2017-2018
Ministero dello Sviluppo Economico
Volume LXI

LA COMUNICAZIONE
Note Recensioni & Notizie

Pubblicazione dell' Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

SICUREZZA INFORMATICA ♦ QUALITÀ DEI SERVIZI ♦ MARCATURA CE ♦ INTEROPERABILITÀ
NUMERAZIONE ♦ INTERNET GOVERNANCE ♦ RETI OTTICHE NGN ♦ MICROONDE ♦ PROGETTI DI RICERCA
PROGETTI EUROPEI ♦ SCUOLA SUPERIORE DI SPECIALIZZAZIONE ♦ PATENTE EUROPEA DEL COMPUTER
CERTIFICAZIONI EUCIP ♦ SEMINARI FORMATIVI ♦ EVENTI DI COMUNICAZIONE ESTERNA
RIVISTA LA COMUNICAZIONE ♦ INTERCONNESSIONE ♦ STANDARDIZZAZIONE ♦ SPECIFICHE TECNICHE

ISCTI
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Ministero dello Sviluppo Economico
ISCTI
Viale America, 201- 00144 Roma
www.mise.gov.it - www.isticom.it

Ministero dello Sviluppo Economico
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

LA COMUNICAZIONE

Note Recensioni & Notizie

Pubblicazione dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Numero Unico Anno 2017 – 2018
Vol. LXI

Direttore: *Rita Forsi*

Redazione ISCOM:
Redattori:
Fabrizio Cardinali, Andrea Ferraris,
Marcella Graziosi, Corrado Pisano
Supporto Tecnico:
Ing. Fabrizio Zanuccoli

SOMMARIO

Rita Forsi
(Direttore dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

5 **Introduzione**

Guglielmo Bonifazi, Giorgia Caldarola, Daniele Lombardi, Federico Gualano, Denise Negri *(Liceo Scientifico S. Cannizzaro – Roma)*	**7**	**Alternanza al Mi.S.E. ogni passione può diventare un lavoro.** Tematiche differenti, coinvolgimento ed applicabilità, i punti cardine del M.i.S.E. per un'A.S.L. di successo. *Alternation to the Mi.S.E.: every passion can become a work.* *Different themes, involvement and applicability, the key points of M.i.S.E. for a successful A.S.L.*
Gianbattista Amati, Simone Angelini, Giuseppe Marcone *(Fondazione Ugo Bordoni)* **Anna Caterina Carli, Giuseppe Pierri** *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)*	**11**	**Analisi di correlazione tra i dati geo-localizzati e temporali da sorgenti informative diverse – Verso l'analisi dei dati IoT.** *Correlation analysis between geo-localized and temporal data from different information sources - Towards the analysis of IoT data.*
Gianbattista Amati, Simone Angelini *(Fondazione Ugo Bordoni)* **Anna Caterina Carli, Giuseppe Pierri** *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)* **Giorgio Gambosi, Daniele Pasquini, Gianluca Rossi** *(Università "Tor Vergata")* **Paola Vocca** *(Università Tuscia VT)*	**29**	**Analisi temporale degli eventi su Twitter.** *Twitter: temporal events analysis.*
Daniela Valente, Gianmarco Fusco, Giuseppe Pierri *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)*	**43**	**Coesistenza tra segnali IoT a banda stretta e segnali del broadcasting televisivo terrestre nelle bande VHF e UHF.** *Coexistence between narrowband IoT and digital video broadcasting in VHF and UHF bands.*

Dario De Leonardis *(Ricercatore dell'Università "La Sapienza" Roma presso ISCTI)* **Silvia Di Bartolo, Vincenzo Attanasio** *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)* **Frank Silvio Marzano** *(Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni – Università "La Sapienza" Roma)*	**63**	**Collegamenti ibridi Free-Space Optics/Radio Frequency (FSO/RF) per rete di fronthaul all'interno del paradigma 5G.** *Hybrid Free-Space Optics / Radio Frequency (FSO/RF) links for fronthaul network within 5G paradigm.*
Massimo Amendola, Giancarlo Gaudino *(Istituto Superiore CTI)*	**75**	**I progetti di alternanza scuola-lavoro dell'Istituto Superiore C.T.I.** *School at Work projects of Higher Institute of Communications and Information Technology.*
Giancarlo Butti *(Europrivacy)*	**81**	**Il rispetto delle normative in tema di sicurezza e le opportunità per il business.** *Compliance with regulations on security and business opportunities.*
Silvia Di Bartolo, Vincenzo Attanasio, Gianpaolo Susanna, Luigi Salamandra, Angelo Pizzoleo, Domenico Carleo *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)* *(Dipartimento di Ingegneria Elettronica Università "Tor Vergata" Roma)* **Valentina Lucli** *(Dipartimento di Ingegneria Elettronica Università "Tor Vergata" Roma)*	**95**	**Influenza meteorologica sui sistemi di trasmissione in spazio libero "Free space optics" (FSO).** *Weather influence on Free Space Optics (FSO) transmission systems.*
Giacomo Assenza, Luca Faramondi, Roberto Setola *(Complex System & Security Lab Università Campus Bio-Medico di Roma)*	**119**	**Peculiarità e problematiche della cyber security per gli Industrial Control System.** *Peculiarities and challenges of cyber security for the Industrial Control Systems.*

Fabio Paternò, **Antonio Giovanni Schiavone** *(CNR – ISTI, Human Interfaces in Information Systems Laboratory)*	**137**	**Valutazione dell'usabilità di applicazioni web su dispositivi mobili tramite individuazione di "bad usability smells".** *Evaluation of web applications' usability on mobile devices through "bad usability smells" detection.*
Sergio Pompei, Edion Tego, Elena Mammi, **Francesco Matera** *(Fondazione Ugo Bordoni)* **Elio Restuccia, Vincenzo Attanasio, Emanuele Nastri, Anna Stefania Michelangeli** *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)*	**147**	**Verso il LAB ISCOM 5G: il segmento XHAUL.** *Towards the 5G LAB ISCOM: the XHAUL segment.*

Guglielmo Bonifazi,
Giorgia Caldarola,
Daniele Lombardi,
Federico Gualano,
Denise Negri
(Liceo Scientifico
S. Cannizzaro – Roma)

Alternanza al Mi.S.E. ogni passione può diventare un lavoro.

Tematiche differenti, coinvolgimento ed applicabilità, i punti cardine del M.i.S.E. per un'A.S.L. di successo

Alternation to the Mi.S.E.: every passion can become a work.
Different themes, involvement and applicability, the key points of M.i.S.E. for a successful A.S.L.

***Sommario**: Uno dei percorsi di Alternanza Scuola-Lavoro (ASL) dell'Istituto Superiore, sviluppato su 40 ore tra lezioni di esperienze pratiche, ha visto il coinvolgimento di una classe del liceo scientifico "Stanislao Cannizzaro" di Roma. Dopo aver seguito alcuni seminari a carattere teorico, gli studenti suddivisi per gruppi di lavoro hanno avuto modo di approfondire gli argomenti trattati attraverso attività di laboratorio come le verifiche di accessibilità del sito della loro scuola, oppure con la preparazione e la conduzione di un meeting internazionale, con la realizzazione di un video clip e la stesura di un articolo su quanto fatto durante la loro permanenza al Ministero. Quello che segue è per l'appunto l'articolo scritto dal gruppo di redazione e che volentieri pubblichiamo.*

***Abstract**: One of the School at Work (ASL) courses, developed over 40 hours of practical experience lessons, saw the involvement of a class from the "Stanislao Cannizzaro" high school in Rome.*

After following theoretical seminars, the students divided into working groups were able to deepen the topics covered through laboratory activities such as checking accessibility of their school's site, or with the preparation and conduct of an international meeting, with video making and drafting of an article on activities done during their stay at the Ministry.

The following is the article written by the student editorial team and which we gladly publish.

Durante i mesi di Aprile e Maggio la classe IV H del liceo scientifico "S.Cannizzaro" ha intrapreso un percorso di alternanza scuola lavoro all'interno del Ministero dello Sviluppo Economico presso l'I.S.C.T.I. (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) per un totale di 40 ore. Questo è stato il primo approccio di noi ragazzi alla Pubblica Amministrazione, già in precedenza infatti ci eravamo avvicinati agli ambiti della tecnologia e dell'informatica ma sempre in settori privati.

All'interno dell'imponente edificio di viale America i temi trattati sono stati i più disparati e hanno spaziato dalle telecomunicazioni, alla sicurezza informatica, all'accessibilità e l'usabilità dei siti web delle PA, alla sorveglianza del mercato degli apparati radio , al sistema di gestione della qualità aziendale, fino alla realizzazione di un meeting aziendale internazionale. Quest'esperienza è riuscita dunque a soddisfare i campi d'interesse di ogni studente toccando ogni giorno settori differenti. Nonostante la difficoltà degli argomenti trattati i relatori hanno saputo calarli perfettamente nella realtà rendendoli idonei alla nostra preparazione. Ogni corso infatti è sempre stato accompagnato da una qualche attività che ci rendesse consci dell'applicabilità di quanto appena trattato. In ciascun incontro veniva sempre evidenziato come ogni nostro interesse potesse realizzarsi in una futura professione, riuscendo così ad adempiere in pieno a quello che dovrebbe idealmente essere l'alternanza scuola lavoro. L'accostamento delle lezioni a visite in laboratori specializzati, tra cui una camera silente e una camera anecoica, ha reso tutto ancora più piacevole e coinvolgente. Siamo stati ad esempio noi stessi chiamati a simulare una comunicazione tra navi o terra-mare presso una sala nautica e a vedere con i nostri occhi la misura dell'interferenza tra due onde (argomento trattato in classe).

Quest'ASL non è stata semplicemente vissuta passivamente ma, da ognuno dei seminari che abbiamo seguito, siamo riusciti a tirare fuori un prodotto finale: il montaggio di un video motivazionale relativo all'esperienza vissuta; un rapporto riguardante le verifiche dell'accessibilità del sito della nostra scuola; la simulazione di un intervento da presentare a un'expo su "L'architettura e l'innovazione tecnologica" (nella quale ognuno di noi rappresentava un paese differente) e, "dulcis in fundo", questo stesso articolo.

Per riuscire a portare a termine ogni progetto siamo stati messi di fronte a sfide come il rispetto delle scadenze e il lavoro di gruppo che ci hanno permesso una notevole crescita personale. Abbiamo addirittura contribuito al miglioramento dell'usabilità dei siti della Pubblica Amministrazione tramite un test effettuato sulla pagina web del M.I.U.R., nel quale siamo stati seguiti da alcuni psicologi dell'Università "La Sapienza di Roma" che sono coinvolti in un progetto di ricerca coordinato dall'I.S.C.T.I.. I dati da noi raccolti contribuiranno a rendere la pagina più semplice da utilizzare e adatta anche ai ragazzi.

Il percorso è stato coronato dalla visita all'interno del Museo Storico delle Telecomunicazioni, l'unico in Italia, dove sono custoditi cimeli quali, ad esempio, il primo computer in assoluto e la macchina criptografica Enigma.

Siamo sempre stati accolti con la massima disponibilità, serietà e gentilezza da dei professionisti che hanno tentato in tutti i modi (pur non avendo alcuna esperienza di insegnamento verso ragazzi della nostra età) di formarci su vari temi, riuscendo peraltro a trasmetterci la loro stessa passione nel mondo del lavoro. Quest'ultimo è un elemento che sinceramente noi ragazzi non ci saremmo mai aspettati di trovare.

Nonostante l'ASL non abbia, ben si sa, così tanti consensi soprattutto tra gli studenti stessi, un caso come questo fa sicuramente parte delle eccezioni e rende speranzosi gli studenti dell'utilità di quest'ultima.

Giambattista Amati, Simone Angelini, Giuseppe Marcone
(Fondazione Ugo Bordoni)

Anna Caterina Carli, Giuseppe Pierri
(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Analisi di correlazione tra dati geo-localizzati e temporali da sorgenti informative diverse - Verso l'analisi dei dati IoT

Correlation analysis between geo-localized and temporal data from different information sources - Towards the analysis of IoT data

Sommario: *Si descrivono alcuni risultati scientifici che sono stati condotti nel progetto "Big Data & Open: metodologie e Tecnologie abilitanti" (BigDOT), dedicato alla definizione e alla validazione di una piattaforma di tipo Big Data per l'analisi di dati provenienti da sorgenti informative eterogenee tra loro.*

Gli obiettivi del progetto sono stati:

- *L'acquisizione e analisi di basi di dati disponibili in rete in modalità Open, oltre a quelle proprietarie, cioè quelle acquisite durante progetti FUB-ISCOM pregressi, al fine di testare e validare la piattaforma di tipo Big Data.*
- *L'individuazione delle tecnologie abilitanti di Big Data in ambiente di programmazione di tipo MapReduce, quali SparkR [1, 2] per le analisi statistiche di dati massivi e GraphX per l'analisi delle reti sociali.*
- *La valutazione della capacità elaborativa della piattaforma rispetto all'infrastruttura attualmente in dotazione del laboratorio Big Data e relativamente a flussi informativi geo-localizzati e temporali.*

Nel seguito si descrivono solo le attività di analisi statistiche su grandi Dataset e si riportano le tecniche e i risultati ottenuti mediante l'infrastruttura del laboratorio Big Data.

Abstract: *We describe some scientific results that have been carried out in the "Big Data & Open: methodologies and enabling technologies" (BigDOT) project, dedicated to the definition and validation of a Big Data platform for the analysis of data coming from heterogeneous information sources.*

The objectives of the project were:

- *Acquisition and analysis of datasets available on the Internet in Open mode, in addition to the proprietary ones, i.e. those acquired during previous FUB-ISCOM projects, in order to test and validate the Big Data platform.*
- *The identification of the enabling technologies of Big Data in a MapReduce programming environment, such as SparkR [1, 2] for statistical analysis of massive data and GraphX for the analysis of social networks.*

- *Evaluation of the processing capacity of the platform compared to the infrastructure currently provided by the Big Data laboratory and relative to geo-localized and temporal information flows.*

Below we describe only the statistical analysis activities on large Datasets and report the techniques and results obtained through the Big Data laboratory infrastructure.

1. Introduzione

L'*Internet of Things* (*IoT*) è un concetto che prevede di dotare il nostro mondo di sensori e di rispondere ai dati ricevuti da questi sensori in modo significativo e tempestivo. Si tratta di aggiungere dei sensori a tutte le cose in modo che sia possibile misurare, analizzare, visualizzare, prevedere e reagire all'ambiente intorno a queste cose. In altre parole, il concetto dell'*IoT* è quello di raccogliere da sensori dati geo-referenziati e distribuiti temporalmente con l'intento di produrre in tempo reale un'analisi e fornire in modo tempestivo qualche risposta. In questo articolo dimostriamo come definire una piattaforma di tipo *Big Data* adattabile al nuovo concetto dell'*IoT* e, un secondo obiettivo di questo lavoro è quello di presentare una infrastruttura e una metodologia per studiare la dinamica di fenomeni complessi. La piattaforma infatti è adattabile a trattare dinamiche complesse in diversi settori sociali o economici, quali quelli di tipo energetico, urbanistico, sociale, dei trasporti, meteorologico, sanitario, ingegneristico, della sicurezza informatica. In particolare la piattaforma comprende due funzionalità importanti:

- funzionalità di *Data Analytics* o *Data Mining* per l'analisi di grandi moli di dati geo-temporali;
- funzionalità per l'analisi della correlazione tra dati eterogenei.
- A tal scopo si sono acquisiti i seguenti dati e studiati i seguenti problemi:
- 745GB dei Big Data Challenge di Telecom, descritto in [3], contenenti informazioni relative al periodo novembre e dicembre 2013 della grid di Milano e Trento (dati mobili, elettrici, qualità dell'aria, meteo e dei social network).
- correlazione tra consumo energetico e traffico mobile.

Analisi predittive del consumo di energia elettrica si trovano in [4], dove viene applicato l'algoritmo Fast Fourier Transform alle serie storiche giornaliere del consumo energetico: vengono estratte le tre componenti (stagionale, rumore e tendenza) e diverse misure statistiche (medie, kurtosis, mediane, varianze di diverse statistiche) per caratterizzarne il consumo in aree diverse. Rimandiamo al lavoro di [5] per una rassegna esaustiva sullo stato dell'arte dell'analisi del traffico mobile, che si concentra su grafici sociali estratti da *dataset* di traffico mobile, e al lavoro di [6] per lo stato dell'arte sugli aspetti e i modelli

spazio-temporali. Più vicino al nostro approccio è il lavoro di [7] che correla tre tipologie di dataset spazio temporali: la popolazione, i dati Twitter e i dati della rete mobile, e il lavoro di [8] che contiene un'analisi della mobilità mediante pattern temporali estratti dai dati di Twitter.

Il progetto BigDOT, nell'ambito del quale è stato svolto questo studio, ha anche riguardato tutte le attività di aggiornamento del laboratorio Big Data di ISCTI realizzato nel corso degli anni di diversi progetti bilaterali tra FUB e ISCTI.

2. Gli Open Big Data raccolti

Nome File	Dimensione	Contenuto
MILANO		
milano-grid.zip	324.4 KB	Grid Milano
december/full.zip	2.5 GB	SMS, Call, Internet - MI
november/full.zip	2.5 GB	SMS, Call, Internet - MI
december/full.zip	1.1 GB	MI - Province
november/full.zip	1.2 GB	MI - Province
december/full.zip	45.6 GB	MI - MI
november/full.zip	47.6 GB	MI - MI
Milano_WeatherPhenomena.zip	153.6 KB	Milano Meteo
mi_meteo_legend.csv	2.2 KB	Milano Meteo
precipitation-milano.zip	96.1 KB	Precipitazioni
pollution-legend-mi.csv	3 KB	Qualità Aria - MI
pollution-mi.zip	153.3 KB	Qualità Aria - MI
TRENTO		
december/full.zip	1.6 GB	SMS, Call, Internet - TN
november/full.zip	1.3 GB	SMS, Call, Internet - TN
december/full.zip	596.4 MB	TN - Province TELCO
november/full.zip	442.3 MB	TN - Province TELCO
december/full.zip	43.1 GB	TN - TN TELCO
november/full.zip	36.8 GB	TN - TN TELCO
precipitation-trentino-data-availability.zip	20.8 KB	Precipitazioni TN
precipitation-trentino.zip	13.1 MB	Precipitazioni TN
air-2013.zip	344.9 KB	Qualità Aria - TN
line.zip	12.2 KB	SET, Electricity ENERGY
SET-dec-2013.zip	3.5 MB	SET, Electricity ENERGY
SET-nov-2013.zip	3.4 MB	SET, Electricity ENERGY

Figura 1. I dati del Big Data Challenge di telecom utilizzati dal progetto BigDot. Contengono circa 83 GB di dati compressi in formato zip, che corrispondono a circa 745 GB di dati complessivi non compressi.

All'inizio del 2014, Telecom Italia ha lanciato la prima edizione del Big Data Challenge, un concorso destinato a stimolare la creazione e lo sviluppo di idee tecnologiche innovative nel campo dei Big Data.

I *dataset* sono stati rilasciati solo per essere utilizzati dai partecipanti, ma dopo la fine del concorso sono liberamente disponibili e pertanto costituis cono un'ottima risorsa per effettuare analisi di *benchmarking*. In particolare è possibile effettuare analisi di correlazione per volumi di dati dell'ordine di diversi *gigabyte* che sono anche fortemente

eterogenei. Tipicamente le analisi di correlazione sono difficilmente trattabili se non in ambiente distribuito. Un tipico problema utile a misurare la capacità di elaborazione delle piattaforme di Data Analytics è ad esempio quello di correlare il traffico mobile e il consumo elettrico per fasce orarie e per aree geografiche.

Il progetto ha analizzato circa 83 GB di dati compressi in formato zip che corrispondono a circa 745GB di dati. Questi dati sono accessibili sul sito https://dandelion.eu/datamine/open-big-data/.

2.1. Dati CDR di Telecom

Tra il set dei dati c'è un surrogato dei Call Detail Record (CDR), che sono generati dalla rete cellulare di Telecom Italia nelle città di Milano e Trento. I dati CDR registrano le attività degli utenti ai fini della fatturazione e della gestione della rete. Ci sono molti tipi di CDR, ma nel *dataset* esistono solo i dati relativi alle seguenti attività:

- *SMS ricevuti*: un CDR viene generato ogni volta che un utente riceve un SMS
- *SMS inviato*: un CDR viene generato ogni volta che un utente invia un SMS
- *Chiamate in arrivo*: un CDR viene generato ogni volta che un utente riceve una chiamata
- *Chiamate in uscita*: CDR viene generato ogni volta che un utente invia una chiamata
- *Internet*: un CDR è generato ogni volta un utente avvia una connessione a internet, un utente termina una connessione ad internet o durante la stessa connessione uno dei seguenti limiti viene raggiunto: 15 minuti o 5 MB prodotti dall'ultimo CDR generato.

Aggregando questi dati CDR è stato creato l'insieme dei dati finali che fornisce il volume di SMS, di chiamate e attività di traffico Internet per intervalli di tempo. La misura è il livello di interazione tra utenti con la rete di telefonia mobile; per esempio maggiore è il numero di SMS inviati dagli utenti, maggiore è l'attività degli SMS inviati. Le misure di chiamata e di attività di SMS hanno la stessa scala e quindi sono comparabili tra loro; quelli relativi al traffico Internet invece hanno una scala indipendente.

2.2. Telecomunicazioni - SMS, chiamate, Internet - Milano e Trento

I dati contengono i seguenti campi:

- *id Square*: l'identificativo numerico del quadrato che fa parte della GRID di Milano; TIPO: numerico.
- *Intervallo di tempo*: l'inizio dell'intervallo di tempo espresso come il numero di millisecondi trascorsi dalla Unix Epoch dal 1 gennaio 1970 UTC. Il termine dell'intervallo di tempo può

essere ottenuto aggiungendo 600.000 millisecondi (10 minuti) a questo valore. TIPO: numerico.

