consigliare**. Non necessariamente, infatti, una persona che risulti "rilassata" è interessata a vedere un film che la faccia rilassare ancora di più: è possibile, al contrario, che la persona sia interessata a vedere un film ricco di azione, perché vuole che il suo stato emotivo diventi più "attivo". Si noti anche che in questo caso emergerebbe un vincolo di ***real time*** piuttosto stringente: il sistema di raccomandazione in questione, infatti, dovrebbe fornire un output quasi immediato.

CONCLUSIONI

In questo articolo è stato presentato il **neuromarketing**, campo applicativo e di studi che sintetizza elementi di **neuroscienze** e **marketing**.

Si sono descritte le **tecnologie utilizzate**, per lo più derivanti dall'ambito biomedicale, inerenti all'analisi dell'attività cerebrale, alla biosensoristica, al rilevamento della direzione dello sguardo e all'analisi dell'espressione facciale.

Le aziende di neuromarketing si basano soprattutto su fMRI e EEG come tecnologie per analisi cerebrale. A partire dal quadro di business emerso sono stati puntualizzati i principali **campi di applicazione**, oggi principalmente legati alla consulenza per **campagne pubblicitarie**.

L'uso degli strumenti del neuromarketing consente di **introdurre un metro di misura per la valutazione diretta dei meccanismi di reazione cerebrali** e fisiologici agli eventi di stimolo, laddove tradizionalmente ci si affida a metodi indiretti (interviste, questionari, osservazione del soggetto). Le ricadute di questa evoluzione tecnologica non sono ancora del tutto chiare e sollevano **obiezioni di natura scientifica ed etica**. È comunque ipotizzabile che per un Operatore di telecomunicazioni il neuromarketing potrà co-

stituire uno strumento per migliorare l'usabilità e la fruibilità dei servizi offerti ai clienti. Inoltre è possibile che nel futuro saranno sviluppati innovativi sistemi di tagging e raccomandazione di contenuti multimediali basati su misure neurofisiologiche.

Le **tecniche di acquisizione dei dati neurofisiologici possono considerarsi ancora primitive**. Gli studi relativi al neuromarketing appaiono però destinati a trovare prossimamente un posto sempre più rilevante nelle applicazioni al servizio dell'uomo. L'introduzione di una chiave per l'identificazione diretta non solo dello stato emotivo-cognitivo, ma anche dell'intenzione conscia o inconscia, offre in prospettiva all'uomo una ben più efficace capacità delle "macchine" di supportarlo nelle sue azioni.

ACRONIMI

EEG ElectroEncephaloGraphy
fMRI functional Magnetic Resonance Imaging
MEG MagnetoEncephaloGraphy
GSR Galvanic Skin Response
RPP heart Rate-blood Pressure Product

BIBLIOGRAFIA

[1] Lindstrom, M., Buyology Truth and Lies About Why We Buy, Doubleday, 2008
[2] http://www.scribd.com/doc/12545630/QABuyology
[3] http://en.wikipedia.org/wiki/Cognitive_load
[4] http://en.wikipedia.org/wiki/Electroencephalography
[5] http://en.wikipedia.org/wiki/FMRI
[6] http://en.wikipedia.org/wiki/Magnetoencephalography
[7] Jarkiewicz J., Rafał Kocielnik R., Krzysztof M., Anthropometric Facial Emotion Recognition, Polish-Japanese Institute of Information Technology Koszykowa 86, 02-008 Warszawa, Poland, http://www.springerlink.com/content/p5878w6267117322/
[8] Parasuraman R., Rizzo M., Neuroergonomics The brain at work, Oxford University Press, 2007
[9] Johnson, S., Hayes, A. M., Field, T. M., Schneiderman, N., Stress, coping, and depression, Psychology Press, 1999
[10] Gruzelier, J., A theory of alpha/theta neurofeedback, creative performance enhancement, long distance functional connectivity and psychological integration, Cognitive Processing Springer Berlin / Heidelberg, 2008
[11] http://www.adweek.com/aw/content_display/news/media/e3i975331243e08d74c5b66f857ff12cfd5
[12] http://www.neurofocus.com/news/media-google.html
[13] http://www.boston.com/ae/tv/articles/2007/05/13/emote_control/
[14] http://www.nytimes.com/2009/07/27/technology/27disney.html
[15] Lee J. C., Desney T. S., Using a Low-Cost Electroencephalograph for Task Classification in HCI Research, 2006, http://research.microsoft.com/en-us/um/people/desney/publications/uist2006-lowcosteeg.pdf
[16] http://wire.ggl.com/news/if-you-want-a-good-fps-use-close-combat/
[17] http://www.nytimes.com/2007/11/11/opinion/11freedman.html
[18] http://www.commercialalert.org/issues/culture/neuromarketing/commercial-alert-asks-senate-commerce-committee-to-investigate-neuromarketing
[19] http://www.commercialalert.org/issues/culture/neuromarketing/commercial-alert-asks-feds-to-investigate-neuromarketing-research-at-emory-university
[20] http://www.dana.org/news/cerebrum/detail.aspx?id=22220

Siti delle aziende di neuromarketing:

[21] http://www.buyologyinc.com/

[22] http://www.emsense.com/
[23] http://www.fkfappliedresearch.com/
[24] http://www.innerscoperesearch.com/
[25] http://www.lucidsystems.com/
[26] http://mindsignonline.com/
[27] http://www.neurofocus.com/
[28] http://www.neurosense.co.uk/
[29] http://www.mapbraincommunication.com/

Si ringrazia Enrico Cauda, partecipante al Master Innovazione di reti e servizi nel settore ICT per aver contribuito in modo sostanziale alla realizzazione di questo studio.

gianluca.zaffiro@telecomitalia.it

AUTORE

Gianluca Zaffiro

laureato in Ingegneria Elettronica presso il Politecnico di Torino, con Master in Telecomunicazioni, entra in Telecom Italia nel 1994 dove si è occupato di reti ottiche, partecipando all'IEC per gli standard e la pubblicazione di numerosi articoli. Da qualche anno opera nel gruppo Innovation Trends di Telecom Italia Lab.
È stato responsabile per Telecom Italia dell'azione di coordinamento IST FP6 Peach per la ricerca sulla Presence, sul cui tema ha pubblicato alcuni articoli.
Si occupa di elaborare scenari innovativi di medio/lungo periodo di interesse per le telecomunicazioni. Nel 2004-2005 ha collaborato a numerose attività sulla Convergenza Fisso-Mobile. Nel 2003 ha collaborato a dare supporto per l'innovazione tecnologica dell'area Mobile Services di TIM. Nel 2001-2002 ha partecipato al lancio del servizio di Mobile Instant Messaging, TIMCafè, focalizzandosi su aspetti di marketing ■

Dalla mela all'Internet quantistica: quantum computing e opportunità per le TLC del futuro

INNOVAZIONE

Valter Bella, Angelantonio Gnazzo

Due delle più grandi rivoluzioni scientifiche del XX secolo sono state la meccanica quantistica e la teoria dell'informazione. La meccanica quantistica descrive la natura a livello di dimensioni atomiche ed è alla base della teoria della microelettronica dei semiconduttori e delle tecnologie fotoniche. La teoria dell'informazione invece si occupa di informazioni e stabilisce un quadro di come queste vengano processate e comunicate in modo efficiente. L'unione di queste due discipline porta a quella che oggi viene chiamata Quantum Information Science (QIS). In questo articolo non si è volutamente entrati nel formalismo matematico, ma si darà una panoramica dello stato dell'arte di questa tematica. Dal punto di vista di un operatore di telecomunicazione l'importanza dell'argomento riguarda la possibilità di realizzare reti fotoniche crittografate su lunghe distanze.

1 Introduzione

La mela e il concetto d'informazione sono da sempre intimamente correlate. Nella storia recente, Alan Turing [1], uno dei padri dell'informatica, ideatore della "Macchina di Turing" e precursore di tutti gli studi sull'intelligenza artificiale, si suicidò nel 1954 mordendo una mela avvelenata, in tono col proprio carattere eccentrico e prendendo spunto dalla fiaba di Biancaneve da lui apprezzata fin da bambino.

Come tributo ad Alan Turing, la mela morsa divenne il simbolo di Apple, una delle più note case produttrici al mondo di sistemi operativi, personal computer, software e multimedia, con sede a Cupertino, nel cuore della Silicon Valley. Il nome Apple, tuttavia pose un problema legale alla società di Cupertino, che nel 1989 fu querelata per violazione dei diritti sul copyright dalla casa discografica del celeberrimo complesso musicale

dei Beatles, la "Apple Records", anch'essa emblema di un'informazione musicale che cambiò il corso della musica.

Partendo dall'inizio, vi è anzitutto l'associazione alla mela biblica, simbolo della conoscenza in quanto contenente l'informazione del bene e del male. Successivamente Isaac Newton si ritrovò ad aver a che fare con una mela in caduta da un albero: un evento già osservato infinite volte, ma per Newton è la rivelazione sull'informazione relativa alle leggi che governano la gravitazione universale. La meccanica di Newton, infatti, può prevedere con precisione straordinaria il movimento non solo dei pianeti, ma, in maniera perfettamente analoga, di un qualsiasi altro oggetto o sistema meccanico, purché si conoscano esattamente le forze che agiscono sul sistema in questione: è possibile sapere in ogni istante posizione e velocità della mela che cade dall'albero.

Verso la fine del XIX secolo sembrava che l'edificio concettuale della fisica fosse ormai completato. Solo alcuni fenomeni, apparentemente marginali, erano al di fuori del quadro interpretativo della fisica classica, ma il convincimento di quasi tutti gli scienziati dell'epoca era che prima o poi anche questi trovassero un'interpretazione all'interno della fisica classica. Ma non fu così: nel mondo microscopico, a livello di atomi e particelle elementari, i comportamenti fisici erano assai bizzarri ed assolutamente inconcepibili per i nostri ragionamenti razionali dettati da un'evoluzione umana basata sul riscontro dei nostri sensi verso oggetti di dimensioni visibili.

Per meglio capire questi aspetti è sufficiente entrare nella mela e fare un viaggio ideale al suo interno, giù verso l'infinitamente piccolo, ossia passando per la sua struttura di catene molecolari, entrando negli atomi costituenti detti molecole, sino ad incontrare la nube di elettroni che circonda il nucleo di ogni singolo atomo. È possibile stabilire la posizione e la velocità in ogni istante di un elettrone contenuto nella mela, come accadeva per la mela stessa? La risposta è negativa ed il motivo è semplice: se si illumina con luce solare o artificiale una mela per vedere dove essa si trovi, non c'è problema, perché questa non si muove, ma se, a scala sub-atomica, si cerca di illuminare un suo elettrone, anche con un solo fotone, l'impatto di quest'ultimo lo fa allontanar via; in altre parole: se si cerca di determinare l'informazione sulla posizione dell'elettrone, si perde l'informazione sulla sua quantità di moto e viceversa.

Quanto appena esemplificato prende il nome di principio di indeterminazione di Heisemberg che recita appunto: "*non è possibile conoscere simultaneamente la velocità e la posizione di una particella con certezza*". È fondamentale comprendere che questa condizione di indeterminismo non è dovuta a una conoscenza incompleta, da parte dello sperimentatore, dello stato in cui si trova il sistema fisico osservato, ma è da considerarsi una caratteristica intrinseca del sistema.

Il principio di indeterminazione, seppur ammesso *obtorto collo* per via della naturale propensione dell'uomo ad avere certezze, è in qualche modo ancora accettato, ma, a livello sub-atomico accadono altri due fenomeni sconcertanti: il dualismo onda-particella e l'*entanglement*[1]. Il primo stabilisce che, mentre nella fisica classica un corpo e un'onda sono due entità ben distinte, nel mondo sub-atomico regolato dalla meccanica quantistica le particelle elementari, come l'elettrone o il fotone, mostrano una duplice natura, sia corpuscolare sia ondulatoria.

L'*entanglement* è invece un fenomeno ancor più inquietante della meccanica quantistica, anche perché è stato ampiamente dimostrato per via sperimentale, e consiste nel fatto che è possibile realizzare un sistema costituito da due particelle il cui stato quantico sia tale che, qualunque sia il valore di una certa proprietà osservabile assunto da una delle due particelle, il corrispondente valore assunto istantaneamente dall'altra particella sarà opposto al primo, anche qualora le particelle fossero separate da anni-luce di distanza.

1 Uno stato di entanglement implica la presenza di correlazioni tra le quantità fisiche osservabili dei sistemi coinvolti ed il termine viene a volte tradotto in italiano con 'non-separabilità'.

Ma la mela è anche informazione: quanti bit di informazione ci sono in una mela? La risposta è relativamente semplice: la meccanica quantistica limita il numero degli stati in cui le particelle della mela si possono trovare, perciò il numero di bit racchiusi in questo frutto è dato dal prodotto del suo numero di atomi moltiplicato per pochi stati possibili per ciascun atomo. Ne consegue un numero piuttosto grande, rappresentante qualche milione di miliardi di miliardi di "bit a zero" e "bit a uno": questa è la mela. Quando un sistema fisico, come appunto una mela, è dotato di energia finita ed è confinato in una regione finita di spazio per le leggi della meccanica quantistica, esso può esistere solo in un numero finito di stati e quindi può registrare una quantità finita d'informazione, ossia di bit. Per dirla con le celebri parole del fisico Rolf Landauer [2]: "*L'informazione è fisica*".

A questo punto sorge spontanea, almeno ai fisici e ai matematici, una seconda domanda: se la quantità di informazione che ogni bit della mela registra è sempre la stessa, è così anche per l'importanza dell'informazione registrata? Indubbiamente no: un bit che ci dice che cosa ci sia in un certo posto nel DNA della mela è molto più importante di quello che ci informa sullo stato di agitazione termica di uno dei suoi atomi di carbonio. Ma c'è un modo rigoroso, matematico, di quantificare l'importanza dell'informazione contenuta in un bit? La risposta è affermativa perché l'importanza di un bit può essere pesata in funzione di come il suo contenuto vada a cambiare il valore di altri bit attorno a sé.

Ovviamente per condurre questo tipo di analisi, indipendentemente dal fatto che l'oggetto in questione sia una mela, oppure una rete di comunicazione metropolitana a crittografia quantistica, gli attuali metodi di computazione classici basati su "bit" divengono assolutamente inefficienti in termini di tempo e risorse. Occorre allora ricorrere alla computazione quantistica, basata sugli stessi strani effetti accennati a scala sub-atomica nella mela, quali dualismo onda-particella, *entanglement* e registrazione dell'informazione espressa in qubit, i cui aspetti concettuali ed implementativi saranno oggetto dei prossimi paragrafi.

2 Cos'è un computer quantistico?

Spiegare cosa sia un computer quantistico senza ricorrere all'uso intensivo del formalismo matematico ad esso sotteso risulta una sfida intellettuale impegnativa. La ragione è che il computer quantistico funziona su fenomeni di pertinenza della meccanica quantistica che, come descritto in precedenza, è quanto di meno intuitivo per noi umani. Sostanzialmente, la meccanica quantistica si distingue in maniera radicale dalla meccanica classica, in quanto non esprime mai certezze, ma si limita a esprimere la probabilità di ottenere un dato risultato da una certa misurazione.

Nel nostro mondo macroscopico la fisica classica fornisce certezze sulle misurazioni e sulle osservazioni che effettuiamo. Ma quando scendiamo nel microcosmo (atomi, elettroni, fotoni ed altre particelle elementari), la fisica classica va in crisi e lascia spazio a quella quantistica, basata appunto sulla probabilità e mai sulla certezza.

La teoria quantistica, dunque, non ci dice mai "*il valore è 1*" oppure "*il valore è 0*, ma descrive i sistemi come una sovrapposizione di stati diversi e prevede che il risultato di una misurazione non sia completamente arbitrario, ma sia incluso in un insieme di possibili valori: ciascuno di detti valori è abbinato a uno di tali stati ed è associato a una certa probabilità di presentarsi come risultato della misurazione.

Un esempio semplice, ma di potente intuitività, è il seguente: se si guarda attraverso il vetro di una finestra, su di esso non si vede solo il paesaggio esterno, ma anche la propria immagine riflessa. La ragione di questo curioso aspetto è dovuta al fatto che la luce è costituita da fotoni, ossia particelle elementari soggette alle leggi della meccanica quantistica. Per quanto detto, ne consegue che i fotoni che colpiscono, dall'esterno o dall'interno, il vetro della finestra hanno una probabilità di attraversarlo, ma hanno anche una probabilità di venire riflessi. Queste probabilità determinano quindi una curiosa "sovrapposizione" di realtà, cosicché sul vetro, il paesaggio e il volto dell'osservatore coesistono

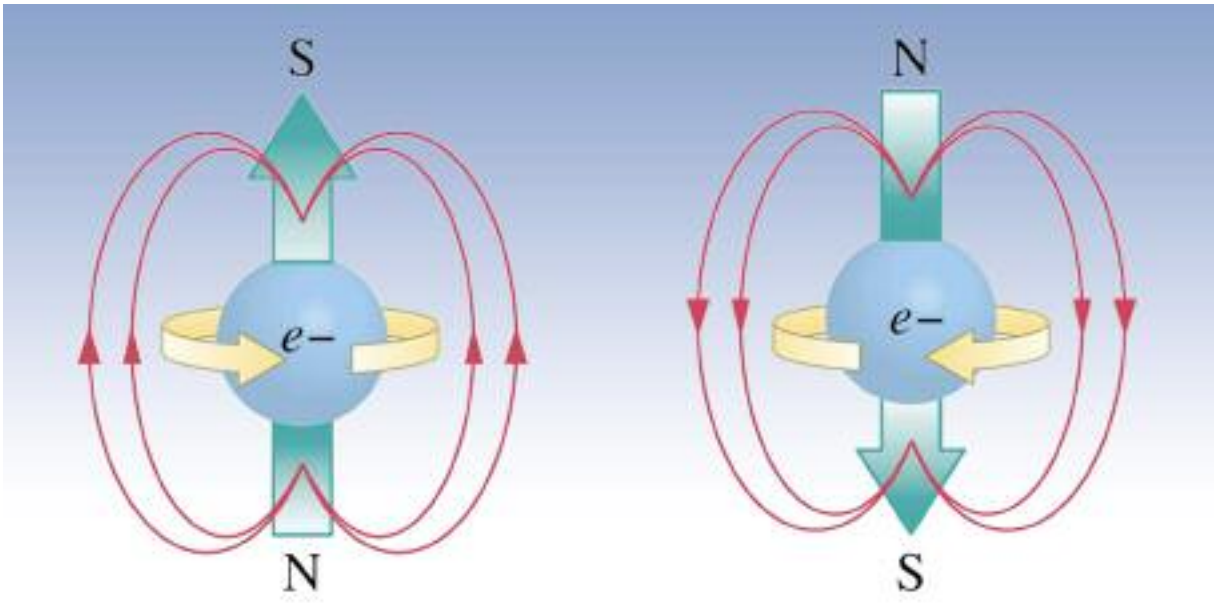
allo stesso tempo nello stesso luogo; possiamo affermare che la sovrapposizione contiene tutti i possibili casi, ma non equivale ad alcuno di essi. Continuando con l'esempio, ad un certo punto l'osservatore deciderà di concentrarsi sul panorama esterno e farà questo mettendo a fuoco i propri occhi su una distanza maggiore, ossia egli deciderà una "misurazione" di ciò che più gli interessa, facendo "collassare" la precedente sovrapposizione d'immagini su di una precisa "soluzione" che è il panorama.

Migrando questi concetti fondamentali al mondo dei computer possiamo ripetere un ragionamento analogo. Il computer "classico", ad esempio quello impiegato per scrivere il presente articolo, appartiene ad una logica classica, dove le unità fondamentali dell'informazione, chiamati "bit" sono governati da certezze: si sa in ogni momento se un certo bit valga "0", oppure "1" e in quale locazione di memoria esso sia memorizzato. Nel computer "quantistico" tutto ciò non è possibile e, al posto dei "bit", avremo dei "qubit" [3], contrazione di quantum bit, il termine coniato da Benjamin Schumacher per indicare il bit quantistico, ovvero l'unità di informazione quantistica. Questi qubit sono rappresentati dagli stati di particelle elementari, come elettroni, fotoni...

Si prenda ad esempio l'elettrone: a seconda se il proprio senso di rotazione su se stesso (detto spin) sia orario o antiorario, si dice che esso abbia "*spin giù*" oppure "*spin su*". Nel mondo classico, quindi nel dominio delle nostre dimensioni, una trottola che gira su se stessa o è "*spin su*", oppure "*spin giù*", mentre nel mondo quantistico lo spin può essere in uno stato di sovrapposizione, ossia in una qualsivoglia combinazione delle due direzioni, per esempio il 40% "*spin su*" e il 60% "*spin giù*" (vedi *Figura 1*). L'intero sistema è, quindi, un aggregato incredibilmente complesso di sovrapposizioni di tutte le possibili combinazioni di spin di ciascuna particella.

Procedendo per l'analogia con l'esempio della sovrapposizione delle immagini sul vetro della finestra, a differenza di un bit classico che può solo contenere l'informazione "0" oppure "1", il qubit può teoricamente contenere sovrapposti tutti i possibili stati compresi tra |0> e |1>, ossia infiniti stati (vedi *Figura 2*). Si sarebbe così tentati di concludere che un solo qubit, almeno in linea di principio, possa tranquillamente contenere una quantità d'informazione pari a tutto lo scibile umano.

Figura 1 – L'elettrone, in funzione del proprio senso di rotazione su se stesso, puo' essere definito con "spin giu'" oppure "spin su" ed essere associato agli stati quantici |0> e |1>



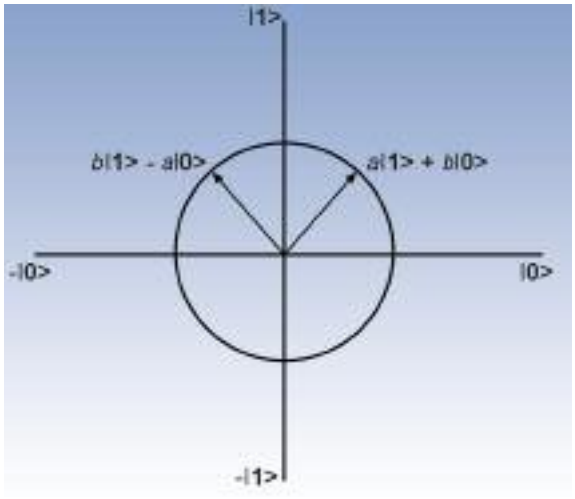


Figura 2 – Lo stato di un qubit [a |0> + b |1>] puo' essere rappresentato da un vettore che raggiunge qualsivoglia punto di una circonferenza se le ampiezze a e b sono numeri reali e se la somma dei loro quadrati e' uguale a 1

Ma, in termini pratici non è così, perché interviene un altro poco intuitivo principio della meccanica quantistica: quando si effettua un'osservazione (misura) su un sistema quantistico che è in sovrapposizione di stati questo "*collassa*" su un solo preciso valore. Va tenuto presente, infatti, che l'esito della misurazione dello stato di un qubit può essere soltanto |0> oppure |1>. Quindi, dalla misurazione di un qubit, è possibile ottenere la stessa quantità di informazione rappresentabile con un bit classico.

3 La potenza elaborativa di un computer quantistico

Ma se dalla misurazione di un qubit è possibile ottenere la stessa quantità di informazione rappresentabile con un bit classico, perché si afferma che un computer quantistico è enormemente più veloce e potente di un computer classico? La risposta si percepisce iniziando a confrontare la differenza tra i registri di bit classici e quelli di qubit quantistici.

Si inizi col considerare un registro classico composto da 3 bit. Un registro a 3-bit classico può contenere esattamente "uno" degli 8 diversi numeri possibili: in altre parole esso può trovarsi in una delle otto possibili configurazioni *000, 001, 010, 011, 100, 101, 110, 111*. Un registro quantistico composto da 3-qubit è in grado di contenere "tutti" gli 8 diversi numeri possibili contemporaneamente in una sovrapposizione quantistica.

Il fatto che 8 numeri differenti possano essere fisicamente presenti in contemporanea nello stesso registro è una diretta conseguenza delle proprietà dei qubit e ha delle grandi implicazioni dal punto di vista della Teoria dell'Informazione. Se fossero aggiunti più qubit al registro, la sua capacità di memorizzare informazioni crescerebbe in maniera esponenziale: 4 qubit possono immagazzinare fino a 16 numeri allo stesso tempo, e in generale N qubit sono in grado di conservare 2^N numeri contemporaneamente.

Un registro classico di 265 bit conterrebbe ad un dato istante "*uno solo*" dei possibili 5E79 valori scrivibili in esso. Un registro di 265-qubit, composto essenzialmente di soli 265 atomi, sarebbe capace di memorizzare "*tutti*" i possibili 2^{265} = 5E79 valori! Per tentare di capire quant'è grande 5E79, ossia un numero formato da 5 e seguito da settantanove zeri, è sufficiente sapere che il numero stimato degli atomi dell'intero Universo è 4E79.

Quando si rende necessario eseguire un calcolo quantistico molto complesso, composto da molti passaggi e quindi più operazioni sui registri, il vero vantaggio del Quantum Computing inizia a manifestarsi: quando un registro contiene una sovrapposizione di molti numeri differenti, infatti, un calcolatore quantistico è in grado di effettuare operazioni matematiche su tutti loro contemporaneamente, allo stesso costo in termini computazionali dell'operazione eseguita su uno solo dei numeri. E il risultato sarà a sua volta una sovrapposizione coerente di più numeri. In altre parole: è possibile eseguire un massiccio calcolo parallelo ad un costo computazionale irrisorio rispetto a quello richiesto dai computer classici, che avrebbero bisogno per compiere la stessa operazione di ripetere il calcolo 2^N volte o di poter contare su 2^N processori paralleli.

Si evince che questa macroscopica differenza di potenzialità tra computer classico e computer quantistico risiede nell'altissimo grado di parallelizzazione di quest'ultimo per via del fenomeno quantistico della sovrapposizione degli stati.

Per rendersi conto della potenza di un computer quantistico si può fare l'esempio del tempo necessario per fattorizzare un numero. Per "*fattorizzare un numero*" n si intende trovare un insieme di numeri tali che il loro prodotto dia il numero originario n.

Attualmente, per fattorizzare un numero di 300 cifre con un computer "*classico*" occorrerebbero alcune decine di migliaia di anni, mentre con uno quantistico sarebbero sufficienti pochi secondi. Da questo esempio si evincono le potenzialità applicative del quantum computing: crittografia, intelligenza artificiale, scienza dei materiali, farmacologia…

4 Ricerche innovative nel settore dei computer quantistici

La tecnologia attuale fa uso di un processo a 32 nano-metri ed è opinione condivisa che essa abbia quasi raggiunto il limite teorico stimato in 10 nano-metri; volendo ancora miniaturizzare i componenti e aumentare le velocità di processamento, bisognerà introdurre nuove tecnologie. Lo studio iniziò negli anni '60 in IBM (Landauer e Bennett) dove ci si chiese fino a che punto si potesse "miniaturizzare" un circuito per eseguire calcoli. Ben presto ci si rese conto che bisognava pensare in termini quantistici.

Le enormi potenzialità legate alla computazione quantistica hanno motivato negli ultimi anni un rimarchevole incremento degli investimenti per la ricerca, sia in ambito teorico che applicativo; inoltre, molti studiosi, primi tra tutti matematici e fisici, considerano questa disciplina uno strumento fondamentale per operare simulazioni non praticabili con le attuali tecnologie di calcolo.

Chi ha cominciato veramente a credere ai computer quantistici è stato Feyman nei primi anni '80, anche se una delle pietre miliari è degli anni '20 e si riferisce all'esperimento di Stern-Gerlach [4] per determinare se gli elettroni avessero un momento angolare intrinseco (spin).

In particolare una particella quantistica ha una specie di dono dell'ubiquità, fatto questo paradossale per la meccanica classica. Su questo principio si basa il qubit l'informazione può essere sia |1> sia |0> allo stesso tempo.

Un qubit è rappresentato da un vettore unitario di uno spazio di Hilbert. Per analogia con il caso classico chiameremo questi due stati |0> e|1>. Grazie al principio di sovrapposizione, è anche possibile combinare linearmente i due stati |0> e|1> per ottenere lo stato di sovrapposizione:

$$|\psi\rangle = a|0\rangle + b\,|1\rangle$$

in cui a e b sono due numeri complessi tali per cui $|a|^2 + |b|^2 = 1$.

Detto in altri termini, lo stato di un qubit è un vettore unitario dello spazio degli stati hilbertiano di dimensione 2, in cui gli stati speciali |0> e|1> formano una base ortonormale detta base computazionale.

Nel caso classico è sempre possibile esaminare un bit per determinare se esso sia nello stato (0) o nello stato (1), mentre nel caso quantistico, non è possibile esaminare un qubit per determinarne il suo stato, cioè per determinare i due coefficienti a e b.

Quando misuriamo lo stato di un qubit possiamo ottenere il risultato |0> con una probabilità $|a|^2$ o il risultato |1> con probabilità $|b|^2$.

C'è un numero infinito di combinazioni lineari della base ortonormale così da permettere, come si è detto, la rappresentazione in un unico qubit di tutto lo scibile umano.

Ma questa conclusione risulta erronea in virtù del comportamento del qubit in fase di misurazione. Va tenuto presente, infatti, che l'esito della misurazione dello stato di un qubit può essere soltanto |0> oppure |1>. Di più, la misurazione del qubit ne cambia inesorabilmente lo stato, riducendo la sovrapposizione in uno dei due specifici stati rappresentati dai vettori della base compu-

tazionale. L'interazione tra sistema quantistico e l'ambiente circostante determina il fenomeno della "decoerenza quantistica".

Nel gennaio 2009, il National Science and Technology Council (NSTC) degli Stati Uniti ha emesso un rapporto dal titolo "A federal Vision for Quantum Information Science"[2]. Il rapporto propone che "*The United States... create a scientific foundation for controlling, manipulating, and exploiting the behavior of quantum matter, and for identifying the physical, mathematical, and computational capabilities and limitations of quantum information processing systems in order to build a knowledge base for this 21st century technology.*"

Il professor Seth Lloyd del MIT insieme ad Avinatan Hassidim e Aram Harrow dell'Università di Bristol ha definito un algoritmo quantistico, che risolve sistemi lineari di equazioni in modo molto efficiente. La risoluzione di questi sistemi ha dei risvolti pratici in tutta una serie di problematiche tecniche ben precise: gestione e processamento dei segnali nelle comunicazioni, modellazione dei fenomeni climatici, modellazione in ambito genetico, analisi statistiche… Per tale ragione, disporre di un metodo veloce ed efficiente per risolvere numericamente questi problemi, migliorerebbe la vita di molti scienziati, spesso costretti a trovare soluzioni artificiose per processare terabyte o petabyte di dati.

L'algoritmo in questione permette la risoluzione di un insieme di equazioni lineari con una velocità che è esponenzialmente maggiore rispetto a quanto possa fare un algoritmo classico, non quantistico. Per la risoluzione di un sistema con *N* variabili, in genere un algoritmo classico impiega un tempo direttamente proporzionale a *N*, mentre il nuovo algoritmo quantistico impiega un tempo che è proporzionale al logaritmo di *N*.

Per quanto riguarda la velocità di processamento nei computer tradizionali, la maggior parte dei lettori conosce la famosa legge di Moore, che prevedeva il raddoppio della velocità dei processori ogni diciotto mesi; questa legge di previsione, fondata sui continui miglioramenti nella tecnologia di assemblaggio dei transistor nei chip, ha avuto dei riscontri positivi nel tempo, sebbene con qualche approssimazione. Ma nel settore della computazione quantistica le cose sono assai differenti.

Volendo fornire un'idea approssimativa delle potenzialità di un computer quantistico, è sufficiente sapere che esso, idealmente, potrebbe svolgere in un secondo un numero di operazioni che è 10E16 (10 milioni di miliardi) volte maggiore rispetto a quanto potrebbe fare il più veloce processore oggi disponibile sul mercato.

5 Basi tecnologiche su cui realizzare un computer quantistico

La realizzabilità fisica di dispositivi per QC è fortemente condizionata da un fenomeno noto come "decoerenza quantistica" [5], ossia l'inevitabile effetto dell'interscambio fra un sistema quantistico e l'ambiente in cui esso è immerso e ha bisogno di circuiti quantistici costituiti da porte logiche chiamate "quantum gates".

Un "quantum gates" è un dispositivo che ricevendo input, svolge un'operazione logica sulla base di essi e genera infine degli output.

Tra le tecnologie in studio per la realizzazione dei "quantum gates" [6] si possono citare:

1. **Il confinamento ionico lineare (trapped ions)**. Nel 1995 Cirac e Zoller [7] hanno messo a punto una tecnologia detta di *confinamento ionico lineare (trapped ions)*. Secondo questa proposta un gruppo di ioni viene sistemato linearmente in un'area di confinamento realizzata mediante opportuno campo elettromagnetico. I due stati stabili dei qubit, rappresentati dai vari ioni (un qubit per ione), sono dati dallo stato di riposo dell'ione e dallo stato di eccitazione del medesimo. I singoli ioni sono allineati come a formare un registro e possono essere singolarmente irradiati mediante impulsi di luce laser. Tali impulsi laser provocano transizioni negli stati

2 http://www.eas.caltech.edu/qis2009/documents/FederalVisionQIS.pdf

ionici eccitandoli convenientemente e, se il caso, posizionando questo particolare registro in uno stato di sovrapposizione. Gli ioni confinati nel registro hanno tutti la stessa carica ed esercitano l'uno sull'altro una repulsione mutua di tipo elettrostatico per modo che il movimento di ciascun ione si trasmette a tutti agli altri, creando vari possibili movimenti collettivi detti *fononi*. Con singoli raggi laser si può agire sui singoli ioni separatamente, in quanto la distanza interionica di separazione fra le particelle è stabilita in modo da essere molto più grande della lunghezza d'onda del laser di eccitazione. A mezzo di opportune manipolazioni è anche possibile realizzare correlazione (*entanglement*) fra le singole coppie di bit. Questo dispositivo costituisce un notevole passo avanti nella tecnologia di realizzazione di computer quantistici: esso permette di realizzare *bus quantistici*, in via di principio, delle dimensioni volute. Il tempo di decoerenza per qubit immagazzinati con confinamento lineare è stato misurato in migliaia di secondi. Il meccanismo di decoerenza più significativo, fra l'altro ancora non perfettamente chiarito, è il riscaldamento dei *modi* dei fononi. A partire dai risultati sperimentali finora ottenuti è prevedibile che entro i prossimi dieci anni sarà possibile realizzare registri a confinamento lineare contenenti qualche decina di ioni. L'ostacolo più significativo che dovrà essere superato è costituito dal fenomeno della decoerenza.