- *Codice del paese*: il codice telefonico del paese di una nazione. TIPO: numerico
- *Attività di SMS-in*: l'attività in termini di SMS ricevuti all'interno della id Square, durante l'intervallo di tempo e inviato dalla nazione identificata dal codice del paese. TIPO: numerico
- *Attività di SMS-out*: l'attività in termini di SMS inviato all'interno della id Square, durante l'intervallo di tempo e ricevuto dalla nazione identificata dal codice del paese. TIPO: numerico
- *Attività Call-in*: l'attività in termini di chiamate ricevute all'interno del id Square, durante l'intervallo di tempo e rilasciato dalla nazione identificata dal codice del paese. TIPO: numerico
- *Attività Call-out* : l'attività in termini di chiamate emesse all'interno del id Square, durante l'intervallo di tempo e ricevuto dalla nazione identificata dal codice del paese. TIPO: numerico
- *Attività di traffico Internet*: l'attività in termini di traffico Internet effettuato all'interno della id Square, durante l'intervallo di tempo e dalla nazione degli utenti che effettuano il collegamento identificato dal codice del paese. TIPO: numerico

I file sono in formato TSV. Se nessuna attività è stata registrata per un campo specificato nello schema di cui sopra, allora il valore corrispondente è assente nel file.

Inoltre, se per una data combinazione di id e Square s, intervallo di tempo e codice paese non viene registrata nessuna attività, allora il record corrispondente non è presente nel set di dati.

2.3. Telecomunicazioni - Da Milano (Trento) alla Provincia

- *id Square*: l'id del quadrato della GRID di Milano (Trento); TIPO: numerico
- *Provincia*: il nome della provincia italiana; Tipo: STRING
- *Intervallo di tempo*: l'inizio dell'intervallo di tempo espresso come il numero di millisecondi trascorsi dalla Unix Epoch dal 1 gennaio 1970 UTC. Il termine dell'intervallo di tempo può essere ottenuto aggiungendo 600.000 millisecondi (10 minuti) a questo valore. TIPO: numerico
- *Interazione da id Square alla Provincia*: un valore che rappresenta l'interazione tra l'id Square e la Provincia. Questo valore è proporzionale al numero di chiamate scambiate tra chiamanti ubicati nella piazza id e ricevitori ubicati nella provincia. TIPO: numerico

- *Interazione da Provincia a id Square* : un valore che rappresenta l'interazione tra l'id piazza e la Provincia. Questo valore è proporzionale al numero di chiamate scambiate tra i chiamanti ubicati nella Provincia e ricevitori situati nella id Square. TIPO: numerico

I file sono in formato TSV. Se nessuna attività è stata registrata per un campo specificato nello schema di cui sopra, allora il valore corrispondente è assente nel file.

2.4. Telecommunications - Milano su Milano (Trento su Trento)

- *id1 Square*: l'id del quadrato della griglia di Milano (Trento) che è l'origine dell'interazione; TIPO: numerico
- *id2 Square*: l'id del quadrato della griglia di Milano (Trento) che è la destinazione dell'interazione; TIPO: numerico
- *Intervallo di tempo*: l'inizio dell'intervallo di tempo espresso come il numero di millisecondi trascorsi dalla Unix Epoch dal 1 gennaio 1970 UTC. Il termine dell'intervallo di tempo può essere ottenuto aggiungendo 600000 millisecondi (10 minuti) a questo valore. TIPO: numerico
- *Forza di Interazione Direzionale*: il valore che rappresenta la forza di interazione direzionale tra id1 Square e id2 Square. Questo valore è proporzionale al numero di chiamate scambiate tra chiamanti ubicati in id1 Square e ricevitori ubicati in id2 Square. TIPO: numerico

2.5. Stazione Meteo Dati

Legenda dei dati:

- *ID sensore*: l'id del sensore. TIPO: numerico
- *Il nome della strada del Sensore*: il nome della via in cui si trova il sensore identificato da l'ID del sensore. TIPO: alfanumerico
- *Latitudine del sensore* : la latitudine geografica specifica della posizione del sensore identificato dall'ID sensore. TIPO: numerico
- *Longitudine del sensore* : la longitudine geografica specifica della posizione del sensore identificato dall'ID sensore. TIPO: numerico
- *Tipo di sensore*: il tipo di sensore identificato dall'ID sensore. TIPO: alfanumerico
- *UOM*: l'unità di misura del valore registrato dal sensore identificato dall'ID sensore. TIPO: alfanumerico

2.6. Fenomeni Meteo

Questo insieme di dati contiene un file per ogni sensore. Il nome dei file ha il seguente formato MI_Meteo_<sensorID>.csv.

- *ID sensore*: l'id del sensore. TIPO: alfanumerico
- *Tempo istantaneo*: l'istante temporale della misura espressa come data e ora con i seguenti formati
- AAAA/MM/DD HH24: MI. TIPO: data.
- *Misura*: il valore dell'intensità dei fenomeni meteorologici misurata nell'istante tempo dal sensore ID. L'unità di misura (UM) del valore registrato dal sensore proposta è specificata nella Legenda dell'insieme di dati. TIPO: numerico
- La direzione del vento viene misurata in gradi aventi il nord, come piano di riferimento (il Nord viene specificato come valore di 0 o 360 gradi). Inoltre, i valori di misurazione direzione del vento possono assumere i seguenti valori speciali:
- 777: calma
- 7777: calma
- 888: variabile
- 8888: variabile

2.7. Precipitazioni

- *Timestamp*: il timestamp con il seguente formato: yyyymmddHHMM. TIPO: numerico
- *ID quadrante*: l'id del quadrante. TIPO: numerico (un valore compreso tra 1 e 4)
- *Intensità*: l'intensità della precipitazione. TIPO: numerico (un valore compreso tra 0 e 3)
- *Copertura*: la percentuale del quadrante che è coperta dalla precipitazione. TIPO: numerico (un valore compreso tra 0 e 100)
- *Tipo*: il tipo di precipitazione. TIPO: numerico (un valore compreso tra 0 e 2)

2.8. Qualità dell'aria - Milano (Trento)

Legenda dei dati:

- *ID sensore*: l'id del sensore. TIPO: numerico
- nome della strada del Sensore: il nome della via in cui si trova il sensore identificato dall'ID del sensore. TIPO: alfanumerico
- *latitudine del Sensore*: la latitudine geografica specifica della posizione del sensore identificato dall'ID sensore. TIPO: numerico

- *longitudine del Sensore*: la longitudine geografica specifica della posizione del sensore identificato dall'ID sensore. TIPO: numerico
- *Tipo di sensore*: il tipo di sensore identificato dall'ID sensore. TIPO: alfanumerico
- *UOM*: l'unità di misura del valore registrato dal sensore identificato dall'ID sensore. TIPO: alfanumerico
- *Formato ora istantaneo*: il formato che rappresenta il tipo di aggregazione temporale, in altre parole la granularità dei dati. Esso varia da sensore a sensore e può essere:
- *aggregazione al giorno* (AAAA/MM/GG). TIPO: alfanumerico.
- *aggregazione all'ora* (AAAA/MM/DD HH24: MI). TIPO: alfanumerico.

2.9. Set dei dati di Inquinamento

Questo insieme di dati contiene un file per ogni sensore. Il nome dei file ha il seguente formato MI_pollution_<sensorID>.csv.

- *ID sensore*: l'id del sensore. TIPO: alfanumerico
- *Istante di Tempo*: l'istante di tempo della misurazione espresso come data o data con l'ora secondo i seguenti formati:
- AAAA/MM/DD. TIPO: data.
- AAAA/MM/DD HH24: MI. TIPO: data.
- *Misura*: il valore dell'intensità dell'inquinamento misurata nell'istante tempo dal sensore ID. L'unità di misura (UM) del valore registrato dal sensore proposta è specificata nella Legenda dei dati . TIPO: numerico

2.10. Pulizia dei dati (cleansing)

I dati in generale possiedono molti campi non definiti o mancanti, alcune misure non sono conformi tra database eterogenei e vanno rese coerenti tra loro. Ad esempio si deve trasformare la colonna TimeStamp dei dataset dal formato data 'YYYY-MM-DD HH24:MI' al valore in milli-secondi tramite la funzione:

*as.numeric(as.POSIXct(Energia$TimeStamp))*1000*

Occorre effettuare una prima fase di pulizia e armonizzazione dei dati, che se non effettuata potrebbe produrre risultati non attendibili. Le operazioni da effettuare sono molto semplici e veloci essendo operazioni riconducibili a due primitive, *subset* e *join*.

Per la città di Trento da un database di 69.877.653 milioni di record, si ottiene un *dataset* della dimensione 33.596.149 milioni di record. Una volta che questo file viene letto come file distribuito (HDFS) è poi possibile utilizzare *SparkR* per elaborarne i dati.

2.11. Analisi dei Dati

L'analisi tra traffico mobile e consumo elettrico è stata effettuata utilizzando i dati del Big Data challenge di Telecom. Questi dati sono rilasciati in modalità open e sono accessibili sul sito https://dandelion.eu/datamine/open-big-data/. Lo studio presente è stato realizzato utilizzando i dati della Grid della provincia di Trento (https://dandelion.eu/datagems/SpazioDati/trentino-grid/description/).

2.12. Infrastruttura di calcolo

Al fine di integrare la piattaforma esistente con ecosistemi software di Big Data Analytics e di valutare l'efficacia dell'infrastruttura tecnologica hardware e software adottata in termini di volume di dati trattati e di scalabilità delle soluzioni, il progetto ha previsto l'acquisizione di un nuovo cluster di macchine. Le analisi sono state effettuate nel laboratorio Big Data mediante la seguente infrastruttura:

Il primo cluster è costituito da 8 macchine con:

- Processore Intel(R) Xeon(R) CPU E3-1225 v3 QuadCore@3.20Ghz
- un hard disk Seagate della capienza di 1TB e velocità di lettura a 5400rpm
- 8 GB di RAM (banco unico) e cache multi-livello L3 di 8MByte.

Il secondo cluster è costituito da 8 macchine Server CX 2550 Fujitsu, (CX 400 M1). Ogni server CX 2550 è configurato con:

- Processore : 2xXeon E5-2630v3 8C/16T 2.40 GHz
- Memoria: 2x 16 GB (1x16GB) 2 Rx4 DDR4-2133 R ECC
- Hard Disk: 1x HD SATA 6G 1TB 7,2K HOT PL 2,5" BC
- Solid State Drivers: 1x SSD SATA 6G 480GB Read Intensive 2,5" H-P

Dal punto di vista software, ogni macchina è equipaggiata con:

- sistema operativo Ubuntu 16.04 LTS Server.
- Java Virtual Machine Oracle v1.8.0

Le macchine sono collegate ad una LAN con schede di rete a 1 Gb/s.

2.13. Analisi del traffico mobile

I dati si riferiscono ai mesi di novembre e dicembre del 2013 relativamente all'area di Trento. Ci sono 166.571.878 record (TNMobile) relativi a tutte le comunicazioni mobili in entrata e uscita effettuate nella provincia di Trento, e al consumo effettuato mediante dispositivo mobile su internet.

- *Square id*: l'identificativo del pixel che fa parte del grid del Trentino; TIPO: numerico
- *Intervallo di tempo*: l'inizio dell'intervallo di tempo espresso come il numero di millisecondi trascorsi dalla Unix Epoch dal primo gennaio 1970 UTC. Il termine dell'intervallo di tempo può essere ottenuto aggiungendo 600.000 millisecondi (10 minuti) a questo valore. TIPO: numerico
- *Codice del paese*: il codice internazionale telefonico del paese di una nazione. A seconda dell'attività misurata, questo valore assume diversi significati. TIPO: numerico
- *Attività SMS-in*: l'attività in termini di SMS ricevuti all'interno del pixel, durante l'intervallo di tempo, e inviato dalla nazione identificata dal codice paese. TIPO: numerico
- *Attività di SMS-out*: l'attività in termini di SMS inviato dall'interno del pixel, durante l'intervallo di tempo, e ricevuto dalla nazione identificata dal codice paese. TIPO: numerico
- *Attività di Call-in*: l'attività in termini di chiamate ricevute all'interno del pixel, durante l'intervallo di tempo, e rilasciato dalla nazione identificata dal codice paese. TIPO: numerico
- *Attività di Call-out*: l'attività in termini di chiamate emesse all'interno del pixel, durante l'intervallo di tempo e ricevuto dalla nazione identificata dal codice paese. TIPO: numerico
- *Attività di traffico Internet*: l'attività in termini di traffico internet effettuato all'interno del pixel, durante l'intervallo di tempo e dalla nazione identificata dal codice paese. TIPO: numerico

Le misure di chiamata e di attività di SMS hanno la stessa scala (quindi sono comparabili); quelle relative al traffico internet invece non lo sono.

Il Traffico da Trento e su Trento ci forniscono informazioni importanti sulle abitudini e sulla stessa possibile composizione della popolazione residente. Comparando il traffico festivo e feriale su 8 giorni ciascuno, la Tavola di Figura 2 mostra un uso minore delle chiamate sia in uscita sia in entrata, compensato da un uso maggiore degli SMS sia in uscita sia in entrata, e da un uso maggiore di internet.

	TRAFFICO FERIALE		TRAFFICO FESTIVO
SMS IN	8,955,804	SMS IN	9,835,057
SMS OUT	5,414,090	SMS OUT	7,035,961
CALL IN	5,118,852	CALL IN	3,498,481
CALL OUT	5,559,843	CALL OUT	3,939,161
INTERNET	77,659,454	INTERNET	93,474,845

Figura 2.. Il traffico mobile durante i festivi a confronto con i feriali. Si usano di più gli SMS e internet per comunicare durante le feste.

La Tavola di Figura 3 invece mostra una asimmetria marcata (*skewness*) nella distribuzione dei dati secondo una power-law dovuta

alla concentrazione della popolazione in alcuni pixel. Da notare che questa asimmetria si attenua durante i giorni festivi probabilmente proprio per un'attenuazione della concentrazione della popolazione su alcuni pixel della griglia.

	TRAFFICO FERIALE			TRAFFICO FESTIVO		
	STAND.DEV.	MEDIA	MODA	STAND.DEV.	MEDIA	MODA
SMS IN	4.348662	0.949	0.156	2.827757	0.875	0.002
SMS OUT	4.594695	1.007	0.003	3.210749	1.017	0.002
CALL IN	3.964936	0.982	0.003	2.013244	0.632	0.002
CALL OUT	4.244486	0.964	0.003	2.151294	0.630	0.003
INTERNET	39.77267	9.789	0.198	29.78781	10.048	0.002

FIgura 3. Il traffico mobile durante i festivi a confronto con i feriali. Si usano di più gli SMS e internet per comunicare durante le feste.

Il traffico da e verso l'estero aumenta in modo significativo durante i festivi anche in modo assoluto e non solo in termini di valori in percentuale come evidenzia la Tavola di Figura 4. Lo scarto tra traffico in entrata e uscita potrebbe essere spiegato in parte da una popolazione residente straniera.

	FERIALE	FESTIVO
Italia	35.8%	30.1%
Fisso	24.1%	21.0%
Germania	5.3%	5.9%
Polonia	3.7%	4.7%
Romania	4.1%	4.3%
Rep Ceca	2.8%	3.6%
UK	1.4%	3.1%
Svizzera	1.0%	1.9%
Belgio	1.2%	1.8%
Francia	2.0%	1.8%
Olanda	0.7%	1.7%
Russia	0.3%	1.5%
USA	0.6%	1.5%

Figura 4. Traffico mobile feriale e festivo a confronto. Il campione è ottenuto selezionando un ugual numero di giorni feriali e festivi (gli otto giorni festivi di dicembre). Il traffico da e verso l'estero aumenta durante le festività. Il traffico su fisso e da e verso l'Italia scende dal 60% al 51%.

2.14. Traffico mobile Trento su Trento

Esiste inoltre un secondo DB ancora più corposo contenente una media di circa 67 milioni di rilevazioni giornaliere relative al dettaglio del traffico da Trento a Trento (TNtoTN). Il DB

TNtoTN infatti contiene un valore aggregato per intervallo di tempo (10 minuti) che definisce un indicatore di intensità di traffico da un pixel a pixel.

Ad esempio la Figura 5 rappresenta il traffico complessivo effettuato nella Grid di Trento.

Questi ultimi dati sono molto preziosi in quanto con altissima probabilità si riferiscono quasi al numero di comunicazioni effettuate da utente a utente per intervallo di tempo. Infatti, considerando le comunicazioni possibili da pixel a pixel (19.584.411) e gli intervalli temporali possibili in una giornata (144) si hanno circa 2.820.155.184 combinazioni possibili. Quelle rilevate sono state invece "solo" 67.770.922 e dunque una comunicazione ha la probabilità del 2.40% di essere effettuata in un dato intervallo e tra due dati pixel. Dunque la probabilità che due utenti possano effettuare nello stesso intervallo di tempo tra due stesi pixel è estremamente bassa. Quindi possiamo assumere che queste informazioni ci possano fornire il numero medio giornaliero di comunicazioni in uscita (tra Sms, chiamate) che è vicino al centinaio ipotizzando che sia presente la sola popolazione residente che è vicina alle 600,000 unità. Questa stima potrebbe essere molto più bassa se potessimo considerare la popolazione non residente presente sul territorio.

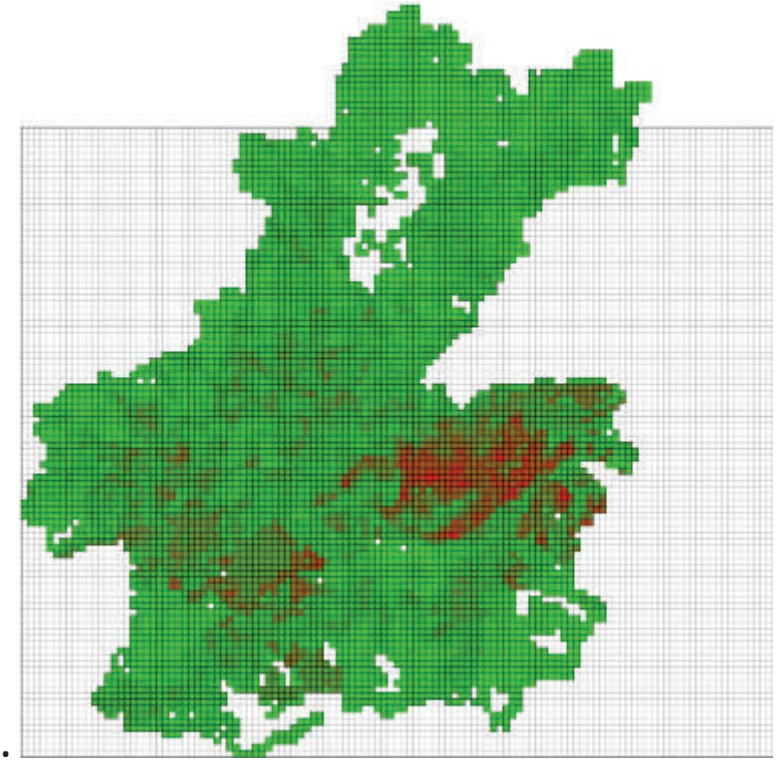


Figura 5: Il traffico mobile Trento su Trento. 67.770.992 record analizzati. La griglia è di 117×98 pixel per un totale di 6.247 pixel attivi

2.15. Analisi del consumo energetico

Purtroppo i dati rilasciati in modalità open forniscono una mappatura molto parziale tra traffico mobile e consumo elettrico (vedi Figura 6).

Si sono potuti utilizzare per la correlazione solo il 31% dei dati mobili.

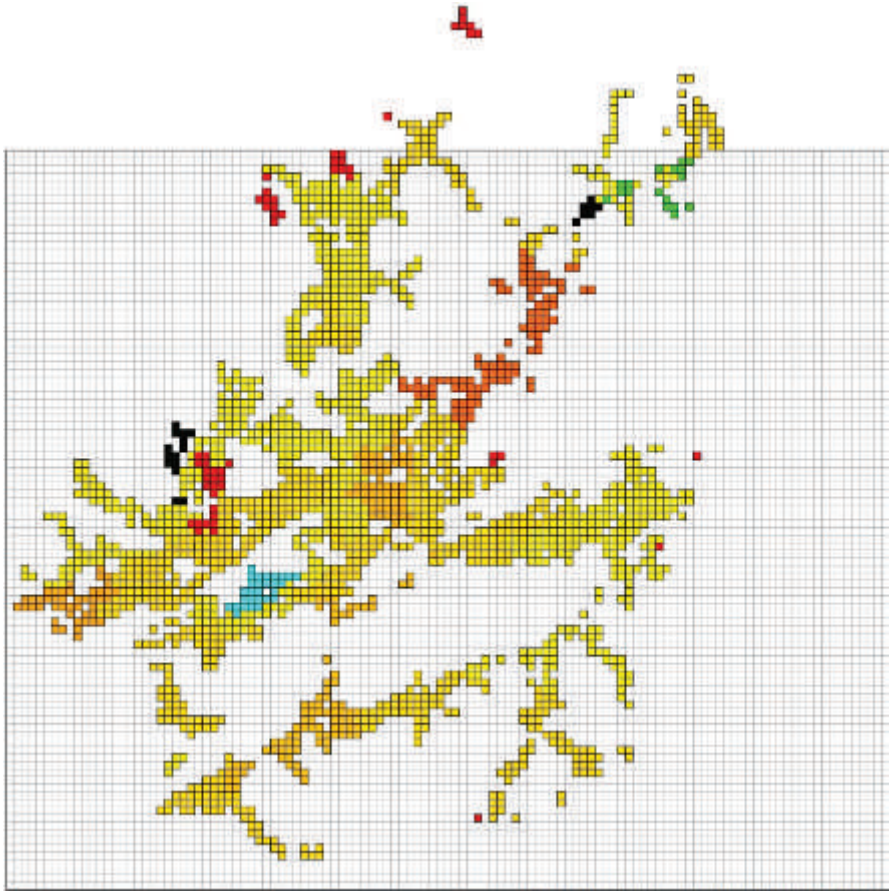


Figura 6: Traffico mobile feriale e festivo a confronto. Il campione è ottenuto selezionando un ugual numero di giorni feriali e festivi (gli otto giorni festivi di dicembre). Il traffico da e verso l'estero aumenta durante le festività. Il traffico su fisso e da e verso l'Italia scende dal 60% al 51%.

La SET gestisce quasi tutta la rete elettrica sul territorio trentino. La SET utilizza circa 180 linee di distribuzione primaria (linee di media tensione) per portare l'energia dalla rete nazionale e distribuirla tra gli utenti del Trentino. Le informazioni nel *dataset* riguardano il flusso di fornitura di corrente elettrica dalle linee di distribuzione, e contengono dettagli su come le linee di distribuzione sono distribuite sul territorio trentino.

Il set di dati è composto da sotto-insiemi di dati:

- *Dati relativi al cliente*: fornisce una descrizione delle linee di distribuzione primaria che servono il territorio trentino. La geometria delle linee non è esplicitamente esposta. La descrizione fisica delle linee è data in termini di sedi di clienti collegate alle linee di distribuzione primaria. Si noti che le sedi dei clienti spesso fornire energia a più di un cliente. In altre parole, possono fornire energia elettrica a un cliente (case unifamiliari), a molti clienti (condomini), alle attività commerciali e a strutture pubbliche.

- *Aggregazione spaziale*: i siti dei clienti per ogni linea sono raggruppati per pixel della GRID del Trentino. Ciò significa che, dato un quadrato della GRID del Trentino e una linea di distribuzione specifica viene solo registrato il numero di siti di clienti che rientrano in tale gruppo.
- *Aggregazione temporale*: la topologia della rete è considerata statica, pertanto l'aggregazione temporale è disponibile.
- *Dati di misurazione delle linee*: questo insieme di dati fornisce la quantità di corrente che fluisce attraverso le linee in istanti specifici.
- *Aggregazione spaziale*: non vi è alcuna aggregazione spaziale per questo insieme di dati.
- *Aggregazione temporale*: la corrente che fluisce attraverso le linee di distribuzione è stata registrata ogni 10 minuti.

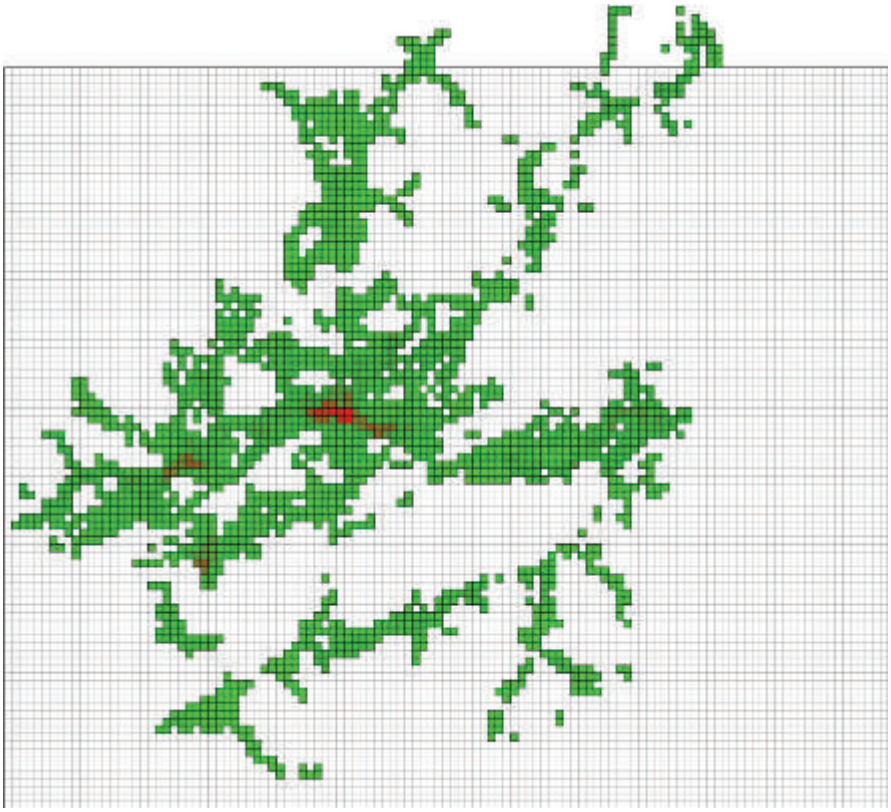


Figura 7: Consumo energia SET nel mese di novembre. La mappatura tra pixel e centraline è però solo parziale. Sono solo 200 le centraline associate a 2.575 pixel e quindi si sono potuti analizzare solo 10.928.880 record relativi al consumo energetico. Da una confronto qualitativo con la Figura 5 i circa 4.000 pixel mancanti sembrano riferirsi proprio alle zone dove esiste un maggior traffico mobile.

3. Esempio di Correlazione per Big Data: consumo energetico e traffico mobile

Abbiamo verificato il modello di regressione lineare e la correlazione di *Pearson* tra consumo elettrico e le cinque voci di consumo dal cartellino CDR del traffico mobile, ovvero consumo Internet da mobile, traffico Sms e chiamata sia in entrata sia in uscita (vedi Tavola 8).

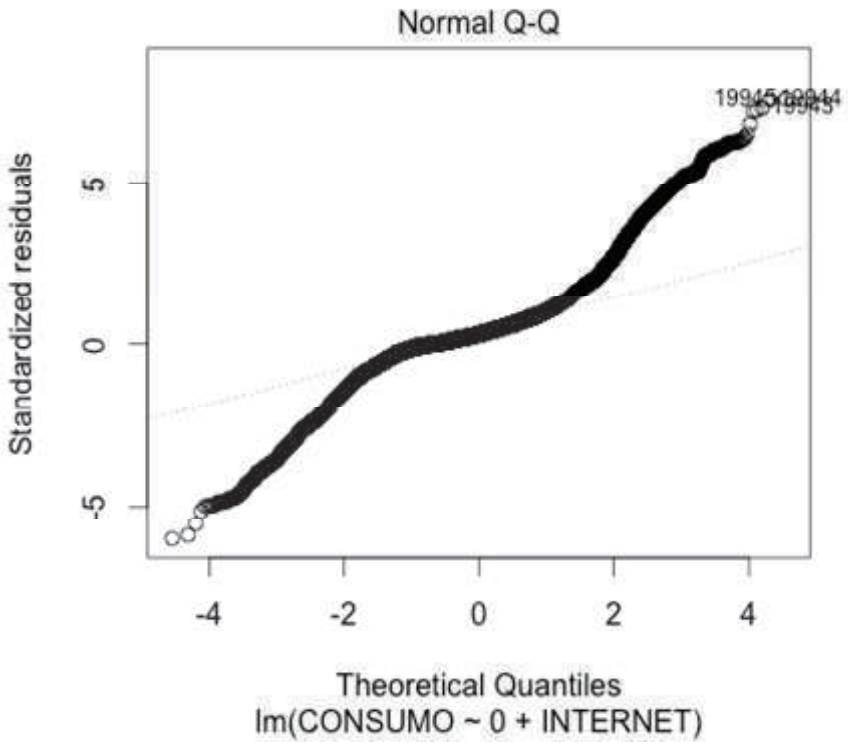
Il consumo Internet (insieme al traffico degli Sms in entrata) è il più correlato linearmente al consumo elettrico. Le chiamate sono correlate in modo meno significativo con il consumo elettrico. Probabilmente l'accesso alla rete da mobile presuppone una minore mobilità nel territorio dell'utente al momento dell'accesso alla rete.

Il valore R-quadratico di regressione è buono tra consumo elettrico e *Internet* è 0,433 con 185.471 gradi di libertà. Pertanto grazie a questo numero elevato di gradi di libertà, sebbene se la correlazione di *Pearson* sia moderata (0,360% Pearson) rimane comunque significativa. L'analisi dei residui mostra però una distribuzione asimmetrica dello scarto tra modello predittivo e dati osservati. Ciò significa che è necessario trovare modelli predittivi più adeguati al fitting dei dati rispetto al modello lineare.

*Figura 8: Correlazione di Pearson e R-squared della regressione lineare per BigData per la provincia di Trento. Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

	R-square	Pearson
FESTIVO	CONSUMO ELETT.	CONSUMO ELETT.
SMS IN	0.334***	0.323
SMS OUT	0.308***	0.291
CALL IN	0.307***	0.332
CALL OUT	0.301***	0.321
INTERNET	0.433***	0.360

Figura 9: Modello di regressione lineare tra consumo elettrico e consumo Internet da mobile. Il consumo Internet (insieme al traffico degli Sms in entrata) è il più correlato linearmente con il consumo elettrico. Il valore R-quadratico di regressione è 0,433 con 185.471 gradi di libertà. Pertanto grazie a questo numero elevato di gradi di libertà la correlazione è moderata ma significativa (0,38% Pearson). L'analisi dei residui mostra però una distribuzione asimmetrica dello scarto tra modello predittivo e dati osservati. Ciò significa che è necessario trovare modelli predittivi più adeguati al fitting dei dati rispetto al modello lineare.



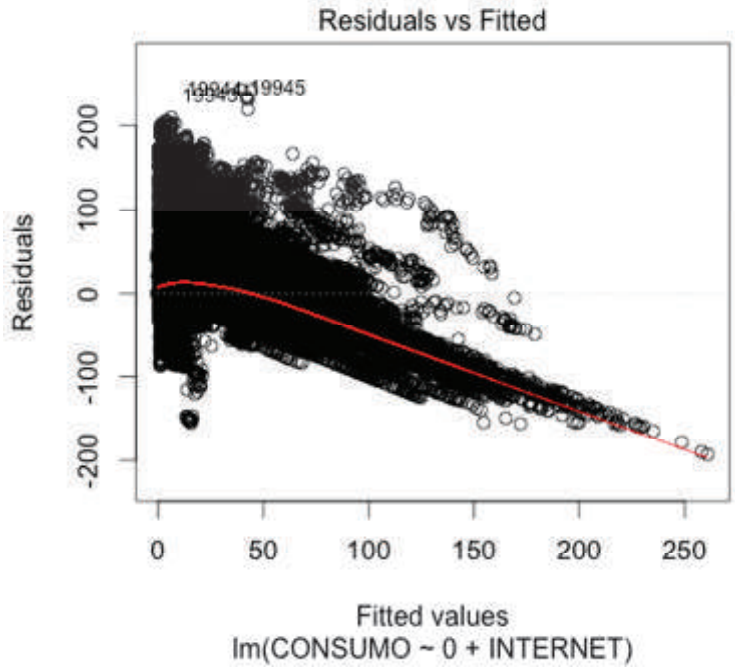


Figura 10: Distribuzione dei residui con il modello di regressione lineare tra consumo elettrico e consumo Internet da mobile. La distribuzione dei residui non è casuale ma ha una tendenza.

Esiste una maggiore correlazione trai dati se si considerano le fasce orarie come si vede dalla Figura 11.

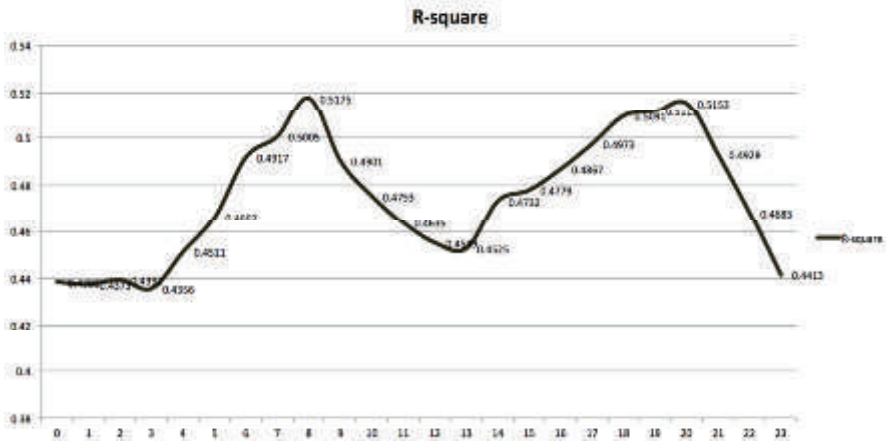


Figura 11: Se si suddividono i dati per fasce orarie si aumenta la correlazione lineare (52% circa) tra consumi elettrici e traffico mobile. In particolare il picco si ha alle ore 8:00 e 20:00 (la correlazione di Pearson è 0,38), cioè nelle ore di minore mobilità delle persone.

4. Conclusioni

I dati open del *Big Data Challenge*, sebbene in forma molto aggregata e con informazioni sulla mappatura molto sparsa tra dati elettrici e mobili e poco granulare rispetto al numero di centraline elettriche e pixel sui dati mobili, forniscono già moltissime informazioni relativamente alla popolazione residente e sulle proprie abitudini. Inoltre i dati dimostrano una correlazione moderata tra consumi elettrici e consumi mobili. Restano ancora da effettuare le seguenti analisi,

previo uno studio di stress test sulla scalabilità sulla nostra piattaforma di calcolo distribuito:

Il traffico da Trento su Trento fornisce un incredibile fonte di informazione sulla mobilità sul territorio della popolazione residente. Si potrebbero analizzare un insieme di circa 70 milioni di record circa al giorno (per una popolazione residente di circa 600.000 persone) relativamente a un grafo contenente 10^10 archi potenziali.

A ogni arco si può associare un peso dovuto al traffico mobile in entrata e in uscita (o meglio solo al numero di interazioni effettuate) che se studiato per fasce orarie può fornire un analisi più precisa della mobilità interna alla *grid* interessata e fornire una stima più precisa della popolazione *stanziale* in ciascun pixel indipendentemente dalla fascia di tempo o relativamente alla fascia di tempo.

In base a questa stima aggregata si potrebbe migliorare la correlazione tra consumo elettrico e mobile.

In effetti una possibile congettura sulla migliore capacità predittiva del traffico internet rispetto agli altri tipi di traffico mobile è che sia un'attività maggiormente di tipo stanziale rispetto a quella delle altre.

Bibliografia

[1] Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., and Stoica, I. (2010). Spark: Cluster computing with working sets. HotCloud, 10(10- 10):95.

[2] Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McCauley, M., Franklin, M. J., Shenker, S., and Stoica, I. (2012). Resilient distributed datasets: A fault-tolerant abstraction for in-memory cluster computing. In Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation, NSDI'12, pages 2–2, Berkeley, CA, USA. USENIX Association.

[3] Barlacchi, G., De Nadai, M., Larcher, R., Casella, A., Chitic, C., Torrisi, G., Antonelli, F., Vespignani, A., Pentland, A., and Lepri, B. (2015). A multi-source dataset of urban life in the city of Milan and the province of Trentino. Scientific Data, 2:150055 EP -.

[4] Bogomolov, A., Lepri, B., Larcher, R., Antonelli, F., Pianesi, F., and Pentland, A. (2016). Energy consumption prediction using people dynamics derived from cellular network data. EPJ Data Science, 5(1):13.

[5] Naboulsi, D., Fiore, M., Ribot, S., and Stanica, R. (2016). Large-scale mobile traffic analysis: A survey. IEEE Communications Surveys & Tutorials, 18(1):124–161.

[6] Blondel, V. D., Decuyper, A., and Krings, G. (2015). A survey of results on mobile phone datasets analysis. EPJ Data Science, 4(1):10.

[7] Lenormand, M., Picornell, M., Cantù-Ros, O. G., Tugores, A., Louail, T., Herranz, R., Barthelemy, M., Frìas-Martìnez, E., and Ramasco, J. J. (2014). Cross-checking different sources of mobility information. PLOS ONE, 9(8):1–10.

[8] Hawelka, B., Sitko, I., Beinat, E., Sobolevsky, S., Kazakopoulos, P., and Ratti, C. (2014). Geo-located Twitter as proxy for global mobility patterns. Cartography and Geographic Information Science, 41(3):260–271. PMID: 27019645.

[9] Deville, P., Linard, C., Martin, S., Gilbert, M., Stevens, F. R., Gaughan, A. E., Blondel, V. D., and Tatem, A. J. (2014). Dynamic population mapping using mobile phone data. Proceedings of the National Academy of Sciences, 111(45):15888–15893.

Giambattista Amati, Simone Angelini, *(Fondazione Ugo Bordoni)*

Anna Caterina Carli, Giuseppe Pierri *(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)*

Giorgio Gambosi, Daniele Pasquini, Gianluca Rossi *(Università Tor Vergata Roma)*

Paola Vocca *(Università della Tuscia - VT)*

Analisi temporale degli eventi su Twitter

Twitter: temporal events analysis

Sommario*: Obiettivo di questo lavoro di ricerca è la classificazione degli eventi in base a differenti pattern temporali, corrispondenti al picco del volume dei messaggi scambiati, per comprendere come gli eventi si propagano sui social network Twitter-like. In prima battuta viene fornita una definizione puntuale di "eventi unici", strettamente correlata al concetto di hashtag. Prendendo in considerazione specifici intervalli di tempo, gli hashtag più popolari sono selezionati tramite la tecnica Seasonal Hybrid ESD (S-H-ESD), introdotta da Twitter. Identificati gli hashtag unici tra i 1000 più popolari, vengono identificati, tramite un algoritmo di Machine Learning non supervisionato applicato alle serie storiche degli hashtag (limitate attorno al picco massimo), i pattern temporali (o cluster) degli eventi. Infine, utilizzando le feature di Twitter, per ogni cluster si studia sia il processo all'origine dell'evento che l'evoluzione di quest'ultimo sulla rete.*

Abstract*: We perform a temporal analysis of the Twitter stream to investigate the evolution of unique events based on the burst of popularity of associated hashtags. We derive a classification of events according to the different patterns corresponding to the peak of the volume of exchanged message and to how these events propagate on any social network with the same characteristics as Twitter. We first provide a precise definition of unique events and correlate them to hashtags. With reference to a specific interval of time, the most popular - with respect to number of tweets- hashtags are then detected using the Seasonal Hybrid ESD (S-H-ESD) technique introduced by Twitter. After identifying the unique hashtags among the 1000 most popular, we have identified, through an unsupervised Machine Learning algorithm applied to the historical temporal series of hashtags limited around the maximum peak, the temporal patterns (clusters) of the events. Finally, using the Twitter features, for each cluster, we have studied both the process at the origin of the event and how they evolve over the network.*

1. Introduzione

Vista la semplice struttura dei dati, le funzionalità basilari offerte e la disponibilità limitata dei dataset, la piattaforma di microblogging Twitter è un punto di riferimento in ambito di ricerca per studiare particolari fenomeni [1] [2] [3] [4]. Lo studio degli eventi è un'area essenzialmente orientata all'individuazione, classificazione e analisi degli eventi significativi che si palesano sui social media, e si distingue da altre aree di ricerca per la sua complessità e per la difficoltà intrinseca di interpretare i risultati.

In questo contesto, è stata eseguita un'analisi adattando il modello proposto da Yang e Leskovec in [5], dove l'individuazione degli eventi unici avviene sulla base della popolarità (numero di tweet) degli hashtag, in uno specifico intervallo temporale. Estendendo la definizione in [6], per evento intendiamo un *fatto che causa, in un determinato periodo di tempo, un incremento sostanziale della frequenza dei messaggi (azioni degli utenti) su Twitter, tutti aventi lo stesso hashtag*; mentre per "unici" denotiamo – osservandone il trend temporale - tutti gli eventi che presentano un picco non ambiguo, e che non risultano pertanto né continui né periodici.

Per individuare gli hashtag più popolari, è stato utilizzato l'algoritmo Seasonal Hybrid ESD (S-H-ESD), una tecnica di Anomaly Detection proposta da Twitter [7] che consente di identificare i picchi sulle serie storiche come "anomalie" nell'evoluzione temporale. Basato sul test ESD generalizzato [8], S-H-ESD risulta più robusto dal punto di vista statistico – poiché utilizza metriche come la mediana e la MAD - e può essere utilizzato sia per l'identificazione delle anomalie globali che per quelle locali.

Il dataset utilizzato, contenente 19 milioni di tweet e più di 300 mila hashtag, è stato analizzato grazie ad un cluster di 8 server con Hadoop HDFS e Apache Spark. Tramite quest'ultimo framework è stato possibile estrarre i soli dati e metadati più significativi dal dataset a disposizione, generare le serie storiche degli hashtag - su scala giornaliera - e, infine, eseguire tutte le operazioni preliminari per la pulizia dei dati, anche sui testi dei singoli tweet. Dopo aver identificato gli hashtag unici tra i 1000 più popolari utilizzando la tecnica S-H-ESD, tramite un algoritmo di Machine Learning non supervisionato applicato alle serie storiche degli hashtag – chiaramente limitate attorno al picco massimo – sono stati individuati i pattern temporali (cluster) degli eventi. L'uso di un approccio non supervisionato è stato preferito a quello supervisionato per evitare ipotesi a priori sul profilo dei picchi, ma anche per evitare l'annotazione manuale del dataset al fine di distinguere i differenti tipi di evento.

Con un algoritmo di clustering sono stati individuati 5 cluster, a cui sono stati successivamente associate specifiche tipologie di evento estraendo i topic dai tweet di ogni classe grazie un Topic Model distribuito sul cluster.

E' senza dubbio possibile affermare che l'individuazione di precisi pattern sul web, come notato da [5], non è banale a causa del comportamento imprevedibile delle persone, che peraltro dipende da diversi fattori (interazione tra i singoli, in piccoli gruppi ma anche in community vaste).

Come già accennato, è stato eseguito il clustering delle serie storiche degli hashtag con un algoritmo altamente scalabile e robusto al fine di verificare l'esistenza di specifiche caratteristiche in ogni classe, anche in base alla tipologia di evento associato (determinato dai topic estratti). Infine, utilizzando le feature di Twitter [9] [10] [11] [12] [13] sui singoli cluster, sono stati studiati I processi all'origine dei profili di popolarità sul social network. Il risultato dell'analisi mostra chiaramente la dualità tra gli eventi endogeni e gli eventi esogeni.

2. Dataset

Per l'analisi è stato utilizzato un sample di Twitter in lingua italiana ottenuto dallo stream della piattaforma, sia filtrando i dati tramite una lista di stopword italiane più utilizzate, sia selezionando la lingua tramite la funzione di selezione interna. Il periodo di riferimento della collezione è compreso tra il 30 ottobre 2015 e il 3 gennaio 2016 (66 giorni totali). La Tabella 1 mostra alcune informazioni preliminari sul dataset usato.

Tabella 1. Informazioni generali dataset

Informazioni generali sul dataset	
Dimensione	21.33 GB
Numero di tweet	19000000
Numero di hashtag	377215
Tweet con hashtag	15754093

3. Tecnologie

Per il caricamento, l'estrazione e la manipolazione del sample di Twitter memorizzato sul file system distribuito di Hadoop (HDFS), è stato utilizzato il framework distribuito Spark (sia in Python che in Scala) su un cluster di 8 server, Spark RDD e Spark Dataframe come strutture dati principali.