2. **Risonanza Magnetica Nucleare (NMR)**. Il metodo della risonanza magnetica nucleare[3] utilizza come supporto lo spin del nucleo atomico. È stato possibile con questo sistema realizzare semplici gate logici che agiscono su di un singolo qubit con l'uso dei campi prodotti con radiofrequenze, mediante i quali si può interagire sugli spin con buona precisione. Azioni più complesse dirette ad influenzare mediante un qubit molti altri qubit hanno trovato difficoltà di implementazione, per la necessità di far sì che gli spin interagiscano fra loro. I sistemi *NMR* si distinguono per il fatto che il segnale ottenibile da una singola molecola è troppo debole per essere rivelato; è, pertanto, necessario ricorrere a molte molecole per ottenere un segnale utilizzabile. Questa circostanza non costituisce di per sé un problema, in quanto per quantità minime di una sostanza chimica si ha a disposizione uno sterminato numero di molecole. La difficoltà nasce dal fatto di riuscire a fare in modo che tutte le molecole nell'effettuare il calcolo partano dallo stesso stato iniziale. Nel 1997, il problema è stato risolto da alcuni ricercatori riuscendo a ottenere uno *stato puro* da una miscela, ottenendo in tal modo di far partire il sistema dallo stesso stato. Alcuni ricercatori sono piuttosto scettici sulla possibilità di poter realizzare computer basati sul principio *NMR* funzionanti con molti qu-bit, dato che il rendimento del processo per l'ottenimento dello stato puro diminuisce sensibilmente al crescere del numero delle molecole. Sono segnalati anche problemi relativamente alla possibilità di riuscire a influire sui singoli spin in presenza di numerose molecole. Si ritiene che sia possibile arrivare in termini temporalmente accettabili alla sperimentazione di computer *NMR* con non più di 6 qubit. Questa dimensione consentirebbe, tuttavia, di risolvere alcuni interessanti problemi e sembra più a portata di mano rispetto a soluzioni ottenute con altre proposte.
3. **Spin nucleare basato sulla tecnologia al silicio**. Questa tecnologia è già collaudata con enorme successo in tutta la moderna tecnologia di produzione elettronica. L'idea è di incorporare gli spin nucleari in un dispositivo elettronico rivelandoli mediante opportune tecniche di controllo. Gli spin elettronici e nucleari sono accoppiati mediante l'interazione iperfine. Sotto convenienti condizioni è possibile effettuare un trasferimento di polarizzazione fra i due tipi di spin riuscendo a rivelare lo spin nucleare attraverso i suoi effetti sulle

3 La Risonanza Magnetica Nucleare è un fenomeno che può avvenire quando i nuclei di certi atomi sono immersi in un campo magnetico statico e vengono esposti ad un secondo campo magnetico oscillante.

proprietà elettroniche del campione. Sono già stati sviluppati dispositivi funzionanti a bassa temperatura su strutture di GaAs/$Al_xGa_{1-x}As$ che sono state incorporate in appropriate nanostrutture. I ricercatori ritengono che la realizzazione di Quantum Computer basati sulla tecnica al silicio sia un'eccezionale sfida che vada affrontata data la possibilità di sfruttare l'enorme rendita di posizione conseguibile dalla conoscenza tecnologica accumulata nella fabbricazione di dispositivi elettronici convenzionali allo stato solido. L'intento è quello di raggiungere ancora più piccole dimensioni e maggiore complessità di funzionamento. La proposta su cui si lavora è quella di utilizzare il silicio (Si) come *host* e il fosforo ($_{31}P$) come *donor*. A concentrazioni sufficientemente basse e alla temperatura di 1,5 K, è noto che il tempo di rilassamento degli spin elettronici ammonti a migliaia di secondi, mentre il tempo di rilassamento dello spin nucleare del ^{31}P è dell'ordine dei 10^{18} s, presentando quindi ottimi valori per la computazione quantistica. Il sistema proposto è anche in grado di fornire un buon isolamento dei qubit da qualsiasi grado di libertà che ne possa provocare la decoerenza. Con la tecnologia proposta diventerebbe possibile realizzare dispositivi per la computazione quantistica, codificando l'informazione negli spin nucleari degli atomi "*donor*" di dispositivi al silicio opportunamente drogati. Le operazioni logiche sui singoli spin verrebbero eseguite applicando campi elettrici esterni e le misure sui valori di spin verrebbero eseguite usando correnti di elettroni polarizzati di spin.

6 La memoria quantistica

Come per i computer tradizionali, anche il processore quantistico necessita di poter memorizzare gli stati di elaborazione: ovviamente su memorie quantistiche. Il 23 ottobre 2008, sulla rivista *Nature* [8], è stato pubblicato un articolo nel quale un team di scienziati, guidati da John Morton della Oxford University, descriveva un esperimento che rappresenta un enorme passo in avanti verso la computazione quantistica.

I ricercatori hanno drogato dei cristalli di silicio isotopicamente puri con atomi di fosforo e hanno proceduto a trasferire l'informazione di un qubit dagli elettroni dell'atomo di fosforo allo spin del nucleo, ritrasferendola in seguito agli elettroni. In altre parole, lo spin del nucleo di fosforo si è dimostrato un supporto fisico adatto ad immagazzinare un'informazione quantistica, anche se per ora per soli due secondi.

Nella computazione quantistica uno dei punti più delicati è proprio la conservazione dell'informazione e, sebbene già fosse noto che lo spin del nucleo poteva essere adatto per il processamento dei dati quantistici, la sua estrema "*sensibilità*", causata dalle influenze degli altri elettroni, ne impediva l'uso effettivo.

L'elemento determinante per ottenere detto risultato, da parte di Eugene Haller e Joel Ager, è stata l'azione chimica introdotta sul substrato di silicio. Il silicio naturale contiene infatti il 92.2% dell'isotopo 28, il 4.7% di silicio 29 ed il 3.1% di silicio 30: l'eliminazione dell'isotopo silicio-29, ha consentito di ridurre drasticamente l'interferenza del rumore nei confronti del processo di "*lettura e scrittura*" dell'informazione. Sempre secondo Haller e Ager con una base di silicio ancora più pura e controllata, in futuro le informazioni dovrebbero poter essere memorizzabili nei nuclei senza alcun limite di tempo.

Altrettanto importante il lavoro condotto dal team di scienziati presso l'Australian National University che è riuscito ad ideare un nuovo modo per conservare le informazioni trasportate per mezzo di impulsi di luce [9]. Gli attuali sistemi, che permettono di utilizzare tecnologie come la crittografia quantistica per rendere sicure le trasmissioni di informazioni sensibili, sono basati proprio sull'invio di dati tramite impulsi di luce; tuttavia, non è possibile coprire distanze maggiori di cento chilometri, restando entro un certo limite di affidabilità. Questa ricerca ha permesso di dimostrare che gli *echi* dei fotoni possono essere usati per creare un dispositivo di memoria quan-

tistica in grado di catturare, conservare e rilasciare le informazioni sulla trasmissione quando richiesto, senza imporre particolari limitazioni sulla distanza massima raggiungibile.

La tecnica consiste nell'assorbire la luce in una nuvola di atomi circondata da un avvolgimento di filo conduttore per poterla manipolare e rilasciare quando necessario. La bobina produce un campo magnetico, che causa un cambiamento nella frequenza degli atomi. Una volta assorbiti gli impulsi di luce, gli atomi iniziano a girare, tutti a velocità diverse tra loro, in accordo con il verso del campo magnetico; se quest'ultimo cambia la propria direzione, anche gli atomi invertono il loro comportamento. Nel momento in cui i movimenti degli atomi ritornano al loro stato precedente, si procede con l'emissione degli impulsi sotto forma di fotoni. Le informazioni trasmesse possono anche essere compresse o divise in più parti e possono venir richiamate in qualsiasi ordine, allo stesso modo di come un accesso casuale in memoria può richiamare un insieme di dati in un ordine qualunque.

Un ulteriore passo avanti nella memorizzazione quantistica è stato poi compiuto dal team guidato da Alex Kuzmich del Georgia Institute of Technology, ed è illustrato in un articolo pubblicato [10] sulla rivista *Nature Physiscs*. In sintesi, attraverso l'utilizzo di un complesso apparato sperimentale, è stato possibile immagazzinare un'informazione quantistica per 7 millisecondi, contro la precedente durata di 32 microsecondi; un tempo brevissimo, ma che sarebbe sufficiente per permettere la trasmissione dell'informazione a lunga distanza (anche un migliaio di chilometri) lungo una rete ottica. L'informazione trasmessa all'unità di memoria, è successivamente letta, attraverso un fotone convogliato da un raggio laser. A differenza di altre strategie di memorizzazione quantistica, gli scienziati dell'istituto della Georgia hanno utilizzato come base non un singolo atomo, ma un gruppo di 87 atomi, bloccati da un reticolo di raggi laser e portati ad una temperatura prossima allo zero assoluto per limitarne i movimenti (e quindi le interferenze).

Sfruttando le leggi della meccanica quantistica, è possibile prevedere lo stato del fotone in uscita dall'unità di memoria generato dal raggio laser usato per "leggere" l'informazione. È tuttavia essenziale che la rete contenga dei ripetitori dotati anch'essi di memoria quantistica, capaci di incanalare nuovamente il segnale sulla fibra ottica.

7 Primi calcoli con due qubit

Oltre alla difficoltà fisica di creare i qubit, esiste anche il problema, non indifferente, di poterli programmare. Scienziati del National Institute of Standards and Technology hanno sviluppato un processore quantico programmabile [11], capace di usare ioni ed elettroni come bit di dati. Ad oggi il processore è capace di processare due qubit e il sistema è stato realizzato manipolando due ioni di berillio con una serie d'impulsi laser, in modo da indurli a processare l'informazione, letta da un secondo laser. L'esperimento ha usato gli ioni per rappresentare 15 input classici, ossia usando tutte le possibili combinazioni di 1 e 0 che possono essere immagazzinate in due qubit. Usando questi stati di partenza, sono state effettuate 160 operazioni casuali, in seguito analizzate usando 100 sequenze sperimentali con nove differenti impostazioni d'analisi. In totale sono state quindi effettuate 900 prove per ognuna delle 160 trasformazioni. Ogni prova avviata sui qubit ha richiesto 37 millisecondi. La precisione ottenuta per ogni input è stata di oltre il 90%, ma quando questi sono messi insieme il dato di precisione scende al 79%. Questi errori possono essere drasticamente ridotti migliorando la stabilità del laser, che è uno dei maggiori fattori di errore, ma gli scienziati sono al lavoro per migliorare anche questo aspetto.

Sempre impiegando due soli qubit, anche il team del professor Andrew White della Facoltà di Fisica australiana dell'Università del Queensland, in collaborazione con l'Università di Harvard, ha condotto un esperimento di computazione quantistica rivolto ad una simulazione chimica [12]. Più precisamente, con sole 20 misurazioni quantistiche è stato possibile ot-

tenere con estrema esattezza l'energia dell'idrogeno molecolare. È importante rimarcare che attualmente, nelle simulazioni chimiche complesse effettuate con i calcolatori classici, i risultati contengono sempre un certo margine di approssimazione proprio per via della necessità di ridurre i tempi di elaborazione altrimenti improponibili anche per *mainframe* di grande potenza.

7.1 *La correzione degli errori nei computer quantistici*

È noto che la quasi totalità degli attuali dispositivi elettronici per la computazione e per le telecomunicazioni non potrebbero funzionare senza la correzione degli errori che inevitabilmente si generano a causa di interferenze esterne dovute al rumore prodotto dall'agitazione termica degli elettroni, alle correnti elettriche indotte e ai campi magnetici irradiati. Questo è vero anche per la computazione quantistica ed esiste un teorema chiamato "*teorema della soglia*", che asserisce che il computer quantistico può comportarsi in modo "*ideale*" solo se il numero degli errori è inferiore ad una certa soglia, stimata in misura di un errore ogni diecimila operazioni. Purtroppo i meccanismi fisici della computazione quantistica sono estremamente delicati e risentono facilmente di dette interferenze.

Gli scienziati del National Institute of Standards and Technology, proprio per ovviare agli errori nei preliminari calcoli a due qubit descritti in precedenza, hanno sviluppato una tecnica capace di ridurre drasticamente gli errori negli elaboratori quantistici, presentando i propri risultati in un recente articolo pubblicato su *Nature* [13]. La metodologia è stata sperimentata su una matrice di mille ioni di berillio portati a bassissime temperature e intrappolati da campi elettromagnetici, una configurazione fisicamente equivalente a una matrice di qubit. La matrice è stata quindi sottoposta a sequenze di impulsi di microonde, che ha portato alla riduzione delle interferenze accumulate. Michael J. Biercuk, uno degli autori dell'articolo, ha sottolineato che l'uso di questa metodologia permette di rimanere molto al di sotto della soglia stabilita del succitato teorema, ed è inoltre molto più vantaggiosa ed efficiente delle altre tecniche di eliminazione degli errori, perché viene applicata preventivamente.

8 D-Wave Systems: un chip da 128 qubit di informazione

Visto cosa si può analizzare con due soli qubit, si comprende la grande attenzione che la comunità scientifica internazionale rivolge oggi al prototipo di chip quantistico a 128 qubit realizzato da D-Wave Systems [14] (vedi *Figura 3*). Esso adotta l'approccio di "Spin nucleare basato sulla tecnologia al silicio" descritto nel capitolo 5 e fa uso della comune tecnologia per i microprocessori classici, sulla quale sono inseriti 128 anelli

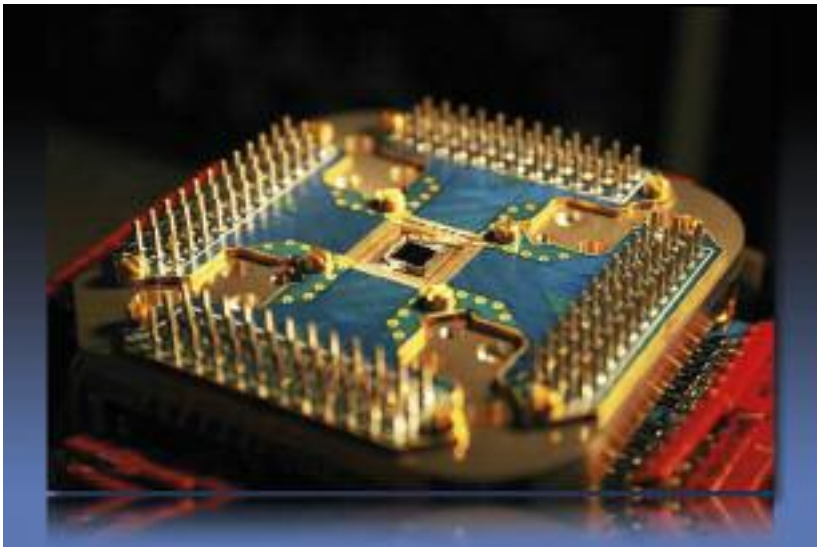


Figura 3 – Il processore quantistico adiabatico a superconduzione prodotto da D-Wave Systems

superconduttori di niobio, uno per ogni qubit di informazione. In ciascun anello scorre corrente in senso orario o antiorario, per rappresentare |0> e |1>; entrambe le correnti, presenti in contemporanea nello stato quantistico di sovrapposizione (*superposition*), rappresentano invece i qubit. Questi vengono manipolati da campi magnetici e l'intero sistema deve essere raffreddato fino a 0,01 °C sopra lo zero assoluto. Essendo i circuiti superconduttori relativamente grandi rispetto ad altri dispositivi che trattano singoli elettroni o fotoni, la loro costruzione è più semplice. Potrebbero essere infatti usate le stesse tecniche utilizzate per i semiconduttori.

La principale sfida da affrontare è stata il superamento della decoerenza, ovvero l'instabilità indotta nell'informazione registrata nel sistema dall'interferenza dell'ambiente esterno. I sistemi quantistici risultano infatti estremamente sensibili a qualsiasi interferenza e questo pone problematiche di non facile risoluzione. L'inconveniente è stato ovviato ricorrendo all'architettura di computer quantistico adiabatico a superconduzione, che consente al chip di tollerare il rumore termico intrinseco della materia e produrre risultati affidabili anche in assenza di un isolamento completo dall'ambiente.

Il dispositivo, per funzionare, deve essere portato alla temperatura critica di 5mK, vale a dire 5 millesimi di grado al di sopra dello zero assoluto (pari a circa 273,16 gradi Celsius sotto zero). Opportuni stadi di prefiltraggio permettono di regolare l'accoppiamento tra i singoli qubit, limitando al minimo l'influenza del rumore. Il processore è progettato per operare in coppia con un chip classico che funziona da controllore e interprete e che ne invoca il funzionamento ogni qual volta si presenti un compito che lo richieda.

8.1 *Google e D-Wave Systems: nasce il motore di ricerca quantistico*

Il processore quantistico a 128 qubit realizzato da D-Wave Systems, non è ovviamente sfuggito ai Google Labs. Ne è scaturita subito una collaborazione che ha portato alla realizzazione di un algoritmo dalle prestazioni incredibili. Il colosso di Mountain View ha affermato che un primo esemplare sarebbe già stato prodotto ed usato.

Google ha rivelato [15] che, dopo tre anni di lavoro sugli algoritmi quantistici, e sfruttando i qubit di D-Wave, un nuovo algoritmo è in grado di riconoscere e catalogare in maniera del tutto automatica gli oggetti partendo da immagini fisse o in movimento. Basato sulle potenzialità di accelerazione promesse dall'algoritmo probabilistico noto come algoritmo di Grover, il lavoro degli ingegneri di Mountain View, sempre in coppia con D-Wave, permetterebbe velocità di ricerca e classificazione mille volte più performanti di quelle eseguite su una potente architettura di computing tradizionale. Questo risultato consente ad un'ipotetica macchina di valutare, ad esempio, un oggetto tramite una telecamera e ricercare tutti gli oggetti simili a quello registrato, addirittura di visualizzare una parte di video e ritornare tutte le informazioni circa il titolo del film, gli attori…, oppure visionare le riprese di una telecamera che ha registrato un reato e fornire immediatamente i dati dell'indiziato.

9 La rete metropolitana cinese a crittografia quantistica

Wuhu è un'importante città cinese, interessante turisticamente ma soprattutto nota per le sue eccellenti università e laboratori di ricerca. Tra questi, vi sono i Key Laboratory of Quantum Information dell'University of Science and Technology of China. Qui è stata presentata una "Quantum Cryptography Network (QCN)" metropolitana per l'Amministrazione Governativa di Wuhu. Il progetto è stato pubblicato sul numero di settembre del *Chinese Science Bulletin* [16].

Questa rete fa uso della crittografia quantistica, basata su elementi fisici, piuttosto che complessi algoritmi software. In altri termini essa fa uso di una Quantum Key Distribution (QKD) unitamente ad un algoritmo noto nella comunità scientifica

come “one-time pad”. Questo algoritmo deriva dal “cifrario di Vernam”, noto sistema crittografico basato sul cifrario di Vigénère, al quale aggiunge il requisito che la chiave sia lunga quanto il testo e non riutilizzabile; per questo viene spesso chiamato OTP, acronimo per l'inglese *One Time Pad* (OTP), letteralmente "blocco monouso". Il cifrario di Vernam è l'unico sistema crittografico, la cui sicurezza sia comprovata da una dimostrazione matematica e per questo si è guadagnato il titolo di "cifrario perfetto".

Confrontata con i precedenti progetti, la rete Wuhu QCN implementa una struttura gerarchica multilivello e presenta tre differenti tecniche di networking. I nodi con differenti priorità ed esigenze si trovano in un backbone centrale, i collegamenti QKD si basano sul protocollo BB84 con il *decoy state method*, e il software di criptazione che gira su tutti i nodi è stato appositamente scritto.

Da un punto di vista fisico, questa rete quantistica implementa il noto interferometro di Faraday-Michelson, uno schema che garantisce la stabilità con auto-compensazione degli effetti negativi del canale trasmissivo. Alcune dimostrazioni sulla sua validità sono già state eseguite a Beijing-Tianjin nel 2004, a Beijing nel 2007, e hanno evidenziato la sua robustezza per applicazioni pratiche. La sicurezza del protocollo è garantita dal teorema di *no-cloning* [17]: esso è il risultato della meccanica quantistica, che vieta la creazione di copie identiche di uno stato quantistico arbitrario sconosciuto. Questo teorema è stato dimostrato da William Kent Wootters, e ha profonde implicazioni nel campo dell'informatica quantistica e campi correlati. Tuttavia, il teorema di *no-cloning* rende difficile l'instradamento del traffico. Per minimizzare queste problematiche, la rete Wuhu QCN utilizza le tecniche largamente usate di quantum router, switch ottici attivi, e trusted relay. I ricercatori si pongono anche l'obiettivo di eliminare totalmente hacker e trojan horse. La rete cinese si propone quindi non solo per le comunicazioni pubbliche sicure, ma anche come banco di prova per l'analisi approfondita delle reti QCN.

10 In Austria una rete quantistica lunga 200 km

Vienna diede i natali a due grandi fisici e premi Nobel, della meccanica quantistica: Wolfgang Ernst Pauli (1900-1958) ed Erwin Rudolf Josef Alexander Schrödinger (1887-1961). A Pauli si deve il principio di esclusione, che prese il suo nome, per il quale due elettroni non possono avere lo stesso stato quantico, perché sarebbero indistinguibili e più tardi il principio fu esteso a tutte le particelle con spin semi-intero (fermioni). Per questo principio Pauli ottenne il Nobel nel 1945.

Schrödinger, ancora fedele ai criteri di visualizzazione dei fenomeni, cercò un modello teorico per la meccanica quantistica ispirandosi alle idee di De Broglie sulla natura ondulatoria dei processi fisici e trovò un’equazione, che prese il suo nome, che descrive il comportamento delle onde associate alle particelle quantistiche. Per l'Equazione di Schrödinger, egli vinse il Premio Nobel nel 1933. Questi e altri eventi occorsi nei decenni successivi hanno da sempre conferito alla capitale austriaca un’interessante tradizione per quanto riguarda lo sviluppo nel campo della crittografia quantistica. Questa tradizione è ancor assai presente ai nostri giorni: la prima transazione di valuta con crittografia quantistica è stata effettuata da due istituti di credito austriaci il 21 aprile 2004.

Non sorprende quindi che, proprio nella capitale austriaca, si sia realizzata la più grande e complessa rete di elaboratori basata sui quanti mai realizzata, tanto da valerle il soprannome di “madre delle reti quantistiche”.

Lunga approssimativamente 200 km e dal costo di 11,4 milioni di euro, la rete connette sei località nei dintorni delle città di Vienna e St. Poelten; per trasmettere i dati essa sfrutta le proprietà quantistiche dei fotoni. Da quando fu proposta come idea, nel 1984, la crittografia quantistica è considerata praticamente inattaccabile. Per le leggi che regolano la fisica dei quanti,

un osservatore che tentasse di leggere i dati durante una trasmissione, nello stesso tempo li modificherebbe, permettendo a chi li riceve di rilevare l'attacco; questo fatto permette quindi un grado di sicurezza mai raggiunto nella trasmissione delle chiavi crittografiche. Peculiarità di questa rete, è l'alto grado di interoperabilità tra le varie tecniche di trasmissione: per la prima volta, tale rete è riuscita a mettere insieme, ad esempio, l'invio dei dati tramite fibra ottica e quello wireless, arrivando a risultare simile alle reti "classiche" su cui si basa Internet.

Una delle maggiori difficoltà incontrate nel conseguimento di questo eccellente risultato è stata quella di sovrapporre al livello trasmissivo in crittografia quantistica la classica suite di protocolli di rete TCP/IP, ossia una pila di protocolli dove ogni livello risolve una serie di problemi che riguardano la trasmissione di dati e fornisce un ben definito servizio ai livelli più alti. I livelli più alti sono logicamente più vicini all'utente e funzionano con dati più astratti, lasciando ai livelli più bassi il compito di tradurre i dati in forme, mediante le quali possono essere fisicamente manipolati. Questa difficoltà è stata superata, come è stato assodato nella prima dimostrazione di funzionamento della rete: nel caso di collegamenti interrotti è stato possibile effettuare nuovamente il routing dei pacchetti senza disturbi nella trasmissione, così come avviene per le reti ordinarie, grazie alla gestione da parte dei livelli più alti.

Questa rete quantistica è stata realizzata nell'ambito del progetto SECOQC (*Secure Communication Based on Quantum Cryptography*) [18]; i brillanti risultati conseguiti hanno indotto a compiere un secondo importante passo, ossia progettare una rete quantistica privata integrata all'attuale sistema di telecomunicazioni. Quest'attività è sponsorizzata da importanti partnership come Siemens e ID Quantique.

Sempre a Vienna si è svolto a luglio del 2009 un workshop sul "Quantum Information Science". All'evento hanno partecipato 180 delegati sia di organizzazioni accademiche sia di aziende, tra cui Microsoft e IBM [19].

11 Il teletrasporto fotonico: dalla fantascienza alle reali applicazioni satellitari

È opportuno citare anche le applicazioni di comunicazione quantistica ottica Terra-spazio, in particolare tra satelliti [20] che potenzialmente potrebbero permettere comunicazioni quantiche su scala globale. In questo modo si supererebbero i limiti attuali della trasmissione in fibra ottica attestati sul centinaio di chilometri. Il tutto è basato sul concetto di *free space optics* e teletrasporto fotonico. Tale fenomeno permette di ricreare in modo perfetto, in un punto diverso dello spazio, un qubit, ad esempio un fotone, il cui stato è sconosciuto a chi deve eseguire la trasmissione. In sostanza si trasporta lo stato quantistico del primo qubit su di un altro qubit, in modo che lo stato iniziale e quello finale siano uguali, pur riferendosi a qubit diversi.

La meccanica quantistica permette il teletrasporto dello stato di una particella e non la particella stessa, come un fotone, un atomo, un elettrone, uno ione…Facendo riferimento al caso che i qubit siano fotoni, possiamo pensare che l'informazione sia codificata nella loro polarizzazione.

Per descrivere il teletrasporto possiamo pensare ai seguenti elementi: il fotone, che chiameremo fotone 1, del quale si vuole teletrasportare la polarizzazione, e altri due fotoni, che chiameremo fotone 2 e fotone 3, i quali vengono generati in uno speciale stato quantistico, detto "*entangled*". Il fotone 2 viene ricevuto dall'osservatore A e il fotone 3 dall'osservatore B (vedi *Figura 4*).

In A i fotoni 1 e 2 arrivano nello stesso istante di tempo su di un *beam splitter*, cioè su uno specchio semiriflettente, (analogamente al precedente esempio della finestra) con uguale probabilità di trasmettere e riflettere la luce. Due rivelatori posti sulle due uscite del *beam splitter* misurano ciascuno un segnale che, da quanto detto, può essere causato, senza possibilità di riconoscimento, dall'arrivo del fotone 1 o del fotone 2. Il risultato della misura di A viene co-

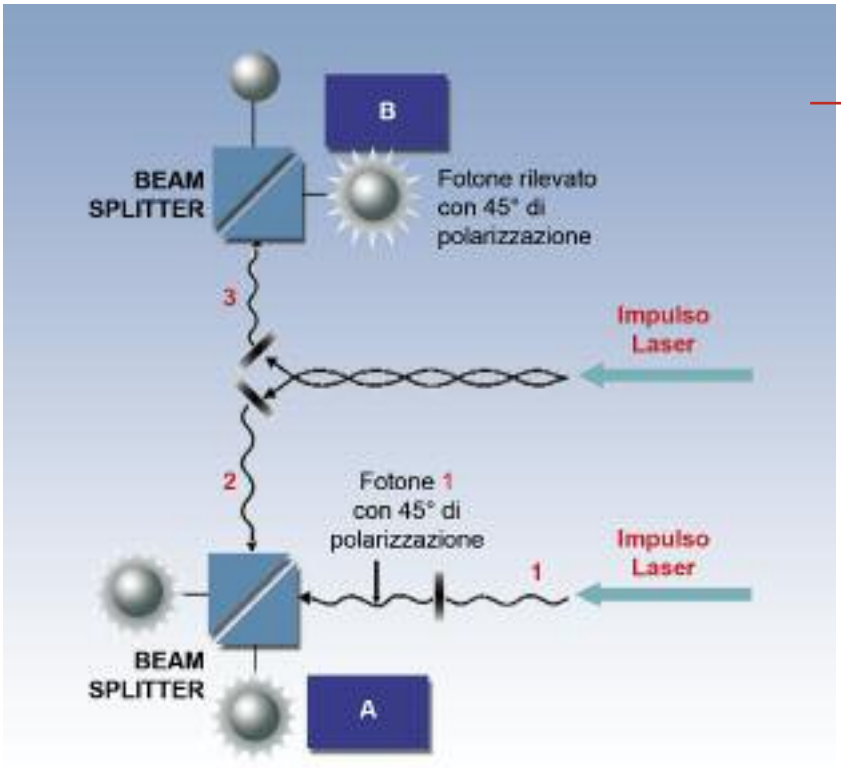


Figura 4 – Meccanismo concettuale per il teletrasporto fotonico

municato a B, che agisce in modo opportuno sul fotone 3. Grazie al fatto che i due fotoni 2 e 3 appartengono allo stesso stato *entangled*, il risultato dell'intera operazione è il trasferimento, cioè il teletrasporto, della polarizzazione del fotone 1 al fotone 3. È molto importante osservare che il teletrasporto non avviene istantaneamente dal momento che A deve comunicare il risultato della sua misura a B attraverso un canale classico, rispettando pertanto il principio di causalità, ossia il principio einsteiniano secondo cui nessuna informazione può viaggiare più veloce della luce.

Recentemente il Politecnico della California ha annunciato di avviare una serie di esperimenti sull'ipotesi di teletrasporto di oggetti inanimati. Come spesso accade, una tecnologia nata dall'immaginazione degli autori di fantascienza (il famoso teletrasporto della serie televisiva "*Star Trek*") si trasforma in un campo di studio della scienza e della tecnologia. Il principio del teletrasporto è già stato testato con successo su particelle elementari e successivamente su singoli atomi. Con l'esperimento del California Institute of Technology (Caltech) si vuole ora sperimentare il teletrasporto su oggetti "*più complessi*" [21].

Gli esperimenti saranno condotti dallo scienziato Darrik Chang, che tenterà di teletrasportare alcune sfere di silicio del diametro di pochi nanometri. Il sistema di teletrasporto proposto da Chang si basa sull'utilizzo della luce laser. Una singola sfera di silicio contiene milioni di atomi. Se l'esperimento di Chang andasse bene, si aprirebbe un nuovo campo di studio sulla materia e l'ipotesi del teletrasporto potrebbe diventare in futuro una realtà della tecnologia.

12 I prodromi dell'Internet quantistica

DARPA [22] è un'agenzia governativa del Dipartimento della Difesa degli Stati Uniti incaricata dello sviluppo di nuove tecnologie per uso militare. I team di ricercatori della DARPA stanno conseguendo una versione definitiva per un sistema di telecomunicazione quantistica. In particolare, recentemente, il team è riuscito a combinare la crittografia quantistica con le reti wireless, utilizzando la tecnologia *free space optics* prodotta dai britannici di QinetiQ [23] per la distribuzione senza fili di chiavi quantistiche.

Grazie anche all'aiuto di una company high-tech del Massachusetts, la BBN [24], il prototipo del network quantistico finanziato dal DARPA è ora svincolato dai fili: i dati potranno essere trasferiti in assoluta sicurezza e in modalità wireless, fino ad oltre venti chilometri di distanza.

QinetiQ, BBN e DARPA hanno definito il risultato conseguito "*un passo in avanti epocale*". Essi ritengono infatti che questo sia il passo decisivo verso una rete globale a crittografia quantistica, il "*futuro delle telecomunicazioni*". Per il momento il network sperimentale di nodi a crittografia quantistica, chiamati QKD, *Quantum Key Distribution*, è costituito da otto server connessi tra loro in maniera tradizionale, con fibra ottica, e due server che utilizzano *free space optics*. I nodi si trovano tutti negli USA e collegano l'università di Harvard, di Boston e gli uffici della BBN.

In merito a questi risultati congiunti tra compagnie britanniche e statunitensi, il governo britannico ha rilasciato una dichiarazione nella quale si asserisce che le reti basate sul sistema QKD sembrano offrire incredibili potenzialità per garantire un'ottima infrastruttura comunicativa in ambito bancario, ma soprattutto militare. Proprio come avvenne per Internet, rete nata nella guerra fredda per essere "*a prova di attacco atomico*", tutti concordano che tra non molto le reti quantistiche prenderanno piede creando un'Internet quantistica.

CONCLUSIONI

Come si evince dai precedenti paragrafi c'è oggi molto fermento sul tema della computazione e della comunicazione quantistica, sia a livello accademico, sia a livello di implementazione e commercializzazione di sistemi di telecomunicazione quantistica. Sebbene è qui impossibile riportare in modo esaustivo tutti gli attori coinvolti, a livello internazionale si segnalano i gruppi di Ginevra [25], di Vienna [26], Erlangen [27], Monaco [28], Cambridge [29], Waterloo [30] e Singapore [31].

Anche in Italia vi è un'intensa attività in ambito accademico, molto apprezzata a livello mondiale. Non a caso infatti IBM ha riconosciuto lo "*IBM Faculty Award*" [32], un premio legato a ricerche innovative nel campo dell'Informatica Quantistica e della Scienza dei Servizi alla Scuola Normale Superiore di Pisa e al Politecnico di Milano. Molto attivi anche i gruppi "*Quantum Information Theory Group*" [33] presso l'università di Pavia, il "*Quantum Optics Group*" [34] presso l'Università la Sapienza di Roma e l'Università di Padova [35].

Per la parte commerciale legata alla crittografia quantistica, IdQuantique [36] (spinoff dell'Università di Ginevra) e MagiQ [37] (New York) hanno entrambe in vendita un modello commerciale ormai stabile. Altre aziende, quali Toshiba e NEC, hanno progetti di sviluppo che potrebbero anche presto portare nuovi modelli sul mercato. Per l'Italia è da segnalare il laboratorio di ottica quantistica presso ELSAG (gruppo Finmeccanica) a Genova che conduce dal 2006 un progetto di R&S in crittografia quantistica [38].

Dinanzi a questa miriade di iniziative pratiche e teoriche si può ragionevolmente supporre che nel prossimo decennio (2011–2020) le computazioni e le comunicazioni quantistiche usciranno progressivamente dai laboratori per trovare concreta applicazione: gli operatori di TLC dovranno quindi prestare grande attenzione a questa rivoluzione tecnologica epocale e ai conseguenti nuovi servizi a valore aggiunto che ne scaturiscono.

In merito ad una previsione temporale più dettagliata sulla messa in campo delle reti quantistiche gli autori del presente articolo, entrambi fisici, preferiscono concludere con una celebre frase di uno dei padri della fisica quantistica Niels Bohr [39],: "*Prediction is very difficult, especially if it's about the future*".