4. Analisi degli hashtag

Per l'analisi degli eventi, ignoriamo tutti i tweet senza hashtag. Dalla Tabella 1 segue che, in questo modo, vengono rimossi meno del 20% dei tweet dal dataset. La Figura 1 mostra la percentuale di tweet con uno specifico numero di hashtag ed è interessante notare che più del 50% di essi ne contiene solo uno.

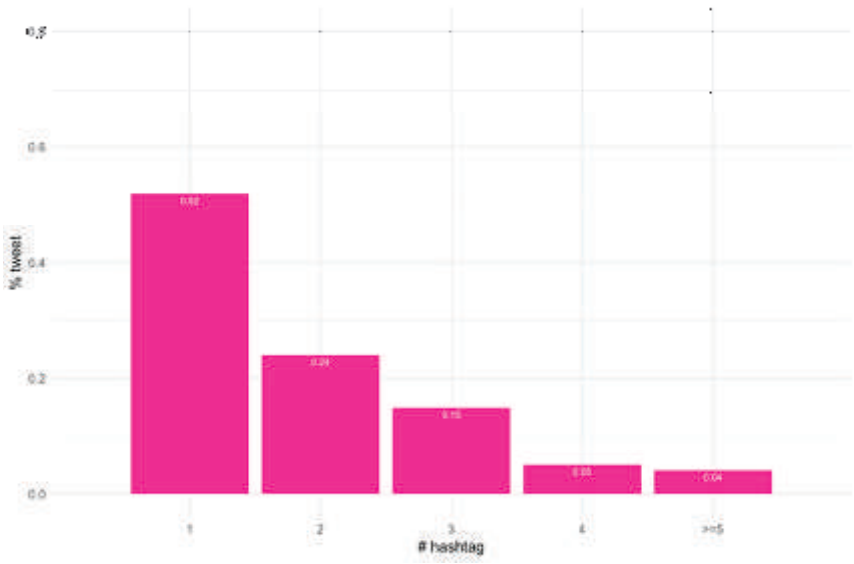


Figura 1. Distribuzione tweet per numero di hashtag

Per ogni hashtag h consideriamo il numero di occorrenze di h, e per ogni x tra 1 e il numero totale di tweet la frazione di hashtag che occorrono in almeno x tweet. La Figura 2 mostra questa relazione, che risulta statisticamente simile ad una distribuzione lognormale con parametri $(-7.99, 4.26)$ e p-value 0.71. Alla luce di quanto detto, vengono considerati i soli 1000 hashtag più frequenti.

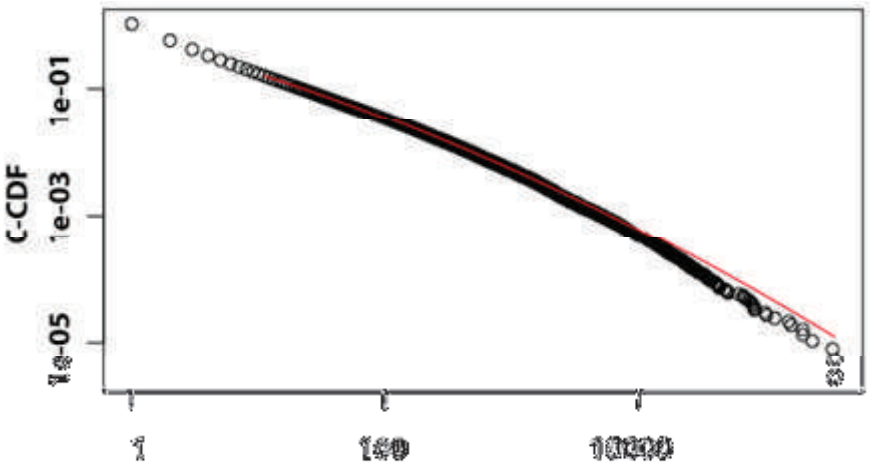


Figura 2. Numero hashtag che occorrono in almeno uno specifico numero di tweet

Siano H i 1000 hashtag più popolari. Definiamo le serie storiche di ogni h in H nell'intervallo di tempo $\tau = [0, \dots, T]$: per ogni h in H e t in τ definiamo x_{h_t} come il numero di tweet contenenti l'hashtag h pubblicati o retweettati al tempo t. In sintesi, il volume di hashtag h al tempo t. La sequenza $x_{h_0}, \dots, x_{h_T}$ è quindi la serie storica dell'hashtag h.

Poiché siamo interessati all'attività giornaliera di ogni hashtag, ogni elemento in τ rappresenta un intervallo di tempo di 24 ore, ovvero $T = 65$ (vedi sezione Dataset).

Possiamo distinguere almeno tre tipologie di serie storiche, in base ai profili emersi: le serie con profilo continuo mostrano un livello costante di attività giornaliera (vedi Figura 3); un profilo periodico è tipico delle serie storiche degli hashtag associati ad eventi che si ripetono in un intervallo fissato come, ad esempio, gli show televisivi di prima serata (vedi Figura 4); infine le serie storiche con un picco isolato rappresentano a tutti gli effetti gli hashtag associati agli eventi unici (vedi Figura 5).

In questo articolo ci si è focalizzati sull'ultima classe di hashtag poiché rappresentano quegli eventi "singolari" più interessanti da studiare. Per individuare i picchi nelle serie storiche utilizziamo l'algoritmo di Anomaly Detection Seasonal Hybrid ESD (S-H-ESD) [14] [7] basato sul test ESD generalizzato, che consente di individuare sia le anomalie locali che quelle globali [15]. Dal momento che le serie storiche degli hashtag possono esibire picchi di tipo differenti, e poiché siamo interessati ai soli picchi isolati che corrispondono alle anomalie globali, per ogni serie storica degli hashtag si ignorano tutti i picchi separati dagli altri da meno di una settimana, così come tutte le serie che non esibiscono picchi nel

proprio profilo. Vengono pertanto presi in considerazione 206 hashtag presenti in 1913470 tweet.

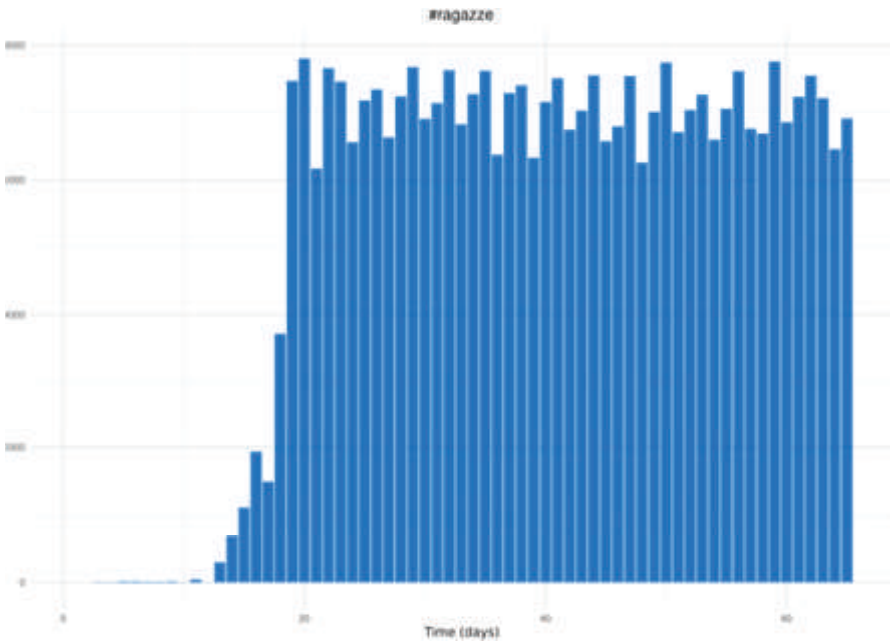


Figura 3. Serie storica hashtag "ragazze"

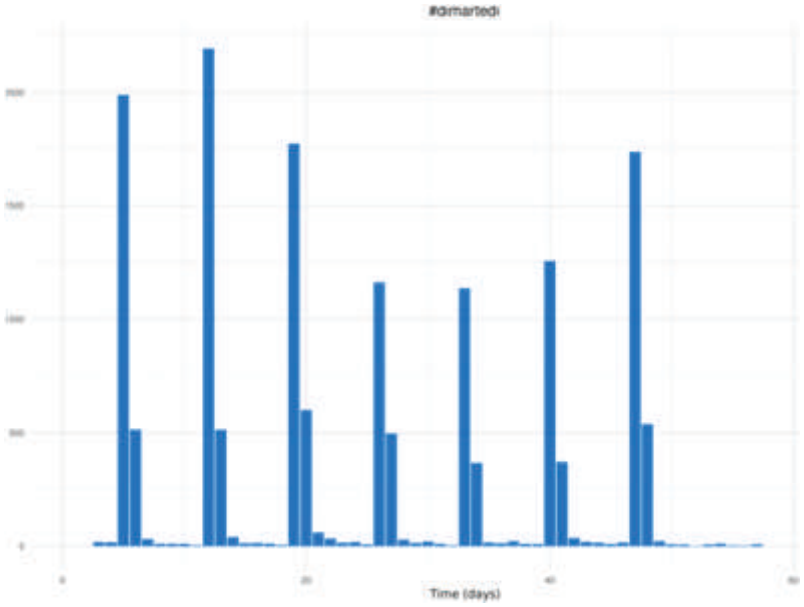


Figura 4. Serie storica hashtag "dimartedì"

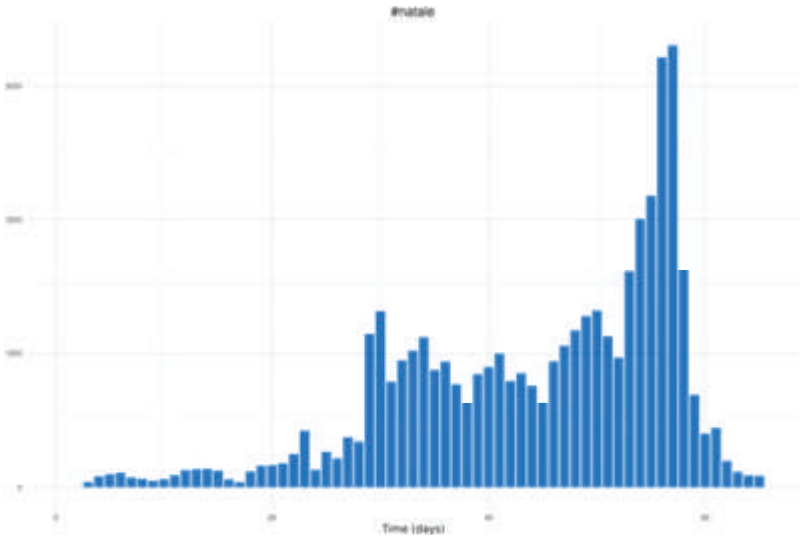


Figura 5. Serie storica hashtag "natale"

5. Periodi attivi

Un hashtag si definisce inattivo se utilizzato in meno di 20 tweet in una finestra temporale di 24 ore. Il limite definito è dovuto al rumore di fondo associato ai tweet più popolari.
La Figura 6 mostra la funzione di distribuzione cumulativa del numero di periodi attivi, mentre la Figura 7 la cumulativa della lunghezza dei periodi attivi. Dalla prima si evince che più del 90% degli hashtag risulta attivo per un massimo di 7 giorni, mentre dalla seconda che la lunghezza dei periodi attivi è sufficientemente corta: circa il 90% degli hashtag hanno periodi attivi che non superano i 10 giorni. Questo suggerisce che, come facilmente ipotizzabile, gli hashtag associati agli eventi unici risultano sporadici, occasionali e volatili

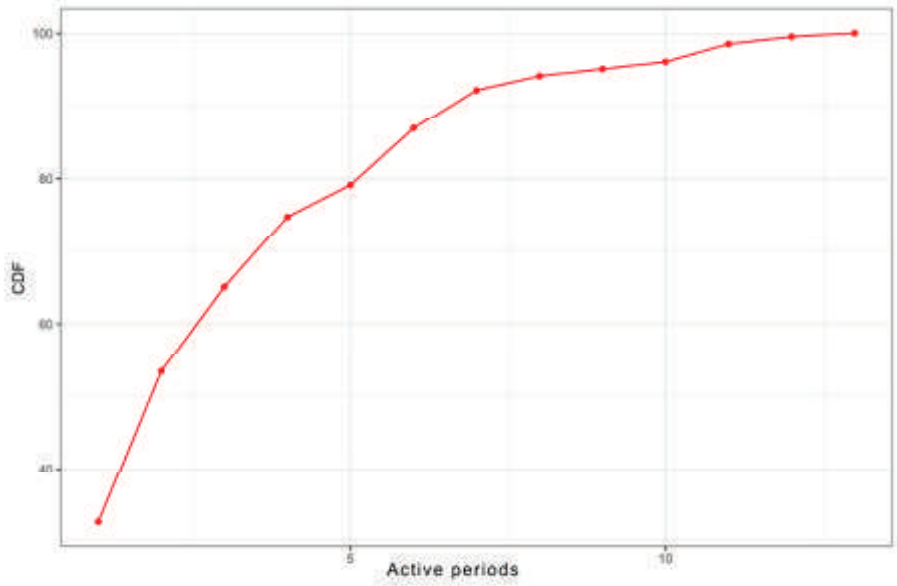


Figura 6. Cumulativa del numero di periodi attivi

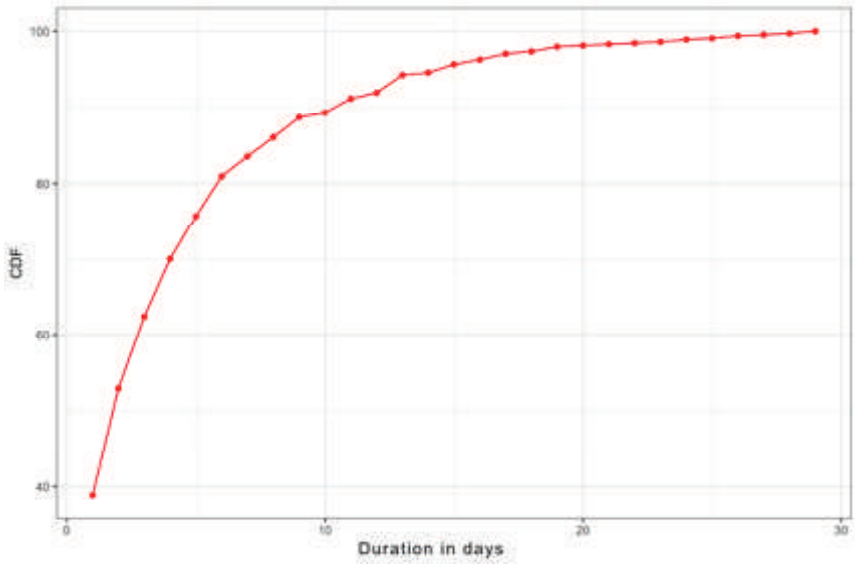


Figura 7. Cumulativa della lunghezza dei periodi attivi

6. Clustering

Classifichiamo le serie storiche degli hashtag contenenti picchi isolati con l'algoritmo di clustering K-SC, proposto in [5]. Peculiarità di questa tecnica è la sua invarianza rispetto alle operazioni di ridimensionamento e traslazione. Ne consegue che i profili con la stessa forma ma differente dimensione o posizione possono essere classificati nello stesso modo, rispetto a quanto avviene nell'algoritmo K-means [16].

Come già accennato, tutte le serie storiche oggetto della nostra analisi hanno una lunghezza pari a 65 giorni: al fine di limitare gli effetti del rumore di fondo abbiamo deciso di troncare le serie e focalizzarci sul solo intervallo di tempo attorno al picco.

Definiamo come "core" di una serie storica l'intervallo di tempo attorno al picco, e tronchiamo la serie storica eliminando i valori al di fuori del core. Sia x_p il valore massimo della serie storica, ovvero il volume al picco; T_p l'istante temporale del picco e α il valore compreso tra 0 e 1 tale che αv_p è il volume minimo che definisce il core. Il core della serie storica è l'intervallo compreso tra $T_1(\alpha)$ e $T_2(\alpha)$ dove $T_1(\alpha) < T_p$, $T_2(\alpha) > T_p$ e per tutti i t tra $T_1(\alpha)$ e $T_2(\alpha)$, il volume a t è almeno αx_p (Figura 8)

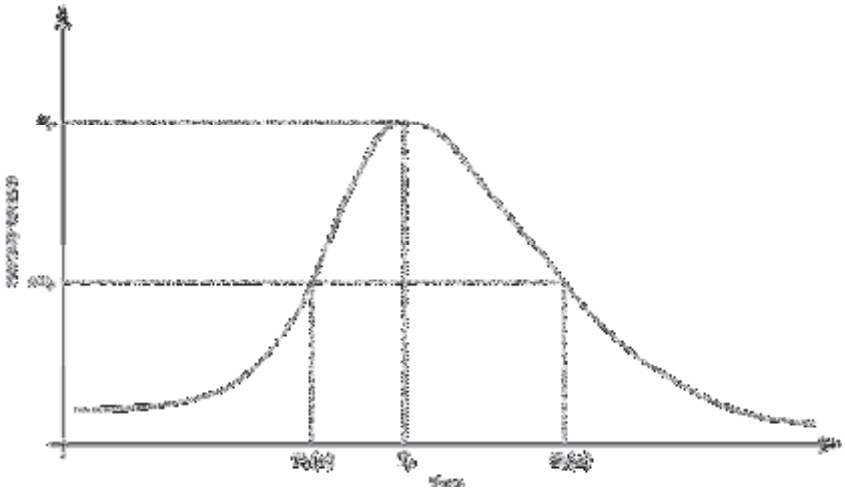


Figura 8. Tipico trend della serie storica di un hashtag

A questo punto possiamo scegliere il valore appropriato per α. Dato α, l'ampiezza del core di una serie storica è $T_2(\alpha)$ - $T_1(\alpha)$, l'ampiezza del core a sinistra è T_p - $T_1(\alpha)$, e l'ampiezza del core a destra è $T_2(\alpha)$ - T_p. La Figura 9 mostra i valori medi delle tre misure. Con valori di α più piccoli di 0.5 l'ampiezza del core a destra è maggiore rispetto a quella di sinistra, e ciò implica che la pendenza a sinistra del core è maggiore rispetto alla pendenza a destra. Abbiamo impostato la dimensione del core a 21 giorni: questo numero si ottiene osservando che in media, in due settimane, il volume minimo del picco è almeno il 12% del valore massimo (vedi Figura 8); vien aggiunta un'ulteriore settimana per gestire i valori anomali.

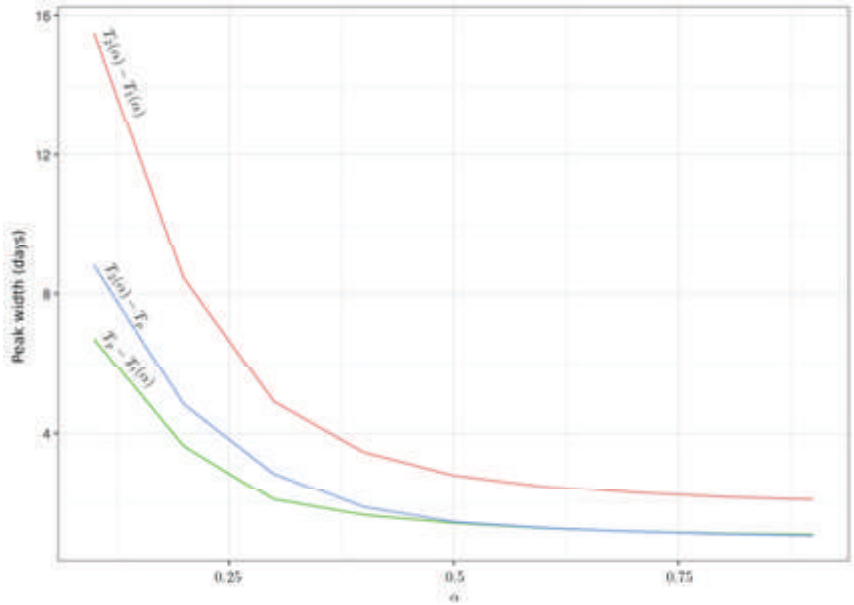


Figura 9. Ampiezza del core in funzione di α

Come noto in K-Means il numero di cluster deve essere specificato come parametro di input; e questo è valido anche per tutte le sue varianti, incluso chiaramente l'algoritmo K-SC qui utilizzato. Al fine di

scegliere il numero più appropriato di cluster, abbiamo eseguito K-SC per diversi valori di k misurando contestualmente la qualità del clustering con la metrica Average Silhouette [16].

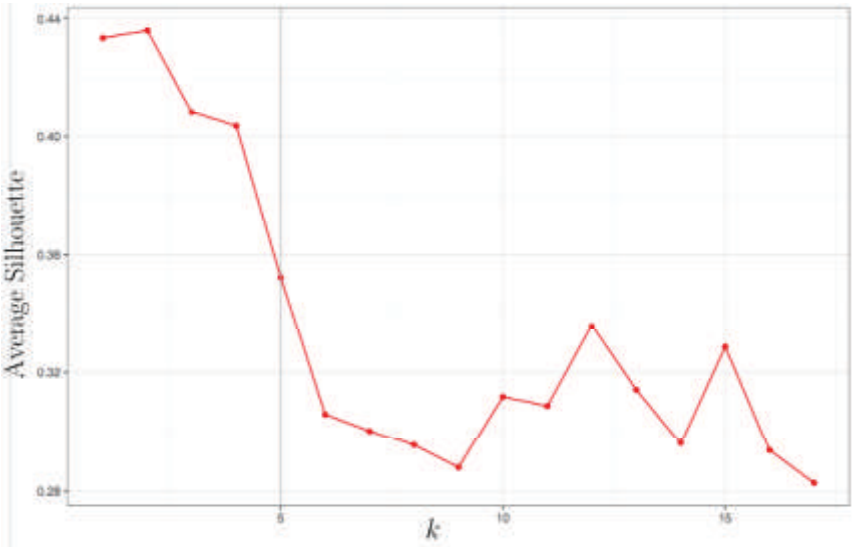


Figura 10. Average Silhouette

La Figura 10 mostra l'Average Silhouette in funzione del numero di cluster: maggiore è il valore della misura, migliore è la qualità del clustering. Nel nostro caso questo risultato si ottiene con valori piccoli di k. Abbiamo scelto quindi k = 5 poiché risulta un ottimo compromesso tra qualità e numero di cluster. Il numero di iterazioni eseguite è stato di 100.