BIBLIOGRAFIA

[1] http://it.wikipedia.org/wiki/Turing
[2] http://en.wikipedia.org/wiki/Rolf_Landauer
[3] http://it.wikipedia.org/wiki/Qubit
[4] http://en.wikipedia.org/wiki/Stern-Gerlach
[5] http://it.wikipedia.org/wiki/Decoerenza_quantistica
[6] Emanuele Angeleri, "Quantum Computing:

sogno teorico o realtà imminente", Mondo Digitale, numero 1 Marzo 2003, pp. 36-50

[7] Cirac JL, Zoller P: Quantum Computation with Cold Trapped Ions. Physical Review Letters, Vol. 74, 1995, p. 4091-4094.

[8] http://www.nature.com/nature/index.html

[9] http://www.sciencedaily.com/releases/2009/09/090911132308.htm

[10] Nature Physics 3, 219 - 220 (2007) - Cavity QED: Photons in single file - Alex Kuzmich

[11] http://www.nist.gov/public_affairs/releases/n02-07.htm

[12] "Towards quantum chemistry on a quantum computer" - B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik & A. G. White - Nature Chemistry 2, 106 - 111 (2009)

[13] "Optimized dynamical decoupling in a model quantum memory" - Michael J. Biercuk, Hermann Uys, Aaron P. VanDevender, Nobuyasu Shiga, Wayne M. Itano & John J. Bollinger - Nature 458, 996-1000 (23 April 2009)

[14] D-Wave Systems http://www.dwavesys.com/

[15] "Machine Learning with Quantum Algorithms" - Tuesday, December 08, 2009 - http://googleresearch.blogspot.com/2009/12/machine-learning-with-quantum.html

[16] Quantum Cryptography Network (QCN) - Fang-xing Xu et al. - Volume 54, Issue 17 (September, 2009) of the Chinese Science Bulletin

[17] Teorema di no-cloning quantistico - http://it.wikipedia.org/wiki/Teorema_di_no-cloning_quantistico

[18] http://www.secoqc.net/

[19] http://www.eas.caltech.edu/qis2009/program.html

[20] "Satellite-based quantum communication terminal employing state-of-the-art technology", Journal of Optical Networking - September 2005/Vol.4,No.9/ pp. 549-580

[21] "Cavity opto-mechanics using an optically levitated nanosphere" - D. E. Chang, C. A. Regal, S. B. Papp, D. J. Wilsonb, J. Yeb, O. Painter, H. J. Kimble, and P. Zoller - "Proceedings of the National Academy of Sciences" - November 10, 2009 - URL: http://www.pnas.org/content/107/3/1005

[22] DARPA (Defense Advanced Research Projects Agency) - http://www.darpa.mil/

[23] QinetiQ - http://www.qinetiq.com/global.html

[24] BBN - http://www.bbn.com/

[25] Universitè de Genève - http://www.gap-optique.unige.ch/

[26] Quantum Cryptography - http://www.quantenkryptographie.at/

[27] Institute of Theoretical Physics of the University Erlangen-Nuremberg - http://kerr.physik.uni-erlangen.de/qit/index.html

[28] Experimental Quantum Physic - http://scotty.quantum.physik.uni-muenchen.de/

[29] University of Cambridge - http://cam.qubit.org/

[30] Institute for Quantum Computing - http://www.iqc.ca/

[31] Centre for Quantum technologies - http://www.quantumlah.org/

[32] IBM Faculty Award - http://www.ibm.com/developerworks/university/facultyawards/index.html

[33] Quantum Information - http://www.qubit.it/

[34] Quantum Optics Group - http://quantumoptics.phys.uniroma1.it/

[35] "La crittografia quantistica: stato dell'arte" Tommaso Occhipinti – Università di Padova http://www.telecomitalia.it/content/dam/telecomitalia/en/archive/Notiziario2_2008/p25_32.pdf

[36] IdQuantique - http://www.idquantique.com/index.php

[37] MagiQ - http://www.magiqtech.com/MagiQ/Home.html

[38] Elsag Datamat - http://www.elsagdatamat.com/EN/PDF/Annual_report_2006.pdf

[39] Niels Bohr - http://it.wikipedia.org/wiki/Niels_Bohr

valter.bella@telecomitalia.it
angelantonio.gnazzo@telecomitalia.it

AUTORI

Valter Bella

laureato in fisica, fino al 2000 si è occupato, presso il Centro Ricerca di Telecom Italia, di microelettronica, partecipando a numerosi progetti di ricerca in ambito nazionale ed europeo. Tra il 2001 ed il 2003 ha condotto per TILab il progetto europeo PASTORAL, dedicato all'emergente tecnologia di Software Defined Radio. Nel 2004 si è occupato di nuove tecnologie wireless quali RFID e ZigBee e contestualmente ha affrontato lo studio delle nanotecnologie MEMS e delle antenne frattali. Dal 2006 è attivo, presso la funzione "Research & Trends", sul tema delle reti di sensori ed attuatori wireless con particolare riferimento alla parte radio e alle tecnologie alternative alle batterie quali l'energy scavenging e la wireless power transmission. È autore di parecchie pubblicazioni e brevetti internazionali ■

Angelantonio Gnazzo

laureato in fisica, nel 1988 è entrato in Azienda dove, fino al 1996, ha lavorato nel campo delle tecnologie per le fibre ottiche, contribuendo al progetto e alla realizzazione di fibre ottiche speciali (a dispersione spostata, a mantenimento di polarizzazione e drogate con terre rare) per la realizzazione di amplificatori ottici e sorgenti laser e dispositivi quali reticoli di Bragg. Nel campo dell'ottica integrata ha progettato e realizzato dispositivi selettivi in lunghezza d'onda, diramatori di potenza e amplificatori ottici. Dal 1996 e fino al 2000, la sua attività ha riguardato gli aspetti di misura sui portanti fisici e sugli impianti di telecomunicazione. Dal 2000 sta lavorando su tematiche di home networking, con particolare attenzione alle attività riguardanti lo studio e l'integrazione delle reti e dei terminali nell'ambito di scenari di servizio multi-play. Ha partecipato a diversi progetti nazionali ed europei, nonché seguito gruppi di normativa, in ambito sia Access Network sia Home Network ■

Uno sguardo alle evoluzioni tecnologiche di questa decade

INNOVAZIONE

Roberto Saracco

In questo articolo si passano in rassegna alcune aree di evoluzione tecnologica attese in questa decade, con un orizzonte al 2020, e si fanno alcune considerazioni sull'impatto specifico che ciascuna di queste può avere sull'evoluzione delle reti di telecomunicazioni, sia sotto il profilo di stimolo alla domanda di connettività e alla sua tipologia, sia sotto quello di abilitazione a nuove architetture di connessione. Nell'ultima parte si condividono alcune riflessioni più generali su come il complesso delle evoluzioni attese possa influenzare globalmente la domanda, la rete e l'infrastruttura dei servizi di un Operatore di Telecomunicazioni.

Le considerazioni che vengono svolte sono una sintesi delle attività di analisi sviluppate nei primi due mesi del 2010 da un gruppo di lavoro Telecom Italia interessato alle reti al 2020.

1 Introduzione

Sul versante dell'evoluzione "evolutiva" (quanto aumenta la capacità di memoria, il processing, la risoluzione degli schermi...) le previsioni passate si sono ragionevolmente verificate nei fatti (vale la regola che un treno in ritardo di quindici minuti viene cosiderato "in orario"… nel nostro caso uno slittamento di un 10% in più o in meno in termini di prestazioni o tempi sull'arco dei 10 anni) e quindi su queste sono abbastanza fiducioso rispetto alle previsioni che farò in questo articolo.

Viceversa, le previsioni fino ad ora fatte sulle tecnologie emergenti sono state in alcuni casi completamente sbagliate; un esempio per tutte quella sui SED e NED, tecnologie emergenti nel 2000, che promettevano di competere con Plasma e LCD per poi surclassarli nei successivi 5 anni e che invece sono rimaste emergenti e rin-

chiuse nei laboratori di ricerca. Quello che è successo, in questo caso, è stata la forte spinta del mercato alla produzione di schermi piatti, possibile solo con le tecnologie affermate dei Plasma e LCD che con i volumi ha portato ad un miglioramento dei processi produttivi, alla diminuzione rapida dei costi ed alla introduzione di evoluzioni "evolutive" che hanno rafforzato la vendibilità di queste tecnologie frenando investimenti per impianti dedicati alla produzione di nuovi schermi basati sulle migliori prestazioni di SED e NED. In altri casi la ragione alla base della errata previsione è stata diversa ma comunque abbiamo visto che poteva sempre essere ricondotta al mercato, al suo disinteresse verso nuove prestazioni piuttosto che alla spinta alla focalizzazione su tecnologie mature.

In questo articolo cercherò quindi di far tesoro di queste esperienze non per migliorare le previsioni, ma associando a queste un elemento di cautela quando l'evoluzione sia fortemente legata alla reazione del mercato.

Le roadmap tecnologiche presentate sono state affinate nel tempo e continuano ad essere monitorate ed aggiornate, per cui potrebbe essere interessante per il lettore andare a vedere la versione aggiornata sul sito del Future Centre di Telecom Italia. In questo articolo si è scelto di fornire un'analisi delle implicazioni di ciascuna roadmap.

I punti di partenza per la creazione di queste roadmap sono informazioni disponibili su Internet pubblicate da vari costruttori e informazioni che derivano dalla analisi di trend intercettabili da articoli e presentazioni effettuate in ambito IEEE e analizzate dal comitato sulle tecnologie emergenti di cui il Future Centre è membro.

Oltre alle roadmap vengono presentate tre sintesi su cosa queste evoluzioni possano significare rispettivamente in termini di sviluppo della domanda da parte dei fruitori del sistema di telecomunicazioni, di sviluppo dell'offerta abilitante (le reti di connessione) e di sviluppo dei servizi (con le relative piattaforme di supporto).

Queste sintesi sono state elaborate in un gruppo di lavoro che ha coinvolto varie funzioni aziendali nei primi due mesi del 2010 e che aveva per obiettivo lo stimolo di una riflessione sulle architetture di reti possibili nel 2020.

2 Storage

La capacità di memorizzazione è aumentata in termini macro, in modo abbastanza regolare a partire dalla metà degli anni '80, diminuendo al contempo di costo. In 25 anni gli hard disk sono aumentati di 100.000 volte in termini di capacità e hanno avuto una diminuzione di costo di 375.000 volte (attualizzato).

In questo periodo sono scomparse le cassette e i floppy e si sono affermati CD, DVD, flash memory, BluRay. I nastri magnetici, utilizzati sostanzialmente nei settori industriali per il back up di

Principali percorsi dello Storage

	2010	2015	2020
CONSUMER	■ Flash - 2-8 GB ■ Magn – 0.1- 1 TB ■ Opt – RO > 5 GB ■ Opt – RW < 5 GB ■ In a few Devices ■ Not connected	■ MRAM – 0.5 -2 TB ■ Magn – 2- 10 TB ■ Opt – RO Polymer ■ Opt – RW < 5 TB ■ In most Devices ■ Loosely Connected	■ Phase Ch- 0.1- 5TB ■ SolidState – 1-5 TB ■ Opt – RO > Polymer ■ Opt – RW < 20 TB ■ In many Objects ■ Wireless Connected
ENTERPRISE	■ Flash – 64-128 GB ■ MagnRaid – 0.1 PB ■ Dissem. Multi TB ■ Opt – RW 2 TB ■ LAN Storage ■ Loose Synch	■ Flash – 2 TB ■ MagnRaid – 1 PB ■ Dissem. Multi TB ■ Opt – RW 20 TB ■ WAN Storage ■ Wireless Synch	■ Flash – 8 TB ■ MagnRaid – PBs ■ Dissem. Multi TB ■ Opt – RW 50 TB ■ WAN Storage ■ Wireless Synch

grandi quantità di dati hanno perso un po' di smalto, progressivamente sostituiti dai RAID, rimanendo confinati a chi necessiti di back up di enormi quantità di dati con basso tasso di utilizzo.

Sono apparse nuove tecnologie, come le memorie a interferenza ottica (olografiche) e quelle a polimeri. In questa decade non si prevede alcun rallentamento nell'evoluzione degli hard disk e delle flash memory, arrivando quindi a capacità dell'ordine di 1-5 TB per le flash memory e di qualche decina di TB per gli hard disk. Le memorie a polimeri potrebbero sostituire i DVD (usati come storage mentre quelli usati come media per video scompariranno a favore dei Blu-Ray multifaccia) e le memorie a cambiamento di fase (tecnologia emergente, da vedere come il mercato reagisce) potrebbero ricavarsi una fetta nel settore *handheld* per i loro minori consumi.

Inoltre le memorie olografiche potrebbero trovare applicazione diffusa in processi industriali (in competizione con i mag tape) e nella logistica, ma avranno come competitor le RFID, per cui sarà da vedere chi prenderà il sopravvento. Una connettività ubiqua e sostanzialmente gratuita a larga banda va a favore delle RFID.

Ci si attende inoltre un progressivo *embedding* nelle flash memory di funzionalità di comunicazione wireless.

2.1 *Impatti*

Nei device e in molti oggetti sarà comune una notevole quantità di memoria, che renderà possibile un'interazione ricca di informazioni. Gli *handhled* avranno centinaia di GB e anche TB in dipendenza dal possibile uso locale di informazioni. Nelle case vi saranno svariati TB di informazioni connesse. La connettività alle informazioni sarà un elemento seamless, su cui si poggeranno servizi a garanzia dell'integrità e vita nel tempo delle informazioni con servizi di riconversione formati. La connettività, peraltro, non porterà, questa è una mia previsione, ad una diminuzione di richiesta e uso di memoria locale.

La memoria verrà considerata un elemento di comunicazione, un'estensione dell'uso odierno delle flash pen, e vi saranno oggetti di design che conterranno informazioni specifiche; ad esempio l'album delle foto potrà essere una memoria a forma di... album, con annessa una funzione di display delle foto, video, suoni contenuti. La fisicità di accesso al file potrebbe vincere sulla comodità di avere tutto all'interno di un "media centre", anche se l'uno non esclude l'altro.

La presenza di enormi quantità di memoria negli *edge* e una sostanziale replica di informazioni in più memorie fisiche porterà ad una equivalenza tra traffico dalla e verso la rete, rendendo praticabili soluzioni di comunicazione tra gli *edge* negli *edge* (senza interessare le reti metropolitane né i backbone).

La disponibilità di memoria in device e punti di accesso e fruizione tenderà a diminuire la necessità di streaming e le richieste da soddisfare in modo sincrono, a favore di comunicazioni *bulk* e differite, spesso in modalità push. Per queste si potrà ricorrere a delle boe informative posizionate in vari punti di passaggio come mall, caselli autostradali, scuole, uffici e ovviamente, abitazioni.

L'*information scavenging*, autorizzato e monitorato, permetterà a terze parti di offrire servizi personalizzati e servizi alla comunità.

3 Processing

I microprocessori hanno avuto un'evoluzione per molti versi simile a quella della capacità di memoria. Per quanto riguarda le memorie flash queste si avvantaggiano degli stessi miglioramenti nella produzione di silicio "*etched*", di cui si avvantaggiano i microprocessori. Come nel settore delle memorie si è vista un'evoluzione architetturale con utilizzo, ad esempio, di molteplici stati per cella, in modo da consentire la memorizzazione di più bit dove una volta era possibile memorizzarne uno solo, così nel settore dei microprocessori si sono sviluppate architetture multicore che ne hanno aumentato la capacità elaborativa.

	2010	2015	2020
CONSUMER	■ 2-4 Cr – Dedicated ■ Embedded Proces. ● Cell Phones ● Televisions ● Media Centre ● White Goods	■ 16 Cr – Shared ■ Embedded Proces. ● Smart Access ● Entertainment ● White Goods ● Robots	■ Processing on tap ■ Connected slates ● Smart Access ● Entertainment ● White Goods ● Robots
ENTERPRISE	■ 4 Cr – Dedicated ■ Embedded Proces. ● Smart Access ● Robots ● Smart tools ■ Thin C. – S.Farms	■ Multi Cr – Shared ■ Embedded Proces. ● Contex. Access ● Collab. Robots ● Shared Tools ■ Printed Electronics	■ Processing on tap ■ Embedded Proces. ● Distrib. Proces ● Robot Swarms ● Collab. Tools ■ Altern Comp Parad.

Principali percorsi del Processing

La crescita di capacità elaborativa per chip indicata da Moore dovrebbe continuare almeno fino al 2016 con le tecnologie che oggi si intravedono e fino al 2020 grazie a sistemi multicore tridimensionali, con comunicazione interna svolta con sistemi radio a 300 GHz e con comunicazione interchip su canali ottici, associati a sistemi di elaborazione con pardigmi non vonNeumann proseguirà perlomeno per quei settori di applicazione in cui è richiesta una elaborazione altamente parallela, tipo rendering, riconoscimento immagine, traduzione simultanea, proteinomica. L'effettivo sfruttamento di sistemi multicore dipende anche dal software che deve essere in grado di parallelizzare l'elaborazione. È anche prevedibile una convergenza tra CPU e GPU (Graphical Processing Unit).

Tuttavia, nel settore dei microprocessori, al di là di un'attesa crescita di capacità elaborativa nei prossimi dieci anni, l'interesse si sta spostando verso la riduzione di consumo energetico e verso la printed electronics (una tecnologia che permette la creazione di circuiti integrati "spruzzando" su una superficie qualunque le sostanze con cui si formano i transistor e i circuiti). La diminuzione di consumo energetico è stata presente fin dal primo transistor ed è proseguita con il progresso del livello di integrazione che ha portato a diminuire la tensione di alimentazione. Tuttavia la diminuzione specifica di consumo energetico è stata più che controbilanciata dall'aumento del numero di transistori per chip. Nuove tecnologie e architetture permettono di ridurre drasticamente il numero di transistori alimentati per chip sulla base del loro effettivo utilizzo, per cui negli ultimi due anni si è assistito, per la prima volta, ad un decremento significativo dei consumi (100 volte dal 2006 al 2010). Un ulteriore elemento che ha iniziato a caratterizzare l'evoluzione dei chip è l'inclusione sullo stesso *fab* della parte di comunicazione radio e, ancora in fase emergente, della parte di comunicazione ottica. Questo porta ad una significativa riduzione dei costi (di packaging) e in prospettiva, a 2 – 3 anni, alla presenza di sistemi di comunicazione radio/ottica su qualunque microprocessore.

La printed electronics sta decollando e nei prossimi anni è prevedibile che i processi di produzione si semplifichino, portando alla possibilità di stampa di circuiti simile a quella che è oggi la stampa di codici a barre su etichette. Questo aprirebbe un mercato significativo nella grande distribuzione. L'attrattività di questa tecnologia risiede nel costo comparabile a quello di una stampa inkjet a colori e nell'assenza di costi di packaging.

3.1 *Impatto*

Si può ragionevolmente ipotizzare che nel 2020 un grande numero di oggetti avrà una capacità elaborativa e comunicativa embedded. Se questa si accompagnerà ad un'infrastruttura (radio principalmente) pervasiva e a costo perce-

pito come nullo, ci si può attendere un notevole sviluppo di servizi "micro". Il traffico generato potrebbe, per un grande numero di oggetti, essere sporadico, mentre per altri potrebbe essere significativo.

La printed electronics, abbattendo i costi e permettendo di creare sistemi elaborativi on demand estremamente specializzati potrebbe aumentare ulteriormente il numero di oggetti, che diventano parte della rete di telecomunicazioni, trasformando questi nei nuovi terminali del 2020, mentre quelli di oggi saranno diventati nodi della rete.

Il bassissimo consumo energetico abiliterà non solo la diffusione massiccia dei sensori ambientali, trasformando settori come l'agricoltura (risparmio nei fertilizzanti che oggi per alcune monoculture costituiscono il 40% dei costi di produzione), ma permetterà anche l'inserimento di sensori nel corpo [1] con alimentazione basata su differenze termiche e consumo di zucchero, nonché la diffusione di sensori in edifici e strade, nei packaging di derrate alimentari e oggettistica varia per il controllo dei rifiuti, per la prevenzione sanitaria con segnalazione di presenza di virus e batteri. Complessivamente, quindi, la diffusione massiccia di sistemi di micro elaborazione renderà più controllabili e configurabili gli ambienti. Il flusso di dati sarà di tipo transazionale e, pur essendo significativo, non sarà paragonabile a quello generato da flussi video ma arriverà a volumi paragonabili al traffico voce.

La crescita di capacità elaborativa locale (che proseguirà e non collasserà nel cloud, anzi, porterà ad una estensione del concetto di cloud ai device) permetterà rendering video e riconoscimento di immagini che a loro volta stimoleranno una crescita di uso (non di richiesta) di banda.

[1] L'inserimento di sensori, attuatori e capacità elaborativa nel corpo umano pone in primo piano gli aspetti di transumanesimo, un concetto che esprime il passaggio ad una situazione di aumentata capacità della persona raggiunta tramite sistemi artificiali embedded, Si veda ad esempio il progetto x10 del MIT in cui l'obiettivo è di aumentare di un fattore 10 le capacità di un individuo.

4 Visualizzazione

I sistemi di visualizzazione sono cambiati significativamente negli ultimi 20 anni con l'avvento degli schermi "piatti". La penetrazione nelle famiglie è considerevole, al punto che si inizia a notare una flessione in diversi mercati di paesi sviluppati, essendo in fase di esaurimento il replacement dei vecchi televisori. L'assenza in Italia di una buona offerta di contenuti HD (in pratica visibili solo a pagamento) dovrebbe essere superata nei prossimi anni, spingendo ad un replacement di quei televisori (molti), che non sono full HD. Dopo il 2015 è probabile l'ingresso di schermi ultra HD, 4k 8Mpixel, in grado di fornire un senso di presenza molto forte, sia per dimensioni sia per definizione. La tecnologia LCD è destinata a dominare il mercato per buona parte di questa decade, anche se nella seconda parte dovrebbero affiancarsi le tecnologie OLED (oggi ancora troppo care e limitate a schermi fino a 11" a prezzi abbordabili) e quelle NED, che diventano indispensabili a dimensioni dell'ordine dei 57" e inferiori per consentire le definizioni 4k. La dimensione dei pixel LCD non può infatti essere ridotta oltre certi limiti in quanto diminuisce la luminosità e inizia a prevalere il dielettrico di separazione tra i pixel portando ad uno schermo "nero" (stesso motivo per cui non ci sono schermi al plasma di dimensioni inferiori ai 32").

Le tecnologie che consentono di visualizzare immagini basandosi sulla riflessione della luce ambientale si stanno affermando oggi con la crescita degli eBook reader. Ad oggi quella che è più utilizzata è eInk, ma sono apparsi prototipi basati su altri principi. Nel corso di questa decade queste tecnologie dovrebbero maturare significativamente. Per fine decade dovrebbero essere disponibili tecnologie in grado di visualizzare immagini a colori e in movimento (la luminosità è in funzione della luce ambientale e la risoluzione non raggiungerà quella di uno schermo NED). Per contro queste tecnologie promettono schermi ultrasottili, a livello della carta, bassi consumi e sono in grado di adattare lo schermo a qualunque superficie, anche curva. Lo strato elettronico

	2010	2015	2020
CONSUMER	■ LCD, LED, Plasma ■ 1920*1080 ■ up to 52” ■ Reflective Scr.7-10” ■ OLED < 4” ■ Most Dev. with Scr.	■ LED, 3D ■ 3840*2160 ■ up to 57” ■ Colour Reflec. Scr. ■ OLED < 42” ■ Several Obj. w Scr.	■ NED, OLED, 3D ■ 3840*2160 + ■ Embed. MultiTouch ■ Embed. Camera ■ Phase Reflec. Scr. ■ Most Obj. w Scr.
ENTERPRISE	■ LCD, LED, Plas., 3D ■ 1920*1080 ■ up to 67” ■ Reflective Scr. 10” ■ Fog Screen ■ 24h*7d	■ LED, NED, 3D ■ 3840*2160 ■ up to 103” ■ Phase Reflec.Scr. ■ Holo Screen ■ 24h*7d	■ NED, OLED, 3D ■ 7680*4320 ■ up to 150” ■ Print. Reflec.Scr. ■ Holo Screen ■ 24h*7d

Principali percorsi della Visualizzazione

si basa su silicio amorfo (non quello cristallino come quello usato negli schermi di oggi). I costi dovrebbero essere paragonabili, per alcune di queste tecnologie, a quelli della carta, anche se non segneranno la scomparsa della carta. Intere pareti potranno essere ricoperte con questi schermi.

Sistemi a microproiezione saranno abbastanza diffusi negli handheld, anche se permane il problema dei consumi e della stabilizzazione dell’immagine. La visualizzazione tridimensionale si svilupperà notevolmente prima in ambiente pubblico (cinema) e poi in quello privato anche se a fine decade continueranno a prevalere i sistemi di visualizzazione bidimensionale in casa con eventualmente la presenza di schermi 3D specializzati ad un uso per gaming ed education. Nel settore business la penetrazione del 3D potrebbe essere maggiore in settori in cui questa sia funzionale alle attività svolte.

Il problema della visualizzazione 3D generalizzata rimane quello di una difficoltà visiva cerebrale, che porta in molti a un senso di nausea o disagio, il che non consente una visione prolungata. Questi tipi di problemi sono legati all’interpretazione delle immagini da parte del cervello e non sono quindi risolvibili in termini di miglioramento tecnologico.

Le tecnologie di proiezione olografica miglioreranno, ma restaranno lontane dal ricreare una percezione reale e saranno relegate ad applicazioni di nicchia e gadget.

Notevoli sviluppi si avranno negli schermi indossabili e nelle proiezioni retiniche. Queste, insieme ai sistemi di proiezione contestualizzata, daranno forte impulso alla realtà aumentata, che dovrebbe essere esperienza comune e generalizzata nel 2020.

4.1 *Impatto*

La combinata disponibilità di tecnologie di visualizzazione ad alto impatto e a costi contenuti stimolerà la crescita della comunicazione visiva a tutti i livelli. L’alta risoluzione presupporrà la disponibilità di canali di comunicazione oltre i 50Mbps a livello residenziale (verosimilmente oltre i 200 Mbps ipotizzando una presenza di più fruitori facenti capo ad una stessa linea di comunicazione). La presenza diffusa, verso fine decade, di carta-schermo abiliterà nuovi sistemi di pubblicità e di interazione con i clienti per negozi, grandi magazzini ambienti, portando a notevoli esigenze di banda locale. Quanto questa banda sarà solo locale piuttosto che una banda fornita dalla rete dipenderà dall’effettiva capacità della rete e convenienza economica nel fornirla. È possibile che grandi magazzini e negozi si organizzino con soluzioni locali, utilizzando, eventualmente, canali di connessione verso la grande rete per interagire con servizi di controllo.

Lo spostamento verso una comunicazione vi-

	2010	2015	2020
CONSUMER	■ Higher quality demand ■ Increased Traffic generation	■ Bandwidth Demand increased to 50 Mbps Fixed 4 Mbps Mobile	■ Bandwidth Demand increased to 100 Mbps Fixed 10 Mbps Mobile
ENTERPRISE	■ Niche usage of video for Biz through the Ntwk	■ Broader usage of video in specific areas of retail ■ Widespread use in tourist engagement	■ Product as a Service ■ Increased transact. Demand ■ Distributed DB with flash update

Impatti della Visualizzazione sulla rete

siva aumenterà ulteriormente la focalizzazione dell'utilizzatore sul terminale-ambiente a scapito della rete. Peraltro lo spostamento verso una comunicazione visiva renderà possibili ed appetibili classi di servizio studiate da anni: telepresenza, telelavoro, gaming immersivo, education. Se si riuscirà a realizzare un'offerta di servizi "avvincente" per le aziende che offrono connettività i ricavi potrebbero essere proporzionali ai problemi risolti e non alla quantità di banda utilizzata. Le aziende potrebbero essere interessate ad investire sulla teleperesence se questa offre dei vantaggi competitivi… questo mercato potrebbe essere "ricco". È comunque un mercato aperto a molti player, non solo a chi offre connettività.

5 Sensori

L'evoluzione dei sensori è il risultato di un convergere di varie tecnologie, dai MEMS, alle nanotecnologie, alle biotecnologie (specie per applicazioni di health care e ambientali, ma non solo), ai sistemi radio, all'elettronica e al software.

Il risultato è la disponibilità di sensori sempre più piccoli, flessibili nel loro utilizzo, a basso costo, comunicanti. Sono partiti diversi progetti, tipo CENSUS di HP, che danno per scontato la presenta di migliaia di miliardi di sensori attivi a fine decade, cooperanti in misura più o meno coordinata.

Principali percorsi dei Sensori

	2010	2015	2020
CONSUMER	■ Stand alone ■ Embedded ■ Function Orientated • Movement • Weather • Ambient	■ Connected ■ Basic Component ■ Function Orientated • Identity • Health care • Energy	■ Meshed ■ Disseminated ■ Function Orientated • Presence • Embodied • Society
ENTERPRISE	■ Local Connection ■ Embedded ■ Function Orientated • Logistics • Agriculture • Robotics	■ Remote Connection ■ Flexible sensing ■ Function Orientated • Service Ctr • Enterprise mgt • Civil Engineer.	■ Shared Connection ■ Open Platform ■ Function Orientated • CRM • Intelligent Ctr • Responsive A.

I sensori diverranno parte integrante della maggior parte dei prodotti e saranno una presenza costante in moltissimi ambienti, naturali e artificiali. Parte della sensoristica embedded sarà mirata al miglioramento dell'interazione con l'utilizzatore (interfacce aptiche) e si vedrà un'integrazione di sensori negli schermi.

I sensori ottici per rilevamento di immagini saranno presenti in molti ambienti e device e permetteranno una comprensione da parte della periferiche del livello di soddisfazione dell'utilizzatore, attivando comportamenti conseguenti.

L'evoluzione della sensoristica rivolta all'health care e alla biometrica permetterà di realizzare sistemi efficaci di controllo dell'identity nel caso di persone e animali (le tag RFID evolveranno trasformandosi in sensori). L'accettabilità di tecnologie biometriche embedded non è chiara, anche se in molti casi questa evoluzione sarà accettata. La biometrica esterna sarà comunque diffusa ed efficace.

5.1 *Impatto*

La comunicazione sarà un elemento fondamentale nei sensori ambientali ed è evidente che i sensori embedded in prodotti e oggetti li rendano più flessibili, adattabili e interattivi, portando quindi ad esigenze di comunicazione e contribuendo a trasformare prodotti in servizi.

Interessante notare come i cellulari stessi possano essere, e saranno, dotati di sensori, venendo quindi a formare una rete di sensori che, nel 2020, sarà composta da 6 miliardi di punti! Gli Operatori sono nelle condizioni migliori per estrarre informazioni da questa sterminata rete di sensori.

La quantità di dati generati da questa miriade di sensori sarà enorme, ma probabilmente l'impatto in termini di richiesta di capacità di trasporto sarà contenuto (ma con volumi simili alla voce). Molti sensori saranno aggregati in reti mesh autocostruite e gran parte dell'analisi si richiuderà all'interno di queste reti e all'esterno della "Rete".

Per contro la gestione di gran parte di questi sensori genererà opportunità di business per varie aziende e potenzialmente gli Operatori possono essere degli attori importanti. Infatti, i service provider potrebbero essere interessati a modelli di diffusione degli eventi gestiti dalla rete di tipo transazionale (ad esempio evento-comando o in generale pubsub). In questo modo le applicazioni potrebbero essere semplificate e la diffusione dele informazioni controllate e determinate a partire da policy dinamiche che il service provider può richiedere all'Operatore.

Parte dei sensori richiederanno connettività wireless con elevati livelli di qualità.

I business models per la gestione di questi sensori non saranno orientati al consumo di banda, ma alle caratteristiche del servizio richiesto. L'internet delle cose e con le cose si avvarrà della presenza di questi sensori.

Sensori biometrici saranno sempre più utilizzati per l'identificazione personale e questo diminuirà da un lato il ruolo della SIM e dall'altro aprirà il business dell'identificazione a terze parti.

6 Terminali Mobili

I terminali mobili catalizzeranno le migliori tecnologie disponibili e saranno all'avanguardia nella loro diffusione al mass market, visti i cicli velocissimi di rinnovamento di gamma. Vi saranno al 2020 probabilmente due piattaforme consolidate di sistema operativo oltre ad una di tipo Open Sw (Linux). La capacità elaborativa dei cellulari di oggi, dual core chip in alta gamma, salirà, arrivando nel 2020 a sistemi oltre i 64 core con una capacità elaborativa superiore di almeno 10 volte a quella di un desktop top di gamma di oggi.

Avranno una capacità di memorizzazione superiore al TB, coppia di telecamere per riprese 3D (solo alcuni modelli) e sensore fotografico con una decina di Mpixel (il limite non è tecnologico ma di utilità oltre al fatto che all'aumentare dei pixel aumenta il rumore degradando la qualità). Alcuni saranno dotati di microproiettore.

2010	2015	2020
■ Dual core chips available. ■ Processors 5K DMIPS ■ Smartphones up to 32 GB, notebooks up to 128 GB SSD. ■ 2D cameras ■ Average phones have 5 Mpixel camera. 12 Mpixel on top phones. ■ 1080p video recording on top phones ■ HSPA 1-28 Mbps	■ 16 Core chips available. ■ Processors 50K DMIPS ■ Smartphones can be sold with 256GB SSD, notebooks 1TB+ onboard . ■ 2D + 3D cameras ■ 20 Mpixel CCD image sensors possible but useless ■ HD video recording / playback in high end devices ■ LTE 10-100 Mbps ■ Projector Embedd.	■ Massive (>64) multi-core chips ■ Processors 500K DMIPS ■ Flash (up to 4 bits / cell), DRAM & CMOS available at 10-15 nm (presumed limit). ■ 3D cameras ■ Possible the 50 Mpixel CCD sensor ■ HD video recording & play a commodity. ■ Tiny affordable pico-projectors commodity on handsets. ■ LTE-advanced 100 Mbps - 1Gbps

Principali percorsi dei Terminali mobili

Diversi cellulari incorporeranno sensori, anche di tipo medicale. Il cellulare sarà in grado di connettersi ad una varietà di reti, negoziando la banda sulla base del servizio richiesto. La velocità di punta (teorica) potrebbe arrivare ai 100Mbps, ma, più importante, la connessione dati intorno ai 5Mbps sarà garantita dalla rete radiomobile e in contemporanea i terminali saranno in grado di selezionare l'accesso più idoneo tra quelli disponibili. Molti cellulari saranno scomparsi all'interno di oggetti, abilitando la connettività radio. In particolare giocattoli, veicoli di qualunque tipo, libri, elettrodomestici, garanzie di prodotti avranno un cellulare incorporato a supportare la comunicazione embedded.

I cellulari in una certa area saranno in grado di dialogare tra loro risolvendo problemi di interferenza aumentando quindi la banda effettivamente disponibile. Saranno inoltre in grado di dialogare con una varietà di devices e oggetti, operando come gateway. In alcuni casi e in alcune aree potrebbero funzionare come nodi di una rete mesh, ad esempio quelli a bordo di autoveicoli, aumentando ulteriormente la banda complessivamente disponibile.

Tecnologie biometriche "on-board" consentiranno il riconoscimento del proprietario o di altre persone autorizzate e il cellulare si configurerà sulla base dell'utilizzatore.

Tra i terminali mobili si possono includere anche i robot, anche se questi meriterebbero una loro roadmap specifica, ma possono essere inclusi in questa per l'assonanza che hanno dal punto di vista della rete e della gestione con oggetti dotati di cellulare embedded.

6.1 *Impatto*

La pervasività dei terminali mobili sarà totale. Si avranno terminali personali, alcuni fortemente basati su video, terminali di ambienti (ad esempio autoveicoli) e terminali embedded in oggetti principalmente deputati a traffico dati M2M e M2P. Tra questi ultimi si possono comprendere i robot, che avranno una diffusione importante sia in ambienti lavorativi, sia residenziali.

I terminali continueranno, sempre più, a guidare l'evoluzione e saranno i terminali a dettare l'evoluzione della rete in termini di domanda prima e di struttura poi. Infatti le capacità di processamento locale, la disponibilità di enormi quantità di dati eventualmente utilizzabili come cash pubbliche e la possibilità di creare reti locali ad hoc li renderenno un'alternativa architetturale alla rete in alcune situazioni. Certamente autoveicoli in una città potrebbero creare delle reti dati mesh estremamente potenti, che, agganciandosi a grandi boe che emettono informazioni su richiesta, potrebbero costituire alternative alle reti pubbliche per una varietà di servizi. La realizzazione o meno di queste reti non sarà in funzione della possibilità tecnologica, ma nella praticabilità di un bisiness model operante su li-

velli di costi marginali. Se gli autoveicoli, ad esempio, per motivi indipendenti dall'obiettivo di creare una rete mobile, dovranno essere dotati di sistemi di comunicazione, (ad esempio per realizzare sistemi anticollisione e gestione automatica dei flussi di traffico, con auto che diventano robot per imposizione legislativa) e utilizzeranno ricariche elettriche quando parcheggiate (probabilmente in tempi più lunghi rispetto al 2020 perlomeno in Italia) allora quegli stessi sistemi realizzati per altri scopi potranno essere utilizzati anche per creare reti ad hoc di telecomunicazioni. Questo porterebbe a notevoli cambiamenti nel modo di concepire una rete di accesso.

7 Riconoscimento Immagini

La potenza elaborativa unita a sterminate banche dati e alla progressiva indicizzazione semantica di miliardi di immagini renderà il riconoscimento di immagini un'ovvietà. L'approccio si sposta da un'analisi intelligente con algoritmi di identificazione di contorni e piani di immagine ad analisi statistiche e pattern matching che, in ultima analisi, si dimostreranno più efficaci. Il riconoscimento di immagini affiancherà i sistemi di localizzazione per la determinazione del contesto.

Tecnologie di riconoscimento di espressioni per l'auto adattamento delle interazioni diverranno sempre più comuni, così come il riconoscimento dei gesti. Questo porterà a sistemi di interfaccia significativamente diversi da quelli attuali, ad esempio facendo scomparire il telecomando nella interazione con il televisore e più in generale con i sistemi di intrattenimento domestico. Alcune applicazioni medicali sfrutteranno il riconoscimento di immagini (gait control) per la diagnosi precoce di certe patologie. Il riconoscimento di immagini, eventualmente associato a sistemi biometrici, diventerà parte del sistema di identificazione personale.

7.1 *Impatto*

Le interfacce saranno sempre più naturali e si svilupperanno molti servizi basati su riconoscimento e contestualizzazione. Il bilanciamento tra quanto sarà fatto in locale, all'interno del terminale, e quanto invece sarà fatto attraverso la rete potrebbe avere degli impatti sul traffico. In generale si può presumere che verranno realizzate soluzioni a costo minimo, il che però significa che in presenza di regimi completamente flat il costo minimo per un fornitore di servizi potrebbe essere quello di eseguire il riconoscimento da remoto e non nel terminale.

Il riconoscimento di immagini è un significativo enabler per tutti i servizi di realtà aumentata e molti terminali si trasformeranno in lenti di ingran-

Principali percorsi del Riconoscimento dell'immagine

	2010	2015	2020
CONSUMER	■ Assisted - Small Set ● Face Rec. ● Landmarks Rec. ■ Autonomous ● Expression Rec. ● Gesture Rec.	■ Embedded ● in Apps ● in Devices ■ Exploitation ● Presence ● Interaction	■ Basic Component ● Appliances ● Devices ■ Exploitation ● Interface ● Access Control
ENTERPRISE	■ Assisted - Large Set ● Face Rec. ■ Autonomous ● Face Spotting ● Landmarks ● Behaviour	■ DB component ● Product Ident. ● Serv. Support ■ Exploitation ● CRM ● Security	■ Process Component ● Robot Funct. ● Open Identity ■ Exploitation ● Search ● Design

dimento, in grado di associare alla realtà fisica, opportunamente riconosciuta, informazioni e servizi presenti nel mondo virtuale. L'intermediazione tra questi due mondi sarà un elemento estremamente importante, in cui il fattore principale è il trust. Le tecnologie forniranno quanto serve per una "seamless experience" entro la prima metà di questa decade.

8 Interfacce "naturali"

L'evoluzione in tutti i settori precedentemente citati verrà sfruttata per semplificare le interazioni con qualunque oggetto e servizio rendendole il più naturali (real life, seamless) possibili.

Alle tecnologie precedentemente citate si aggiungono quelle di rilevazione di campi magnetici (nel caso di particolari patologie, come tetraplegie) per la trascodifica dei pensieri in azioni. Nel 2020 è ragionevole aspettarsi una capacità di interazione da parte delle macchine (embedded negli oggetti che diventano assimilibili a robot) quasi umana.

Inoltre l'affinamento e semplificazione di tecnologie aptiche (tecnologie che permettono di trasferire sensazioni complesse, incluso il tatto e l'accelerazione) consentiranno di coinvolgere il tatto nella comunicazione con gli oggetti reali e virtuali. In questo settore giocheranno un ruolo abilitante gli sviluppi nel settore delle nanotecnologie e degli smart materials, tra cui i materiali a memoria di forma. Per il 2020 il riconoscimento della voce e comprensione del parlato con traduzione in tempo reale tra ogni lingua sarà una realtà pervasiva e scontata, come oggi è il rilevatore ortografico di errori in un programma di battitura.

8.1 *Impatto*

La naturalezza dell'interazione aumenterà probabilmente la frequenza delle interazioni e il senso di presenza fornito dalle interfacce a oggetti remoti aumenterà il loro utilizzo tramite la rete.

Per molti servizi, che sfruttano il senso del tatto, diventa cruciale una bassissima latenza di rete e a sua volta questa potrebbe richiedere architetture che avvicinano il punto di risposta al punto di interazione.

Nel fornire il senso di presenza giocano la qualità dell'immagine, la fluidità e sincronizzazione dei movimenti, la possibilità di interazione a gesti e quella di toccare oggetti. La tridimensionalità potrebbe non essere così cruciale e anzi potrebbe rendere non naturale l'interazione (problema del blocco nel passaggio tra piani diversi, esempio tipico la spada che passa attraverso una persona riprodotta virtualmente in quanto non viene fermata da un oggetto -il corpo della persona-).

Principali percorsi delle Interfacce "naturali"

	2010	2015	2020
CONSUMER	■ Touch Interface ● Multi Touch – ● A few devices ■ Visual ● display ● gesture Recog.-	■ Haptic Interface ● Multi Touch + ● Sense FeedBk ■ Many devices ■ 3D screen – special. ■ Focussed Sound	■ 3D screen + ■ Wall Screens ■ Immersive Envir. ● Specialised - ■ Augmented Reality ■ Objects Interaction
ENTERPRISE	■ Haptic Interfaces ● Process Orient. ■ Real Life Video C. – ■ Simulated Envir. ■ Presence	■ Immersive Envir. ● Process Orient. ■ Real Life Video C. + ■ Simulated Envir. ■ Presence + ■ Robots Interaction	■ Make-Believe Env. ● Process Orient. ■ Real Life 3D Video ■ Simulated Envir. ■ Seamless AR ■ Avatar Interaction

9 Reti Locali

2010	2015	2020
■ Local Area • WiFi • Ethernet • BlueTooth • IR	■ Local Area 2010+ • 50GHz • POF • PwLines • NFC	■ Local Area + 2015 • Mesh • BAN

Principali percorsi delle Reti locali

WiFi, UWB, 50GHz WLAN, Bluetooth, POF, Power lines. Sono molteplici le tecnologie già oggi disponibili per creare reti locali. In prospettiva si prevede uno sviluppo significativo sia in ambiente domestico (spinto dalla varietà di elettrodomestici con connettività embedded), sia in ambienti enterprise, che in ambienti aperti. La banda fornita è destinata a crescere, il WiFi potrebbe arrivare al Gbps e Gbps saranno anche forniti dalle reti wireless sulla frequenza dei 50GHz per collegamento tra apparati di intrattenimento domestico.

Interessante la crescita di reti di sensori, in genere di tipo mesh, sia a livello residenziale, sia industriale e ambientale. In queste la comunicazione sarà effettuata con protocolli ad hoc con basso consumo (non IP).

9.1 *Impatto*

La maggioranza di reti locali non saranno di proprietà di un Operatore e saranno utilizzate a fini specifici e privati. I dati raccolti potranno essere analizzati e "consumati" a livello locale, oppure portati, tramite rete pubblica, a punti di controllo ed elaborazione. Il traffico generato sarà variabile, da bassissimo e transazionale per reti di sensori, a significativo per reti di sorveglianza tramite videocamere. Alcune reti locali potranno drenare un traffico significativo dalle celle radiomobile, dirottandolo su linee fisse (tipicamente con aree WiFi). Le Femtocelle, pur facendo lo stesso, hanno un impatto positivo, in quanto il traffico trasportato rimane di competenza dell'Operatore che serve quel terminale. Le reti locali saranno semplici da realizzare (soprattutto a livello residenziale) ma la loro progressiva aggregazione di una varietà di sistemi ne renderà sempre più complessa la gestione aprendo una opportunità per una gestione garantita da remoto tramite un service provider che potrebbe gestire anche le varie device che gravitano su tale rete. Ovviamente, l'Operatore potrebbe benissimo offrire questo tipo di servizi.

10 Infrastruttura di trasporto in fibra

L'optoelettronica continuerà a progredire in questa decade. I volumi, inoltre, contribuiranno ad abbassare i costi, spostando sempre di più la convenienza verso sistemi Point to Point, per quanto riguarda la pura terminazione ottica, anche se il costo complessivo continuerà a rendere più praticabili, economicamente, strutture GPON WDM-PON.

Il progresso dell'optoelettronica moltiplicherà le lambda utilizzabili, arrivando a qualche migliaio con conseguenti capacità dell'ordine dei 100 Tbps per fibra con singola modulazione superiore ai 100 Gbps (rispetto ai 40 di oggi). Oltre i 100 Tbps al momento sembra difficile andare, in quanto le potenze in gioco portano alla fusione del core della fibra. Considerando comunque che i cavi posati contengono ciascuno una molteplicità di fibre, è ovvio come non si ponga un problema di saturazione della capacità di trasporto. A livello rete di accesso prevarrà la tecnologia CWDM con un minor numero di lambda.

Dal punto di vista del trasporto ottico, specie in previsione di una diffusione significativa, si viene ad attenuare la differenza tra i vari segmenti di rete e sarà possibile avere un unico punto di controllo per tutto lo strato ottico a livello di una rete nazionale.

	2010	2015	2020
CONSUMER	■ ADSL 20 Mbps ● most at 7Mbps ■ Fibre 100 Mbps ● limited avail. ■ GPON	■ ADSL 20 Mbps ● VDSL 50 Mbps ■ Fibre 100 Mbps ● increased avail ■ GPON	■ VDSL 50 Mbps ■ Fibre 100 Mbps ● Widespread ■ Fibre 1 Gbps ● hot areas ■ GPON, Pt2Pt, WDropl
ENTERPRISE	■ ADSL 20 Mbps ● VDSL 50 Mbps ■ Fibre 100 Mbps ● niches ■ Fibre 1 Gbps - ■ Pt2Pt	■ ADSL 20 Mbps ● VDSL 50 Mbps ■ Fibre 100 Mbps ● increased ■ Fibre 1 Gbps + ● CWDM	■ VDSL 50 Mbps ● SOHO ■ Fibre 100 Mbps ● widespread ■ Fibre 10 + Gbps - ● CWDM

Principali percorsi delle Linee di accesso fisso

10.1 *Impatto*

La diffusione della rete in fibra sul versante offerta moltiplica la banda e quindi il gap tra offerta e domanda in futuro tenderà ad ampliarsi. Difficile pensare ad un premium sulla banda. Oltre il Gbps non esiste, almeno al momento, alcuna applicazione di tipo residenziale (e per la maggioranza del mondo business) che ne possa fruire.

Al 2003 era stato stimato un traffico complessivo intorno ai 17 EB (Exabyte, miliardi di miliardi di byte), secondo le ultime stime di Cisco nel 2009 si è arrivati a superare i 60 e saranno 667 nel 2013. Al Future Centre di Telecom Italia si è provato a fare il conto dell'asintoto di crescita di traffico dati, ipotizzando che 7 miliardi di persone fruiscano per 24 ore al giorno di trasmissioni (bidirezionali) in formato 4k (limite della risoluzione dell'occhio umano) e che a questo si aggiunga un traffico ambientale video di 10 miliardi di telecamere. Su questa base tutto il resto del traffico (voce, transazionale...) può essere considerato marginale. Il totale risulta intorno ai 200 ZB anno e richiederebbe 6 cavi da 96 fibre ciascuno per il trasporto. Oggi, attraverso l'Atlantico e il Pacifico abbiamo già un numero maggiore di cavi (anche se operano a velocità più basse viste le capacità dell'elettronica di oggi sui punti terminali; basterà comunque aggiornare le terminazioni con le nuove tecnologie per aumentarne la capacità). Non esisterà quindi un problema di capacità di trasporto nelle reti core. Nelle parti terminali della rete le capacità sono ovviamente molto ridotte, ma pure il traffico gestito è enormemente inferiore. La commutazione sarà sempre più orientata alla commutazione di flussi con add-drop e multiplexer ottici, senza riconversione del segnale in elettrico. Varie tecnologie di deep packet inspection saranno disponibili e permetteranno interventi sia agli edge, sia al core, anche se è ragionevole attendersi che gran parte del controllo sarà effettuato tra edge e terminali, lasciando al control plane (centralizzato) i compiti di macro configurazione dei flussi.

Sul versante dei costi di gestione l'infrastruttura in fibra (supponendo di muoversi in un'ottica di total replacement) porta ad una significativa diminuzione sia per i minori costi energetici, sia per il minor costo di interventi data la maggiore affidabilità e sopravvivenza complessiva del trasporto, anche in caso di interruzione focalizzata di un cavo (discorso molto diverso se si ipotizza di mantenere la secondaria in rame). Inoltre una struttura di accesso totalmente in fibra consente di creare un continuum tra rete core, rete metro e reti di accesso, portando alla diminuzione delle installazioni fisse (edifici di centrale).

La pervasività della fibra, inoltre, costituisce la piattaforma su cui innestare le antenne per una fitta copertura radiomobile, quale quella che sarà necessaria al crescere della domanda di banda creata da terminali wireless.

11 Infrastruttura di trasporto wireless

L'evoluzione tecnologica di questa ultima decade, OFDM, QAM64, MIMO, Smart Antenna, ha di fatto avvicinato lo sfruttamento dello spettro al limite di Shannon, al punto che non è pensabile un ulteriore miglioramento nell'efficienza di uso spettrale. Questo spinge l'evoluzione che vedremo nei prossimi anni su tre direttrici di evoluzione: architetturali, spettrali e autonomici. Più precisamente:

- diminuzione del raggio delle celle con miglioramenti architetturali per un miglior sfruttamento dello spettro disponibile (SON- Self Organised Network, uso del White Spectrum, uso del MuliCarrier Multispectrum). Al 2020 si prevede la possibilità di fornire 1 Gbps per torre. La copresenza di varie celle in un determinato punto (da quelle pico a quelle satellitari) consentirà al terminale di scegliere di volta in volta la soluzione di accesso più adatta, negoziandola anche con la rete che potrà indirizzarne l'uso sulla base del carico istantaneo. Questo richiede una gestione di roaming verticale, oltre che orizzontale, per cui occorrerà risolvere problemi di interoperabilità e multi-domain ownership;
- ottenimento del diritto di uso dello spettro intorno ai 700 MHz (per le sue buone caratteristiche di propagazione e bassa attenuazione in ambienti urbani). Verso fine decade dovrebbero rendersi disponibili nuove tecnologie di antenna che permettono una riduzione di un fattore 100 delle dimensioni. Questo permetterebbe uno sfruttamento anche di frequenze portanti inferiori da parte di terminali handheld. Tuttavia, lo spettro associabile, ancora migliore in termini di propagazione, sarebbe in grado di modulare una minor quantità di dati. La ridotta dimensione di molte celle permetterà di utilizzare frequenze portanti più elevate, a dispetto della maggiore difficolta di propagazione e quindi di modulare una maggiore quantità di dati. Si ipotizzano spettri dell'ordine dei 0,5-1 GHz;
- verso fine decade la drastica riduzione di consumo energetico da parte del chip del terminale handheld permetterà un significativo aumento del processing locale e questo consentirà la risoluzione dei problemi di interferenza tramite un'elaborazione autonomica locale tra terminali situati in una cella. In pratica questo significa poter moltiplicare il numero di bit per Hz di un fattore che crescerà nel tempo in linea con i progressi dell'elettronica. Diventerà quindi possibile far entrare in una spirale positiva il numero di bit per Hz, abbattendo drasticamente i vincoli oggi presenti nell'uso dello spettro.

11.1 *Impatto*

Il progresso tecnologico nel settore wireless sarà probabilmente quello con l'effetto maggior-

Principali percorsi delle Linee di accesso mobile

	2010	2015	2020
CONSUMER	■ 3G 5 MHz spectr.	■ Fading GSM, 3G on virtual ntw ■ LTE 80 Mbps Beam ■ MSR diffuse ■ Avail. Port. < 1GHz	■ 0,5-1GHz spectr.? ■ Complex clover ■ 1 Gbps per tower ■ SON ■ Multi Carr. Mband ■ Use of WhiteSpace
ENTERPRISE	■ 3G 5 MHz spectr.	■ Fading GSM, 3G on virtual ntw ■ LTE 80 Mbps Beam ■ MSR diffuse ■ Avail. Port. < 1GHz	■ LTE 100MHz spectr. ■ Complex clover ■ 1 Gbps per tower ■ SON ■ Multi Carr. Mband ■ Use of WideSpace

mente dirompente sulle regole del gioco di oggi. Il premium richiesto dall'uso dello spettro (risorsa scarsa) che oggi si affievolisce a seguito di una competizione serrata, si affievolirà ulteriormente al diminuire della sua scarsità.

La presenza di strutture di copertura multicella, di cui in parte fornite da privati (picocelle), contribuirà ulteriormente a portare il wireless nella struttura di valore del fisso. La rete di accesso sarà praticamente indistinguibile, l'ultimo metro sarà wireless e la "lunghezza" di questo metro varierà da zona a zona.

Perchè questo si verifichi nel medio termine, è necessaria una maggiore disponibilità di spettro (100-200 MHz) e quindi una pervasiva presenza di fibre per alimentare la densità di celle richieste. Nel lungo termine il problema dell'interferenza, e quindi del limite di Shannon, sarà superato, ma, perchè questo avvenga, è necessario che si realizzino le condizioni del primo punto. Infatti, solo all'interno di celle ragionevolmente piccole (100-200 m) è possibile ipotizzare un sistema autonomico formato dai terminali handheld per il trattamento del segnale.

12 Macro trends

Ho cercato di sintetizzare nelle parti precedenti alcuni impatti che possono essere fatti risalire direttamente a specifiche roadmap tecnologiche. Tuttavia, occorre fare uno sforzo di comprensione più allargato, in quanto il vero impatto discenderà dalla contemporanea evoluzione delle diverse tecnologie, ovviamente nel momento in cui queste sono adottate. Certo, anche questa visione è parziale e rimane sul piano del possibile, non dice molto sul piano del probabile. Per questo occorrerebbe da un lato considerare l'evoluzione dei costumi, del mercato, della possibilità di spesa e il contesto regolatorio. Elementi importanti, ma che non sono stati oggetto di studio.

L'esercizio di considerare solo l'impatto possibile in termini di abilitazione tecnologica è quindi inutile? Non necessariamente. Sapere quanto sia possibile, permette di operare anche sugli altri versanti per renderlo più o meno probabile. Inoltre fa capire cosa potrebbe comportare la scelta di non perseguire questa possibilità nel caso in cui questa venga invece perseguita da altri, competitor classici o attori in altri settori, che vengono poi ad essere competitor di un Telco, perchè arrivano allo stesso suo bacino di revenue (eventualmente distruggendolo).

13 Evoluzione tecnologica: impatto sulla domanda

La crescita di capacità di memoria, di elaborazione, la maggior risoluzione degli schermi e la possibilità di un loro utilizzo generalizzato, unite alla tariffazione flat rate generalizzata su fisso e su mobile hanno stimolato la domanda di banda, ma al tempo stesso la competizione e la sensitività dei clienti residenziali ai prezzi da un lato e la forza negoziale dei clienti business dall'altro hanno ulteriormente abbattuto i prezzi ad un livello in cui la percezione di costo è praticamente scomparsa.

La sostanziale sovrabbondanza di offerta di capacità sul fisso e la qualità offerta dalle tecnologie ottiche di trasporto hanno fatto scomparire ogni premium basato su livelli di servizio. Una percezione di qualità insoddisfacente aumenta il *churn*, non provoca un aumento di richiesta di SLA. Nel settore business si sono sviluppati sistemi multiaccesso che in pratica forniscono la protezione automatica da difficoltà di connessione su di uno specifico canale. Sul versante del mobile residenziale l'offerta di banda in alcuni punti e in alcuni periodi non soddisfa pienamente la domanda, ma questa preferisce accontentarsi piuttosto che passare a livelli di qualità minima garantita. Sul versante business questo non è vero, ma spesso la forza negoziale dei grandi clienti riesce ad ottenere livelli di servizio garantiti a prezzi contenuti.

La domanda continua ad essere asimmetrica, con maggior richiesta centrifuga che centripeta, ma il flusso centripeto del singolo utilizzatore in certi istanti equivale a quello centrifugo. Per que-

sto motivo soluzioni altamente asimmetriche non sono gradite. La banda in upstream minima è intorno ai 10 Mbps su fisso, 1Mbps su mobile.

Alla richiesta esplicita di connettività (data comunque per scontata) si accompagna una richiesta implicita generata dall'uso diffuso di sistema a connettività embedded. Molte appliances, come libri, "post-it windows", specchi, tourist's lens magnifiers, giocattoli, white goods, sistemi medicali di monitoraggio, così come ambienti (automobile, ascensore, negozio, supermercato, parco divertimenti) hanno una connettività embedded, che non è neppure percepita dall'utilizzatore, essendo trasparente in termini di costo e basata su di un Operatore non scelto dal cliente e spesso neppure conosciuto.

L'augmented reality è diventata parte integrante del paesaggio. Il compratore si aspetta di poter dialogare con un prodotto e di acquisire una svariata quantità di informazioni, spesso fornite in modo accattivante. Questo richiede una capacità di percezione del contesto, il riconoscimento dell'ambiente e degli oggetti in questo presenti da parte di chi offre i servizi di augmented reality. Nella stragrande maggioranza dei casi questi servizi saranno abilitati da un service enabler che effettua mash ups e personalizza informazioni e servizi sulla base di terminale e persona che lo utilizza, pensando a gestire la monetarizzazione dei valori messi in gioco in un contesto B2B2C.

L'augmented reality diventa un modo di fornire customer service e anche un modo di trasformare prodotti in servizi. La funzione di intermediazione diventa fondamentale anche per garantire diritti di proprietà e si fa garante di qualità dell'informazione aumentata (e relativi servizi a questa connessi).

Il concetto di personalizzazione è assimilato e dato per scontato. Quando si chiama un centro servizi ci si aspetta che chi risponda sia perfettamente a conoscenza della nostra storia ed esperienza relativamente al servizio in oggetto. In alcuni settori il rapporto ad alta qualità con il cliente, mediato da sistemi di smart relation è percepito come un valore differenziante e per cui il cliente è disposto a pagare un premium. In molti, tuttavia, questa relazione ad alta qualità è percepita come un elemento scontato e la sua assenza, o insoddisfacenza, come un disvalore che porta alla scelta di un altro provider.

L'enorme quantità di dati che vengono generati a livello consumer ha fatto crescere la coscienza del valore di preservare i dati e di poterli fruire in una varietà di modi. La privacy rimane un elemento di forte valore e molti Operatori sono diventati Trusted Parties. Per contro, molti dati personali sono neutralizzati e resi disponibili ad applicazioni di interesse generale, come il controllo del traffico, di epidemie... Pur essendo possibile "tenere" in rete tutti i propri dati la maggioranza delle persone e delle aziende continuano ad avere repository locali sotto il diretto controllo, anche se i dati sono garantiti da terzi, che ne conservano copia e la rendono disponibile su richiesta.

Il trust sul digitale è aumentato (anche se non mancano utilizzi fraudolenti e "crisi") e tutti affidano ai bit la storia della loro vita. Le policy di enforcing della privacy e ownership dei dati potranno divergere in questa decade, da una parte i garantisti (Operatori di TLC in primis) e dall'altra gli aperti (WebCo). Questo potrebbe favorire per un certo numero di servizi "sensibili" i garantisti che potrebbero diventare trusted parties anche per l'accesso agli altri servizi.

La connettività è un elemento essenziale alla vita, così come nelle decadi precedenti lo era l'elettricità. La rivoluzione nell'health care ha avuto nella connettività uno degli elementi abilitanti. Le medicine sono spesso personalizzate e si è quindi sottoposti durante la cura ad un monitoraggio continuo. La continuità di servizio è considerata caratteristica imprescindibile. Questo, paradossalmente, ha ulteriormente diminuito la percezione di connettività.

Servizi che si basano sul senso di presence sono ormai diffusi nelle case, negli uffici, nei negozi. Questo ha portato ad un uso massiccio della banda, visto che molti schermi sono diventati finestre virtuali, accese (aperte) 24 ore al giorno. Il denaro in carta non è ancora ufficialmente scomparso, ma praticamente non viene più usato. Il telefonino (o una personal device) hanno sostituito il borsellino e gran parte dei pagamenti "impor-

tanti" è effettuato elettronicamente. In Italia oltre 10 miliardi di fatture sono completamente elettroniche, così come i titoli di viaggio, i buoni sconto, gli scontrini le garanzie. La scuola è in gran parte digitale sia per i libri di testo sia per i laboratori.

14 Evoluzione tecnologica: impatto sull'offerta di connettività

La distinzione tra la rete core, quella metro e quella primaria è praticamente scomparsa con il passaggio alla fibra. Le prestazioni dello strato ottico saranno con un unico Policy Control (o pochi in una fase transitoria), con un restroration/Control Plane più sofisticato man mano che aumenterà il volume di trasporto (il core di oggi). L'accesso in secondaria è realizzato in varie tecnologie:

- radio (con presenza di uno spettro assegnato oltre i 200 Mhz e con utilizzo anche di frequenze intorno ai 700 MHz);
- fibra con anelli, GPON e CWDM e punto punto;
- rame (sarà ancora presente in una parte non trascurabile del territorio).

Complessivamente il progresso tecnologico ha ampliato ulteriormente la capacità di trasporto con drop in fibra che arrivano ad 1 Gbps bidirezionale se serve (in realtà pur con la richiesta aumentata di banda a livello residenziale 1 Gbps non serve ancora).

A livello radio le celle sono aumentate e offrono una banda densa, in grado di assicurare bande intorno ai 10 Mbps con punte ovviamente molto maggiori. I terminali radio sono in grado di negoziare lo spettro con la cella e con altri terminali nella zona, moltiplicando quindi l'efficienza complessiva.

La disponibilità di grandi capacità di storage consente di creare architetture di *storage at the edge* in alcune parti della rete, mantenendo quindi il traffico a livello di rete locale. Il peer to peer è utilizzato come architettura di rete per molti servizi di connettività.

Le reti locali si sono moltiplicate, da quelle di sensori a quelle formate da aggregati di utilizzatori. In alcuni casi si assiste a reti ad hoc, come quelle formate da autoveicoli.

L'affidabilità del sistema di telecomunicazioni è ulteriormente cresciuta, relegando gli interventi di pronto intervento sulla rete (e anche sulle customer premises) a casi eccezionali. Questo ha spostato la gestione dalla fase correttiva "acuta", a una gestione periodica programmata. Gli skill necessari sono cambiati, molti interventi sono robotizzati, quando non richiedono semplicemente un cambio di scheda per ripristinare le condizioni di duplicazione. A livello di customer premises la connettività è assicurata da un mix di linee fisse e radio, per cui in caso di danneggiamento alla linea fissa si supplisce con la connettività radio, portando ad un degrado del servizio, ma non ad una sua interruzione. Il concetto di qualità di servizio rimane importante ma viene dato per acquisito. Difficile creare un premium su diversi livelli di QoS.

15 Evoluzione tecnologica: impatto sull'offerta dei servizi

L'enorme potenza elaborativa e la capacità di memoria presente nei terminali rendono conveniente l'esecuzione della maggior parte dei servizi in locale. La grande banda disponibile rende trasparente la rete, collegando direttamente il terminale all'eventuale service provider.

L'IP, la banda sovrabbondante (in genere) e il flat rate contribuiscono a disaccoppiare la connettività dai servizi. Questo porta ad una varietà di service provider, che hanno come confini il mondo e utilizzano qualunque network provider. Non solo. Alcune funzioni, come quelle di autenticazione, possono essere svolte da un network provider su di una rete di un altro. Telecom Italia potrebbe offrire servizi di autenticazione collegati al M2M ad aziende che vendono prodotti con connettività embedded in qualunque parte del mondo.

Alcuni elementi specifici della rete, come la lo-

calizzazione di un terminale, sono facilmente acquisibili anche da terzi, per cui hanno perso il loro valore network based. Rimangono elementi come l'autenticazione e la gestione dell'identità e associati a questi il trust. Alcuni Operatori sfruttano la loro capacità di gestione di sistemi complessi e la presenza pervasiva sul territorio per offire servizi di outsourcing a molte aziende. La crescita di prodotti con connettività embedded ha creato un nuovo mercato e un'opportunità per gli Operatori di Telecomunicazioni di offerta di servizi per conto di queste aziende.

Le logiche di offerta di servizio vanno oltre la rete e la sua "ownership". Buona parte dei servizi ha cicli di vita rapidissimi, che richiedono strutture organizzative diverse rispetto a quelle in auge solo dieci anni prima. Alcuni Operatori hanno mantenuto significative revenue da servizi, ma per fare questo hanno disaggregato la struttura in strutture più snelle focalizzate in aree specifiche che fanno leva sugli asset dell'Operatore e tra questi il trust, come spesso ricordato, si rivela uno degli elementi fondamentali.

La relazione con il cliente person-to-person, anche se i processi di automazione, coinvolgenti avatar e robot, proseguiranno, continuerà ad avere un valore enorme e costituirà elemento di differenziazione, al punto che, grazie alle evoluzioni tecnologiche nell'area del trattamento dei dati, gestione di DB distribuiti, meta analisi di dati con possibilità di semantics and experience extraction, il Customer Care potrebbe diventare un servizio in se stesso (trasformandosi da costo a revenue). Saranno molte le aziende che a fine decade offriranno servizi di Customer Care per contro terzi e questo sarà un business enorme sia in termini di revenue, sia in termini di controllo del mercato.

Questa è forse l'area maggiormente strategica per un Operatore di Telecomunicazioni e buona parte degli investimenti dovrebbero essere indirizzati in questo senso. Aspetto fondamentale, a questo riguardo, è la gestione della identità (e delle identità). È anche un'area in cui sono maggiormente delicati gli aspetti di relazione personale e quindi necessità di nuovi skill e personale con preparazione a più ampio spettro, adatto a fare da interfaccia coadiuvato da una organizzazione e tecnologia che ne renda effettivo l'empowerment e in cui maggiormente delicati sono gli aspetti di privacy e quindi, nuovamente, il ruolo fondamentale del trust.

CONCLUSIONI

Il futuro, per quello che può insegnarci il passato, è sempre stato migliore. Non esiste un'epoca nel passato che complessivamente, possa dirsi migliore di quella attuale. Certo, i problemi non mancano e sembrano moltiplicarsi ogni giorno, ma, complessivamente, oggi stiamo meglio di 100 anni fa. Alcune zone (troppe) del mondo soffrono di denutrizione, malattie facilmente debellabili costituiscono in molte aree un flagello, ma teniamo presente che 100 anni fa la percentuale di persone che viveva come oggi vivono persone in aree sottosviluppate era maggiore. Non il numero assoluto. Oggi la popolazione mondiale è 3-4 volte quella di inizio '900 e questo ha aumentato il numero di "poveri". Il consumo energetico oggi, e ancor più tra 10 anni, è enormemente maggiore di quello di cento anni fa e la crescita del benessere (positiva) è destinata ad aumentare i problemi connessi all'energia.

Le telecomunicazioni sono un vorace consumatore di energia, così come i trasporti, l'agricoltura e l'allevamento intensivo. Le telecomunicazioni, però, possono anche essere un elemento fondamentale per il contenimento della crescita dei consumi, portandolo a livelli gestibili. Gli Operatori di Telecomunicazioni possono contribuire significativamente alla sostenibilità energetica, ma ovviamente non possono farlo da soli. Devono collegarsi ad una pluralità di settori, fornendo loro gli strumenti per una reingegnerizzazione dei processi. Questa decade sarà infatti caratterizzata da una profonda revisione dei processi complessivi. Gli anni 90, grazie alla progressiva automazione, hanno portato alla reingegnerizzazione dei processi interni alle aziende, questa decade, grazie alla comunicazione pervasiva a basso costo, vedrà la reingegnerizzazione dei processi

intra-imprese e a livello di ecosistemi di business, portando la comunicazione all'interno del processi stessi (e annullandone parecchi). Si pensi alla produzione personalizzata e decentralizzata, spesso spostata o complementata dalla personalizzazione effettuata al punto di vendita o addirittura nella casa del cliente durante la vita del prodotto.