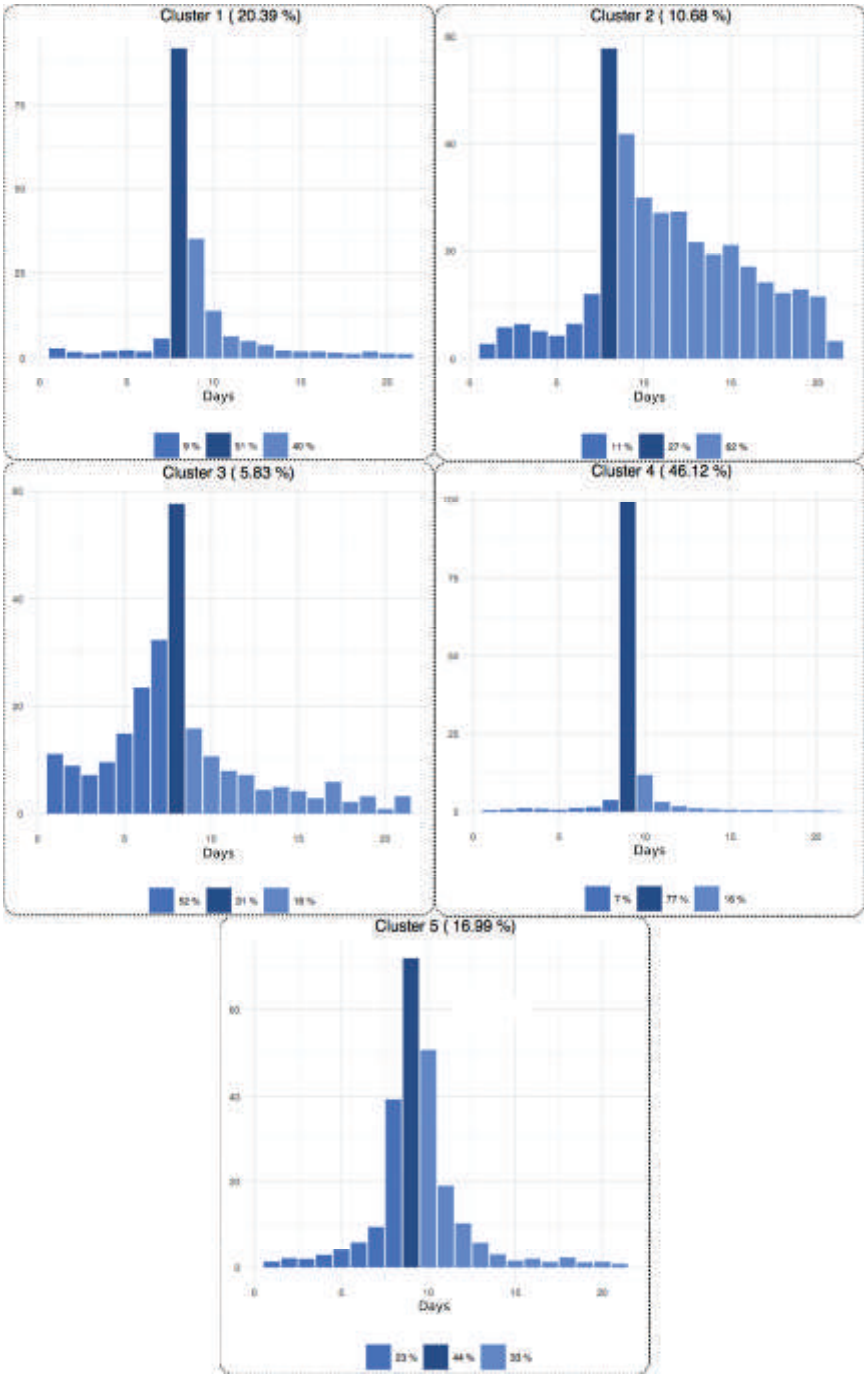


Figura 11. Risultato del clustering

La Figura 11 mostra il risultato del clustering. Per ogni cluster è indicato il numero di hashtag in esso contenuti (in percentuale), il volume al picco, a sinistra e a destra di esso (in percentuale). Il Cluster 4 contiene il maggior numero di hashtag (46.12%): il volume di tweet è concentrato in gran parte in un singolo giorno. Il pattern temporale del Cluster 1 è simile a quello del Cluster 4, se non per una coda più pronunciata: questo denota un interesse relativo della community agli argomenti trattati. Il Cluster 3 e il Cluster 4 risultano a tutti gli effetti opposti: il primo è caratterizzato da un volume relativamente elevato

dopo il picco, mentre il secondo da un volume elevato prima del picco. Infine il Cluster 5 è sostanzialmente simmetrico.

E' interessante notare che circa il 70% degli hashtag è presente in soli due cluster (1 e 4), i cui volumi sono concentrati attorno al picco.

7. Individuazione dei topic

Nel prossimo step esaminiamo i topic che caratterizzano i cinque cluster individuati.

Definiamo il singolo documento d_h per ogni hashtag h ottenuto aggregando tutti i tweet che contengono l'hashtag h. La collezione di documenti relativa ad un cluster i (con $i = 1, \dots, 5$) contiene tutti i documenti d_h tali che l'hashtag h è nel cluster i; denotiamo questa collezione con D_i. Le cinque collezioni $D_1, \dots, D_5$ vengono utilizzate come input per l'algoritmo Latent Dirichlet Allocation (LDA) al fine di estrarre i topic dei 5 cluster [17]. Il numero di topic k è un parametro dell'algoritmo, e il suo valore viene scelto eseguendo 200 iterazioni di LDA per diversi numeri di topic, al fine di individuare il numero che massimizza la log-likelihood. Valorizziamo inoltre I parametri α e β rispettivamente a $\frac{50}{k} + 1$ e 1.1.

Per ogni cluster, abbiamo quindi una lista di topic identificati dalle 5 parole più probabili. Nella Tabella 2 viene illustrata per brevità la lista relativa al solo cluster 1.

1. discorso, mattarella, presidente, italia, politica
2. grillo, italia, dittatore, blog, renzi
3. dignità, unità, papa, soldi, storia
4. renzi, italiani, italia, conferenza stampa, auguri
5. champions league, juventus, roma, italiane, mercato
6. paralizzati, mercoledi, concorso, domani, assunti
7. elezioni, prossime, partito, vince, elettorale
8. pompei, soldi, scavi, renzi, posizione
9. turchia, isis, erdogan, città, turco
10. parigi, terrorismo, morti, sicurezza, guerra
11. buonanotte, lettori, notte, libro, serata
12. renzi, ponte, acqua, messina, stretto
13. renzi, mannoia, concerto, fiorella, esclusa
14. gara, giovani, sanremo, nomi, festival
15. natale, egidio, santo, pranzo, misericordia
16. sinistra, renzi, fassina, nasce, politica
17. cinema, star, wars, forza, risveglio
18. banchetti, coraggio, scavi, piazza, renzi
19. apple, iphone, fisco, accordo, samsung
20. sanremo, giovani, solidarietà, scialpi, discriminazione
21. livorno, bilancio, società, buco, rifiuti
22. laurea, poletti, giovani, orario, italia
23. dignità, unità, papa, soldi, storia
24. bollo, targa, proposta, legge, biciclette
25. expo, milano, successo, italia, finito

Tabella 2 Topic cluster 1

Come si può evincere, i topic trattano essenzialmente eventi inattesi, spesso di carattere politico. Sono presenti inoltre topic che trattano di sport (Champions League) e intrattenimento (Festival di Sanremo). Il cluster 2 è caratterizzato da eventi inattesi come il crack di Banca Etruria. Il cluster 3 risulta invece completamente differente poiché relativo a eventi programmati come i festeggiamenti per il Natale e il Nuovo Anno, ma è presente anche Telethon, il processo Vatileaks e un evento dedicato ai libri. Il cluster 4 è caratterizzato da eventi sostanzialmente giornalieri: Black Friday, l'apertura della Porta Santa al Vaticano ed alcuni eventi sportivi. Infine, nel cluster 5 sono presenti eventi misti dal ridotto impatto sull'opinione pubblica.

8. Conclusioni

L'analisi degli eventi sui social media, la loro classificazione in base ai pattern temporali e lo studio della loro propagazione sulla rete è un'area di ricerca ampiamente studiata, spesso con tecniche e approcci totalmente differenti. A differenza di altri studi, in questo articolo è stato adottato un algoritmo di clustering degli eventi - e delle loro serie storiche - altamente scalabile. Con il dataset a disposizione, siamo riusciti ad identificare 5 differenti cluster di eventi, precedentemente selezionati tramite una tecnica di Anomaly Detection: Seasonal Hybrid ESD (S-H-ESD), proposta da Twitter e testata anche da Netflix, preferita al classico ESD poiché statisticamente più robusta.

Successivamente è stato utilizzato LDA, aggregando i tweet per ogni hashtag, con cui è stato possibile identificare le tipologie di evento associate a specifici pattern temporali, tramite un'annotazione semantica – seppur manuale - degli stessi. In particolare, il cluster 3 - poiché caratterizzato da un elevato volume di messaggi prima del picco - può essere associato agli eventi programmati. E' bene notare che questa tipologia di pattern è tipicamente associata agli eventi scatenati da fattori endogeni. Il cluster 4, invece, è associato a pattern temporali che si riferiscono agli eventi giornalieri one-shot, che risultano popolari tra gli utenti nel solo giorno in cui avvengono. Considerando l'alta proporzione di retweet, è possibile ipotizzare che siano scatenati da fattori esogeni. I cluster 1 e 2, d'altro canto, sono associati ad eventi inattesi che impattano in modo differente sulla community. Mentre nel primo caso possiamo interpretare il fenomeno come propagazione endogena, nel secondo - osservando l'elevata proporzione di tweet con url – possiamo affermare che gli eventi sono stati guidati da fattori esterni, iniettati nella rete tramite i mass media. Infine, il cluster 5 mostra un profilo simmetrico, e corrisponde a eventi misti, in cui sia i processi endogeni che quelli esogeni contribuiscono alla propagazione dell'informazione. E' chiaro che l'analisi eseguita può essere migliorata: utilizzando un dataset di dimensioni maggiori l'algoritmo K-SC potrebbe potenzialmente identificare nuovi cluster e, quindi, nuovi pattern temporali. Inoltre potrebbe essere interessante studiare la propagazione degli eventi analizzando il Follow Graph di ogni utente [1], così come

utilizzare algoritmi di Natural Language Processing e Named Entity Recognition assieme a LDA per migliore il risultato del topic model.

Bibliografia

[1] G. Amati, S. Angelini, G. Gambosi, G. Rossi, P. Vocca e G. Marcone, Moving Beyond the Twitter Follow Graph, Lisbon: KDIR 2015 - Proceedings of the International Conference on Knowledge Discovery and Information Retrieval, part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2015), Volume 1, Lis- b, 2015.

[2] G. Amati, S. Angelini, F. Capri, G. Gambosi, G. Rossi e P. Vocca, Twitter Temporal Evolution Analysis: Comparing Event and Topic Driven Retweet Graphs, Funchal: {BIGDACI} 2016 - Proceedings of the International Conference on Big Data Analytics, Data Mining and Computational Intelligence, Volume 1, 2016.

[3] G. Amati, S. Angelini, F. Capri, G. Gambosi, G. Rossi e P. Vocca, Modelling the temporal evolution of the retweet graph., IADIS International Journal on Computer Science and Information Systems, 2016.

[4] G. Amati, S. Angelini, F. Capri, G. Gambosi, G. Rossi e P. Vocca, On the Retweet Decay of the Evolutionary Retweet Graph, Venice: Smart Objects and Technologies for Social Good: Second International Conference, GOODTECHS 2016, 2017.

[5] J. Yang e J. Leskovec, Patterns of Temporal Variation in Online Media, New York: Proceedings of the Fourth ACM International Conference on Web Search and Data Mining (WSDM '11)., 2011.

[6] W. Dou, X. Wang, D. Skau, W. Ribarsky e M. X. Zhou, LeadLine: Interactive visual analysis of text data through event identification and exploration, 2012 IEEE Conference on Visual Analytics Science and 593 Technology (VAST), 2012.

[7] S. Kelly e K.Ahmad, Propagating Disaster Warnings on Social and Digital Media, Intelligent Data Engineering and Automated Learning -- IDEAL 2015, 2015.

[8] B. Rosner, Percentage Points for a Generalized ESD Many-Outlier Procedure, Technometrics, 1983.

[9] M. Armbrust, R. S. Xin, C. Lian, Y. Huai, D. Liu, J. K. Bradley, X. Meng, T. Kaftan, M. J. Franklin, A. Ghodsi e M. Zaharia, Spark SQL: Relational Data Processing in Spark, Melbourne: Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data, 2015.

[10] W. X. Zhao, J. Jiang, J. Weng, J. He, E.-P. Lim, H. Yan e X. Li, Comparing Twitter and Traditional Media Using Topic Models, Berlin: Advances in Information Retrieval, 2011.

[11] S. Asur, B. A. Huberman, G. Szabo e C. Wang, Trends in Social Media : Persistence and Decay, CoRR, 2011.
[12] J. Lehmann, B. Goncalves, J. J. Ramasco e C. Cattuto, Dynamical Classes of Collective Attention in Twitter, Lyon: Proceedings of the 21st International Conference on World Wide Web, 2012.
[13] W. Guan, H. Gao, M. Yang, Y. Li, H. Ma, W. Qian, Z. Cao e X. Yang, Analyzing user behavior of the micro-blogging website Sina Weibo during hot social events, Physica A: Statistical Mechanics and its Applications, 2013.
[14] A. Kejariwal, Introducing practical and robust anomaly detection in a time series, https://blog.twitter.com/engineering/en_us/a/2015/introducing-practical-and-robust-anomaly-detection-in-a-time-series.html, 2015.
[15] B. Rosner, Percentage Points for a Generalized ESD Many-Outlier Procedure, Technometrics, 1983.
[16] L. Kaufman e P. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis, Number Book 59 in Wiley Series in Probability and Statistics. Wiley-Interscience., 2005.
[17] D. Blei, A. Ng e M. Jordan, Latent Dirichlet Allocation, J. Mach. Learn. Res., 2003.
[18] S. Kelly e K. Ahmad, Propagating Disaster Warnings on Social and Digital Media, Cham: Intelligent Data Engineering and Automated Learning – IDEAL 2015,, 2015.

Daniela Valente,
Gianmarco Fusco,
Giuseppe Pierri,
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Coesistenza tra segnali IoT a banda stretta e segnali del broadcasting televisivo terrestre nelle bande VHF e UHF

Coexistence between narrowband IoT and digital video broadcasting in VHF and UHF bands

Sommario: *L'oggetto del presente lavoro è rappresentato dallo studio delle eventuali situazioni interferenziali, su impianti TV riceventi il segnale del digitale terrestre, provocate da un ipotetico downlink di traffico IoT (Internet of Things) proveniente da stazione radio-base.*

La sperimentazione ha avuto il fine di proporre e testare la coesistenza, nella banda di frequenze destinata alla radiodiffusione televisiva, tra segnali a banda stretta per applicazioni di Internet delle cose (NB-IoT) e segnali radiotelevisivi. Le prove effettuate hanno avuto lo scopo principale di individuare il livello minimo di segnale indesiderato che provoca il primo evento di quadrettamento del segnale televisivo.

Tale studio si colloca tra le attività di ricerca volte a rispondere alle sfide trasmissive che la prossima generazione (5G) di sistemi di radio-comunicazione pone e che prevede per il prossimo futuro un enorme aumento di connessioni IoT di tipo wireless [1].

In particolare, con il presente lavoro si vuole rispondere alle esigenze di un certo tipo di traffico dati in espansione, ponendosi nella inevitabile prospettiva di ottimizzazione dell'uso dello spettro radio e nella reale previsione di futura cessione di frequenze del segnale televisivo digitale (DVB-T/T2 – Terrestrial Digital Video Broadcasting) al radiomobile [2], [3]. Gli scenari simulati potranno essere di interesse per i competenti organi di regolamentazione e standardizzazione nella determinazione del ruolo dello spettro UHF (Ultra High Frequency) e VHF (Very High Frequency) nelle comunicazioni di quinta-generazione (5G).

A tale proposito il gruppo RSPG (Radio Spectrum Policy Group) della commissione Europea, competente in materia di politica dello spettro radio, si è già espresso affermando che la quinta-generazione di sistemi radiomobili avrà bisogno di utilizzare anche le bande armonizzate al di sotto di 1 GHz (inclusa la banda a 700 MHz) per fornire copertura 5G sui territori nazionali e per fornire copertura indoor [4].

Abstract: *The objective of the present work is the investigation of potential interference effects, on tv digital receiving systems, due to the downlink transmission of IoT (Internet of Things) radio-base stations.*

Specifically, the aim is to propose and test the coexistence between narrowband signals for Internet of Things (NB-IoT) applications and

broadcasting signals in the frequency bands allocated to the broadcasting service.

The objective of the field-testing is to measure the minimum level of the unwanted signal that causes degradation in the reception quality of the television signal according to given picture degradation conditions.

Our work is motivated by the challenges posed by next-generation cellular networks (5G – fifth generation) in identifying spectrum to cope with the increasing traffic demand of wireless IoT connections [1].

In particular, our perspective is to propose a solution for some type of IoT traffic while considering the efficiency of spectrum usage and the future assignment of some DVB-T/T2 (Terrestrial Digital Video Broadcasting) frequency portions to radio mobile systems [2], [3].

Simulated scenarios can also be utilized by regulation and standardization forums for studying the future role of UHF (Ultra High Frequency) and VHF (Very High Frequency) in the evolution of mobile communications toward fifth-generation (5G).

In this regard, the RSPG (Radio Spectrum Policy Group) group of the European Commission, responsible for radio spectrum policy, is of the opinion that 5G mobile radio systems will also need to use the harmonized bands below 1 GHz (including the 700 MHz band) to provide 5G coverage nationwide and to provide indoor coverage [4].

1. Introduzione

La quinta generazione di reti radiomobili (5G) ha il fondamentale obiettivo di fornire una connettività diffusa e flessibile che permetta alle persone, le applicazioni, gli oggetti di uso quotidiano, i sistemi di trasporto ed altri attuatori di servizi, di comunicare tra di loro con l'obiettivo generale di migliorare la qualità della vita dell'utente.

L'ampia gamma di requisiti (quali: elevati data-rate (>Gb/s), comunicazioni a bassa latenza (~ms), applicazioni a basso consumo di potenza, terminali a ridotta complessità) e di scenari applicativi (Enhanced mobile broadband, Ultra-reliable and low-latency communications, Massive machine-type communications – vedi Figura 1) attesi per IMT-2020/5G, richiederà sia nuove interfacce radio che l'impiego di nuove bande di frequenza (tra cui le onde millimetriche), nonché l'interoperabilità tra tecnologia presente (IMT-Advanced/4G) e futura (IMT-2020/5G) [5], [6].

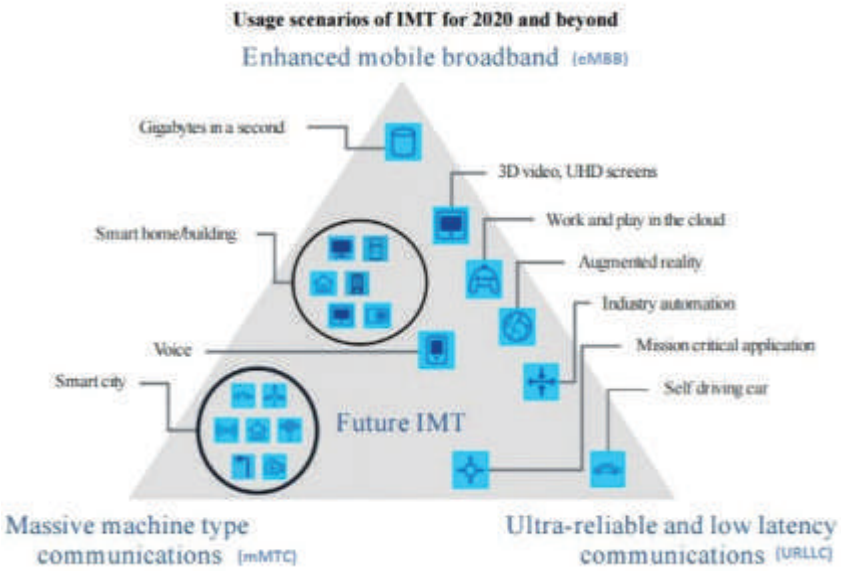


Figura 1. Scenari applicativi, immagine tratta da "Recommendation ITU-R M.2083-0 (09/2015)"

In particolare, il presente studio fa riferimento a scenari applicativi di tipo machine-type communications, quali: smart metering, telematica, intelligent transport systems, mobile health, personal monitoring, elettronica di consumo, etc. In questo contesto, si parla di paradigma IoT che include comunicazioni tra sensori, oggetti dotati di intelligenza, interrogazione di server di dati, ovvero comunicazioni di tipo-macchina. Ad esse ci si riferisce come ad una modalità di trasmissione dell'informazione che non richiede necessariamente l'interazione umana e che è caratterizzata da un traffico dati discontinuo e a basso rate. Tipicamente, i dispositivi coinvolti hanno bassa mobilità e sono caratterizzati da ridotte capacità computazionali e di memoria ed hanno un limitato budget energetico. Per rispondere a questo tipo di traffico, esistono soluzioni tecnologiche basate su reti locali in grado di interconnettere dispositivi MTC (machine-type communications) presenti su una stessa area locale, tuttavia tali soluzioni non riescono ad offrire una copertura ubiqua o a garantire un controllo altamente affidabile della rete [7]. Sono anche presenti sul mercato soluzioni proprietarie in grado di soddisfare alcuni dei requisiti ma devono affrontare la sfida di raggiungere la scala globale (LoRa, SigFox e Weigthless) [8], [9]. Pertanto, la soluzione più naturale sembra essere quella offerta dalle esistenti reti cellulari che garantiscono una copertura mondiale e vantaggi legati ad efficienza, robustezza e sicurezza. Inoltre, queste ultime hanno la potenzialità di implementare opzioni specifiche per il traffico MTC, ma nonostante ciò potrebbero avere difficoltà a fronteggiare la prevista crescita di tali servizi. Recentemente il 3GPP (Release 13) ha introdotto due nuovi standard cellulari per l'IoT a banda stretta: il più promettente è basato sull'LTE ed è denominato NB-IoT (narrowband IoT) con canali da 200 kHz e capacità fino a 250 kbit/s, mentre l'altro è basato sul GSM ed è denominato EC-GSM (Extended Coverage GSM). Il dispiegamento della tecnologia NB-IoT avviene tramite l'impiego di stazioni 4G/LTE e quindi la copertura dipende

dall'area di fornitura dell'esistente rete cellulare. NB-IoT è licenziata (usa le bande dell'LTE) ed ha vantaggi in termini di QoS (Quality of Service), latenza, affidabilità e copertura.