L'evoluzione verso le reti in fibra e verso sistemi radio a microcelle abbatte significativamente i consumi "delle telecomunciazioni". Spostare un bit sulla fibra costa mille volte in meno che spostarlo sul rame. Una cella radio piccola e con sistemi di antenne intelligenti (direzionali e ad abbattimento di potenza) può trasmettere bit con un centesimo dell'energia usata da una cella di oggi. Inoltre le nuove reti sono in grado di sostenere quei flussi di comunicazione tali da permettere la reingegnerizzazione indicata come uno strumento per il contenimento della crescita dei consumi.

Certo lo "snellimento" della forza lavoro, reso possibile dall'evoluzione tecnologica desta preoccupazione. Di nuovo, però, uno sguardo al passato dovrebbe confortarci. La meccanizzazione in agricoltura ha abbattuto l'occupazione in quel settore, ma il contesto complessivo, diventando più efficiente, ha permesso il reimpiego della manodopera a livelli maggiori di quelli che erano possibili nel settore agricolo. Sono cambiati ovviamente gli skill richiesti e questo sarà vero anche per il futuro.

Guardando al passato, comunque, non possiamo che guardare con fiducia al futuro, specie se saremo parte attiva nella sua costruzione.

ACRONIMI

CWDM: Coarse Wavelength-Division Multiplexing
GPON: Gigabit-capable Passive Optical Network
GPU: Graphical Processing Unit
LCD: Liquid Crystal Display
MEMS: Micro Electro-Mechanical Systems
MIMO: Multiple-input and multiple-output
NED: Nano Emissive Display
OFDM: Orthogonal Frequency-Division Multiplexing
OLED: Organic Light Emitting Diode
POF: Plastic Optical Fibre
RAID: Redundant Array of Independent Disks
RFID: Radio Frequency IDentification
SON: Self Organised Network
SED: Surface-conduction Electron-emitter Display
UWB: Ultra Wideband
WDM: Wavelength-Division Multiplexing
WLAN: Wireless Local Area Network

roberto.saracco@telecomitalia.it

AUTORE

Roberto Saracco
diplomato in informatica e laureato in matematica con un perfezionamento in fisica delle particelle elementari. Negli oltre trent'anni in Telecom Italia ha partecipato a molti progetti di ricerca in commutazione, reti dati, gestione della rete, occupando varie posizioni di responsabilità. Negli ultimi dieci anni i suoi interessi si sono spostati verso gli aspetti economici dell'innovazione. Attualmente è responsabile per Future Centre e Comunicazione Tecnica di Telecom Italia, dove guida gruppi di ricerca sulle implicazioni economiche dei nuovi ecosistemi e scenari di business.
È senior member dell'IEEE, tra i direttori della Communication Society, nonché autore di numerose pubblicazioni in Italia e all'estero ■

Barcode Security

SICUREZZA

Maurizio Ghirardi

Questo articolo costituisce un'estensione di quello recentemente pubblicato sul tema dell'utilizzo dei Barcode bidimensionali [1] (2D Barcode), nel quale si è parlato della tecnologia e della loro progressiva diffusione nel mercato consumer. La loro peculiarità è quella di rappresentare una sorta di "automazione", che consente al cliente di accedere a contenuti e a servizi in rete, anche multimediali, semplicemente "fotografando" il barcode, ad esempio su di una rivista, sulla confezione di un determinato prodotto, sullo schermo del proprio PC o del televisore.

L'estrema semplicità di utilizzo, unita all'evoluzione tecnologia dei terminali mobili sempre più simili ad un personal computer che ad un telefono e la scarsa partecipazione dell'utente al processo, la possibilità di produrre o riprodurre "in casa" i barcode e le modalità operative e le logiche dei sistemi, che consentono l'espletamento del servizio richiesto, possano far insorgere inattesi e insospettabili problemi di sicurezza.

In analogia, quindi, con quanto già accade oggi sui PC, i rischi a cui un terminale mobile e l'utente potrebbero andare in contro sono: installazione di spyware o virus, azioni di phishing sull'acquisto di prodotti o il furto di dati personali e di identità per l'accesso a servizi on line.

In questo articolo vedremo come sia possibile difendersi da tali attacchi.

1 "Codici a barre: tecnologia e campi applicativi - Corbi, Lisa, Piersantelli" - Notiziario tecnico luglio 2009

1 Introduzione

Le tecnologie dei barcode bidimensionali, grazie alle fotocamere presenti ormai su tutti i cellulari di ultime generazioni, si stanno progressivamente diffondendo nel mercato consumer, dopo il Giappone, anche in Europa come una modalità, che consente al cliente di accedere a contenuti ed a servizi in rete, anche multimediali, semplicemente "fotografando" il barcode su di una rivista, su di una maglietta, alla fermata dell'autobus, su di un bigliettino da visita o su qualsiasi altro supporto (*figura 1*). Purtroppo questa tecnologia presenta alcuni aspetti operativi che potrebbero esporre l'utente a rischi legati alla sicurezza del terminale o delle informazioni scambiate per poter accedere o utilizzare un servizio in rete.

Attualmente alcuni fornitori di servizi basati su Barcode Bidimensionali utilizzano un loro formato grafico (BeeTagg, ScanLife, ColorCode, MaxiCode, Microsoft HCCB), ma questo approccio limita il potenziale numero di utenti in grado di utilizzarlo. In ambito OMA[2], al contrario, sono stati definiti due formati standard che i lettori di codici a barre installati nei terminali mobili dovranno riconoscere: il QRCode di origine giapponese ed il DataMatrix di origine statunitense.

L'indirizzo OMA nell'utilizzo di formati standard ha un duplice scopo: facilitare l'espansione del servizio allargando il bacino dei possibili utilizzatori a livello globale; aumentare il livello di cooperazione per le aziende che offrono questa tipologia di servizio.

In generale l'utilizzo di questa tecnologia su terminale mobile non sempre consente, per la

2 Open Mobile Alliance si occupa della definizione di standard aperti alla "mobile industry", contribuendo alla creazione di servizi interoperabili tra diversi paesi, operatori e terminali mobili.

Figura 1 – Esempi di differenti utilizzi dei barcode

sua stessa natura, una partecipazione attiva dell'utente. L'utente infatti dopo aver "fotografato" il Barcode resta, nella maggior parte dei casi, passivamente in attesa che il processo si concluda. In tale situazione l'utente non è più in grado di verificare se quanto stia accadendo rappresenti "esattamente" quanto atteso (es. scaricare la suoneria desiderata oppure accedere alle informazioni richieste, effettuare la registrazione al congresso o accedere al portale web della conferenza).

La tecnologia che è utilizzata "al contorno" del servizio è quella a cui siamo abituati quando ci affacciamo al mondo di Internet utilizzando i nostri Personal Computer e cioè connessioni http/https, Web Service; il tutto fruito attraverso un Browser Web.

Infine occorre ancora dire che l'utilizzo di formati grafici standard come DataMatrix e QRCode, ma anche nel caso di formati proprietari, espone ad un ulteriore rischio. Il rischio è quello della contraffazione; infatti in rete è possibile reperire sia software a pagamento che libero in grado di riprodurre la grafica barcode e in alcuni casi gli stessi operatori o fornitori di servizi offrono la possibilità agli utenti, al fine di verificare la validità della metodologia, di produrre barcode personalizzati (*figura 2*).

Per capire bene quali strategie Telecom Italia offra per ovviare a questi problemi tecnologici facciamo una breve descrizione delle due modalità di utilizzo dei barcode bidimensionali: il modello diretto ed il modello indiretto.

Modello diretto

Il modello diretto, utilizzato in particolar modo in Giappone, prevede che il client del terminale mobile acquisisca, riconosca (1) e decodifichi (2) il codice a barre, quindi ottenuta una URI, la utilizzi per mezzo del browser web (3) collegandosi al servizio richiesto (4). In questo caso l'operatore è sicuramente coinvolto nel fornire la connettività al cliente ed eventualmente, ma non necessariamente, nella mediazione svolta tra il cliente e chi offre il servizio (*figura 3*).

Modello indiretto

Il modello indiretto è una soluzione adottata principalmente dagli operatori Europei e Americani e consente di variare nel tempo sia i contenuti sia la tipologia di servizio offerto senza la

Figura 2 – Esempi di servizi on-line e software gratuito per la generazione barcode bidimensionali

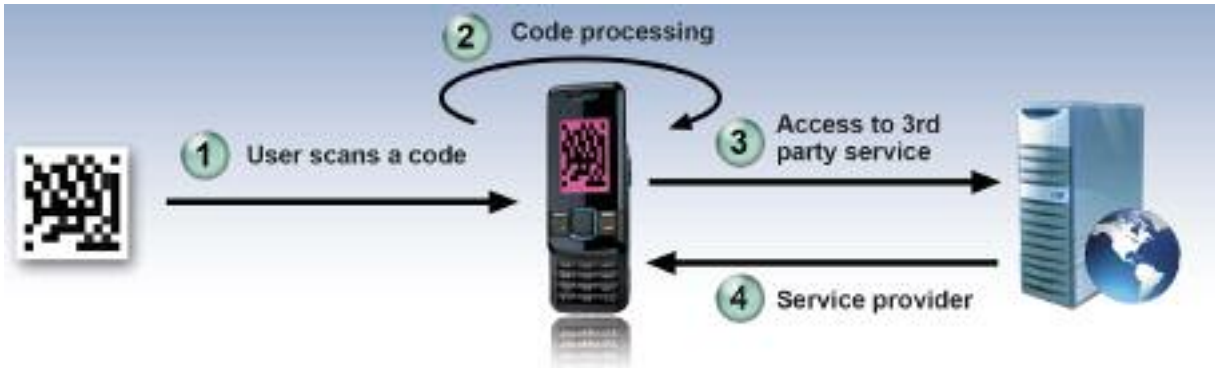


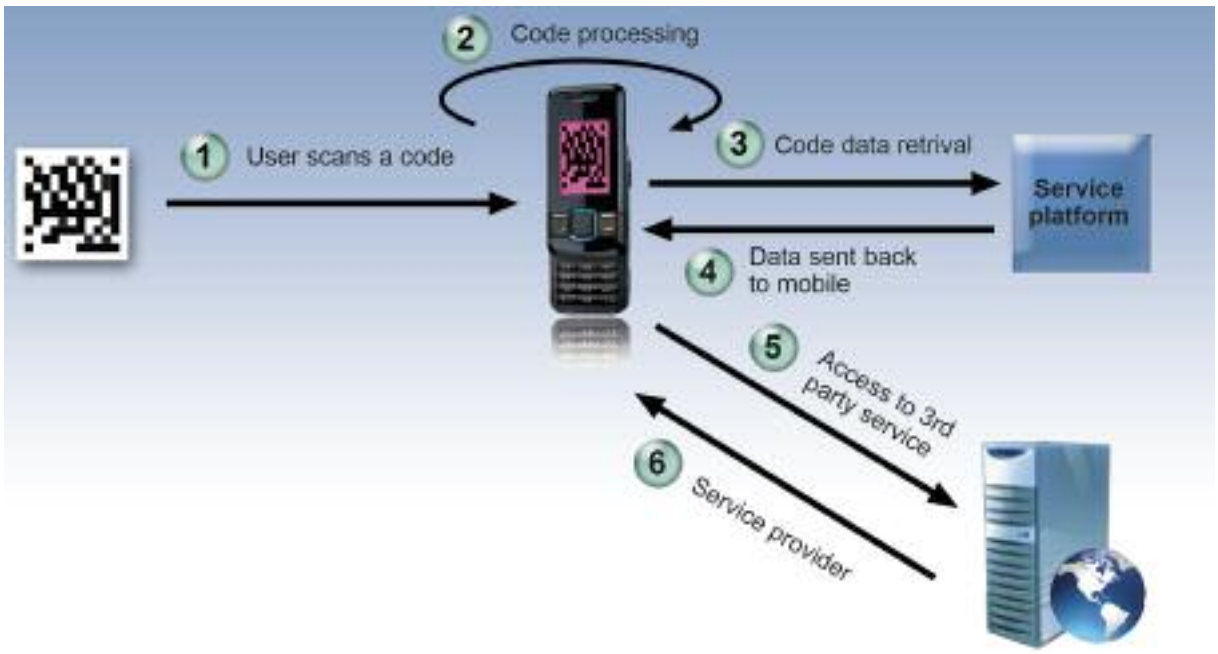
Figura 3 – Metodo Diretto

riemissione di nuovi codici a barre. Sostanzialmente il barcode contiene un "identificativo", e non una URI, che viene inviato e "risolto" (3), ovvero associato al reale contenuto da proporre all'utente, solo da un apposito servizio di rete. Il servizio di rete invia al browser del terminale una "http Redirect" (4) che contiene la URI che il browser utilizzerà (5), al fine di contattare il server di rete reale ed ottenere il servizio richiesto (5). In questo caso l'operatore è sicuramente coinvolto nel fornire la connettività, ma è anche coinvolto con il fornitore di servizi, con il quale ha stipulato un contratto di servizio (*figura 4*).

Sarebbe troppo semplicistico pensare che la "Service Platform" possa essere costituita da un solo sistema, infatti nella realtà si tratta di una vera e propria infrastruttura di rete costituita da sistemi nazionali e internazionali interconnessi. Perché questa complicazione? La ragione risiede nel fatto che da un lato si vuole fornire un servizio globalizzato all'utente finale e al contempo si devono rendere consistenti le relazioni commerciali ed economiche tra tutte le componenti dell'ecosistema, vale a dire l'Operatore, il fornitore dei servizi di traduzione e/o il fornitore del servizio vero e proprio.

La *figura 5* descrive un modello di interconnessione nazionale e internazionale tra i sistemi

Figura 4 – Metodo Indiretto



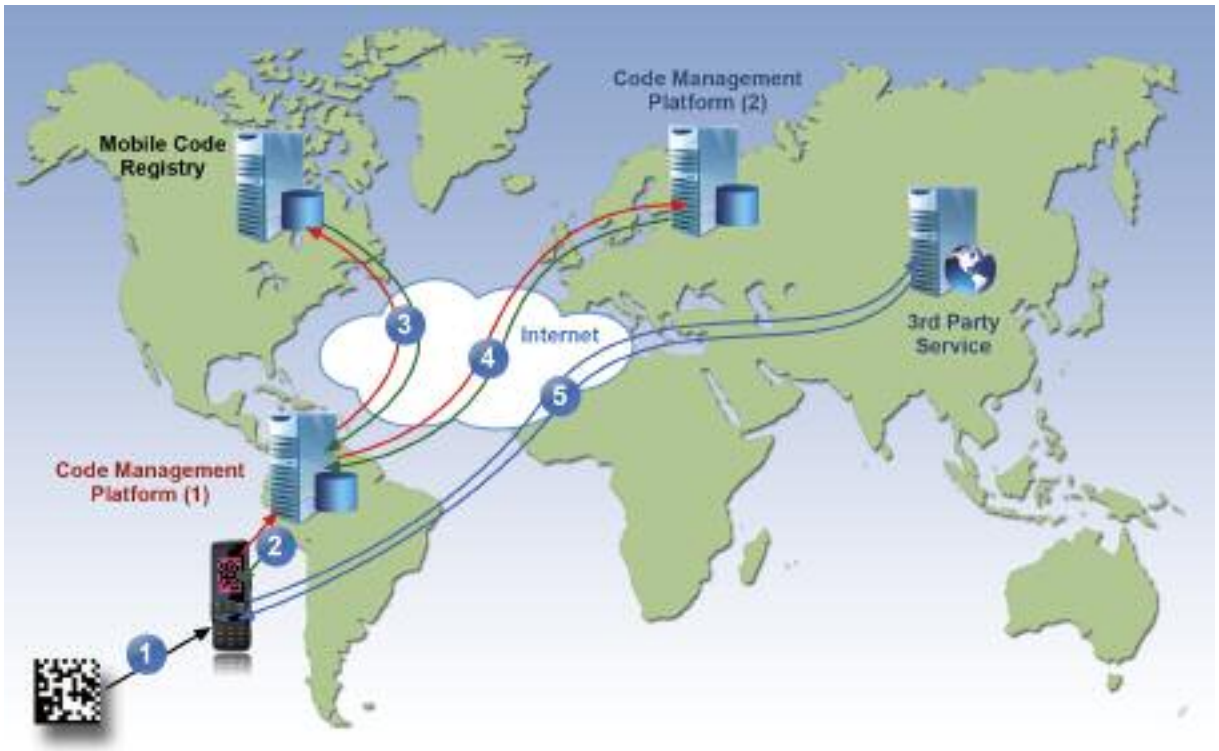


Figura 5 – Esempio operativo metodo indiretto

che offrono il servizio di "risoluzione", ovvero la conversione dei codici in URI.

Facciamo un esempio; il cliente desidera avere maggiori informazioni sull'indumento che desidera acquistare. L'indumento è dotato di un codice a barre bidimensionale, il Cliente ne fotografa l'etichetta (1), il client del terminale mobile invia il codice contenuto nel Barcode, utilizzando la rete dati dell'operatore radiomobile, alla propria "Code Management Platform" (2). La propria CMP rileva l'impossibilità ad effettuare la traduzione del codice ricevuto, conseguentemente contatta una risorsa internazionale o nazionale chiamata "Mobile Code Registry" per verificare se esista un CMP in grado di tradurre quello specifico codice (3). La MCR risponde con l'indicazione del CMP in grado di risolvere il codice ricevuto. Il CMP del cliente contatta il CMP indicato dal MCR (4) e ricevuta la URI della risorsa Web da contattare la comunica al client. Il browser Web del terminale mobile è finalmente in grado di contattare la risorsa finale direttamente (5), nell'esempio specifico la fabbrica che ha confezionato l'indumento.

Da questo esempio emerge come l'utilizzo di servizi mediati attraverso l'automazione supportata dai barcode bidimensionali sia ad oggi in grado di esporre l'utente agli stessi pericoli a cui è esposto utilizzando il PC di casa. In particolare i rischi ai quali gli utenti possono essere esposti vanno dall'installazione di Malware (Virus, Spyware, ecc.), alla sottrazione di informazioni sensibili utilizzando strategie di Phishing, fino all'incauto acquisto, nel caso in cui venga falsificato il barcode fotografato dal cliente.

La febbre del Click, quindi, potrebbe diventare molto pericolosa!

2 La contraffazione dei contenuti e i possibili rischi

Vediamo ora cosa contiene al suo interno un barcode e come sia possibile contraffarlo. Il contenuto dei barcode è solitamente costituito da una stringa di caratteri ASCII che permette l'esecuzione di diverse tipologie di automazione, al-

cune applicabili principalmente al modello diretto e altre utilizzabili soprattutto nel modello indiretto.

Nel modello diretto il barcode può contenere ad esempio una URI per l'accesso ad una risorsa Web (*http://web_site_url/*), oppure contenere una stringa opportunamente formatta che consente, ad esempio di effettuare una chiamata telefonica (Call: 33901010101) oppure di compilare automaticamente un SMS (SMS:33901010101" INVIO INFO 24").

Nel modello indiretto, invece, il barcode contiene un codice numerico, che viene utilizzato quale identificativo del servizio richiesto; questo ultimo viene inviato alla "Service Platform" utilizzando una "http GET" al fine di ottenere una "URL redirect" o "URL forwarding" contenente l'indirizzo di rete che il browser utilizzerà per accedere al servizio vero è proprio. Supponiamo che il codice identificato contenuto nel barcode sia, ad esempio 431000000000800016, una volta estratto dalla grafica, il client provvede a comporre la richiesta alla "Service Platform" di riferimento utilizzando una URI cablata nell'applicazione Client (*http://service_platform_url/query?Code=*) aggiungendovi quanto letto all'interno del barcode e generando una chiamata come quella descritta di seguito.

http://service_platform_url/query?Code=4310 00000000800016.

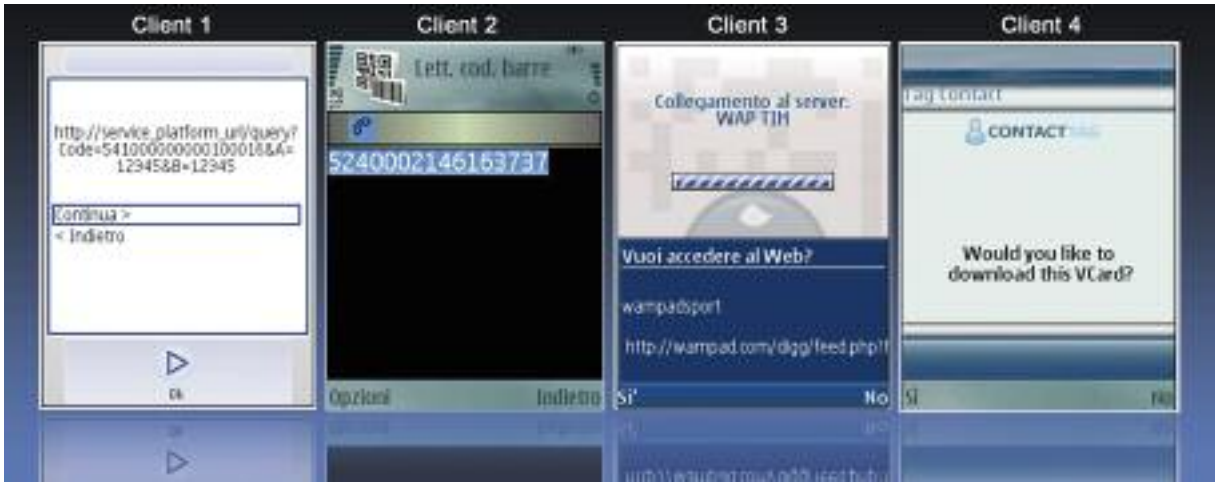
Di seguito e descritta, a titolo esemplificativo, una possibile risposta di tipo "URL redirect" alla richiesta precedente che consentirà al browser del terminale mobile di contattare il servizio all'indirizzo Web indicato, in questo caso *"http://www.online_service.it/login_form/"*.

"HTTP/1.1 301 Moved Permanently Location: http://www.online_service.it/login_form/"

Le *figura 6* descrive quanto invece viene visualizzato all'utente dal Client a bordo del terminale mobile subito dopo la decodifica del barcode e prima che venga inoltrata la richiesta di accesso al servizio. È evidente come le informazioni visualizzate non consentano all'utente di verificare l'autenticità dell'informazione visualizzata (Client 1 e 2) e, in altri alcuni casi, l'informazione presentata risulta essere largamente incompleta (Client 3) o completamente nascosta (Client 4).

Come abbiamo appena visto la possibilità di contraffare o alterare il contenuto di un barcode è reale, sia perché la metodologia utilizzata è poco sofisticata, sia perché chiunque abbia la possibilità di generare un barcode graficamente rispondente allo standard è in grado di condizionare in modo sostanziale il comportamento del Client del terminale che, dal canto suo, non è in grado di fornire all'utente alcuna informazione sulla "autenticità" del barcode. Nella maggior parte dei casi il Client presenta all'utente il contenuto del barcode, chiedendo conferma per la prosecuzione del processo, ma quanto presentato, cioè un codice numerico o una URI o qualsiasi altra cosa, non consente all'utente di

Figura 6 – Esempio di interfacce Client



rilevare la legittimità o meno del contenuto della richiesta e quindi anche dei successivi risultati.

Il possibile sfruttamento delle caratteristiche appena descritte apre scenari di sicurezza che meritano di essere descritti e presi in dovuta considerazione. È facilmente immaginabile come sia possibile sfruttare tali caratteristiche per consentire ad un attaccante ad esempio l'installazione di malware (virus, spyware, ecc.) sul terminale dell'utente, oppure trarre in inganno l'utente, sfruttando congiuntamente tecniche di social engineering (Phishing), che permettono il recuperare informazioni e dati elettronici sensibili, quali, ad esempio, le credenziali di accesso a siti di social networking, posta elettronica on-line o internet banking. Un altro rischio non meno importante è quello rappresentato dalla possibilità di indurre l'utente ad acquistare merce contraffatta.

3 La soluzione per un modello indiretto sicuro

Telecom Italia ha portato la tematica inerente la sicurezza all'attenzione del gruppo OMA che si occupa della standardizzazione del Client del terminale mobile e delle funzionalità dell'infrastruttura (Mobile Codes Enabler Group).

Considerato il livello di dettaglio raggiunto dalle specifiche in ambito OMA e il fatto che alcuni Operatori (TI, NTT DoCoMo) e fornitori di servizi (MobileTAG, ScanBuy, Nokia, Upcode) offrano già soluzioni commerciali basate sulla tecnologia 2D Barcode, la soluzione doveva conciliare diverse esigente tecniche e architetturali fornendo al contempo una funzionalità di sicurezza che utilizzasse dei modelli tecnologici di sicurezza standard e avesse il minimo impatto sull'esistente.

La proposta formulata utilizza un algoritmo di cifratura asimmetrica (RSA, Curve Ellittiche) del contenuto del 2D Barcode le cui chiavi sono gestite per mezzo di certificati digitali X.509. La proprietà fondamentale della cifratura asimmetrica è quella di utilizzare una coppia di chiavi una pubblica (da diffondere) e una privata (da tenere segreta) distribuite utilizzando dei certificati digitali. La chiave pubblica serve unicamente per cifrare il messaggio, mentre quella privata serve unicamente per decifrarlo. Facendo un esempio pratico, Alice vuole spedire un messaggio segreto a Bob e desidera che solo Bob possano leggerlo, semplice, Alice deve cifrare il messaggio con la chiave pubblica che Bob le ha inviato. Essendo Bob l'unico a possedere la chiave inversa, cioè quella privata, sarà anche l'unico a poter decifrare il messaggio, che rimarrà così segreto per tutti gli altri. Anche l'utilizzo della chiave pubblica di Bob di un altro utente non permette di decifrare il messaggio creato da Alice, più sicuro di così!.

Queste due tecnologie, l'utilizzo di "certificati Digitali" e l'adozione della cifratura asimmetrica, sono in grado di garantire il miglior livello di sicurezza attualmente disponibile e contemporaneamente garantire l'autenticità del contenuto del 2D Barcode, poiché, come abbiamo visto solo una coppia di chiavi congruenti cioè associate ad ogni relazione tra chi crea il barcode e chi lo deve decifrare.

L'implementazione di ciò in un contesto differente dall'usuale (SSL, SSH, PgP) ha richiesto l'individuazione di una soluzione specifica in grado di risolvere il problema legato al fatto che gli algoritmi di cifratura producono come output dati di lunghezza correlata alla lunghezza della chiave utilizzata, che per poter essere trasformati in un formato 2D barcode DataMatrix o QRCode, fanno in alcuni casi aumentare, anche considerevolmente, le dimensioni della grafica risultante e la sua complessità d'interpretazione (*figura 7*).

La soluzione proposta prevede la cifratura del contenuto del Barcode, utilizzando la chiave pubblica della Service Platform presso la quale i codici sono registrati. L'identificazione della Service Platform avviene per mezzo di un "codice identificativo" ad essa univocamente associato. Il materiale crittografico viene poi suddiviso in due porzioni: una contenuta all'interno del Barcode, tale da evitare l'incremento delle sue dimensioni grafiche, e l'altra resa disponibile alla Service Platform. Al fine di consentire alla Service Platform la corretta ricomposizione delle due porzioni del materiale crittografico ed effettuarne la deci-

Figura 7 – Esempio di grafica 2D barcode con contenuti differenti

fratura con la propria chiave privata, viene utilizzato un "identificatore di porzione", che deve essere posto nel barcode tra il codice identificativo della Service Platform e il materiale crittografico. Lo stesso identificatore di porzione e la seconda porzione del materiale crittografico deve esse inviato alla Service Platform di riferimento affinché possa essere ricostruito il codice di servizio. La *figura 8* descrive, ad alto livello, il formato della registrazione di un codice.

Nello specifico questa metodologia consente di proteggere adeguatamente la modalità indiretta dai possibili attacchi effettuabili per mezzo della modifica o ricodifica del contenuto dei barcode, vediamo perché.

Il codice del servizio non è più in chiaro come in precedenza e quindi facilmente modificabile, perchè protetto da un meccanismo di cifratura con chiavi protette da certificati digitali. Gli stessi certificati digitali rappresentano un elemento di sicurezza, in quanto consentono alla Service Platform di controllare l'intero processo e di verificare l'autenticità del contenuto dei codici a barre e contestualmente anche del fornitore del servizio.

La suddivisione del materiale crittografico rappresenta un ulteriore elemento di sicurezza, poiché è dimostrato che non possederlo interamente complica di molti ordine di grandezza la complessità di analisi rispetto a possederlo interamente e sul quale ad esempio sono possibili attacchi di tipo *brute force* o statistici. L'attacco brute force o "forza bruta" consiste nel generare tutte le combinazioni crittografiche teoricamente possibili fino a trovare quella effettivamente corretta, cioè con un contenuto dal significato compiuto mentre l'attacco statistico consiste nell'individuare particolari ricorrenze crittografiche riconducibili a determinati contenuti che consentono di "indovinarne" il risultato finale della decifratura senza realizzarne una vera e propria.

Con la soluzione proposta anche il cliente può essere e sentirsi protetto da eventuali contraffa-

Figura 8 – Esempio di processo di registrazione di codici

Contenuto del 2D Barcode	Informazioni inviate alla Service Platform
<SERVICE_PLATFORM_ID><PART_ID><CRYPTOMATERIAL> 10000000199999999999ALhawuzSZ9tOc7wT2MTGQ	<PART_ID>,<CRYPTOMATERIAL> 999999999999e314nb0o+FNVLL7EjBGFZQ=

zioni o abusi del servizio, poiché è estremamente semplice per l'intero ecosistema riconoscerle; infatti qualsiasi informazione modificata genera degli errori specifici lato Service Platform (Identificatore di porzione sconosciuto, decifratura errata, Service Platform sconosciuta) in grado di evidenziare e identificare la tipologia di abuso compiuta e quindi di informarne tempestivamente l'utente, attivando le procedure di indagine.

La *figura 9* propone un esempio di applicazione del metodo indiretto per la ricarica di cellulari con scheda prepagata. Tale metodo consentirebbe di ridurre e/o eliminare la produzione di carte plastificate usa e getta per la ricarica dei cellulari utilizzando un "Totem Servizi" dotato di display.

4 La tecnologia di autenticazione dell'utente SC@CCO

In ambito IT.TS - Security Innovation, utilizzando la tecnologia dei 2D Barcode, è stata messa a punto una soluzione che affronta e risolve in modo "innovativo" alcuni dei problemi legati all'autenticazione forte dell'utente. L'autenticazione forte dell'utente è divenuta fondamentale con l'aumento sia del numero sia della crescente complesità degli attacchi informatici perpetrati, della necessità di aprire le reti aziendali per includere fornitori, clienti e partner commerciali e l'inasprimento delle normative al riguardo.

Si definisce "autenticazione" il processo attraverso il quale due o più entità separate, ad esempio un client e un server, possono stabilire la reciproca identità. Nel caso dell'autenticazione umana ad un sistema informatico è possibile stabilire l'identità dell'interlocutore utilizzando una o più tra le seguenti metodologie di verifica: qualcosa che egli è (es. impronte digitali, impronta vocale, modello retinico, sequenza del DNA, calligrafia o altri identificatori biometrici); qualcosa che egli ha o possiede (es. tesserino identificativo, un dispositivo hardware) (*figura 10*); qualcosa che egli conosce (es. password, parola chiave o numero di identificazione personale).

Il continuo aumento dei servizi "on-line" (Servizi

Figura 9 – Ricarica di cellulari con scheda prepagata con servizio Kiosk

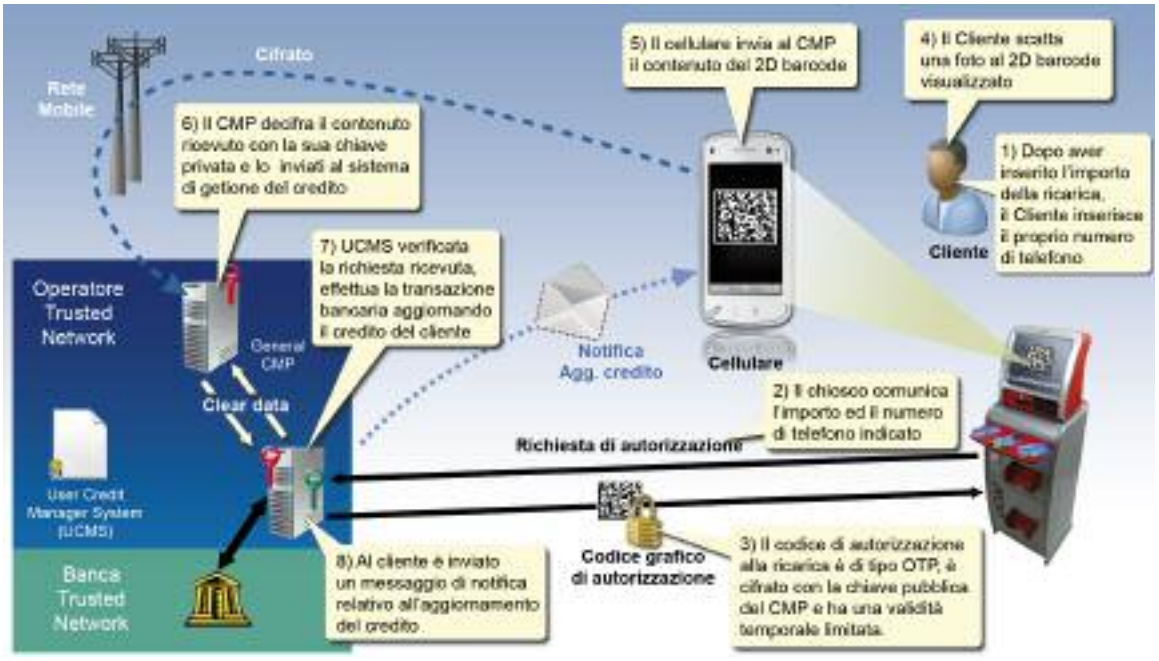


Figura 10 – Attuali strumenti hardware per l'autenticazione forte degli utenti

Bancari, Trading, eMail, RSS, newgroup, ecc.) fruibili dall'utente attraverso una rete informatica (Internet, Intranet ed Extranet aziendali) e nell'ultimo periodo, anche servizi di "intrattenimento" con contenuti a pagamento basati su DTT e IPTV rende il tema dell'autenticazione dell'utente ancora più sentito che un tempo. Inoltre occorre anche considerare che la presenza di innumerevoli elementi non direttamente controllabili o verificabili dall'utente (PC Client, Server, Software, Protocolli, Rete dati, ecc.), la presenza di problemi legati all'usabilità di certe tecnologie di sicurezza e la necessità di effettuare un bilanciamento tra l'esposizione al rischio e il costo economico sostenibile per la sua mitigazione o l'eliminazione, rendono le aziende e i loro clienti ancora esposti, a pericoli come le frodi informatiche o il furto di identità elettroniche (attraverso, ad esempio, il phishing).

La soluzione proposta da Telecom Italia prende il nome di SC@CCO [3] ed è una nuova modalità per l'autenticazione dell'utente su reti informatiche e dispositivi insicuri, utilizzando la tecnologia 2D Barcode unita alla metodologia "Challenge-Response", solitamente utilizzata in ambito protocollare (Kerberos authentication sviluppato dal MIT, CHAP - Challenge Handshake Authentication Protocol) e in particolari "Smart Card". La modalità d'autenticazione dell'utente SC@CCO, condensa le caratteristiche migliori delle attuali metodologie e tecniche d'autenticazione come token hardware (es. la Smart Card) o software, One-Time Password, anche via SMS, ed è in grado di offrire un servizio di autenticazione robusto, affidabile, con una "user experience" semplice, intuitiva e a basso impatto computazione sul terminale mobile.

La modalità di autenticazione dell'utente utilizzata è da considerarsi "a due fattori"; infatti l'utente dimostra sia di "conosce qualcosa" (vale a dire il proprio PIN o una Passphrase), sia di "possedere qualcosa" (vale a dire il terminale mobile).

La metodologia "Challenge – Response" prevede che due entità, prima di instaurare qualsiasi forma di comunicazione siano in grado di verificare reciprocamente l'identità del rispettivo interlocutore senza scambiarsi informazioni sensibili. Facciamo un esempio.

Il client applicativo A invia il proprio identificativo al server B, con il quale desidera mettersi in contatto; il server B risponde al client A con una "sfida", la challenge appunto, costituita da un numero casuale. Il client esegue ad esempio un'operazione di codifica non reversibile (es. Message Authentication Code – MAC) elaborando il numero casuale ricevuto con l'informazione segreta in suo possesso, quindi restituisce il risultato al server B. Il server B, conoscendo l'informazione segreta associata all'entità richiedente, è in grado di eseguire lo stesso calcolo e quindi comparare il valore ricevuto con quello calcolato, verificandone l'identicità. Se i valori non corrispondono l'entità del Client A non è fidata, quindi la richiesta di comunicazione viene rifiutata dal server B.

3 Il nome "SCACCO" deriva dal concetto di "scacco matto" che nel gioco degli scacchi rappresenta la mossa con cui uno dei due giocatori vince la partita perché il re avversario non può sottrarsi alla cattura, una "mossa vincente".

In breve, i vantaggi di questa metodologia sono:

- l'informazione segreta dell'utente non circola mai in rete, circola infatti solo una rappresentazione dinamica, poiché all'informazione statica viene aggiunta una informazione variabile, la "sfida";
- la "sfida" è generata solo quando è richiesta, cioè "al momento";
- la "sfida" è rivolta ad un solo "Client", l'unico in grado d'interpretarla;
- la "sfida" è valida una sola volta e non è ripetibile, perché è generata casualmente;
- la "sfida" è poco sensibile a latenze temporali, perché normalmente utilizzata su di una rete informatica;
- il "Server" non richiede al "Client" una sincronizzazione temporale.

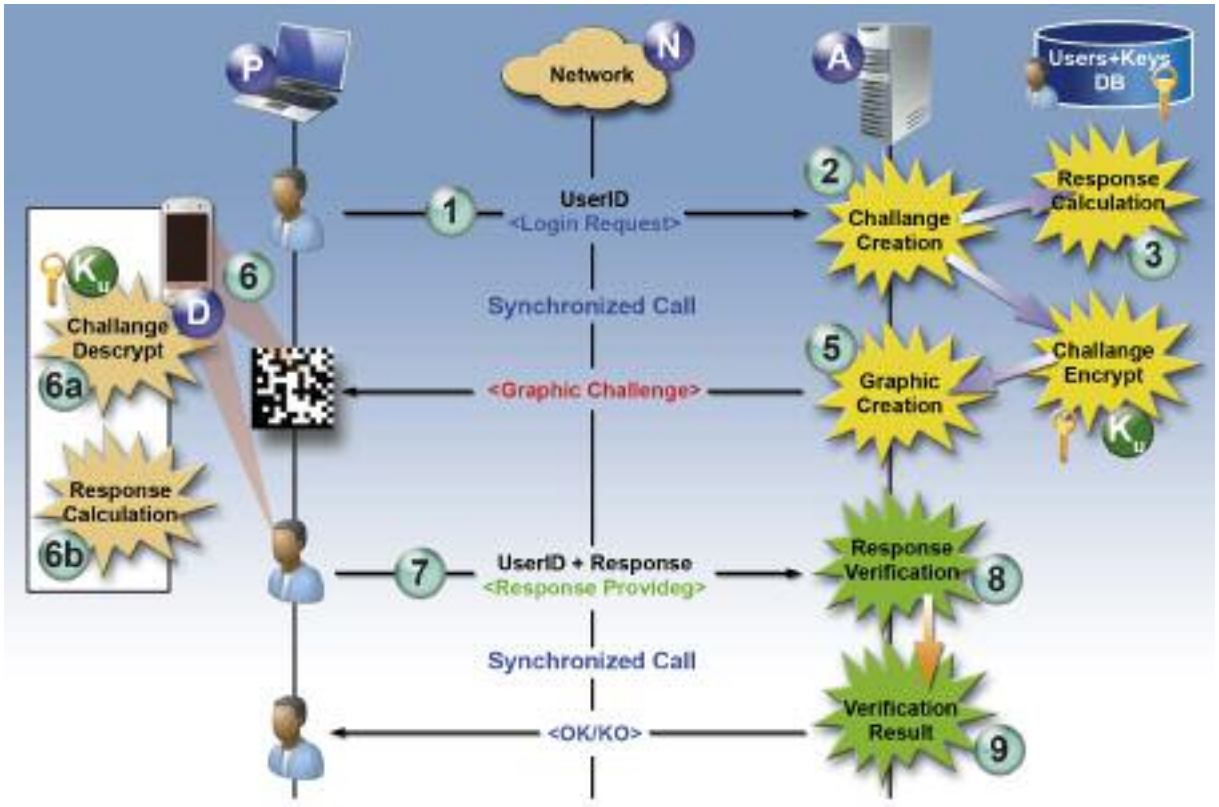
L'unico elemento critico della metodologia "Challenge – Response" risiede nel fatto che l'informazione segreta condivisa tra "Client" e "Server" debba essere sincronizzata, in quanto deve essere nota "a priori" ad entrambe le entità coinvolte.

SC@CCO pone rimedio anche a questo problema, vediamo come.

La soluzione SC@CCO (*figura 11*) in alternativa alla password di utente, utilizza in combinazione un PIN per sbloccare l'avvio dell'applicazione sul terminale ed una password di tipo OTP, ovvero una password numerica generata casualmente e con valenza temporale limitata. La "Challenge" inviata all'utente per mezzo del barcode è rappresentata dalla cifratura del suo contenuto, cioè la OTP, realizzato utilizzando un robusto algoritmo di "Encryption" simmetrico come AES-CBC [4]; l'utente deve dimostrare di essere in grado di decifrare correttamente la "Challenge" ricevuta e restituire la "Response" attesa, ovvero la OTP "in chiaro". In questo modo l'utente dimostra di avere il terminale giusto con al chiave

4 L'algoritmo utilizza una chiave a 128bit e metodo di cifratura Cipher Blocker Chaining con Initialization Vector che consente di ottenere anche a parità di informazione da cifrare sempre del materiale crittografico diverso.

Figura 11 – SC@CCO modalita' di interazione



correttamente associata al servizio sul quale sta operando e di essere a conoscenza del PIN con il quale è stato possibile avviare l'applicazione. La chiave utilizzata per la cifratura / decifratura della "Challenge" è composta dalla combinazione di più elementi: una "chiave personale dell'utente" generata per ogni servizio a cui l'utente viene abilitato; un PIN assegnato all'utente e che inserito consente l'avvio dell'applicazione. È importante far notare qualche altro aspetto relativo alla sicurezza della soluzione SC@CCO, un primo aspetto riguarda il fatto che la "Challenge" acquisita "otticamente" dal terminale mobile dell'utente impedisce qualsiasi forma di contatto con il "device" considerato "insicuro"; un altro aspetto riguarda l'utilizzo del PIN con una doppia valenza, come informazione che solo l'utente conosce e come elemento in grado di condizionare le operazioni di cifratura / decifratura della "Challenge" caratteristica questa che rappresenta non solo una efficace protezione contro il furto o la perdita del terminale ma anche contro il furto delle sole chiavi dell'utente che rimangono inefficaci senza la presenza del PIN dell'utente.

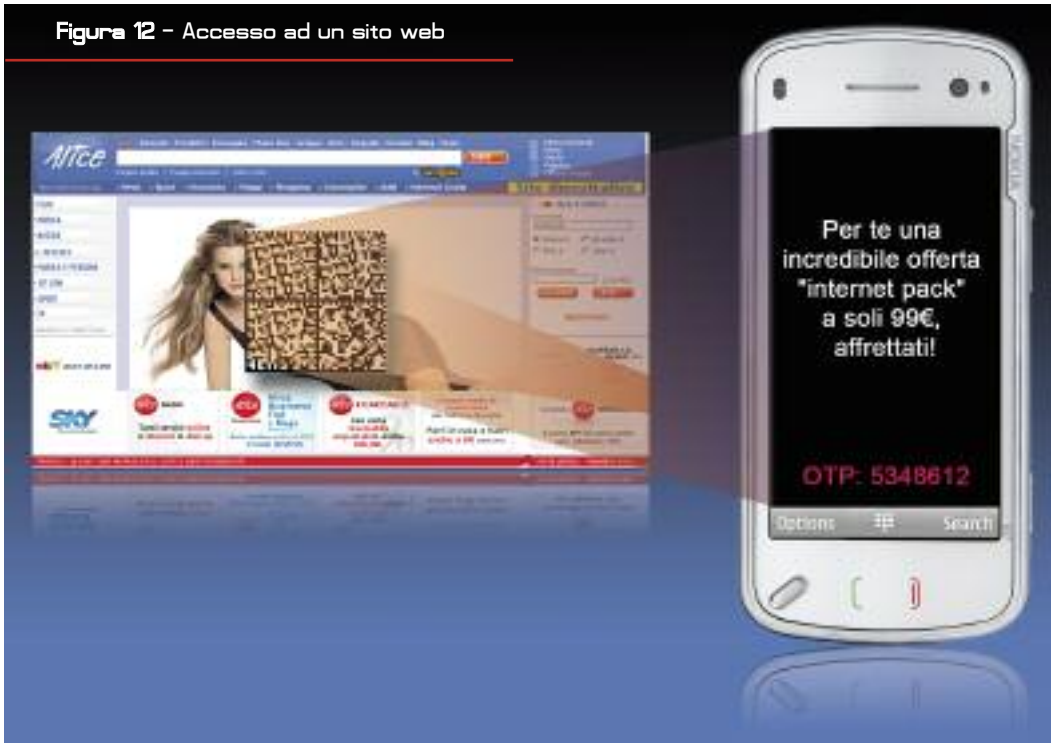
In sintesi la metodologia SC@CCO è in grado di mantenere elevato il livello di sicurezza dell'autenticazione dell'utente anche su terminali fissi "non fidati" (es. PC in alberghi, Internet point, chioschi, ecc.) eliminando le limitazioni delle altre metodologie e al contempo, impedendo la fattibilità tecnica delle maggiori tipologie di attacco informatico. Infine, non richiedendo un hardware dedicato come nel caso "Token" e "SmartCard" e non utilizzando risorse radiomobile, salvo che per l'installazione "una tantum" della chiave personalizzata del servizio richiesto, la metodologia proposta può anche essere considerata oltre che sicura anche economicamente conveniente. Nel seguito vedremo alcuni esempi di possibili applicazioni della tecnologia SC@CCO.

La prima applicazione riguarda l'accesso ad un sito web (*figura 12*). L'utente non dispone di una password "statica", ma ne utilizza una "dinamica" (OTP), sul modello token, fornita dal sistema all'utente solo in seguito ad una esplicita richiesta di accesso fatta utilizzando esclusivamente la propria username.

È importante far notare come all'interno della OTP inviata all'utente sia possibile inserire anche altre informazioni, in questo caso un messaggio pubblicitario.

In questa nuova modalità di implementazione

Figura 12 – Accesso ad un sito web



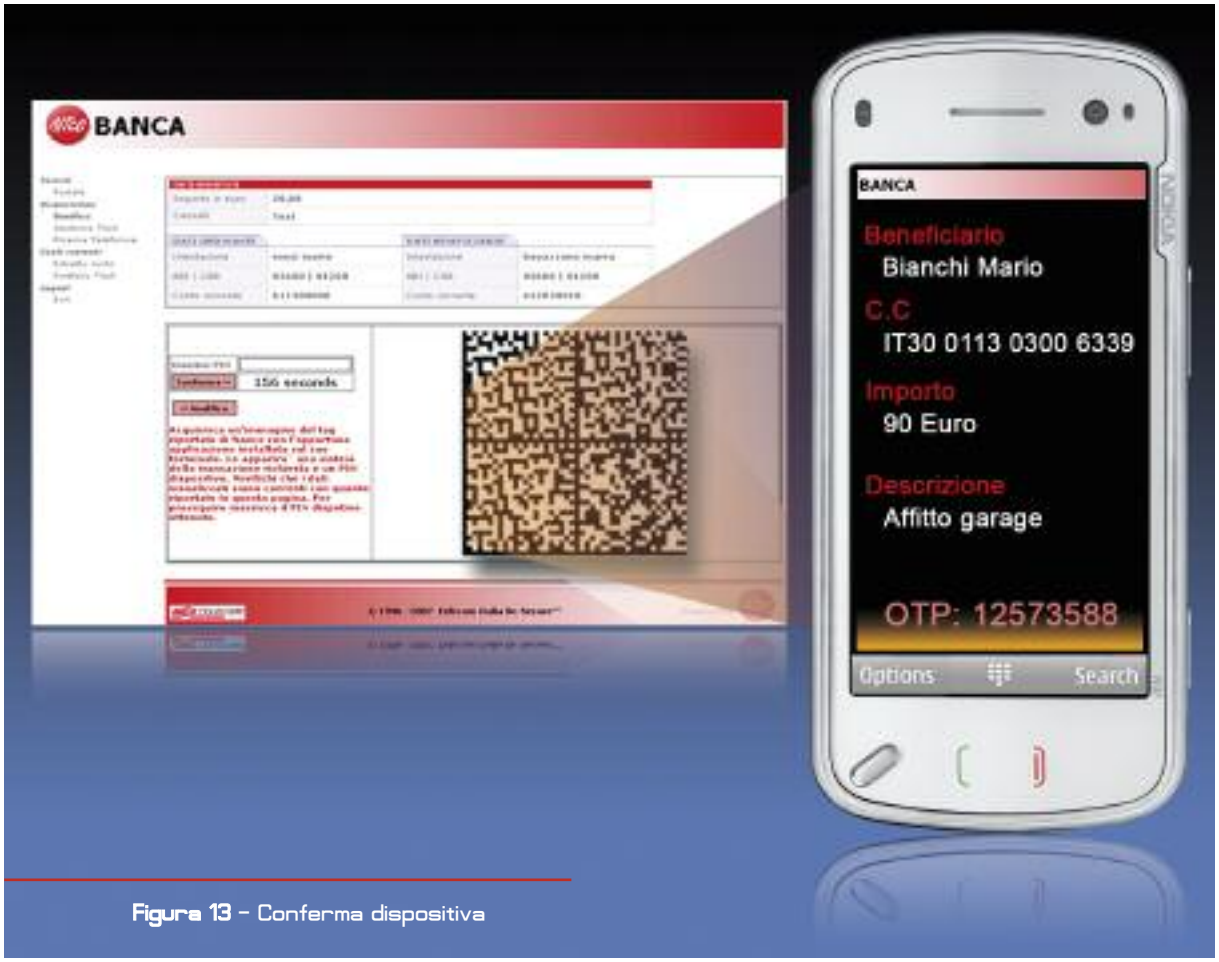


Figura 13 – Conferma dispositiva

della soluzione viene fornita una contromisura alla tipologia di attacco denominata "man in the middle attack"[5] durante un'operazione dispositiva (es. Bonifico bancario, Acquisto on-line di bene o servizi).

Un attaccante, in grado di interporsi attivamente tra l'utente e il Server della banca, può essere in grado di alterare le informazioni relative alla transazione che l'utente invia al Server (es. Destinatario e Importo). In questo caso nella "Challenge" generata dal server, quale conferma della transazione sono inserite e cifrate anche le informazioni salienti relative alla transazione.

L'attaccante, pur essendo in grado di alterare le informazioni inviate dall'utente, non è però in grado di alterare le informazioni sintetiche della transazione contenute nel "Challenge" grafica cifrata consentendo in tal modo all'utente di accorgersi della manomissione delle informazioni da parte dell'attaccante (*figura 13*).

Un'altra implementazione della soluzione consente di aumentare il livello di sicurezza della posta elettronica al fine di limitare il fenomeno del Phishing[6].

Nella *figura 14* l'utente riceve dal un mittente

5 Il "man-in-the-middle" è una tipologia di attacco che consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingerà di essere l'utente legittimo della comunicazione. Lo scopo in questo caso è quello di modificare a proprio vantaggio le informazioni dispositive dell'utente legittimo.

6 Il "Phishing" è un fenomeno di frode informatica dilagante, che prevede il ricevimento da parte dell'utente di un messaggio di posta elettronica, proveniente apparentemente dalla propria banca o da una società operante nel commercio on-line, che lo invita a collegarsi, attraverso un hyperlink link HTML, ad una pagina Web del tutto "simile" a quella originale. Le informazioni fornite dall'utente sono catturate (rubate) dal phisher, che le utilizzerà per effettuare acquisti indebiti o transazioni fraudolente.

Figura 14 – Esempio di Mail Anti Phishing

"certificato" una mail tradizionale e non una "mail certificata", dentro la quale è stata inserita una grafica 2D barcode dal contenuto cifrato e leggibile solo dal legittimo destinatario, una sorta di "francobollo di sicurezza".

Vediamo ora come l'utente sia in grado di verificare l'autenticità e la legittimità della mail ricevuta. L'utente dopo aver aperto la mail e averla visualizza sul personal computer attiva l'applicazione sul proprio terminale mobile, utilizzando il proprio PIN e fotografa il Barcode. Se il terminale mobile non è in grado di decodificarla è chiaro che l'associazione "Contenuto" della mail e "Utente" non è affidabile e l'utente potrà eliminarla tranquillamente. Se il contenuto è stato decodificato, invece, il destinatario è corretto ma si pone il problema della verifica della sua autenticità. Il terminale mobile, in questo caso, utilizzerà la URI contenuta nel Barcode che include un "Codice di Invio" e contatterà direttamente il servizio on-line del mittente "certificato", un esempio di contenuto del barcode è il seguente;

https://bank_verification_url/doc_verification?ID=93659.29012008

Come risultato della richiesta effettuata è possibile ottenere informazioni di dettaglio sul documento o mail ricevuta (codici identificativi o porzioni di testo), informazioni temporali di emissione (data e ora invio), informazioni sull'utilizzo del "codice di invio" sottomesso (termini di validità, data e ora ultimo accesso, numero di accessi effettuati).

È possibile realizzare ulteriori tipologie di servizio basate que questo principio, ad esempio un servizio nel quale l'informazione da comunicare o l'attività richiesta all'utente, quella "vera", non sia contenuta nella mail ricevuta ma presentata o inviata all'utente solo successivamente alla "verifica dell'autenticità" del messaggio utilizzando una codice "usa e getta" oppure utilizzare il barcode allegato alla mail per veicolare la "password" per la lettura dell'eventuale allegato.

È evidente, anche in questa esemplificazione come la clonazione della grafica barcode inserita nel messaggio di posta elettronica non fornisca all'attaccante alcun vantaggio.

CONCLUSIONI

Telecom Italia, da sempre sensibile ai temi legati alla sicurezza, ha portato all'attenzione del gruppo di standardizzazione in ambito OMA il problema, più precisamente nel gruppo che si occupa dei servizi basati su barcode bidimensionali, fornendone un'accurata analisi e proponendo una possibile soluzione. Attualmente la discussione della proposta è giunta alla sua fase conclusiva e l'inserimento nel documento di "Tecnical Specification" è atteso entro il 1Q 2010.

La direzione IT.TS - Security Innovation ha sviluppato nel corso del 3Q 2006 una tecnologia di sicurezza "innovativa" come SC@CCO, poi oggetto di deposito brevettale nel 2007, che utilizzando i barcode bidimensionali unitamente a consolidati algoritmi di sicurezza, consente di veicolare sul terminale dell'utente, un servizio di autenticazione forte multi-fattore, che non necessiti più di sincronizzazione temporale come per i token hardware o di copertura radio come nel caso della MOTP [7], e sia utilizzabile in svariati contesti applicativi da quello strettamente lavorativo ad altri inerenti la vita privata e senza l'utilizzo di dispositivi esterni. Fattore non meno importante è rappresentato dalla possibilità di "trasferimento" in ambito commerciale di soluzioni "Made in Telecom Italia" che possono contribuire ad aumenta la percezione del valore trasferito dall'azienda ai propri clienti con evidenti ritorni economici e d'immagine.

La tecnologia SC@CCO sarà integrata all'interno della piattaforma di M-OTP come meccanismo di autenticazione alternativo in situazioni nelle quali la rete radio mobile non sia disponibile o accessibile e nei casi in cui la latenza dell'invio degli SMS risulti particolarmente elevata. SC@CCO è stato inserito come offerta in bandi di gara per Istituti di Credito ed Enti Pubblici come strumento alternativo, più sicuro e più economico degli attuali dispositivi hardware, come Token, e.Token, OTP Card.

7 Vedi news diffusa da Noi.TV del 30 gennaio 2009

ACRONIMI

AES	Advanced Encryption Standard
CGI	Common Gateway Interface
PIN	Personal Identification Number
MOTP	Mobile One Time Password
OMA	Open Mobile Alliance
OTP	One Time Password
QRCode	Quick Response Code
URI	Uniform Resource Identifier
URL	Universal Resource Locator

URLOGRAFIA

Di seguito alcuni siti Web che mettono a disposizione dei generatori di barcode on-line e/o librerie software per la loro produzione.

- *http://www.barcode-generator.org/*
- *http://www.morovia.com/free-online-barcode-generator/*
- *http://www.barcodesoft.com/online-barcode-generator.aspx*

La tecnologia barcode è così diffusa che esistono anche progetti di tipo opensource che mettono a disposizione codice sorgente per la produzione e interpretazione anche dei barcode, anche per diversi sistemi operativi.

- *http://code.google.com/p/zxing/*
- *http://qrcode.sourceforge.jp/*
- *http://www.libdmtx.org/*

Molto interessa è l'iniziativa "Semapedia" che ha come obiettivo quello di collegare il mondo virtuale con quello fisico utilizzando i barcode bidimensionali e interagendo con Wikipedia [8], ad esempio per avere informazioni su di un monumento. Realizzare tutto questo è veramente semplicissimo, una volta raggiunto il sito è sufficiente inserire la URL della pagina Wikipedia che si intende far raggiungere e "clickare" sull'apposito bottone "Genera" per ottenere, in formato PDF, 4 o 8 etichette pronte per essere stampate su di un foglio A4.

- *http://en.semapedia.org/*
  http://it.semapedia.org/

8 Wikipedia è la nota enciclopedia online, multilingue, collaborativa, e gratuita.

BIBLIOGRAFIA

[DATAMATRIX] "Information technology — International symbology specification — Data Matrix", ISO/IEC 16022:2000.

[AES] "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer-Verlag, 2002. ISBN 3540425802.

[FLASHCODE] "Flashcode Reader International Specification", Version 1.0 http://www.mobiletag.com/beta/en/contactspecification.html

[NTTDOCOMOGUIDE] "Guidelines and criteria for creating QR codes compatible with all terminals", NTT DoCoMo, http://www.nttdocomo.co.jp/english/service/imode/make/content/barcode/about/#p02

[NTTDOCOMOFUNC] "Bar Code Function", NTT DoCoMo, http://www.nttdocomo.co.jp/english/service/imode/make/content/barcode/function/

[URI] "Uniform Resource Identifiers (URI): Generic Syntax", RFC 3986. IETF. ed. T. Berners-Lee, R. Fielding, and L. Masinter. 1998.

[OMAURI] "URI Schemes for the Mobile Applications Environment", Version 1.0, Open Mobile Alliance™, OMA-TS-URI_Schemes-V1_0-20070718-D, URL:http://www.openmobilealliance.org/.

[QR] "Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification", ISO/IEC 18004:2006.

[SPRTD] "NFC Smart Poster RTD Technical Specification", NFC Forum

[TAGURI] "RFC 4151. The 'tag' URI Scheme", IETF, http://www.faqs.org/rfcs/rfc4151.html.

[URI] "RFC 3986. Uniform Resource Identifier (URI): Generic Syntax", IETF, http://www.ietf.org/rfc/rfc3986.txt.

[X.509] ITU-X Recommendation X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

[URNRES] "RFC 2169 - A Trivial Convention for using HTTP in URN Resolution", IETF, http://www.faqs.org/rfcs/rfc2169.html.

maurizio.ghiradi@telecomitalia.it

AUTORE

Maurizio Ghirardi

lavora in Telecom Italia dal 1980 come ricercatore. Ha partecipato a progetti nazionali e internazionali, occupandosi della specifica, della progettazione e del design di sistemi di gestione per reti di telecomunicazioni di nuova generazione. Attualmente opera presso la direzione IT.TS - Security Innovation, occupandosi dell'ideazione, dello studio e della prototipazione di nuove soluzioni in ambito ICT Security ■

Caso Miroglio Fashion: la moda in "prossimità"

MOBILE

Elisa Alessio, Simonetta Mangiabene, Davide Pratone

Miroglio Fashion, casa di moda italiana, ha avviato da settembre 2009 la prima iniziativa a livello nazionale di fidelizzazione della clientela attraverso rete mobile.
Il progetto, sviluppato con il supporto di Telecom Italia, permette ai clienti degli outlet "Vestebene Factory Store" di raccogliere i punti fedeltà attraverso il telefono cellulare dotato di tecnologia radio a corto raggio NFC (Near Field Communication), visualizzarne il saldo direttamente sul display e ricevere i bonus via sms.
Il servizio consente ai clienti di registrare i punti fedeltà, avvicinando semplicemente il telefonino al sistema di cassa e di controllare in tempo reale il punteggio acquisito direttamente sul display, senza dovere avere un'apposita tessera. Il sistema centrale di Miroglio Fashion, collegato tramite la rete a banda larga Telecom Italia al registratore di cassa, registra le operazioni di acquisto e invia al cliente, tramite sms, i punteggi raggiunti e i buoni sconto. Sono inoltre previsti l'invio alla clientela di sms informativi sull'arrivo delle nuove collezioni o dei saldi e sulla possibilità di usufruire del servizio di Mobile Payment.

1 Introduzione

Near Field Communication (NFC) è uno standard wireless a corto raggio che abilita semplici e sicure interazioni tra dispositivi elettronici, sviluppato congiuntamente da Sony e Philips nel 2004.

NFC si sviluppa a partire dalla combinazione di tecnologie di identificazione e di interconnessione e, come tale, rappresenta **un'evoluzione della tecnologia RFID**, **compatibile con la diffusa architettura delle smart card contactless**. L'integrazione di NFC in un terminale mobile, trasforma il cellulare in un passepartout, con il

Figura 1 – NFC Use-Case *[Fonte NFC Forum]*

quale sarà possibile disporre di una vasta serie di servizi, fruibili in modo semplice e sicuro, tra i quali: controllo accessi, m-payment/ticketing e advertising, data sharing e content downloading (*figura 1*).

Alcune manifatturiere di terminali mobili hanno già integrato nei loro dispositivi la tecnologia NFC. Il numero dei terminali verrà incrementato nel 2010 e Juniper Research sostiene che **entro il 2012 oltre il 16% dei terminali venduti (circa 210 milioni) avrà l'interfaccia NFC inclusa**.

Tale evoluzione ha generato una notevole crescita di interesse sulla tecnologia stessa e un'estensione dei possibili ambiti applicativi, con sperimentazioni attualmente in corso in tutto il mondo.

La tecnologia NFC lavora su frequenza non licenziata a **13,56 MHz**, esente, oltre che da licenze, da particolari restrizioni, con esclusione delle norme che limitano le emissioni elettromagnetiche nella banda di riferimento. Tali limitazioni fanno sì che la distanza massima di comunicazione, che varia da nazione a nazione e dal particolare standard di riferimento, sia comunque nel **range 0-20 cm**.

Il funzionamento operativo prevede l'interazione di due elementi tramite un'interfaccia di comunicazione wireless, definiti "Initiator" e "Target" a seconda del ruolo svolto nell'interazione.

Sono, infatti, previste due tipologie di interfacciamento: un "active communication mode" e un "passive communication mode", tramite i quali NFC abilita il cellulare a lavorare in tre modalità di funzionamento: come lettore, in peer-to-peer e come emulazione di una smartcard contactless (*figura 2*).

Nel caso di active mode (in cui entrambi i dispositivi generano e sfruttano il loro campo RF) si parla di **modalità peer-to-peer**: viene infatti sostanzialmente creata una rete peer-to-peer tra i due dispositivi e per entrambi è possibile inviare e ricevere informazioni, interagendo nelle due direzioni con operazioni di lettura/scrittura.

Nel caso di passive mode, l'Initiator, un dispositivo che ha funzione di **Reader/Writer** (si comporta da lettore), genera il campo, mentre il Target è passivo e ha funzione di **Card Emulator** (emula una Smart Card Contactless).

Una peculiarità della tecnologia è la **semplicità di utilizzo**: l'NFC non ha bisogno di setting particolari come altre tecnologie a corto o a lungo raggio (es. Bluetooth, WiFi) e l'utilizzatore non deve quindi confrontarsi con la complessità di

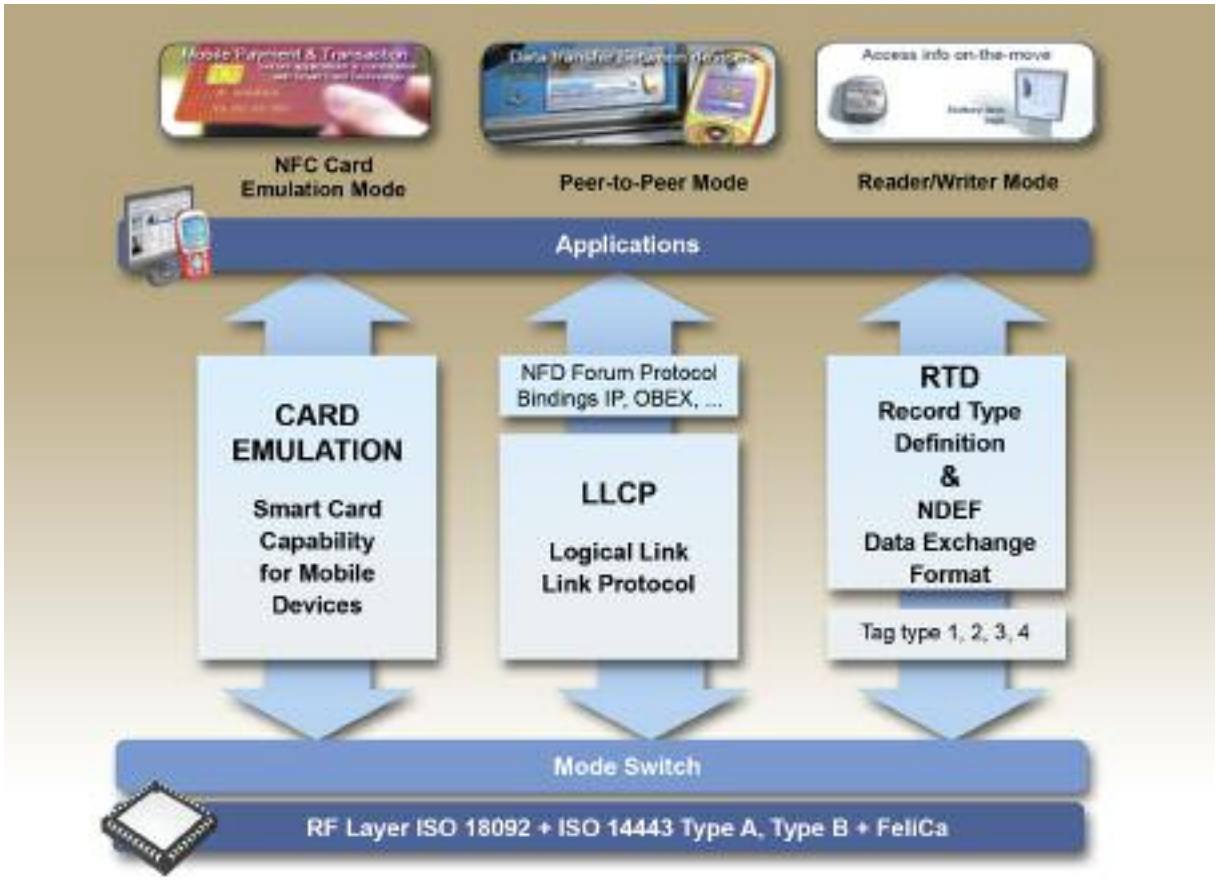


Figura 2 – Modalita' di funzionamento e architettura NFC Forum

configurare parametri di rete o altro. La procedura per inizializzare una comunicazione è semplice: se si vuole comunicare con qualche dispositivo basta "toccarlo".

Alcuni dei principali **ambiti applicativi** della tecnologia NFC sono:

- **Payment**: sfruttare il terminale mobile per transazioni di acquisto di beni o servizi in sicurezza (avvicinato ad un POS abilitato, il cellulare si comporta come una carta contactless di credito/debito o prepagata);
- **Ticketing**: gestire acquisto, validazione e controllo di biglietti e carnet di varia natura;
- **M-fidelity**: gestire fidelity card con punti ed eventuali buoni sconto;
- **Access Control**:
  - ***Accesso fisico***: utilizzare il proprio cellulare come badge/chiave per accedere a varchi equipaggiati con la stessa tecnologia;
  - ***Accesso logico***: utilizzare il proprio cellulare come chiave di accesso e autenticazione a servizi personalizzati in base al profilo dell'utente e fruibili attraverso device dotati di lettore NFC:
    - accesso a risorse informatiche personali o condivise (es. PC/Laptop) per login alla postazione, ad aree WEB personali, mail, e servizi di mobile office in genere;
    - accesso personalizzato ai servizi offerti da apparati multimediali (aree WEB personali, stampa documenti, …);
- **Data sharing**: condividere informazioni, contenuti, dati tra dispositivi mobili dotati della stessa tecnologia (es. scambio business card);
- **Content downloading**: scaricare dati o informazioni da apparati multimediali o Smart Poster (es. messaggi pubblicitari, promozioni, coupon, …).
- **Data Connection Enabling**: scambiare i parametri necessari ad abilitare il proprio dispositivo mobile ad altre connessioni a lunga di-

stanza per superare barriere di usabilità, o in generale, agevolare la configurazione di parametri necessari all'abilitazione di servizi specifici sul cellulare.