In questo contesto, la presente campagna di misure ha avuto l'obiettivo di testare l'impiego delle frequenze al di sotto dei 700 MHz per la trasmissione di segnali di tipo IoT a banda stretta, e rispondere alle esigenze di una tipologia di traffico IoT. La banda del broadcasting televisivo terrestre in Italia, 470-790 MHz e 174-230 MHz, è ideale per fornire servizi trasmissivi di alta qualità date le caratteristiche propagative delle bande UHF e VHF. La banda sopra i 700 MHz è già in parte destinata a passare dal broadcasting televisivo al radiomobile nei prossimi anni (~2022) [10], [11]. Inoltre esistono studi, soluzioni e normative (ETSI EN 301 598 [12]) sull'impiego di tecnologie che utilizzano i white spaces televisivi per l'erogazione di servizi di comunicazione*, grazie a procedure e meccanismi di cognitive radio (CR) per ascoltare quando il canale radio è libero, o tramite interrogazioni di database che hanno capacità di geolocalizzazione e sono in grado di comunicare i parametri trasmissivi ai terminali.*

La sperimentazione ha previsto l'utilizzo delle bande di guardia (circa 400 kHz per canale) tra canali adiacenti del servizio televisivo digitale per le suddette trasmissioni a banda stretta (200 kHz), di tipo IoT. L'eventuale successo di questo tipo di trasmissione è determinato dalla capacità di coesistenza con l'erogazione del servizio televisivo digitale che è primario in tali bande. La degradazione di quest'ultimo viene valutata in termini di "quadrettamento" dell'immagine su schermo tv. I canali televisivi testati sono nella banda UHF, con frequenza centrale 666 MHz e nella banda VHF, con frequenza centrale 198.5 MHz.

Il documento è così articolato: nella sezione 2 viene descritta la metodologia adottata, il banco di simulazione ed i segnali generati per effettuare le misure; nella sezione 3 vengono illustrati gli scenari simulati e le misure acquisite successivamente analizzate, nella sezione 4, in termini di distanze tra stazioni trasmittenti ed antenne televisive riceventi; infine, le conclusioni vengono tratte nella sezione 5.

2. Metodologia e banco di misure

Il laboratorio di radiodiffusione sonora e televisiva dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione ha predisposto un banco di simulazione ed ha effettuato prove nello scenario in cui le interferenze sono causate dal downlink proveniente da una stazione radio-base IoT direttamente sull'antenna TV ricevente.

Il banco, schematizzato in Figura 2, è costituito da due generatori, uno genera il segnale televisivo DVB-T/T2 mentre l'altro genera il segnale IoT. I due segnali vengono poi sommati attraverso un power divider ed inviati, a seguito del passaggio attraverso un matching-pad 50/75 ohm, al televisore in esame.

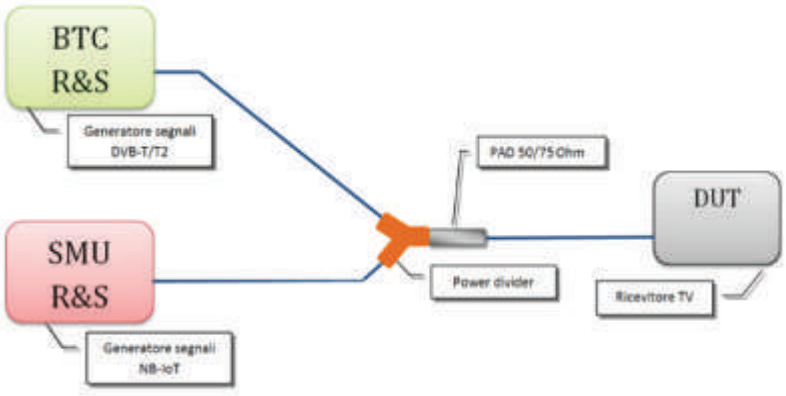


Figura 2. Schema del banco di misure

Il segnale di tipo IoT è generato, via software, come forma d'onda arbitraria in banda base che è l'input per il generatore SMU200A della Rohde&Schwarz (R&S). Quest'ultimo ha il compito di collocare il segnale di 200 kHz di banda alla frequenza di interesse. Nello specifico, il segnale IoT viene inserito nella banda di guardia del canale televisivo che si vuole testare. Tale segnale IoT in uscita dal generatore è inviato come segnale interferente all'ingresso RF del televisore (DUT – Device Under Test), tramite cavo (in modalità condotta), miscelato con il segnale utile del quale si studia il degradamento.

Il segnale televisivo (in Figura 3), invece, viene generato dal generatore di segnale broadcast BTC (Broadcast Test Center) della (R&S). Per le misure nella banda UHF, attraverso il generatore SMU200A, il segnale IoT di 200 kHz di banda (in Figura 4) viene centrato alla frequenza di 662 MHz (in Figura 4), nella banda di guardia sinistra del canale televisivo 45 centrato alla frequenza di 666 MHz (larghezza di banda 8 MHz). Per le misure nella banda VHF, invece, il segnale IoT è stato centrato alla frequenza di 195 MHz, nella banda di guardia sinistra del canale televisivo 8 che è centrato alla frequenza di 198,5 MHz (larghezza di banda 7 MHz), come mostrato in Figura 5.

Il passo successivo è stato quello di individuare la potenza del segnale IoT che produce il "quadrettamento" del segnale tv, il cui effetto sull'immagine a schermo è esemplificato in Figura 6.

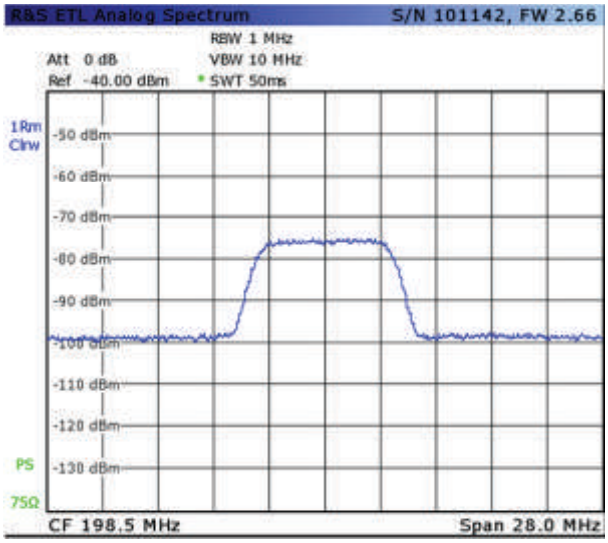


Figura 3. Spettro segnale televisivo

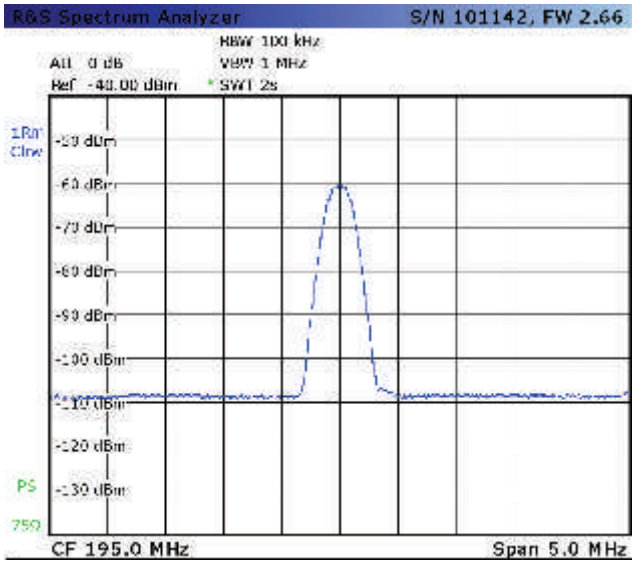


Figura 4. Spettro segnale IoT

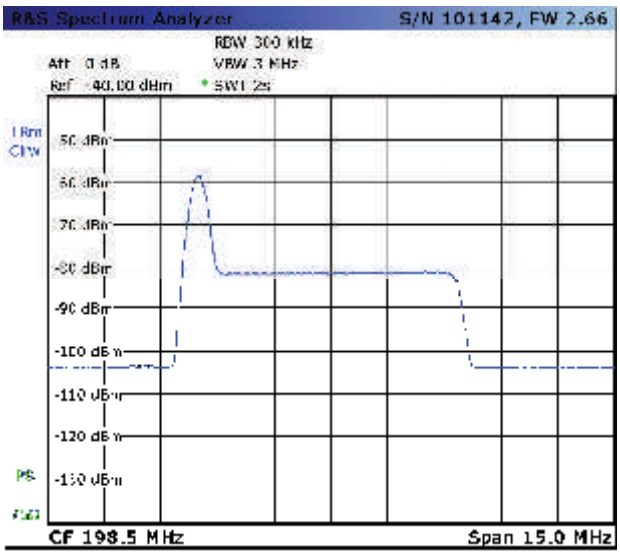


Figura 5. Spettro aggregato, segnale televisivo e segnale IoT

Le prove effettuate hanno avuto lo scopo principale di determinare il valore minimo di segnale interferente (IoT), misurato all'ingresso del dispositivo sotto prova [2] e valutato in corrispondenza della soglia di degradamento dell'immagine su schermo. La soglia è determinata con un metodo definito dalla funzione *onset of picture degradation* della norma EN 303 340 che consiste nell'individuare il livello minimo di segnale indesiderato che provoca il primo evento di quadrettamento - in un prefissato periodo d'osservazione (~15 s.) - dato un livello fisso di segnale desiderato.

Figura 6. *Degradazione segnale televisivo (esempio di quadrettamento è indicato in rosso)*

2.1 Il segnale IoT

Il segnale NB-IoT, generato con il simulatore WinIQSim2 della R&S e dato in input al generatore SMU200A, è un segnale di downlink (DL) di tipo LTE FDD OFDMA (Frequency Division Duplex, Orthogonal Frequency Division Multiple Access) con occupazione di banda pari a 200 kHz (come mostrato in Figura 7) e modulazione QPSK (Quadrature Phase Shift Keying). E' ottimizzato per traffico dati a basso-rate (e non voce) e per mobilità limitata; secondo indicazioni da manuale, in DL si ha un data-rate di picco pari a 226,7 kbit/s ed un flusso medio di circa 30 kbit/s [13], [14]. La banda effettivamente occupata è pari a 195 kHz e la dimensione della FFT è 128. Il resource block (RB) prevede in downlink un'occupazione spettrale di 12 sottoportanti distanziate di 15 kHz ed il prefisso ciclico è di tipo normale. Il filtro in trasmissione è predefinito ed è quello previsto dallo standard Eutra/LTE. Il segnale generato prevede che ci sia un unico utente di tipo NB1 attivo. La trasmissione è in formato N1 e prevede che il canale NPDCCH (narrowband physical downlink control channel) trasporti l'informazione di allocazione dei dati ed il numero di volte che essi sono ripetuti nel NPDSCH (narrowband physical downlink shared channel).

La sperimentazione descritta nella sezione 2 ha previsto che il segnale IoT venisse inserito nella banda di guardia (vedi Figura 11) del canale televisivo che si vuole testare [15]. Idealmente, per non creare nessuna interferenza al segnale televisivo, bisognerebbe riservare al segnale IoT una porzione di spettro di circa 400 kHz per contenere anche i "lobi laterali" che però hanno un livello di potenza che è a -20 dB rispetto al picco del segnale stesso.

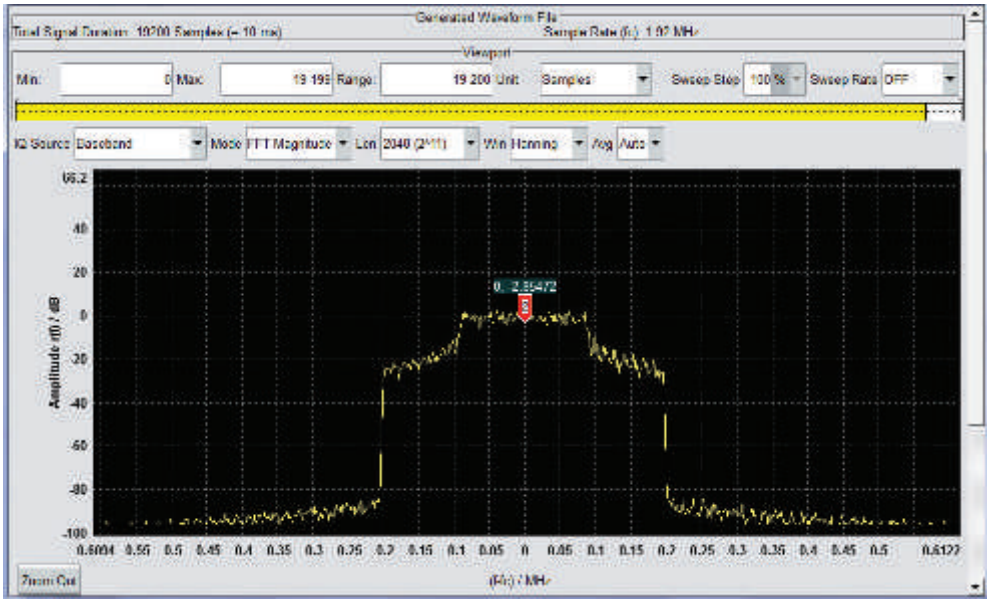


Figura 7. *Spettro segnale OFDM 200 kHz, dall'interfaccia del simulatore WinIQSim2 della R&S*

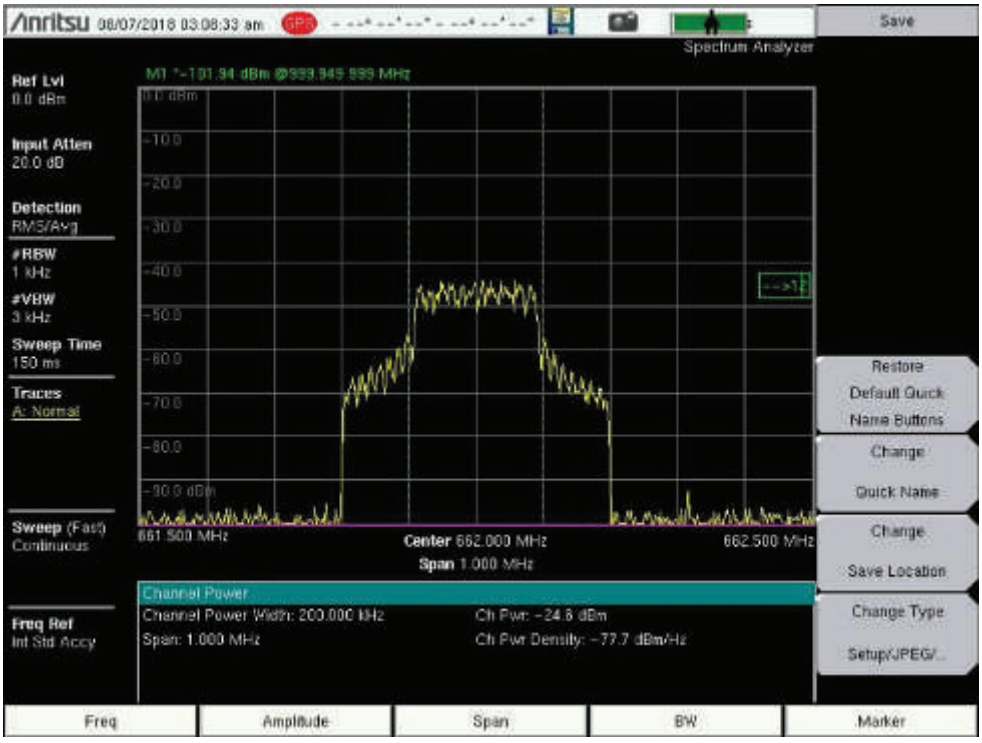


Figura 8. Spettro segnale IoT centrato a 662 MHz

2.2 Il segnale televisivo

Le impostazioni dei parametri dei segnali DVB-T/T2 utilizzate ai fini della sperimentazione sono state ricavate dalla norma ETSI EN 303 340 [16]. Il segnale televisivo di banda base usato è un transport stream in standard definition con data-rate pari a 5 Mbit/s e livello di potenza all'ingresso del ricevitore televisivo pari a -63/-70 dBm.

Gli standard DVB-T/T2 prevedono un'occupazione nominale di banda del segnale televisivo pari a 7 MHz nella gamma VHF e pari a 8 MHz alle frequenze UHF. Per i segnali DVB-T sono stati scelti: una dimensione di FFT (Fast Fourier Transform) di 8k, uno schema di modulazione 64 QAM (Quadrature Amplitude Modulation) – mostrato in Figura 9 - ed un intervallo di guardia (I_g) pari a 1/4. Invece, per i segnali DVB-T2 generati è stato previsto: una dimensione di FFT di 32k, una modalità (carrier mode) *estesa* e *non estesa*, uno schema di modulazione 256 QAM ruotato – mostrato in Figura 10 - ed un intervallo di guardia (I_g) pari a 1/16.

Sia per i segnali DVB-T che per quelli DVB-T2, sono state considerate due opzioni di code-rate: 2/3 e 3/4.

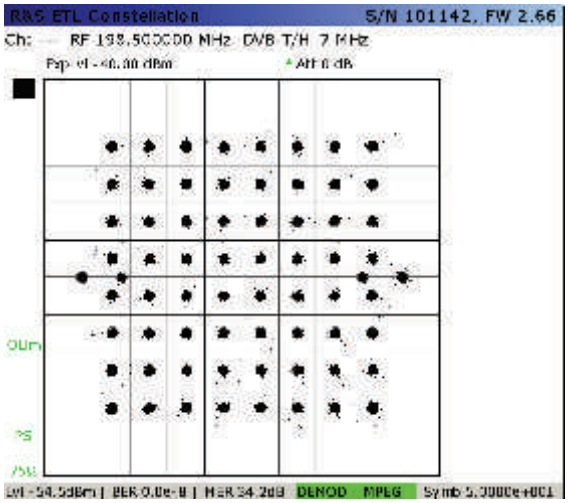


Figura 9. Schema modulazione 64QAM, per segnale DVB-T a 7 MHz

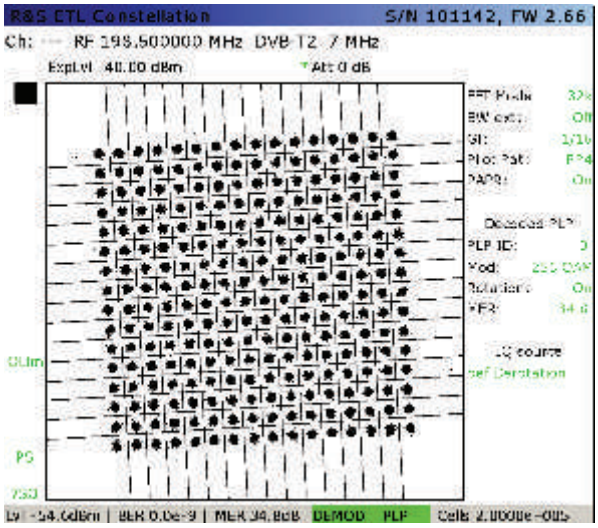


Figura 10. Schema modulazione 256QAM (ruotata), per segnale DVB-T2 a 7 MHz

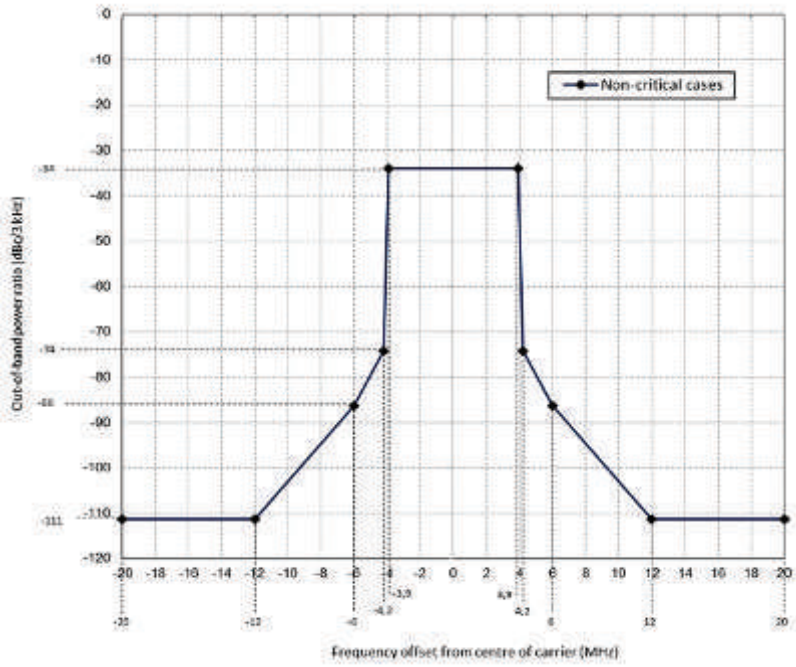


Figura 11. Occupazione di banda effettiva; emissioni fuori banda per trasmettitore DVB-T di classe H0 con canali da 8 MHz, maschera tratta da "ETSI EN 302 296 V2.0.2 (2016-10)"

3. Misure: grafici potenza interferente vs. potenza utile al variare dello standard, del code-rate e dei DUT

I DUT (device under test) usati nella campagna di misure sono due televisori (TV1 e TV2) in dotazione del laboratorio. Nello specifico, il confronto è avvenuto tra televisori di diversa generazione. Entrambi sono compatibili con lo standard DVB-T/T2, ma il TV2 è di generazione più recente ed è dichiarato conforme alla norma ETSI EN 303 340 a differenza del TV1 in quanto fabbricato prima della pubblicazione della norma stessa. Come anticipato, il segnale televisivo giunge all'ingresso del ricevitore sotto test con due possibili livelli di potenza, -63 dBm e -70 dBm, avvicinandosi a quanto previsto dalla norma ETSI EN 303 340 in termini di soglia di sensibilità del ricevitore televisivo. È, inoltre, importante notare che le misure effettuate prendono in considerazione scenari applicativi con impianti televisivi non dotati di amplificatore di testa.