2 Enti di standardizzazione

2.1 *NFC Forum*

NFC Forum (*www.nfc-forum.org*) è un'associazione non-profit fondata nel 2004 da Sony, Philips e Nokia che conta ormai più di 140 membri facenti parte di tutte le principali aree dell'ecosistema NFC (*figura 3*), tra cui manifatturiere, sviluppatori di applicazioni e istituzioni finanziarie. Gli obiettivi principali del forum sono quelli di garantire l'interoperabilità tra i dispositivi e i servizi, sviluppare specifiche e promuovere sul mercato la tecnologia NFC.

Inoltre NFC Forum collabora con i principali enti di standardizzazione e associazioni come: ETSI, GSMA, EMVCo, Smart Card Alliance e Mobey Forum.

Figura 3 – Ecosistema NFC *[Fonte NFC Forum]*

2.2 *ETSI e l'implementazione SIM-based*

ETSI (European Telecommunications Standards Institute – *www.etsi.org*) è l'ente europeo di standardizzazione nel campo delle telecomunicazioni. Al suo interno opera il Technical Commitee Smart Card Platform (SCP), che ha il mandato di definire e gestire la smart card per le telecomunicazioni (UICC). La UICC è la smart card normalmente utilizzata per le SIM e USIM in commercio, per cui in questo contesto le sigle SIM, USIM e UICC hanno tutte lo stesso significato.

L'SCP ha lavorato per integrare la tecnologia NFC con l'ambiente sicuro della SIM, mettendo insieme l'ubiquità del dispositivo mobile con una serie di servizi di forte appeal per cittadini e utenti in genere.

Del resto la SIM gioca un ruolo chiave nel mercato delle telecomunicazioni mobili per gli asset che può vantare.

La SIM garantisce:

- un metodo sicuro di autenticazione forte;
- indipendenza dal terminale utilizzato ove il terminale sia compliant alle specifiche di riferimento;
- scalabilità;
- facile gestione di aggiornamenti;
- ampia diffusione (circa due miliardi di SIM Card sono già distribuite in tutto il mondo).

L'architettura (*figura 4*) definita dall' ETSI SCP si basa sul concetto di accedere alle risorse radio NFC presenti sul terminale attraverso un protocollo wire che collega la UICC al contactless front-end (CLF - il chipset che implementa la tecnologia NFC sul telefono).

I dati applicativi sono quindi trasferiti dal device esterno al terminale attraverso un'interfaccia radio NFC e successivamente trasferiti dal CLF alla UICC (*figura 5*), attraverso il protocollo wire chiamato SWP (Single Wire Protocol – in quanto utilizza solamente un contatto (C6) della UICC) e standardizzato in ambito ETSI.

Il Single Wire Protocol è un protocollo di comunicazione full duplex, in cui il segnale

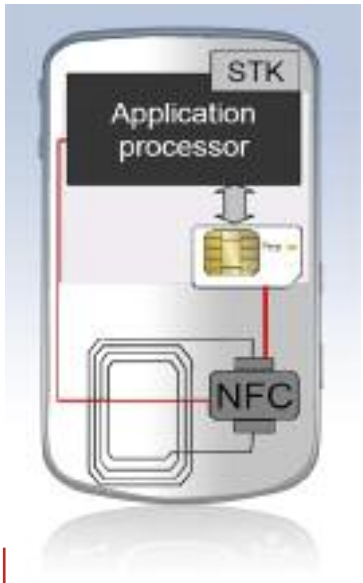


Figura 4 – Architettura NFC definita da ETSI SCP

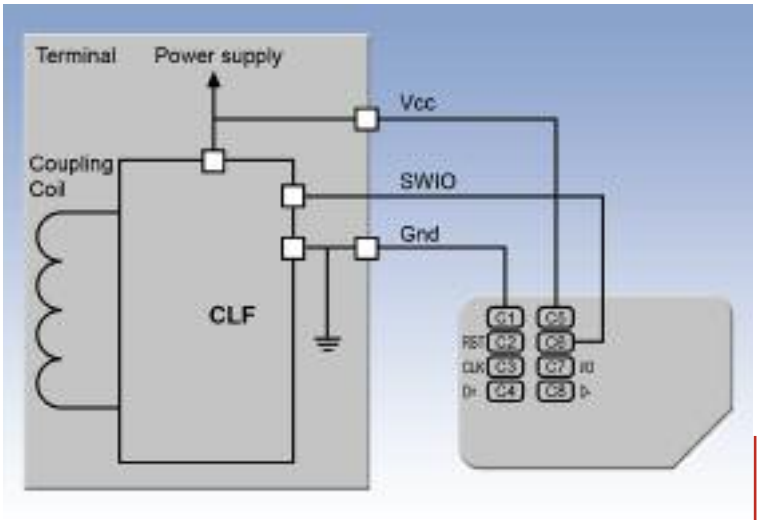


Figura 5 – Connessione CLF-UICC

Figura 6 – Single Wire Protocol

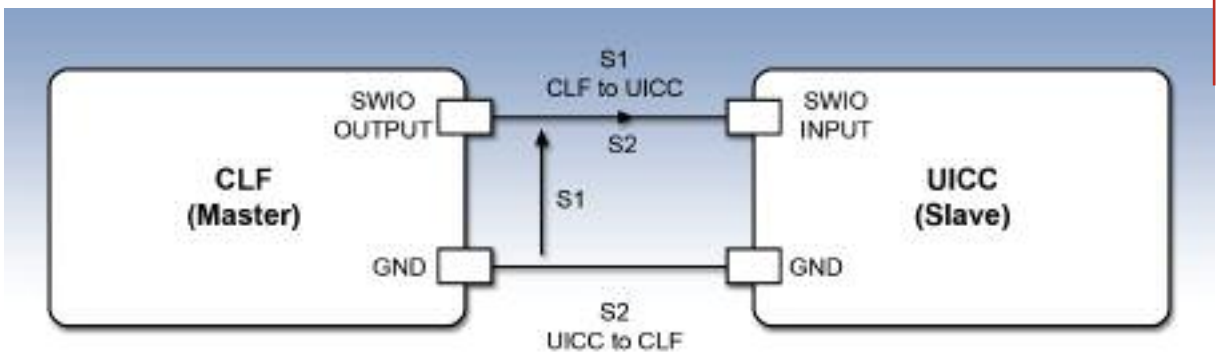
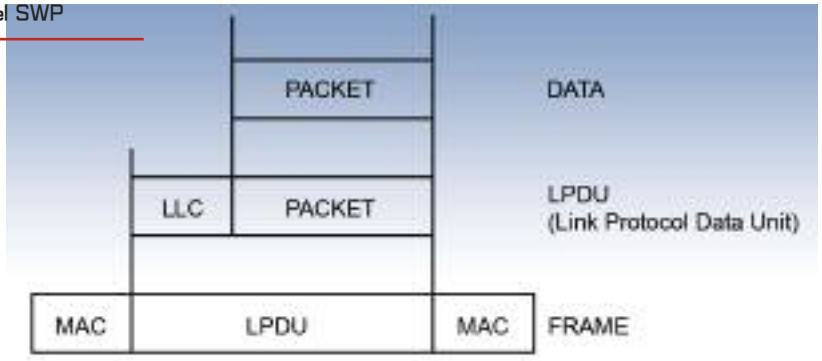


Figura 7 – Protocolli di trasporto del SWP



S1 (modulazione di tensione) trasporta le informazioni dal CLF alla UICC ed il segnale S2 (modulazione di corrente) trasporta le informazioni dalla UICC al CLF (*figura 6*).

Il Single Wire Protocol ha un Data Link Layer costituito da un Link Protocol Data Unit (LPDU) e un livello MAC. Il Logical Link Layer è chiamato Simplified High Level Data Link Control (SHDLC), ma per alcune tipologie di tecnologie RF (es. Mifare, Felica) si utilizzerà il ContactLess Tunnelling protocol (CLT).

Sopra il livello di trasporto è stato definito un livello applicativo e di controllo per la gestione delle applicazioni contactless memorizzate nella UICC. Questo livello è chiamato Host Controller Interface (*figura 8*) ed è specificato in ETSI.

L'architettura dell'HCI è multi host, ossia è in grado di gestire applicazioni contactless che risiedono sulla UICC, sul Secure Element embedded nel terminale o sul Secure Element

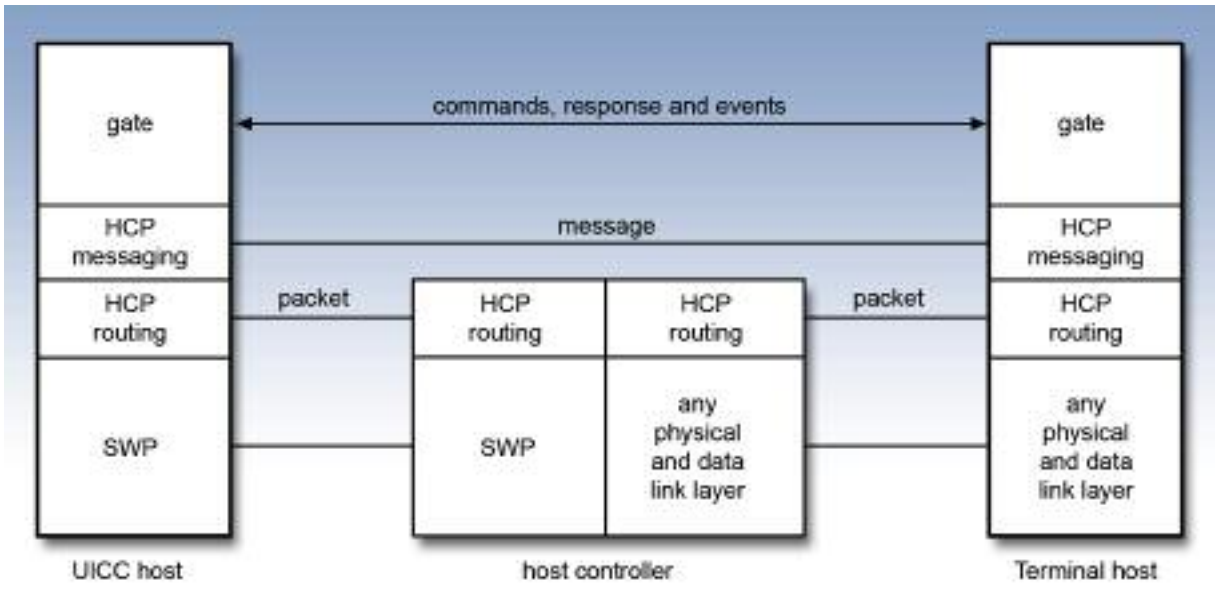


Figura 8 – Host Controller Interface

residente su di una memory card; per comunicare con questi ultimi due Secure Element è sufficiente aggiungere il relativo livello fisico.

L'Host Controller Interface si occupa di gestire i flussi applicativi sui vari livelli fisici e di creare le connessioni opportune (Gate) tra le applicazioni. Ad esempio se sulla UICC sono memorizzate due applicazioni contactless che utilizzano lo stesso protocollo RF in card emulation mode il livello HCI creerà un'unica Gate tra il CLF e l'UICC relativo a questo protocollo RF e le applicazioni utilizzeranno entrambe questo Gate. I flussi dati all'interno di questi Gate sono raccolti in Pipe ed ogni Pipe è associata ad un'applicazione (*figura 9*).

Oltre a queste due specifiche ETSI SCP ha anche definito gli standard di test per certificare l'implementazione del SWP e dell'HCI su carte e terminali, molto importanti per garantire un'implementazione omogenea di queste caratteristiche e l'interoperabilità dei servizi indipendente dal tipo di carte e terminale utilizzato.

Il prossimo passo in ETSI SCP sarà quello di definire delle API Java Card per sviluppare servizi contactless sulle UICC, sfruttando i meccanismi presentati in questa sezione. Queste API permetteranno una facile programmazione, rendendo astratto tutto il protocollo HCI e garantendo l'interoperabilità delle applicazioni.

2.3 *GSMA e l'approccio PayBuyMobile*

La GSM Association (GSMA), gruppo che riunisce i principali operatori di telefonia cellulare a livello mondiale, ritiene che sia giunto il momento di adottare le soluzioni Near Field Communication (NFC). I sistemi NFC consentono di usare il proprio telefono come carta di credito o di debito, semplicemente avvicinando l'apparecchio a un particolare lettore. La spinta della GSMA verso l'adozione della tecnologia NFC è motivata dal successo di diversi progetti pilota che coinvolgono otto paesi e nove operatori e presto partiranno altri quattordici esperimenti. Alcuni test su larga scala (in Francia, Taiwan e Corea) hanno infatti dimostrato che i clienti erano soddisfatti di usare il proprio cellulare per pagare le spese nell'85-90 % dei casi. E la maggioranza di loro riteneva che fosse un processo sicuro e l'avrebbe raccomandato ad amici e parenti.

A questo proposito, il Barometro ISPO ha recentemente condotto per MasterCard la ricerca

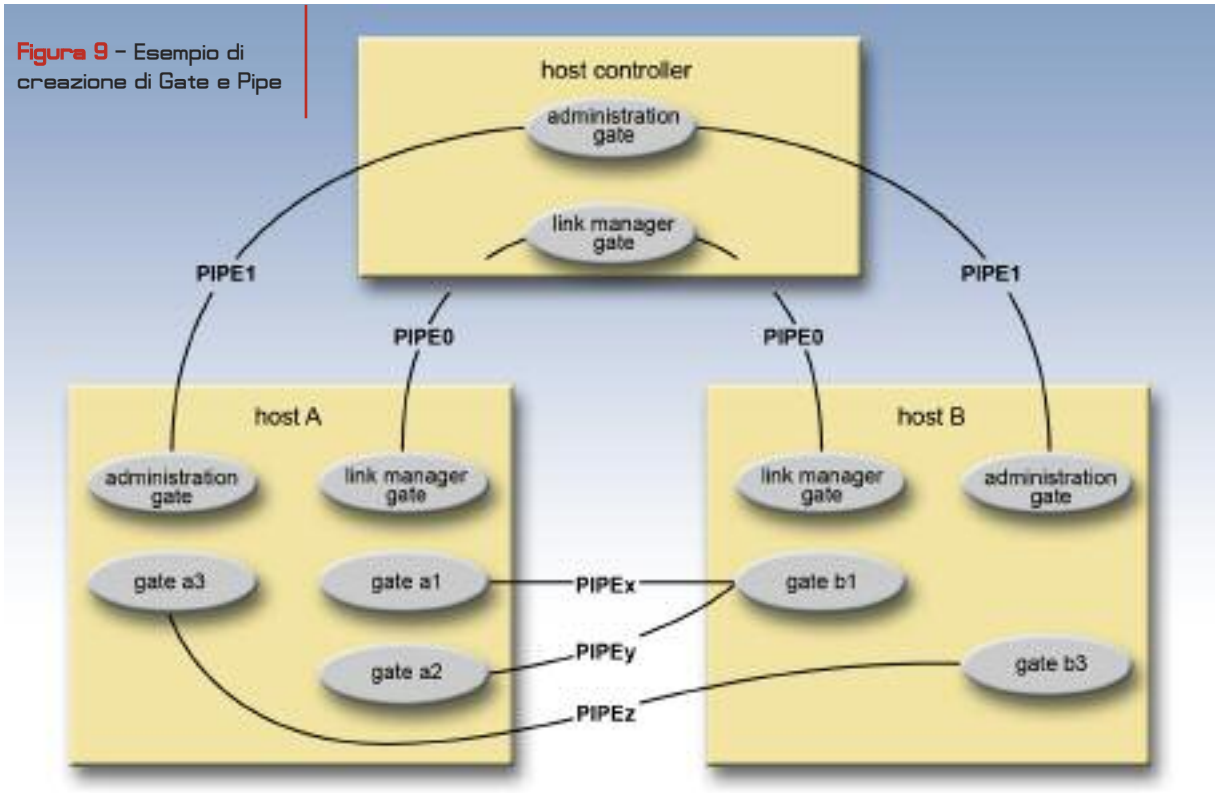


Figura 9 – Esempio di creazione di Gate e Pipe

"**Gli Italiani e la voglia di semplificarsi la vita**", dalla quale è emerso che il desiderio principale della gente risulta essere proprio quello di facilitare la routine quotidiana, facendo leva sulla velocità, l'ingrediente principale per renderla meno complicata. Le tecnologie ovviamente in questo giocano un ruolo importante.

"Gli italiani cercano di destreggiarsi tra i molti impegni e il poco tempo a disposizione, con interessanti risultati: il 58% degli intervistati, in particolare la fascia attiva della popolazione (25-54 anni), ha un atteggiamento "frenetico", mille impegni e responsabilità da gestire in poco tempo" dichiara Paolo Battiston – Direttore Generale MasterCard Italia. "La tecnologia contactless facilita l'utilizzo della carta di pagamento specialmente in quelle situazioni in cui la velocità è essenziale, come ad esempio prendere un caffè, fare la spesa, noleggiare un film o comprare un libro ". Il 72% degli intervistati ritiene che le tecnologie abbiano realmente semplificato la vita, tuttavia alcuni ritengono che i prodotti scientifici nascondano delle piccole insidie: per il 65% infatti risultano difficili da usare. Chi invece guarda alla tecnologia con assoluta fiducia è una quota pari al 32%, più spesso giovane (i 18-24enni sono il 58%) e istruita (i laureati sono il 55%).

Ma quali sono i prodotti che più incidono positivamente nella gestione della quotidianità? Innanzitutto il telefonino (80%), seguito dalle carte di pagamento (74%) e da Internet (72%). E cosa rende "indispensabili" questi prodotti? Per la maggioranza assoluta degli utilizzatori (52%) è la comodità, poi la velocità (15%) e la sicurezza (14%).

"I pagamenti in modalità 'contactless' rispondo perfettamente a queste esigenze: la transazione si effettua avvicinando semplicemente la carta al POS abilitato, senza dover firmare lo scontrino o digitare il PIN. Al risparmio di tempo si aggiunge un'evidente praticità: la possibilità di pagare in tutta sicurezza, dal momento che la carta non lascia mai le mani del proprio titolare" commenta sempre Paolo Battiston.

Ma questo implica che la maggior parte degli apparecchi commerciali si debba adeguare a uno standard. In questo caso, **secondo la GSMA**, **le industrie produttrici dovrebbero affidarsi al Single Wire Protocol (SWP)**, **che consente al chip NFC integrato nel telefono di interagire con la Sim card**. Un modello verso il quale

spinge anche l'ETSI (European Telecommunications Standards Institute).

La GSM Association ha inoltre lanciato l'iniziativa ***Pay-Buy-Mobile***, evoluzione naturale del programma sul NFC lanciato al fine di incoraggiare un approccio comune per l'integrazione la tecnologia wireless Near Field Communications (NFC) in ambito mobile. L'iniziativa, che vede anche Telecom Italia tra i partecipanti 'più attivi', ha in particolare l'obiettivo di incoraggiare un approccio comune all'implementazione della tecnologia, soprattutto per quanto riguarda la sicurezza della fatturazione e delle informazioni personali contenute sulla SIM card degli utenti.

"Dopo diverse iniziativa frammentate, l'industria mobile si è ora unita per permettere l'utilizzo del cellulare al posto della carta di credito", ha dichiarato il Ceo della GSMA, Rob Conway. "Il supporto dei maggiori operatori mobili e produttori di cellulari assicurerà l'adozione globale di Pay-Buy Mobile, permettendo ai vendor di ottenere economie di scala e ai consumatori di utilizzare il telefonino per pagare beni e servizi dovunque essi siano", ha aggiunto Conway. A questo scopo, la GSMA vuole assicurare l'esistenza e l'adozione massiva di un set di standard ben definiti che garantiscano un ecosistema sicuro oltre all'interoperabilità internazionale. L'interoperabilità e la standardizzazione sono infatti fattori cruciali per il successo dell'NFC sul mercato della telefonia mobile.

Lo scopo della GSMA è quello di aprire la strada all'implementazione di un business model sostenibile, che includa tutte le parti coinvolte nella catena di valore e aggiunga un nuovo tassello alle già numerose possibilità offerte dai cellulari.

3 La sperimentazione con Miroglio Fashion

In quest'ottica Telecom Italia, oltre ad avere grande esperienza nell'implementazione e messa in campo di servizi a valore aggiunto basati sull'utilizzo della SIM, dal 2006 lavora alla standardizzazione delle tecnologie in questione (NFC e SWP). Il know how acquisito ha quindi permesso all'Azienda di essere il primo operatore italiano a lanciare trial di servizi di m-ticketing con aziende trasporti e di m-fidelity con partner commerciali, sfruttando le opportunità offerte dalle tecnologie di prossimità e si appresta a breve ad introdurre massicciamente servizi di m-payment dedicati al mondo bancario.

Anche nel settore del mobile fidelity Telecom Italia ha introdotto per prima la tecnologia NFC, realizzando insieme a Miroglio Fashion un servizio di fidelizzazione delle clienti degli outlet Miroglio. Il progetto prevede la distribuzione di telefoni e SIM card che supportino i protocolli NFC e sistemi di lettura integrati ai punti cassa che emulano le funzionalità di base della gestione elettronica del Customer Loyalty Program grazie ad un'applicazione residente sulla SIM card, nonché la possibilità di consultare lo stato del punteggio maturato e gestirne il trasferimento e la spesa attraverso i menù del cellulare.

I Clienti degli Outlet disporranno quindi di un vero e proprio portafoglio elettronico che si sostituisce all'attuale Fidelity Card. Il progetto ha come obiettivo quello di eliminare la gestione cartacea dei buoni sconto e ridurre progressivamente quella delle Fidelity Card, con conseguente riduzione a regime dei costi di gestione per il l'Azienda Miroglio Fashion. In una prima fase sono stati attrezzati 5 negozi e sono stati distribuiti 100 telefoni NFC. Il progetto sarà poi esteso al resto del programma fidelity "Cartaffari", che coinvolge attualmente più di 300.000 consumatrici e circa 80 Outlets.

Telecom Italia si è occupata dello sviluppo del progetto, che ha visto anche la collaborazione di Olivetti,,definendo le specifiche della SIM NFC e dell'applicazione Fidelity Card che risiede a bordo della SIM stessa. L'applicazione Fidelity Card è infatti una applet SIM Application Toolkit che risiede sulla SIM e sfrutta le funzionalità JavaCard™ della carta.

CONCLUSIONI

I pagamenti elettronici hanno visto nel corso degli ultimi anni un'evoluzione dalla carta a banda magnetica, alla carta di credito con chip fino a soluzioni di carte contactless che hanno permesso di raggiungere soluzioni sempre più sicure ed user friendly ('tap and go').

I servizi mobili di interesse per il mondo bancario e finanziario possono essere sostanzialmente suddivisi in 4 macroaree:

- security;
- banking;
- pagamenti remoti;
- pagamenti diretti.

Le tecnologie tradizionali (es. SMS, browsing...) soddisfano le esigenze delle prime tre macroaree; l'introduzione della tecnologia NFC nel mondo mobile permette l'apertura all'area dei pagamenti diretti (POS, m-ticketing, access control...).

È altresì importante evidenziare che la maggiore usabilità di questa soluzione (velocità e semplicità), unita ad un controllo diretto del rischio, offre al mondo bancario uno strumento efficace per tentare di aggredire il mercato dei micro pagamenti, ad oggi puramente dominato dall'utilizzo del denaro contante. In particolare, nel caso della sperimentazione con Miroglio Fashion si sono evidenziati vantaggi per tutta la catena del valore:

Il service provider, in questo caso Miroglio, ha potuto approfittare di una riduzione dei costi di gestione del programma di fidelizzazione, ed ha introdotto un nuovo canale pubblicitario diretto con i clienti introdotto oltre che una gestione sicura dei buoni sconto.

Il cliente finale può usufruire di un servizio migliore, avendo sempre a disposizione i dati del proprio programma di fidelizzazione senza doversi più ricordare di portare con sè la tessera loyalty o il buono sconto cartaceo.

L'operatore telefonico, in questo caso Telecom Italia, abilitando un servizio che fidelizza la clientela, può creare nuove opportunità di business in settori in precedenza non considerati.

Nel contesto del servizio CARTAFFARI di Miroglio il telefono NFC è stato utilizzato unicamente in modalità Card Emulator, ma sfruttando le possibilità date dalle altre modalità, il Reader ed il Peer to Peer, si aprono numerosi scenari applicativi. Rimanendo in quest'ambito è possibile prevedere la realizzazione di vetrine attive in cui sono presenti delle etichette NFC che il cliente può leggere tramite il proprio telefono NFC. Le informazioni contenute nelle etichette possono svariare dai dettagli e gli sconti sul prodotto a link web verso siti pubblicitari visitabili dal cliente. Nella modalità Peer to Peer è invece immaginabile uno scenario in cui i clienti si scambiano punti e buoni sconti del loro programma di fidelizzazione.

Le differenti modalità con cui utilizzare la tecnologia NFC abbinata alla connettività del cellulare ed alla sua predisposizione ad ospitare servizi a valore aggiunto lasciano agli application provider ed agli operatori di telecomunicazioni ampie possibilità di individuare servizi utili e remunerativi. Nel futuro prossimo vedremo un'infinità di oggetti connessi tramite la tecnologia NFC ed il cellulare sarà il punto di collegamento tra questi oggetti connessi e la rete di telecomunicazione.

ACRONIMI

API	Application Programming Interface
CLF	ContactLess Front-end
CLT	ContactLess Tunnelling protocol
ETSI	European Telecommunications Standards Institute
EMV	EuroPay MasterCard Visa
GSMA	Global Systems Mobile Alliance
HCI	Host Controller Interface
HCP	Host Controller Protocol
LLC	Logical Link Control
LLCP	Logical Link Control Protocol
LPDU	Link Protocol Data Unit
MAC	Medium Access Control
NFC	Near Field Communication
NDEF	NFC Data Exchange Format
RF	Radio Frequency
RFID	Radio Frequency IDentification
RTD	Record Type Definition
SCP	Smart Card Platform

SHDLC	Simplified High Level Data Link Control
SIM	Subscriber Identity Module
STK	SIM ToolKit
SWP	Single Wire Protocol
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

BIBLIOGRAFIA

[1] NFC Forum, *www.nfc-forum.org*

[2] ETSI TS 102 613 " Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics"

[3] ETSI TS 102 622 " Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)"

[4] ETSI TS 102 705 " Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications"

[5] GSMA Pay-Buy-Mobile white paper

elisa1.alessio@telecomitalia.it
simonetta.mangiabene@telecomitalia.it
davide.pratone@telecomitalia.it

AUTORI

Elisa Alessio

ingegnere delle telecomunicazioni, dal 2001 è in Telecom Italia, dove si è occupata di soluzioni avanzate di "network processor" e della progettazione di un "system on chip" per la sicurezza di dati e comunicazioni. Dal 2003 si occupa di tecnologie di prossimità e della loro applicazione in scenari verticali.
Dal 2007 è responsabile di un progetto sul m-commerce e attualmente, all'interno dell'area "Strategia ed Innovazione", coordina le attività relative a soluzioni di m-commerce e trusted environment in ambito mobile ■

Simonetta Mangiabene

è project manager in Telecom Italia dal 2005, attualmente all'interno dell'area 'Innovation and Strategies' coordina il progetto sull'evoluzione delle SIM cards.
Dal 1998 si occupa di SIM card e relativi servizi in ambito mobile, ha partecipato a numerosi progetti di ricerca finanziati ed è attualmente delegato rappresentante di Telecom Italia presso l'ente di standardizzazione ETSI Smart Card Platform (SCP) Plenary and Requirements Groups dedicato alla specifica di nuove features per smart e sim cards ■

Davide Pratone

è responsabile del laboratorio Integrated Circuit Cards all'interno dell'area Innovation and Strategies. Dal 2002 si occupa della progettazione e sviluppo di servizi a valore aggiunto basati su SIM card ed attualmente segue le attività relative ai servizi di prossimità Near Field Communication (NFC) e di mobile payment. In ambito 3GPP Davide riveste la carica di vice-chairman del gruppo CT6 che si occupa della standardizzazione della USIM, inoltre è delegato rappresentante di Telecom Italia presso l'ente di standardizzazione ETSI Smart Card Platform (SCP) Technical Group che si occupa della standardizzazione della UICC ■

Tecniche di posa a basso impatto ambientale

AMBIENTE

Paola Finocchi, Paolo Trombetti

La fruizione dei servizi, offerti attraverso reti tecnologiche avanzate, è sinonimo di sviluppo e di benessere sociale ed economico.
Un recente studio dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) "Infrastructure 2030", evidenzia che, in futuro, gran parte degli stati avrà difficoltà ad affrontare la crescente necessità di sviluppare nuove infrastrutture.
Nel presente articolo viene illustrato come l'innovazione tecnologica nei sistemi di realizzazione possa rappresentare l'unica via sostenibile per permettere questo sviluppo, coniugando le esigenze di tutti i soggetti coinvolti.

1 Introduzione

Nel settore delle telecomunicazioni, lo sviluppo delle reti a "larga banda" ha creato forti aspettative da parte dei cittadini, delle imprese e delle Amministrazioni pubbliche.

In particolare i cittadini intravedono la possibilità di usufruire di tutta una serie di servizi innovativi che facilitino loro la vita - quali ad esempio effettuare acquisti e operazioni bancarie on-line, prenotare visite, richiedere certificati tramite portale informatico, accedere ad Internet per semplici consultazioni... - con forti benefici in termini di minori oneri di spostamento, di traffico, di file agli sportelli e di perdita di tempo.

Per le imprese la disponibilità dei servizi di comunicazione, vuol dire aumentare significativamente la potenzialità di crescita e quindi dell'economia in generale, traducendosi nel poter effettuare in maniera veloce, transazioni, compra-vendite, pubblicità, partecipazione a bandi di gara nazionali e internazionali, e soprattutto abbattimento di ogni "barriera" territoriale.

Per il settore pubblico, infine, vuol dire snellire significativamente la propria burocrazia interna,

ridurre i costi di gestione, rendere più efficienti e accessibili le strutture rivolte al pubblico anche attraverso lo sviluppo di strumenti dedicati (totem multimediali).

Ma il "gap" infrastrutturale registrato oggi nella fornitura della "larga banda", il cosiddetto digital divide, è ancora alto. Lo studio del dott. Caio, commissionato dal Ministero dello Sviluppo Economico, evidenzia che per ridurre il *digital divide* fino al 2-3 % entro il 2011, sono necessari investimenti per circa 1,4 Mdi Euro, di cui almeno il 50-60 % è relativo alla realizzazione di infrastrutture.

In una congiuntura economica così poco favorevole come quella attuale, le cifre in gioco appaiono quasi proibitive. Cosa fare allora? La soluzione è davvero solo quella di riuscire a trovare un investitore "forte"?

Parlando di innovazione, forse è proprio in questa che va ricercata la chiave di volta. Innovazione intesa non solo "dei servizi", ma anche delle tecniche di realizzazione delle reti tecnologiche, oltre che degli strumenti finanziari "ad hoc", messi a disposizione degli investitori.

Infatti, l'impiego di tecniche di posa alternative a quelle tradizionali che, rispetto a queste, risultano molto più economiche e veloci, congiuntamente a forme di finanziamento agevolato o che vedano il concorso di soggetti pubblici e privati, incentiverebbe le imprese ad investire.

È, infine, utile evidenziare che il forte abbattimento nei costi di realizzazione delle infrastrutture non va letto solo come "risparmio per gli Operatori", ma anche, soprattutto, come "opportunità e vantaggio" per la collettività. Prima di tutto perché, a parità dì investimenti, gli Operatori potrebbero sviluppare in maniera geograficamente più ampia la propria rete, e poi perché lo sviluppo della banda larga è finanziata principalmente da risorse pubbliche.

2 Le tecniche

Per tecniche di posa innovative ci si riferisce in particolare alle cosiddette tecniche "no-dig" o "trenchless technology", letteralmente "senza scavo", che rispetto a quelle tradizionali, risultano veloci, economiche e molto meno invasive.

Non sono tecniche nuovissime, anche se in Italia se ne è sempre fatto scarso ricorso. Gli Operatori hanno cominciato a guardarle con interesse solo negli ultimi anni, apprezzandone anche la caratteristica di essere a "basso impatto ambientale".

Queste tecniche, infatti, essendo per definizione "senza scavo", comportano una minima movimentazione di materiali e di macchinari e richiedono aree di cantiere di dimensioni ridotte, incidendo quindi positivamente anche sulla sicurezza dei cantieri.

Inoltre, intervenendo in maniera limitata sul manto stradale, se ne riduce il danneggiamento, abbattendone così i costi di manutenzione.

In Italia, l'associazione IATT (Italian Association for Trenchless Technology) - senza fini di lucro - promuove la diffusione della conoscenza di queste tecniche anche attraverso sperimentazioni.

Nel campo delle telecomunicazioni, le tecniche no-dig maggiormente utilizzate sono le *perforazioni orizzontali*, la *minitrincea* e la posa in infrastrutture esistenti, anche destinate ad altri sottoservizi. Propedeutica per l'impiego di queste tecnologie è un'accurata indagine del sottosuolo, realizzata, di norma, con il *georadar*.

Di queste tecnologie se ne fornisce, nel seguito, una breve descrizione con riguardo all'ambito di applicazione, ai vantaggi di impiego, nonché ai limiti applicativi.

2.1 *Indagini Conoscitive: sistemi Georadar (Ground Penetrating Radar, GPR)*

Questi sistemi consentono di rivelare in modo non distruttivo e non invasivo la presenza e la posizione di oggetti presenti nel sottosuolo, fino ad una profondità di diversi metri, utilizzando il fenomeno della riflessione delle onde elettromagnetiche a particolari frequenze.

Il sistema è costituito da un'unità di controllo e di acquisizione dei dati e da una o più antenne e permette di acquisire, elaborare, interpretare i dati e di restituire elaborati grafici (cartacei o elettronici) bi/tri dimensionali in pianta o in sezione. A seconda del numero di antenne e della frequenza utilizzata per l'introspezione, la tecnica permette di rilevare, più o meno accuratamente, la posizione e la dimensione degli oggetti presenti nel sottosuolo.

L'uso della tecnologia è propedeutico all'impiego delle tecniche di posa no-dig, ed è utile per la progettazione di reti tecnologiche, permettendo di effettuare analisi dei profili stratigrafici, indagini archeologiche e ambientali...

Il suo impiego è però condizionato principalmente dalle caratteristiche geologiche del terreno (la presenza di acqua, infatti, attenua la capacità di penetrazione dell'onda elettromagnetica) e dal tipo di oggetti presenti nel sottosuolo (per esempio la presenza di maglie metalliche) (vedi *figura 1*).

Figura 1 – Schema di rilevamento degli impianti nel sottosuolo con la tecnica del Georadar

2.2 *Perforazioni orizzontali guidate: Trivellazione Orizzontale Controllata (Horizontal Directional Drilling)*

Questa tecnica consente la posa di tubazioni in polietilene o acciaio, atte alla fornitura di tutti i tipi di sottoservizi (compresi prodotti petrolchimici) del diametro di (40 1.600) mm.

La posa avviene mediante una trivellazione guidata elettronicamente dal punto di ingresso ad uno di arrivo, senza la necessità di effettuare scavi a cielo aperto.

La tecnologia prevede varie fasi di lavorazione e può essere effettuata "a secco", oppure "ad umido" (con avanzamento coadiuvato da getto fluido costituito da acqua e bentonite):

- viene realizzato un foro pilota mediante l'introduzione nel punto di ingresso di una colonna di aste, con un utensile di perforazione posto in testa, guidata alla quota e nella direzione voluta;
- raggiunto il punto di uscita, sulla testa di perforazione viene montato un opportuno alesatore, che permette di allargare il diametro del foro fino a raggiungere le dimensioni utili alla posa dei tubi previsti;
- completata la posa, l'area di lavoro viene chiusa mediante il ripristino dei punti di ingresso e di uscita.

In caso di posa di piccole condotte, come per le telecomunicazioni, la fase di alesatura del foro può essere evitata, riducendo quindi, oltre i tempi di lavorazione, anche le dimensione delle macchine impiegate e, quindi, l'area di cantiere.

Inoltre per la posa in area urbana, sono state messe a punto macchine di piccole dimensioni, in grado di essere posizionate in pozzetti e/o camerette esistenti o nelle buche che ospiteranno i manufatti, riducendo ulteriormente gli ingombri dei cantieri e la movimentazione di materiali.

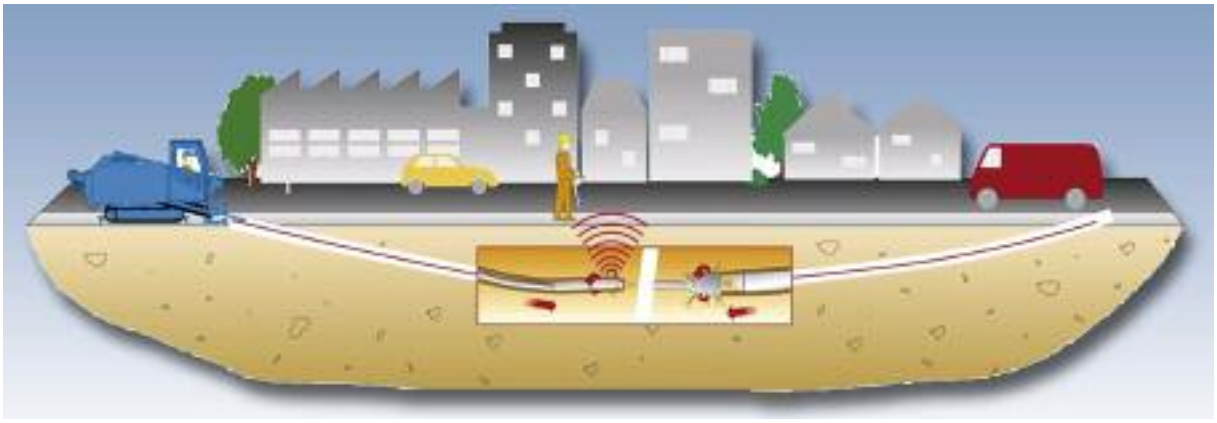


Figura 2 – Schema di posa realizzata con la tecnica della Perforazione Orizzontale guidata

Il Directional Drilling è quindi particolarmente adatto per il superamento di ostacoli, quali fiumi, canali, strade di grande comunicazione, aree pubbliche (vedi *figura 2*), è normalmente usato per la posa longitudinale, e trova impiego anche nel consolidamento di versanti franosi e nel risanamento e contenimento di siti inquinati.

L'impiego di questa tecnologia può essere condizionato dalla presenza di pietre o rocce di dimensioni notevoli o in terreni sciolti, quali ghiaia o sabbia. Inoltre, a seconda del diametro della condotta da posare e della lunghezza dell'impianto da realizzare, le dimensioni dell'area di cantiere possono essere tali da impedirne l'apertura in area urbana.

2.3 *Perforazioni orizzontali guidate: Microtunneling*

Il Microtunneling consente la posa di tubazioni di diametro di (250-2.500) mm in acciaio, in calcestruzzo o in gres ceramico.

La posa avviene mediante la spinta, da un pozzo di partenza fino ad uno di arrivo, di sezioni di tubo della lunghezza variabile da 1 a 3 metri. La sezione più avanzata del tubo è costituita da una fresa o da una trivella con testa orientabile, che disgrega il materiale durante l'avanzamento. Il materiale di risulta viene portato in superficie tramite un sistema chiuso di circolazione d'acqua e bentonite mantenuto in movimento da grosse pompe.

L'orientamento della testa di perforazione è controllato tramite un segnale laser inviato dal pozzo di partenza lungo la direzione della perforazione, che incide su un rivelatore solidale con la testa fresante, la quale può essere guidata da un operatore per mezzo di un sistema di martinetti idraulici.

La tecnologia viene prevalentemente impiegata per la posa di condotte idriche e fognarie, in generale di grandi dimensioni, e può essere utilizzata con buoni risultati su tutti i tipi di terreno.

Nel settore delle telecomunicazioni, questa tecnica, è pressoché abbandonata a favore del directional drilling, che, grazie allo sviluppo di macchinari di dimensioni ridotte, risulta più economica e più adatta alle tipologia di impianto del settore.

2.4 *Perforazioni orizzontali non guidate: Mole (siluro)*

La tecnica consente la posa di tubazioni del diametro di (90 180) mm, che viene realizzata tramite perforazione a secco, con sistemi di spinta ad aria compressa, da una buca di partenza fino ad una di arrivo. Il tubo viene posato direttamente durante la perforazione, collegandolo alla coda della lancia mediante opportuni attacchi (vedi *figura 3*).

Non potendo apportare correzioni significative

Figura 3 – schema di posa con la tecnica del "Mole" o "Siluro"

alla traiettoria della perforazione, questa dovrà essere orientata opportunamente all'avvio, alla giusta profondità.

Il suo impiego è ottimale per lunghezze limitate di posa e in ambito urbano, per via delle ridotte dimensioni dei macchinari, mentre è condizionato dalla presenza di trovanti di significative dimensioni rispetto al macchinario.

2.5 *Perforazioni orizzontali non guidate: Spingitubo*

Questa tecnica consente la posa di tubazioni del diametro di (600 1.500) mm; è analoga al Microtunnelling, ma si differenzia da questo per l'assenza di fresa posta sulla testa di perforazione e per il fatto che lo scavo non può essere direzionato.

Questa tecnologia viene prevalentemente impiegata per l'attraversamento di linee ferroviarie e stradali ed è adatta per perforazioni di lunghezza limitata.

Il suo impiego non è fattibile in presenza di terreni rocciosi o di falde acquifere e può essere condizionato in ambito urbano dalla necessità di avere a disposizione un'area di cantiere di dimensioni notevoli.

2.6 *Tecnologie associate: Minitrincea*

La tecnologia permette la posa di impianti per il servizio idrico, di energia o di telecomunicazione, attraverso l'esecuzione contemporanea o meno, di fresatura di dimensioni ridotte del manto stradale, di sistemazione di tubi e/o cavi e del riempimento del solco con malta cementizia.

La tecnica è applicabile su tracciati che contemplino, generalmente, superfici asfaltate, cementate, aventi un sottofondo di materiale compatto e si esegue normalmente in prossimità del ciglio stradale.

Le fasi di lavorazione prevedono la fresatura del manto stradale (taglio) per una larghezza massima di 15 cm con una profondità massima di 40 cm, la posa dei cavi o dei tubi (fino ad un massimo di 3 di 40-50 cm di diametro) e il riempimento dello scavo (vedi *figura 4*).

Per quest'ultimo si utilizza, generalmente, malta cementizia aerata fino a 3 cm dal piano di calpestio, completando il riempimento con il materiale con cui si realizza il tappetino di usura. Il crescente interesse nell'impiego di questa tecnologia, soprattutto nel settore delle telecomunicazioni, ha portato allo sviluppo di nuovi materiali di riempimento (malta rapida) con la caratteristica di avere prestazioni superiori alle classiche malte e

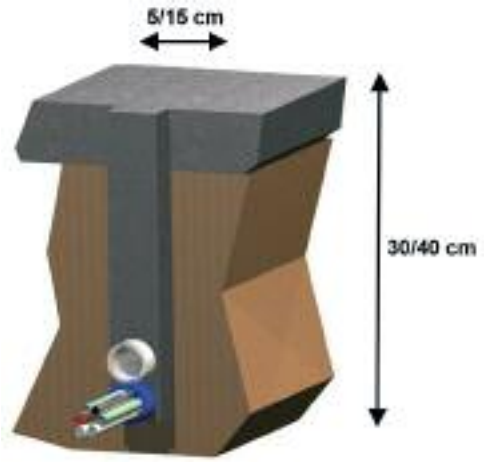


Figura 4 – Sezione di scavo della "minitrincea"

di consentire il riempimento della minitrincea fino al piano di calpestio o carrabile, evitando così il ripristino del tappetino di usura (vedi *figura 5*).

Le attrezzature impiegate sono di dimensioni tali da consentire di allestire cantieri in spazi estremamente contenuti, permettendone un agevole utilizzo sia in ambito urbano che extraurbano.

2.7 *Tecnologie associate: Microtrincea*

Questa tecnologia è analoga alla minitrinca, ma sia lo scavo sia le attrezzature impiegate sono di dimensioni molto ridotte. In particolare il taglio della pavimentazione ha una larghezza massima di 1,6 cm con una profondità massima di 15 cm.

Tale tecnica risulta particolarmente adatta, sia in abito urbano che extraurbano, per la posa di sottoservizi su marciapiedi, strade, banchine e/o aree di parcheggio o campus universitari, dove le sollecitazioni sull'impianto, posato superficialmente, sono ridotte (vedi *figura 6*).

Figura 5 – Confronto tra uno scavo tradizionale ed uno realizzato con la tecnica della "minitrincea"

3 I rapporti con le Amministrazioni Pubbliche

Le Amministrazioni pubbliche particolarmente attente alla salvaguardia della tutela ambientale, alla sicurezza e alla salute dei cittadini, individuano nel razionale utilizzo del sottosuolo, lo strumento gestionale capace di limitare la rottura del manto stradale, l'apertura di cantieri e di conseguenza i disagi alla cittadinanza.

Le tecniche "‘’" appaiono quindi perfette per soddisfare queste esigenze di minimo impatto socio-ambientale; tuttavia oggi, non sono molte le Amministrazioni pubbliche ad autorizzarne l'impiego.

In particolare, mentre per le tecniche di perforazione orizzontale questo è vero solo in parte - anche perché il loro impiego è consigliato dal regolamento d'attuazione del Codice della Strada - per la minitrincea, gli Operatori denunciano una forte resistenza nell'ottenere i permessi.

Figura 6 – Posa di una canaletta con la tecnica della "minitrincea"

Il principale motivo di questa ritrosia è la ridotta profondità di scavo prevista dalla tecnica, in netto contrasto con la prescrizione del Codice della Strada di scavare ad almeno 1 metro di profondità in carreggiata.

Ma il quadro normativo è recentemente mutato e diverse disposizioni di legge permettono ormai alle Amministrazioni pubbliche di derogare al metro di profondità, qualora motivate ragioni di interesse pubblico lo consiglino (Legge 69/2009).

Altro motivo che frena l'impiego della minitrincea è l'idea che impianti posti ad una profondità ridotta possano interferire con gli interventi di manutenzione stradale straordinaria e di conseguenza allungarne i tempi di lavorazione per effettuare il coordinamento tra le varie imprese.

4 Considerazioni sulle tecniche no-dig

Nel settore delle telecomunicazioni, il *must* è sempre stato l'innovazione tecnologica. Gli Operatori, infatti, hanno sempre investito nella ricerca, sperimentando sistemi all'avanguardia e contribuendo, in maniera rilevante, anche allo sviluppo e al miglioramento delle tecnologie *no-dig*.

Un esempio significativo è proprio la tecnica della minitrincea.

Fino a 10 anni fa, questa trovava impiego solo in ambito extraurbano per via delle grandi dimensioni dei macchinari. L'interesse ad utilizzarla anche in ambito urbano ha indotto i costruttori a sviluppare macchine sempre più piccole e, nell'ottica di ricercare soluzioni economicamente vantaggiose, sono stati messi a punto particolari materiali di riempimento dello scavo, le cui caratteristiche permettono di evitare il ripristino del manto stradale.

Oggi la minitrincea, contraddistinta da una lavorazione veloce e da un ingombro minimo, trova il suo impiego ottimale proprio in città, dove le strade hanno dimensioni ridotte e il traffico veicolare e pedonale è intenso.

La sperimentazione *no-dig* a Milano

Il Comune di Milano, coadiuvato dall'associazione IATT e dai principali Operatori del settore delle telecomunicazioni, ha avviato un programma di sperimentazioni, finalizzato alla validazione di un sistema innovativo per la posa dei sottoservizi in ambito urbano, denominato "Minitrincea".

La possibilità di poter usufruire di tale tecnologia costituisce una significativa spinta propulsiva per la realizzazione delle reti a larga banda di nuova generazione in fibra ottica.

La prima sperimentazione è stata eseguita su un cantiere della Società Metroweb, in via Assietta, per una lunghezza di circa 300 metri, 90 dei quali sono stati realizzati su marciapiede, mentre i restanti in carreggiata. Obiettivo della sperimentazione è stato quello di verificare sul campo gli impatti realizzativi, ambientali e normativi legati all'uso di questa tecnica in ambito metropolitano.

La necessità di posare anche in carreggiata, per un tratto del tracciato, è nata dai risultati delle indagini e dei saggi effettuati con il sistema georadar, che hanno evidenziato sul marciapiede, dove si ipotizzava di effettuare la posa, una fitta presenza di sottoservizi, tale da non consentire l'impiego della Minitrincea.

5 Le iniziative per la promozione delle tecniche *no-dig*

Per la promozione dell'impiego delle tecniche *no-dig*, e in particolare della minitrincea, l'associazione IATT (Italian Association for Trenchless Technology) ha avviato diverse iniziative, anche d'intesa con gli Operatori di TLC, come ad esempio:

- ha favorito l'inserimento nel "regolamento d'attuazione" del nuovo Codice degli Appalti (D.Lgs n.163/2006 e s.m.i.) di una nuova categoria di Opere Speciali (OS 35) denominata "*interventi a basso impatto ambientale*", che riguarda proprio la "*costruzione e la manutenzione di qualsiasi opera interrata, mediante l'utilizzo di tecnologie di scavo non invasive che comprende in via esemplificativa, le perforazione orizzontali guidate e non, e l'eventuale riutilizzo e sfruttamento delle opere esistenti*".
  In tal modo le Amministrazioni pubbliche potranno ricorrere direttamente all'impiego di queste tecniche, prevedendole nei propri bandi di gara;
- ha stipulato con l'Associazione dei Comuni Italiani (ANCI) e con l'Unione delle Province Italiane (UPI) una serie di Protocolli d'Intesa volti alla promozione e alla diffusione presso le Amministrazioni pubbliche delle tecnologie *no-dig*;
- ha siglato con la Regione Lombardia (aprile 2009) un protocollo d'Intesa volto alla "*promozione di soluzioni innovative per le attività di posa e manutenzione degli impianti e delle reti di pubblica utilità*", dove per "soluzioni innovative" si intende l'utilizzo delle tecnologie no-dig;
- ha effettuato, con la collaborazione degli Operatori Telecom Italia, Metroweb e Wind, sperimentazioni di minitrincea e di microtrincea nei Comuni di Milano (vedi Box) e di Roma .

CONCLUSIONI

In un contesto normativo e culturale che guarda con attenzione allo sviluppo, all'innovazione, alla ricerca, alla tutela dell'ambiente e al tema dell'infortunistica, è importante dare il giusto peso anche alle tecniche di intervento *no-dig*.

Molte Amministrazioni pubbliche cominciano ad apprezzarne i vantaggi e le potenzialità e, consce dell'importanza che la loro diffusione sul territorio avvenga salvaguardando gli interessi della collettività, collaborano in maniera costruttiva con gli Operatori per individuare "regole" gestionali e operative precise.

L'auspicio è che tali regole diventino poi una prassi operativa diffusa in tutto il nostro Paese.

Questo aspetto mostra quando sia importante, soprattutto prima di utilizzare una qualsiasi tecnologia non invasiva effettuare una mappatura di dettaglio delle reti del sottosuolo.
Circa il riempimento dello scavo, è stata utilizzata una malta speciale, che ha valori di derapaggio uguali o superiori a quella degli asfalti normalmente usati, e la caratteristica di essere carrabile già dopo due ore dalla posa, consentendo quindi il libero transito ai veicoli in tempi molto rapidi.
La soluzione della Minitrincea ha incontrato quindi i desiderata del Comune: cantiere piccolo, veloce (mediamente 300 metri giorno finiti), senza necessità di effettuare ripristini del manto stradale, ridotto disagio per i cittadini e sicura riduzione dei costi per gli eventuali futuri interventi dovuti al cedimento della strada, fattore questo inevitabile con lo scavo tradizionale.
Un'altra sperimentazione è invece in corso su un impianto della Società Wind (Via Talete), presso il cui cantiere hanno fatto un sopralluogo Bruno Simini, Assessore ai Lavori Pubblici del Comune di Milano, e Antonio Acerbo, Direttore Centrale dell'Area Tecnica, allo scopo di verificare i vantaggi della tecnica no-dig, soprattutto in vista del Piano Lavori che prepara Milano all'Expo 2015 ■

paola.finocchi@telecomitalia.it
paolo.trombetti@telecomitalia.it

AUTORI

Paola Finocchi

laureata in Fisica, è in Azienda dal 1996, dove si è occupata di progettazione e realizzazione della rete in rame e di sviluppo della rete ADSL. Attualmente è in Operational Planning dove si occupa di convenzioni con Enti per la definizione dei rights of way. Dal 2005 è socia IATT dove segue progetti inerenti principalmente le TLC. Collabora con DEI Tipografia del Genio Civile per il monitoraggio dei prezzi di riferimento delle tecnologie no-dig ed è docente ed autrice di diversi articoli sul tema. Attualmente coordina i Tavoli di lavoro tra Operatori delle reti del sottosuolo, la Regione Lombardia e le Associazioni degli Enti locali (UPI e ANCI), per la definizione dei criteri di redazione dei "regolamenti scavi" degli Enti, per la gestione del sottosuolo ■

Paolo Trombetti

in Azienda dal 1987 ha svolto molteplici incarichi specializzandosi in ingegnerizzazione dei materiali di reti di TLC,apparati di rete e tecniche di posa con sistemi a basso impatto ambientale. Attualmente nell'ambito della funzione Operational Planning è in Certification System e si occupa di convenzioni con Enti per la definizione dei rights of way.
È docente e autore di diversi articoli e metodologie sulle tematiche relative alle tecnologie di posa non invasive, è stato Rapporteur in ambito ITU (International Telecommunication Units) nella commissione di diffusione delle raccomandazioni per l'impiego di queste tecniche.
È Presidente dello IATT (Italian Association for Trenchless Technology) per il periodo 2008-2012 ■

FOSDEM 2010: *Free and Open Source Software Developers' European Meeting*

Enrico Marocco

Nel weekend tra il 5 ed il 7 febbraio si è tenuta a Bruxelles la decima edizione della più popolare conferenza europea dedicata all'open source. Un evento all'apparenza irrilevante, che nasconde però un fortissimo spirito innovativo, da cui hanno preso vita alcune tra le più dirompenti novità tecnologiche degli ultimi anni. L'avanguardia dell'industria "tradizionale" sembra essersene accorta e le dinamiche che si stanno creando tra i due mondi una volta agli antipodi promettono risvolti interessanti.

1 FOSDEM 2010

Prima novità dell'edizione 2010 del Free and Open Source Software Developers' European Meeting [1]: l'agenda è disponibile come applicazione per Android. E anche per iPhone, e per Maemo, la piattaforma Linux degli smartphone Nokia. Non è la prima volta che il programma di una grande conferenza viene distribuito in un formato più pratico di quello cartaceo, ma è facile prevedere che questa novità diventerà presto la norma.

1 http://fosdem.org

È stato sicuramente così per diverse tra le novità che si sono viste nelle edizioni precedenti. L'anno scorso il leitmotif era Android, la naturale evoluzione del "hot topic" dei due anni precedenti: sistemi Linux-based su "constrained device", hardware depotenziato, set-top-box e, soprattutto, terminali mobili.

In altre parole, se è sicuramente esagerato dire che l'innovazione nel computing e nell'IT parte da qui, è comunque vero che molti trend tecnologici degli ultimi anni si sono sempre visti con discreto anticipo tra gli stand di FOSDEM.

A Bruxelles, 5000 tra "developer", techno-fan e curiosi si sono radunati per confrontare le loro esperienze. La location è costituita dai cinque ettari del campus dell'Université Libre de Bruxelles. Il programma prevede più di duecento presentazioni, su sette percorsi sovrapposti, divisi per tematica. Una quindicina di developer room per singoli progetti/comunità tipo Mozilla, OpenOffice ed XMPP, organizzate autonomamente con discussioni, sessioni di hacking e ancora presentazioni. E decine di stand con poster e demo.

1.1 *Chi sono i developer?*

A prima vista la categoria appare vasta e variegata, quasi impossibile da catalogare. Decine di libri sono stati scritti sul tema, ma una definizione efficace ancora non è stata proposta.

Più facile partire da quello che non sono: non sono sviluppatori. Non solo, almeno. Possiedono generalmente una padronanza dei linguaggi di programmazione pari almeno a quella della lingua parlata, ma non è quella la caratteristica che li contraddistingue. Non sono necessariamente studenti, anche se molti di loro hanno iniziato – o stanno iniziando – la loro avventura durante qualche corso di laurea.

La qualità forse più diffusa riguarda la comunicazione, dal vivo e, ancora di più, online. La misura del "successo" di un pro-

Photo courtesy of Robert Nyman, available for download at *http://www.flickr.com/photos/robertnyman/4346697895/* under a Creative Commons license

getto e/o di un developer è proporzionale alla dimensione della community di sviluppatori e di utenti che riesce a coinvolgere. Di conseguenza il successo dipende direttamente dalla capacità di promuovere e coinvolgere persone nel proprio lavoro. E in effetti le star si riconoscono anzitutto dallo stile con cui scrivono le email: educate, dirette e, soprattutto, brevi.

La carriera del developer segue un percorso che parte in genere da qualche progetto universitario. Dopo la fase iniziale, i progetti – e di solito anche le carriere del developer – hanno tre alternative: il declino e l'abbandono nella maggior parte dei casi, talvolta la sopravvivenza in forma di hobby, raramente il successo in qualche modo economico e commerciale. Il terzo caso è sicuramente il più interessante ed è senza dubbio il percorso che hanno seguito i progetti più famosi del calibro di Linux, Apache, Mozilla e MySQL.

Di conseguenza il developer ha spesso tratti in comune con studenti universitari. Talvolta tecnici informatici o ingegneri che, insieme ad un lavoro "normale", coltivano la passione dello sviluppo open source. Raramente imprenditori, investitori ed executives. In quest'ultima categoria ricadono certamente Linus Torvalds, creatore del kernel Linux, Mark Shuttleworth, sviluppatore Debian e imprenditore di successo nella dot-com economy, divenuto famoso più per essere stato il secondo "turista dello spazio" che per avere fondato la distribuzione Linux Ubuntu, Paul Graham (Yahoo! Store), Marc Andreessen (Netscape) e molti altri i cui nomi risuonano spesso, oltre che al FOSDEM, anche nei programmi delle conferenze della Silicon Valley.

1.2 *Il modello di business*

L'organizzazione è imponente, messa a punto per accogliere 5000 persone in decine di conference room e spazi espositivi; il tutto supportato e corredato da un'infrastruttura di rete impeccabile, composta da centinaia di access point e con una connessione ad Internet di qualche decina di Gigabit per secondo. Poche altre conferenze vantano numeri del genere, ma la differenza sostanziale è che la partecipazione a FOSDEM è gratuita, in quanto le spese sono totalmente coperte dagli sponsor. Sponsor del calibro di Google e Facebook, fornitori di servizi online da sempre vicini al mondo open source, ma anche Cisco, Qualcomm, Nokia e Sun, vendor di hardware ed apparati di rete "tradizionali".

Il fattore economico – la cosidetta "commoditizzazione" del software – è probabilmente forte motivo di attrazione per aziende che ricoprono un ruolo nel settore dell'hardware, ma l'interesse dell'industria è ancora di più da ricercare nell'innovatività del software presentato, discusso e sviluppato nelle comunità open source. Innovatività probabilmente dovuta alla contingenza con l'ambiente accademico, all'elasticità dell'approccio aperto ed alla totale e libera circolazione delle idee.

Non a caso molte tra le innovazioni tecnologiche che di recente hanno raggiunto il mercato hanno origini nel mondo open source: dalle piattaforme per device mobili Android e Maemo (rispettivamente di Google e Nokia) discendenti diretti del kernel Linux, ai sistemi di messaggistica Jabber/XMPP, passando per la quasi totalità delle tecnologie per la creazione di contenuti web basati su Apache, Java, Javascript, PHP e MySQL.

Il modello di business che sta dietro all'organizzazione della conferenza FOSDEM è il medesimo che supporta i progetti e gli sviluppatori open source: le aziende il cui business è sì legato al software, ma che non dipende direttamente dalla vendita di software, ottengono un profitto maggiore, contribuendo ad iniziative aperte, il cui prodotto è il risultato di un'ampia collaborazione, piuttosto che sviluppando in casa in maniera proprietaria le soluzioni di cui hanno bisogno. Tali contributi avvengono in genere sotto forma di sponsorizzazioni, oppure assumendo direttamente sviluppatori con un ruolo attivo nei vari progetti.

1.3 *Gli hot topic del 2010*

Tra gli argomenti che hanno attirato più attenzione ci sono sicuramente le tecnologie web e in

particolare il nuovo standard HTML5. Mozilla ha suscitato molto interesse per la versione mobile del browser Firefox (nome in codice: Fennec) e per il servizio Sync/Weave che permette agli utenti di sincronizzare informazioni quali bookmark e password su PC e terminali mobili. Tra i server per la fornitura di contenuti, FFmpeg ha raccolto particolari consensi per la piattaforma di streaming che, tra gli altri, include il supporto del codec video H.264, alternativa standard alla soluzione proprietaria Flash di Adobe.

Come nelle edizioni precedenti, molto spazio è stato dato al software e ai sistemi operativi specifici per embedded device – terminali mobili, netbook e set-top-box – tra cui ovviamente spicca l'ecosistema Android. Oltre che nella developer room riservata all'argomento, applicazioni per il sistema open source di Google erano presenti nella maggior parte degli altri stand: SIP Communicator (VoIP, presence ed instant messaging), Zarafa (sistema di collaboration compatibile con Microsoft Exchange), Mozilla e molti altri includevano nel portfolio di demo anche i porting per Android delle loro applicazioni. Degno di nota anche quello che è successo sul fronte concorrente a Google, dove le comunità di Maemo (fondata e sponsorizzata da Nokia) e Moblin (guidata da Intel), entrambe piattaforme basate su Linux per device mobili e underpowered, hanno discusso una possibile roadmap comune (annunciata in seguito al Mobile World Congress di Barcellona, due settimane dopo il FOSDEM).

L'altro argomento principe del 2010 è stata la tecnologia di comunicazione realtime Jabber/XMPP, a cui erano dedicati uno stand e una developer room gremita per tutto il weekend. Le novità di quest'anno riguardavano principalmente le estensioni al protocollo e il relativo software per collaboration e comunicazioni realtime (voce e video). In questo caso, ad aumentare l'enfasi avevano contribuito le notizie provenienti dall'industria a riguardo dell'acquisizione di Jabber Inc. da parte di Cisco, la nuova conclamata applicazione Wave lanciata da Google e il supporto per XMPP annunciato da Facebook.

Infine, tra gli interventi [2] più seguiti si sono sicuramente distinti quelli di Adrian Bowyer (University of Bath), inventore della "RepRap machine", la stampante 3D auto-replicante in grado di riprodurre oggetti fisici di discreta complessità, del professore Andrew Tanenbaum (Vrije Universiteit), autore di famosissimi testi sul design di sistemi operativi e leader del progetto MINIX, e di Richard Clayton (Cambridge University), esperto in sicurezza, famoso, tra l'altro, per il reverse engineering del "Great Firewall of China".

[2] Tutti gli interventi nei track principali ed i lightening talk sono stati filmati e resi disponibili al link *http://video.fosdem.org/2010/*

enrico.marocco@telecomitalia.it

AUTORE

Enrico Marocco

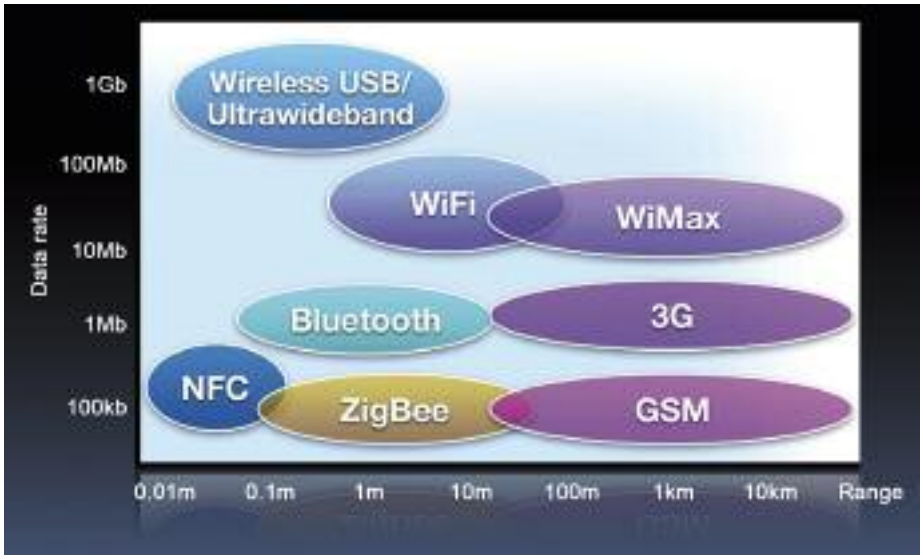
laureato in Informatica, entra in Telecom Italia nel 2003, prendendo parte da subito a progetti di sviluppo e messa in campo della prima rete SIP di Telecom Italia. Dal 2005 è coinvolto in attività di ricerca su tecnologie di comunicazione peer-to-peer; guida il progetto open-source SIPDHT e contribuisce a varie attività di standardizzazione in IETF, in particolare su tematiche legate a SIP e P2PSIP. Dal 2008, sempre in IETF, ricopre la carica di chair del working group Application-Layer Traffic Optimization (ALTO) ■

A cosa serve l'NFC?

Elisa Alessio,
Simonetta Mangiabene

NFC (***Near Field Communication***) è una tecnologia standard *contactless* che abilita semplici interconnessioni tra dispositivi elettronici: lavora ad una frequenza di 13,56 MHz con un raggio di azione di pochi centimetri. La figura seguente mostra il confronto tra NFC ed altre tecnologie wireless, in termini di range di funzionamento e data rate.

NFC può essere considerato come un'evoluzione delle tecnologie contactless RFID, con cui è compatibile, e ne rappresenta l'integrazione all'interno del cellulare che viene abilitato a funzionare in tre modalità: come emulazione di una tag passiva (il telefonino si trasforma in un badge, un ticket o una carta di credito), come lettore di una tag e come dispositivo che comunica in peer-to-peer con un altro per lo scambio di informazioni.



Lo scenario attuale potrebbe ben prestarsi a cogliere con entusiasmo le nuove opportunità fornite dalla tecnologia Near Field Communication (NFC), soprattutto quando abbinate ad un elemento così protagonista del mercato come il cellulare. Il semplice contatto di un telefono NFC con un altro terminale/lettore abilitato permetterà infatti di poter leggere o scrivere su ognuno dei due, ma anche di scambiarne le rispettive informazioni. I nuovi cellulari consentiranno anche di effettuare pagamenti con carta di credito, prenotazioni, effettuare scambio dati e informazioni con un semplice gesto della mano: basterà accostare il terminale mobile al dispositivo/interfaccia per fruire dei servizi.

I punti di forza della tecnologia NFC possono essere riassunti evidenziando che non sono richiesti al cliente settaggi particolari del telefono, che sono garantiti intuitività e semplicità d'uso oltre a sicurezza e velocità di scambio ma, soprattutto, il punto di forza principale è sicuramente rappresentato dall'integrazione con l'inseparabile compagno di vita e di business: il cellulare.

Gli ambiti tipici di applicazione del NFC possono essere quelli delle transazioni 'contactless' per pagamenti di beni, di biglietti per mezzi di trasporto, di parcheggi, ma anche quello del trasferimento rapido delle informazioni da un dispositivo all'altro per sincronizzare rubriche o scambiare biglietti da visita.

Del resto si prevede che a breve questo tipo di tecnologia venga integrato in un numero sempre crescente e variegato di dispositivi e quindi non solo nei telefoni cellulari ma anche in PC, parchimetri, vending machine, fermate dell'autobus, smart posters,..

In un mondo dove "si corre" e si va sempre più veloci potremo dunque immaginare al ristorante di avvicinare il telefono al menu per pagare il pranzo dal tavolo e senza dare la carta di credito al cameriere, oppure potremo avvicinarci ad un poster all'ingresso del cinema per leggere direttamente dal display del cellulare le informazioni disponibili sui film in programmazione e magari a quel punto comprare o prenotare il biglietto evitando code e attese alle casse.

Ma questi sono solo alcuni dei possibili casi d'uso di una tecnologia che, anche se forse ancora non ce ne accorgiamo, inizia a penetrare il nostro ecosistema partendo dai tornelli d'ingresso a metropolitane, stadi, aziende, per arrivare ai primi POS di pagamento NFC (a Milano) seguendo l'onda lunga dei mercati Statunitense ed Asiatico dove tali metodi di pagamento sono già ampiamente diffusi ■

elisa1.alessio@telecomitalia.it
simonetta.mangiabene@telecomitalia.it