I segnali televisivi, impiegati nella campagna di misure, sono sia di tipo DVB-T (Figura 12, Figura 13) che DVB-T2 (Figura 14 – Figura 17) in entrambe le gamme di frequenze considerate. Ai fini dell'analisi dell'interferenza per il setup descritto nel paragrafo 2, è importante considerare gli aspetti evidenziati nel seguito. Il segnale DVB-T/T2 ha una banda nominale pari a 7 MHz nella gamma VHF (canale 8 a 198.5 MHz) e pari a 8 MHz in quella UHF (canale 45 a 666 MHz). L'occupazione effettiva di banda del segnale DVB-T è pari a 6.66 MHz nella banda VHF (Figura 12) e 7.61 MHz nella banda UHF (Figura 13). Per il segnale DVB-T2, c'è l'ulteriore differenza tra occupazione *non estesa* ed *estesa*. Nel caso di DVB-T2 *non esteso* (*n.e.*), la banda effettivamente occupata è identica a quella del caso di trasmissione in tecnica DVB-T (Figura, Figura). Per quanto riguarda il DVB-T2 *esteso* (*e.*), la banda effettiva è di

6.796 MHz (~6.8 MHz) nel VHF (Figura) mentre è pari a 7.767 MHz (~7.77 MHz) nell'UHF (Figura). Ovviamente, è possibile prevedere che quando c'è una maggiore spaziatura tra canali televisivi adiacenti, dovuta ad una minore occupazione della banda nominale, l'interferente IoT con banda *totale* di circa 400 kHz (considerati anche i lobi laterali) ha un impatto inferiore sul degradamento del segnale televisivo. A conferma di ciò, si osservino le buone prestazioni del TV2 nel canale 45, con segnale DVB-T (Figura) e con segnale DVB-T2 *n.e.* (Figura), e spaziatura tra canali adiacenti pari a 390 kHz in entrambi i casi.

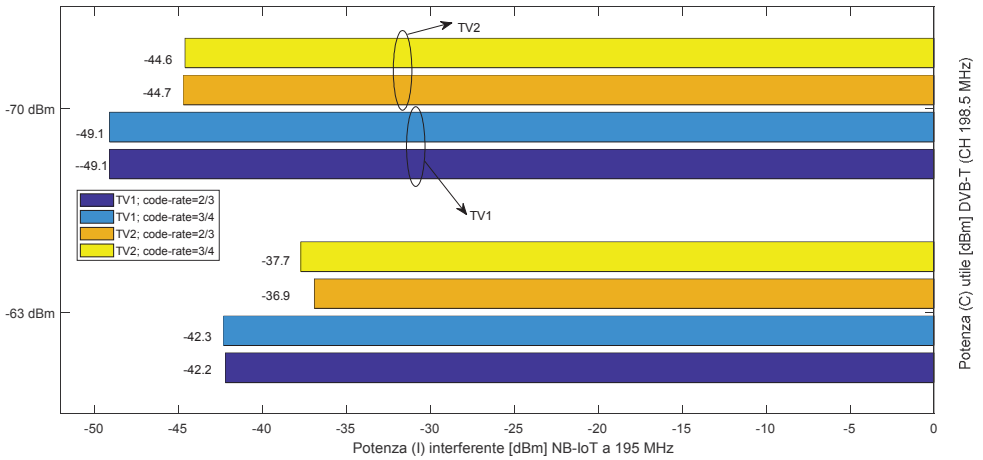


Figura 12. DVB-T - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 8 (198.5 MHz).

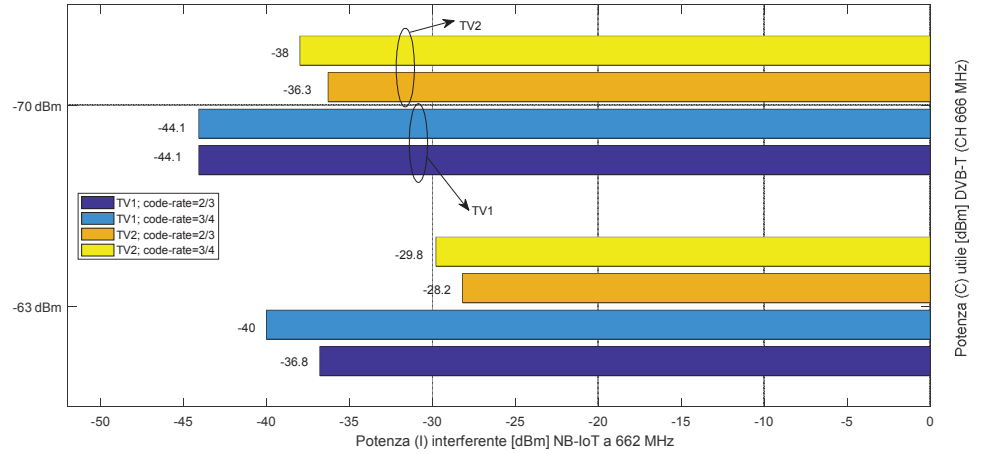


Figura 13. DVB-T - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 45 (666 MHz).

L'andamento delle prestazioni in termini di potenza interferente (I) varia anche a seconda delle impostazioni di code-rate. Nello specifico, con code-rate 2/3 il segnale televisivo è sempre più robusto

all'interferenza rispetto al caso di code-rate 3/4, a parità di altri parametri.

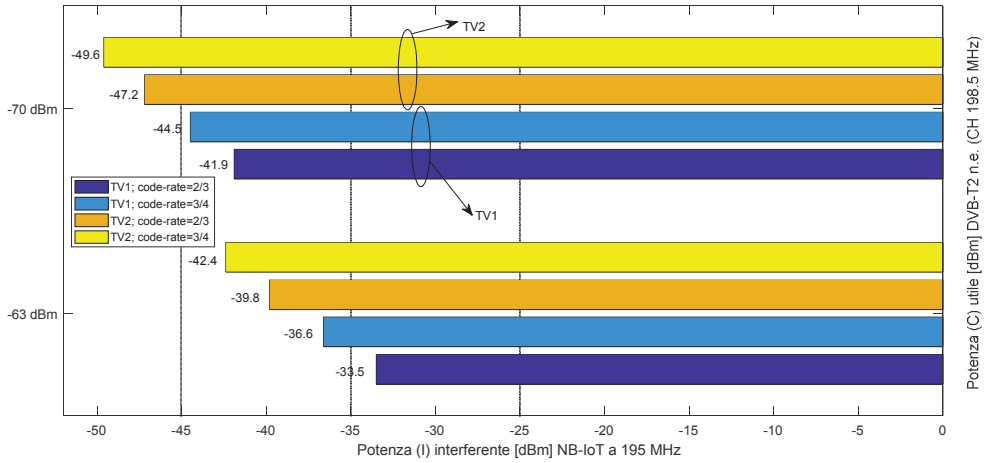


Figura 14. DVB-T2 non esteso - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 8 (198.5 MHz).

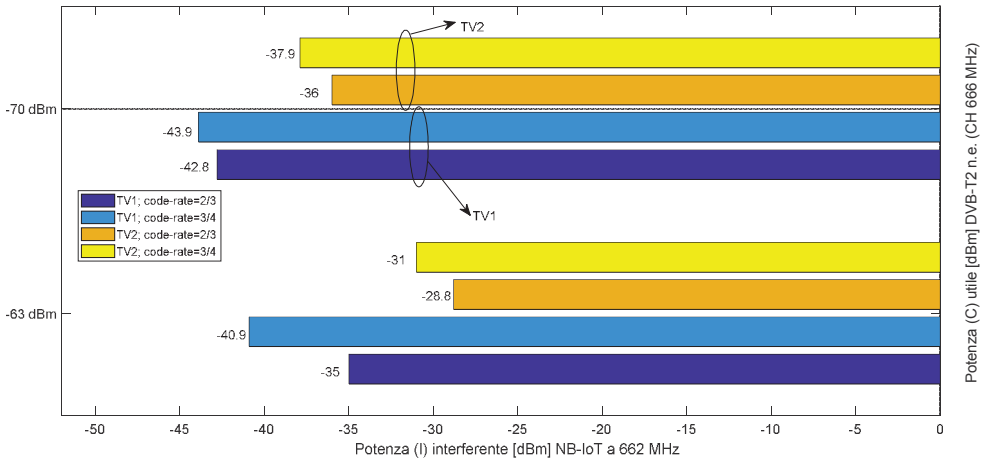


Figura 15. DVB-T2 non esteso - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 45 (666 MHz).

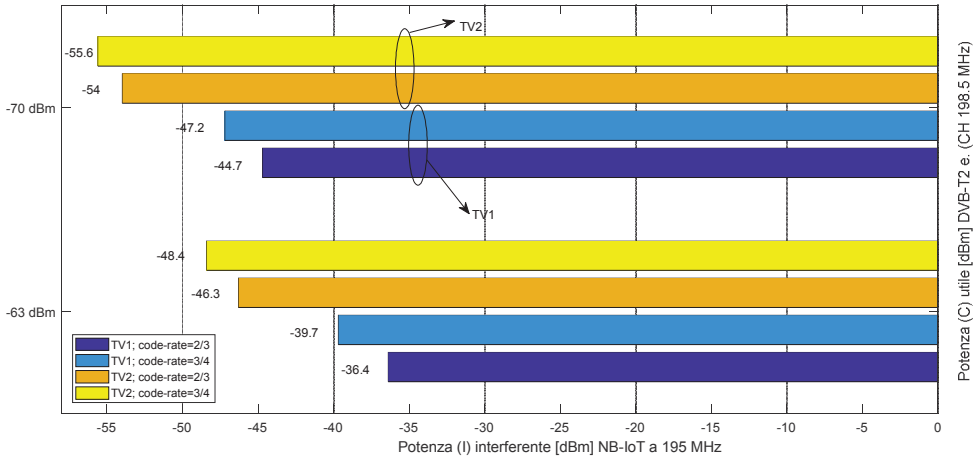


Figura 16. DVB-T2 esteso - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 8 (198.5 MHz).

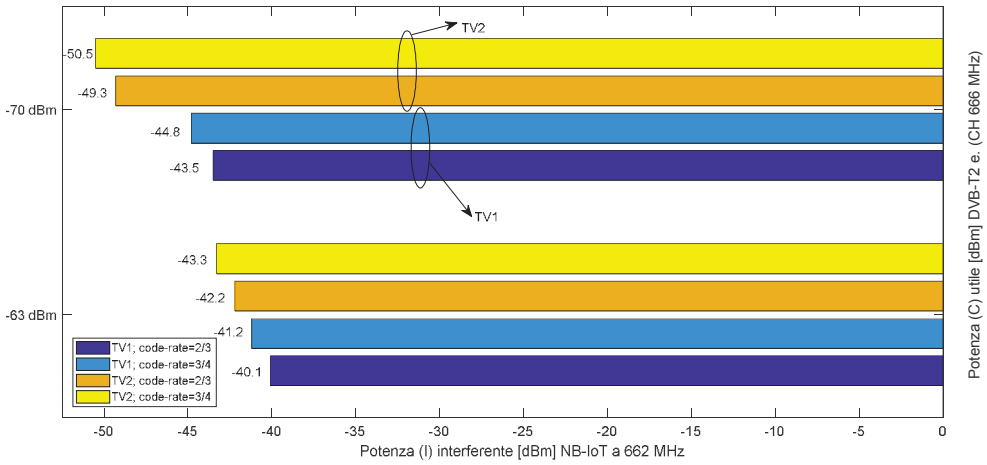


Figura 17. DVB-T2 esteso - Livello di potenza interferente IoT (I), all'ingresso dei DUT TV1 e TV2, che genera il fenomeno del quadrettamento a parità di potenza utile C=-63 dBm e C=-70 dBm e al variare del code-rate, per il canale 45 (666 MHz).

4. Interpretazione delle misure di potenza interferente: distanza di protezione

Le misure di laboratorio illustrate nei paragrafi precedenti hanno permesso di valutare il livello minimo di segnale interferente (IoT), all'ingresso del ricevitore televisivo, che consentisse di rispettare i già descritti requisiti di qualità (soglia di degradamento), al variare di prefissati livelli di segnale utile (DVB). Dalle misure di potenza

interferente limite, il passaggio successivo è consistito nell'effettuare un'analisi di link budget.

È possibile quindi ricavare, almeno in prima approssimazione, il valore limite del rapporto tra potenza irradiata (*EIRP* - Effective Isotropic Radiated Power) massima del segnale IoT e la distanza minima (d) tra stazioni radio base ed antenne televisive riceventi, per la salvaguardia della qualità della ricezione televisiva.

In particolare, nel caso di brevi distanze ed in assenza di ostacoli tra antenna trasmittente ed antenna ricevente ed assumendo valida l'ipotesi di propagazione in spazio libero,

$$P_{R=}P_T G_T G_R \left(\frac{c}{4\pi df}\right)^2 A$$

è possibile interpretare le misure di potenza interferente (I) e trarre alcune conclusioni a fronte dello studio presentato. Nell'equazione valida per propagazione in spazio libero, il termine $(c/4\pi df)^2$ corrisponde all'attenuazione di spazio libero FSPL (*free-space path loss*) mentre il termine A include effetti di attenuazione aggiuntiva [11].

Nel caso in questione tale equazione è la seguente e mette in relazione il valore limite di potenza *EIRP* e la rispettiva distanza di protezione d:

$$EIRP[dBm] - 20\log(d)\,[m] = I[dBm] - G_R[dBi] + 20\log(f)\,[MHz] + A_p[dB] + A_c[dB] - 27{,}6 \qquad (1)$$

con i seguenti parametri:

- $EIRP = P_T G_T$: potenza equivalente irradiata isotropicamente dall'antenna IoT in direzione dell'antenna TV (dBm);
- d: distanza tra l'antenna IoT e l'antenna ricevente TV (m);
- f: frequenza centrale del segnale IoT (MHz);
- G_R: guadagno dell'antenna ricevente riferito ad antenna isotropa alla frequenza f in direzione dell'antenna IoT (dBi);
- A_p: perdita per disadattamento in polarizzazione (dB);
- A_c: attenuazione del cavo dell'impianto d'antenna TV (dB);
- $I = P_R$: livello di potenza del segnale IoT all'ingresso del DUT (apparato televisivo) in corrispondenza del valore I/C critico (soglia di degradamento) (dBm).

I valori dell'*EIRP* e del guadagno dell'antenna ricevente si intendono misurati nella direzione in cui le due antenne (IoT e TV) sono in linea di vista.

La distanza di protezione (d) che viene ottenuta al variare dell'EIRP IoT nei seguenti grafici, rappresenta quella distanza per cui il segnale televisivo non viene interferito dal segnale proveniente dal downlink IoT. In Figura 18 vengono riportati i valori della distanza di protezione (espressa in metri) al variare dell'EIRP IoT (espresso in dBm) per code-

rate 2/3 al variare di standard del segnale voluto (DVB-T, DVB-T2 n.e., DVB-T2 e.) e frequenza del segnale IoT (195 MHz e 662 MHz) per entrambi i DUT (linea continua per TV1 e linea tratteggiata per TV2).

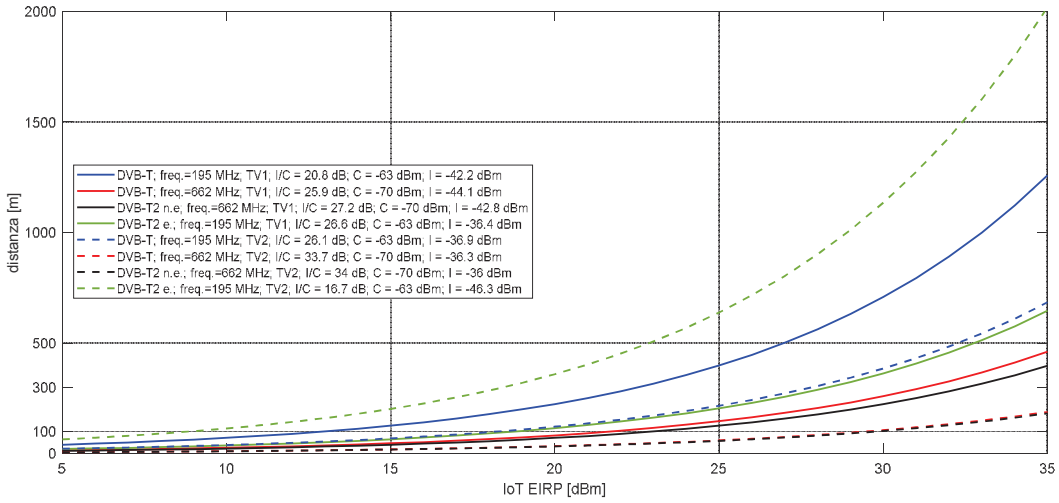


Figura 18. Distanza di protezione vs. EIRP; code-rate 2/3

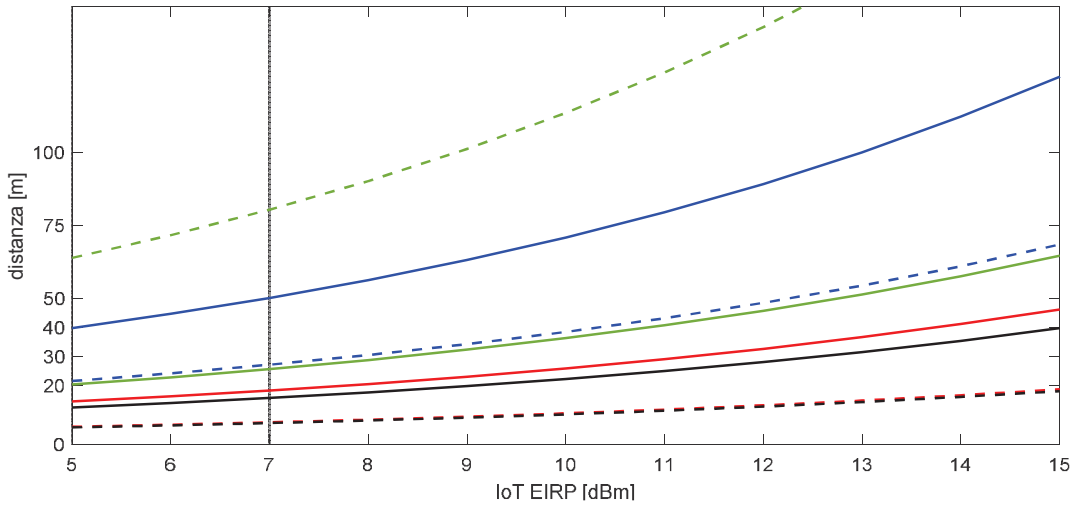


Figura 19. Distanza di protezione dalla Figura 18 , per EIRP da 5 a 15 dBm

In Figura 20, per completezza, vengono riportati i valori della distanza di protezione (espressa in metri) al variare dell'EIRP IoT (espresso in dBm) per code-rate 3/4 nelle stesse configurazioni riportate in Figura 18. L'EIRP IoT proviene dalla stazione radio-base, pensata per traffico IoT di

downlink, ed è fatto variare da 5 a 35 dBm in considerazione delle caratteristiche del segnale IoT a banda stretta (200 kHz) [17].

Nello specifico, a titolo esemplificativo sono estratti dai grafici in Figura 18 e Figura 20 degli scenari per il calcolo della distanza di protezione espressa dalla formula (1), dove G_R = 9 dBi, A_c= 3 dB.

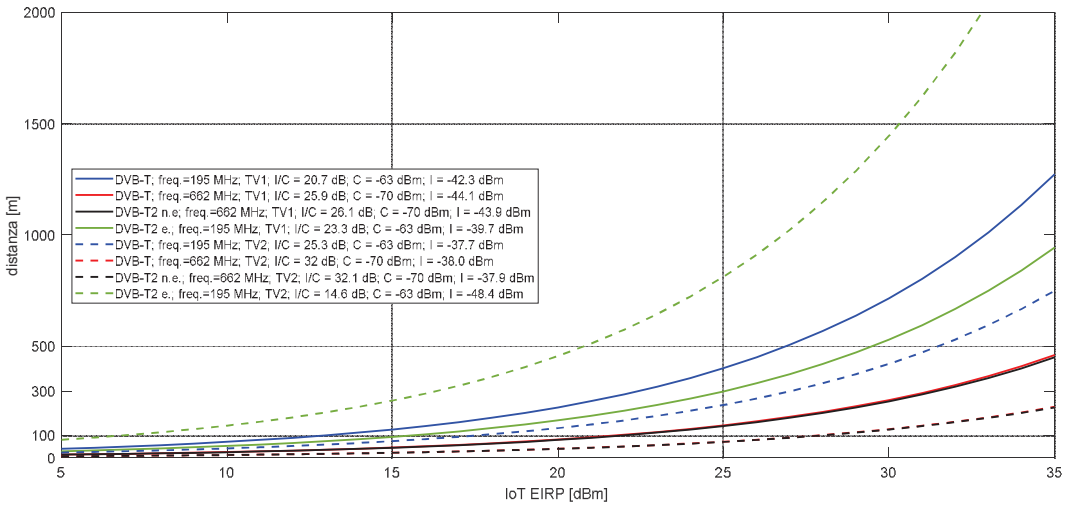


Figura 20. Distanza di protezione vs. EIRP; code-rate ¾

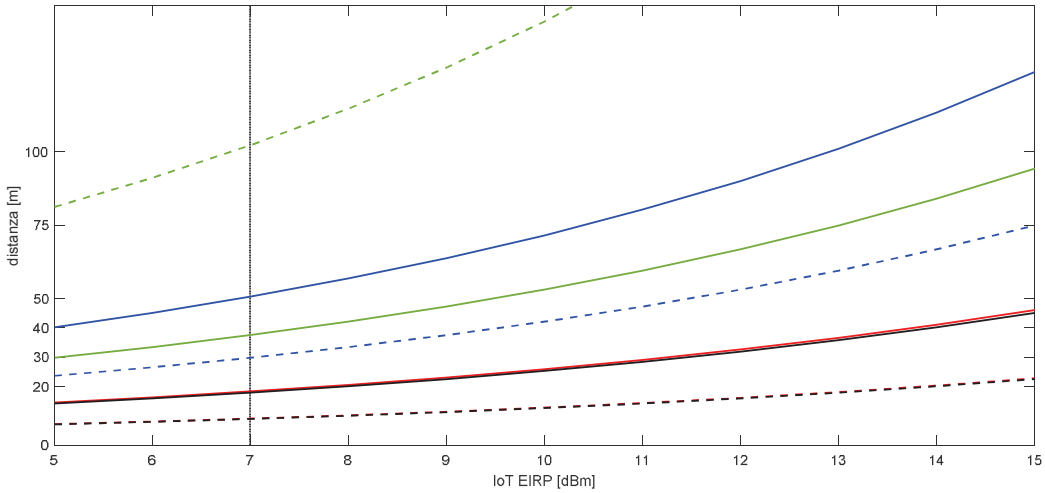
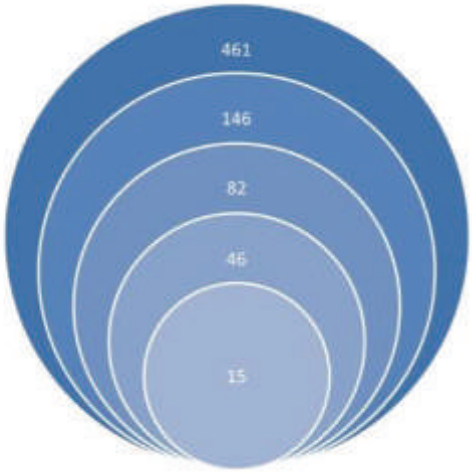


Figura 21. Distanza di protezione dalla Figura 20, per EIRP da 5 a 15 dBm

Esempio 1: Quadrettamento all'ingresso del ricevitore TV1, scenario da

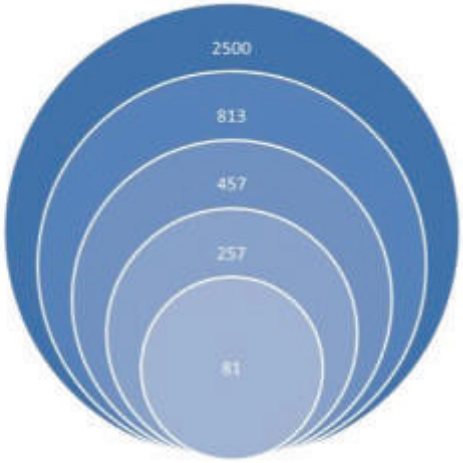
Figura 18 con code-rate 2/3 per standard DVB-T; freq.= 662 MHz; C = -70 dBm; I = -44.1 dBm; $A_p = 3\ dB\ (45°)$

NB-IoT Downlink EIRP [dBm]	d_{min} [m]
5	~15
15	~46
20	~82
25	~146
35	~461



Esempio 2: Quadrettamento all'ingresso del ricevitore TV2, scenario da Figura 20 con code-rate 3/4 per standard DVB-T2 *esteso*; freq.= 195 MHz; C = -63 dBm; I = -48.4 dBm; $A_p = 3\ dB\ (45°)$

NB-IoT Downlink EIRP [dBm]	d_{min} [m]
5	~81
15	~257
20	~457
25	~813
35	~2500



È evidente, quindi, dai valori delle distanze di protezione vs. EIRP, riportati nelle tabelle, che a seconda dei parametri del segnale DVB sono prevedibili scenari applicativi in cui la coesistenza in banda con il segnale IoT è possibile: in ambienti con bassa concentrazione di antenne televisive riceventi (quali zone rurali) - esempio 2 - o in ambienti più urbanizzati - esempio 1. Come accade nello scenario di coesistenza dell'esempio 1, in corrispondenza di più alti valori di I è tollerabile un più

alto livello di segnale interferente a parità di segnale utile. Ovvero, l'esempio 1 (DVB-T nelle UHF) rappresenta un caso con minore interferenza in uno prefissato scenario reale rispetto all'esempio 2 (DVB-T2 *e*. nelle VHF), per cui nel primo caso si potrebbe pensare ad applicazioni IoT a più lungo raggio mentre nel secondo caso ad applicazioni IoT a corto raggio.

5. Conclusioni

Nell'articolo sono stati presentati i risultati di una campagna di misure eseguite in laboratorio per simulare e validare l'introduzione di un potenziale servizio di trasmissione IoT a banda stretta (200 kHz) e basso bit-rate nelle bande VHF e UHF del servizio di broadcasting televisivo terrestre (DVB-T/T2). Il banco di misure, appositamente realizzato, è servito a testare la coesistenza della trasmissione IoT con il servizio televisivo digitale negli intervalli di frequenze tra canali televisivi adiacenti, valutando gli eventuali effetti interferenziali sul segnale televisivo che ha accesso primario in suddette bande.

La degradazione del servizio di trasmissione televisiva è stata valutata in termini di "quadrettamento" dell'immagine su schermo e misurata come livello di potenza interferente che genera il quadrettamento per un prefissato valore di segnale televisivo, misurati entrambi in ingresso al televisore. Gli scenari simulati hanno previsto l'impiego di impianti televisivi non dotati di amplificatore di testa. I risultati in termini di distanza di protezione vs. EIRP IoT permettono di valutare il dimensionamento della soluzione proposta per traffico IoT al variare delle caratteristiche del segnale televisivo.

Bibliografia

[1] RSPG 16-45 (European Commission RADIO SPECTRUM POLICY GROUP), «Draft Opinion on the Spectrum Aspects of the internet-of-things (IoT) including M2M,» Novembre 2016.
[2] M. Fuentes, C. Garcia-Pardo, E. Garro, D. Gomez-Barquero e N. Cardona, «Coexistence of Digital Terrestrial Television and Next Generation Cellular Networks in the 700 MHz band,» IEEE Wireless Communications, vol. 21, n. 6, pp. 63-69, 2014.
[3] S. Yrjola, E. Huuhka, P. Talmola e T. Knuutila, «Coexistence of Digital Terrestrial Television and 4G LTE Mobile Network Utilizing Supplemental Downlink Concept: A Real Case Study,» IEEE Transactions on vehicular technology , vol. 66, n. 6, pp. 5422 - 5434, 2017.
[4] RSPG 16-031 European Commission RADIO SPECTRUM POLICY GROUP, «RSPG Strategic roadmap towards 5G for Europe-Draft RSPG Opinion on spectrum related aspects for next-generation wireless systems (5G),» 2016.
[5] F. Rancy, «Sviluppo di standards e allocazione dello spettro in supporto di IMT-2020 (5G),» ITU Radiocommunication Bureau, 29 Marzo 2017.
[6] Recommendation ITU-R M.2083-0 (09/2015), «IMT Vision - Framework and overall objects of the future development of IMT for 2020 and beyond,» 2015.
[7] A. Biral, M. Centenaro, A. Zanella, L. Vangelista e M. Zorzi, «The challenges of M2M massive access in wireless cellular networks,» Digital Communications and Networks, vol. 1, n. 1, pp. 1-19, 2015.
[8] R. S. Sinha, Y. Wei e S.-H. Hwang, «A survey on LPWA technology: LoRa and NB-IoT,» ICT Express, vol. 3, n. 1, pp. 14-21, 2017.
[9] Rivista, «Mondo Digitale,» AICA Associazione italiana per l'Informatica ed il Calcolo Automatico, Febbraio 2018.
[10] ECC Report 266, «The suitability of the current ECC regulatory framework for the usage of Wideband and Narrowband M2M in the frequency bands 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2.1 GHz and 2.6 GHz,» Giugno 2017.
[11] M. Ferrante, G. Fusco, E. Restuccia, M. Celidonio, P. G. Masullo e L. Pulcini, «Experimental results on the coexistence of TV broadcasting service with LTE mobile systems in the 800 MHz band,» in 2014 Euro Med Telco Conference (EMTC), 2014.
[12] ETSI EN 301 598 V2.1.1 (2018-01), «White Space Devices (WDS); Wireless Access Systems operating in the 470 MHz to 790 MHz TV broadcast band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU,» 2018.
[13] Whitepaper Rohde & Schwarz, « Narrowband Internet of Things Measurements,» 2017.

[14] Whitepaper Rohde & Schwarz, «Narrowband Internet of Things,» 2016.
[15] ETSI EN 302 296 V2.0.2 (2016-10), «Digital Terrestrial TV Transmitters; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU,» 2016.
[16] ETSI EN 303 340 V1.1.2 (2016-09), «Digital Terrestrial TV Broadcast Receivers; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU,» 2016.
[17] Whitepaper Huawei, «NB-IoT Enabling New Business Opportunities,» 2015.
[18] ITU-R BT.2215-7 (04/2018), «Measurements of protection ratios and overload thresholds for broadcast TV receivers,» 2018.
[19] J. Finnegan e S. Brown, «A Comparative Survey of LPWA Networking,» arXiv preprint arXiv:1802.04222. , 2018.

Dario De Leonardis
(Ricercatore dell'Università "La Sapienza" di Roma presso Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Frank Silvio Marzano
(Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni dell'Università "La Sapienza" di Roma)

Silvia Di Bartolo, Vincenzo Attanasio
(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Collegamenti ibridi Free-Space Optics/Radio Frequency (FSO/RF) per rete di fronthaul all'interno del paradigma 5G

Hybrid Free-Space Optics / Radio Frequency (FSO/RF) links for fronthaul network within 5G paradigm

Sommario: *I sistemi di trasmissione ibridi Free Space Optics / Radio Frequency (FSO/RF) sono emersi recentemente come una delle soluzioni ottimali di integrazione con le tratte in fibra ottica, per mantenere alti flussi-dati in quella sezione della rete, in letteratura tecnica nota come fronthaul, che realizza l'accesso al backhaul: queste due sezioni della rete costituiscono un ponte tra le stazioni radio-base e la rete centrale, il quale permette di superare il cosiddetto problema del collo di bottiglia in merito alla distribuzione del carico informativo tra le maglie del sistema radio-mobile. Ai progressi in termini di efficienza nell'impiego delle risorse, la soluzione ibrida FSO/RF aggiunge altri vantaggi, come quelli derivanti dalla riduzione del consumo energetico e dei costi di dispiegamento della rete e si candida pertanto come una delle più innovative forme di integrazione tecnologica all'interno del paradigma 5G attualmente in linea di sviluppo. Nel presente articolo verranno messi in luce, dal punto di vista prestazionale e del costo di rete, quali e quanti gradi di libertà permettano alla tecnica di trasmissione ibrida FSO/RF di migliorare il servizio complessivo laddove i collegamenti in spazio libero si rivelano necessari per affiancare la fibra ottica nelle odierne strutture di fronthauling.*

Abstract: *HybridFree-Space Optics / Radio Frequency (FSO/RF) systems have recently emerged as one of the most promising solutions integrating optical fiber segments that are able to keep high data-rates in that network section, known in technical literature as fronthaul, which provides the access to backhaul: these two network sections compose a bridge between the base stations and the core network that allows to overcome the so-called matter of bottleneck with respect to the distribution of information load among the links of the radio-mobile system. Hybrid FSO/RF solution can provide other advantages besides the improvement in terms of spectral efficiency, as the ones deriving by energy saving and the reduction of deployment network costs; thus, it becomes a serious and original candidate to be one of the main technological proposals for the developing 5G paradigm. In the present paper, how the employment of FSO/RF transmission technique may improve the overall service in the case that free space links show to be necessary to sustain optical fiber in today fronthauling architectures, will be highlighted from the perspective of link performance and average network cost analysis.*

1. Introduzione

La nuova generazione di rete mobile (5G) è proiettata verso una gestione sempre più flessibile del servizio e non si limita a conservare o migliorare quello di base (fonia) e quelli già garantiti dai precedenti modelli sviluppati (3G e 4G), ma mira anzi a inglobare altri servizi, come ad esempio "Internet of Things", in un panorama sempre più composito e multiforme dei sistemi di telecomunicazione. Le tecnologie dispiegate per un contesto di rete così eterogeneo devono necessariamente essere varie e duttili a possibili cambiamenti infrastrutturali o di assetto nel trasferimento delle informazioni; la ricerca sta muovendo pertanto verso l'integrazione di supporti già studiati in letteratura, ma considerati ad hoc per la nuova generazione, come ad esempio le Ultra-Dense Networks (UDNs) ed il Multiple-Input-Multiple-Output (MIMO) massivo, per incrementare l'efficienza spettrale delle comunicazioni mobili 5G e ridurre, al contempo, il consumo energetico come necessario nello sviluppo delle reti future [1].

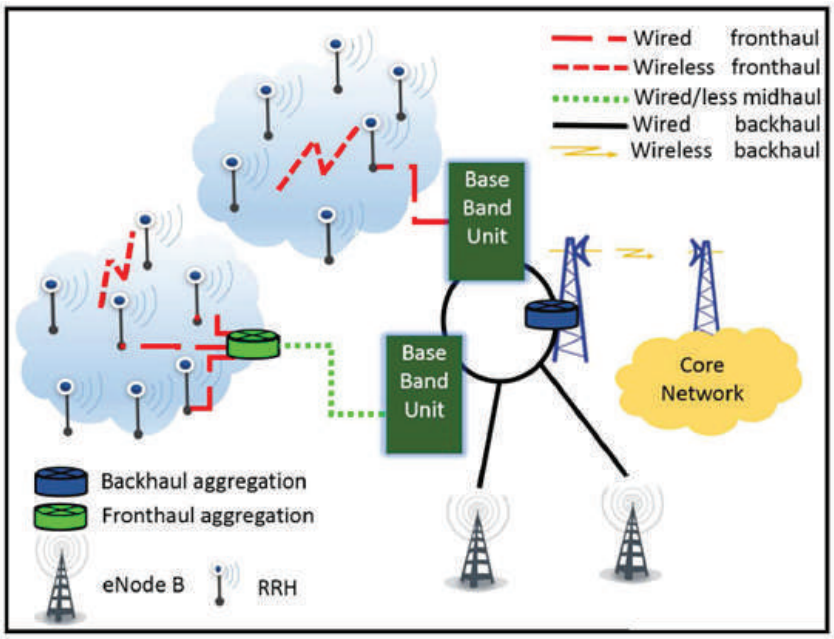


Figura 1. Esempio di rete mobile 5G, divisa in fronthaul, midhaul e backhaul:
I) il fronthaul copre l'ultimo miglio (rete d'accesso);
II) il midhaul riguarda il collegamento tra fronthaul e il backhaul;
III) il backhaul connette le Base Band Units (BBUs) alla sezione centrale della rete.

Anche a livello fisico si prevede un'ampia gamma di soluzioni applicative, in particolare nel sistema costituito da fronthaul e backhaul (vedi Figura 1), quel duplice strato della rete di trasporto interna che media la comunicazione tra le stazioni radio-base (Base Transceiver Stations - BTSs), i nodi di rielaborazione del segnale noti in letteratura come Base Band Units (BBUs) e la sezione centrale della rete (core network), tradizionalmente caratterizzato da collegamenti in fibra ottica (OF) e wireless (microonde) e occasionalmente da doppino in rame o collegamenti satellitari. Uno studio condotto nel 2014 mostra che l'infrastruttura in fibra ottica per fronthaul/backhaul non è garantita in tutte le nazioni europee e il suo rimpiazzamento con collegamenti nelle microonde non sembra in grado di sostenere la crescita del traffico di

rete, per l'impiego delle tecnologie LTE, prevista nel biennio 2017-2018 [2]. E' opinione comune che un rinnovamento di questa doppia sezione della rete si rivela dunque necessario, specialmente se considerato in prospettiva del paradigma 5G. Tuttavia, bisogna aggiungere che, in Italia, la gestione delle risorse riguardanti il dimensionamento del segmento di rete del backhaul, in vista del piano 5G, verte piuttosto all'impiego massivo di soluzioni già consolidate, come la fibra ottica, in grado di creare collegamenti considerevolmente capaci per molti chilometri di distanza e garanti di affidabilità.

Diverso è il quadro relativo al segmento di rete del fronthaul, in cui la convivenza tra la fibra ottica e altre tecnologie di trasmissione come quelle in spazio libero sembra invece possibile, dal momento che la dimensione cellulare della copertura di servizio prevista dal sistema 5G risulta molto varia e dipende piuttosto dalle caratteristiche orografiche del terreno o dalla necessità di coprire solo aree geografiche ben circoscritte, nel raggio di pochi chilometri. In questo scenario, l'adozione di tecnologie di recente raffinamento quali le onde millimetriche (che, coprendo la banda compresa tra 70 e 80 GHz, possiamo considerare Radio Frequency – RF) [3] e i collegamenti ottici in spazio libero (Free Space Optics – FSO, che copre la parte dello spettro superiore ai 300 GHz) [4] permette di incrementare notevolmente la banda di trasmissione rispetto ai dispositivi che operano nelle microonde (la cui banda è compresa tra i 6 e i 60 GHz): infatti si possono sperimentare flussi-dati (throughput) di down-stream e up-stream che arrivano fino a 10 Gb/s (nelle microonde si raggiunge 1 Gb/s) anche per tratte in linea di visibilità di 3 km, senza dover cedere alle restrizioni di latenza (che resta minima) che sono tipiche dei collegamenti in spazio libero [2].

Ove non sia possibile implementare la fibra ottica per motivi orografici o di efficienza costi/benefici, la soluzione combinata delle due tecnologie (onde millimetriche e ottica di spazio libero), chiamata in letteratura sistema ibrido FSO/RF, garantirebbe persino una maggiore stabilità rispetto alla variazione delle condizioni atmosferiche e di puntamento, che rappresentano da sempre un vero tallone d'Achille per i collegamenti FSO, consentendo il recupero di segnale grazie ad una semplice commutazione.

2. Sistema Ibrido FSO/RF: Stato dell'Arte

Nel contesto delle comunicazioni ottiche in spazio libero, i collegamenti ibridi FSO/RF sono al centro dell'interesse della ricerca contemporanea, specialmente per quanto attiene al dimensionamento di alcune sezioni della rete 5G (ad esempio con interventi occasionali a livello di fronthaul, come sopra osservato). Un motivo non indifferente che spinge in questa direzione riguarda non tanto la chiara possibilità di mantenere l'efficienza spettrale del collegamento, comunque garantita dai numeri di banda prima citati, ma la necessità di progettare reti a costi ridotti [5] e basso consumo energetico (meno impattanti sull'ambiente, cioè più "green" come da protocollo UE), per mezzo di

una soluzione che si mantiene purtuttavia attigua ai già collaudati impianti in fibra ottica. Oltretutto, se le tecnologie tradizionali del campo includono sistemi a radiofrequenza o in fibra ottica, è semplice intuire che un collegamento RF è più ridotto nei costi ma trasmette a più basse bit-rate rispetto ad uno OF. Pertanto, la scelta di impiegare un collegamento FSO, ridotto nei costi e potenzialmente capace in termini di bit-rate, risulta promettente, in special modo quando viene applicato in una soluzione ibrida con il sistema RF, combinazione che permette di consolidare i vantaggi di entrambe le tecniche trasmissive. Nella fattispecie, le comunicazioni ottiche in spazio libero sono molto sensibili al cambiamento delle condizioni atmosferiche e di puntamento: in particolare, la presenza di nebbia o di turbolenza (variazione dell'indice di rifrazione locale) come eventuali errori di puntamento della sorgente laser possono causare ampie fluttuazioni tanto nell'intensità quanto nella fase del segnale ricevuto e di conseguenza intaccare pesantemente le prestazioni del collegamento. Per aggirare il problema sono state proposte in letteratura diverse soluzioni, come, ad esempio, il "multi-hop relaying", che consiste nella mediazione di alcuni relays nella trasmissione dell'informazione fino a destinazione [6], e, appunto, l'ibrido FSO/RF, che accoppia due tecnologie sostanzialmente complementari, dato che FSO è sensibile a determinate condizioni atmosferiche come la nebbia, che non inficiano minimamente i dispositivi RF, i quali, di contro, risultano tuttavia molto sensibili alla caduta di forti piogge [7].

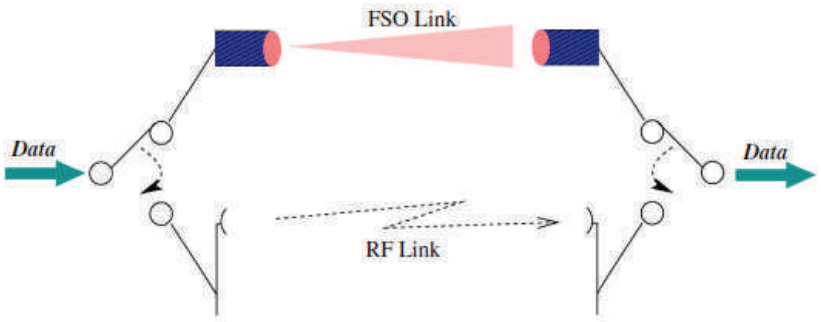


Figura 2. Diagramma a blocchi di un sistema FSO/RF ibrido con commutazione esclusiva (hard-switching)

Fondamentalmente esistono due configurazioni tipiche di sistema ibrido FSO/RF: i) a commutazione esclusiva (hard switching) - mostrato in Figura 2 - in cui, quando le condizioni atmosferiche sono perfette, il collegamento FSO è attivo ma non quello RF, viceversa altrimenti; ii) a commutazione inclusiva (soft switching), in cui i due collegamenti operano in parallelo attraverso la codifica di canale. In [8] viene mostrato un sistema di comunicazione ibrido FSO/RF basato su adaptive combining, una configurazione che permette di sfruttare al massimo le risorse spettrali: infatti, in questo scenario, finché il rapporto segnale-rumore istantaneo (Signal-to-Noise Ratio - SNR) misurato in ricezione resta al di sopra di una determinata soglia, il solo collegamento FSO resta attivo; quando tale rapporto scende al di sotto di questa, viene attivato il collegamento RF in parallelo a quello FSO e i segnali corrispondenti ai due canali di trasmissione vengono poi ricombinati in ricezione attraverso un sistema dual-branch Maximal Ratio Combining

(MRC). Questo schema permette di sommare al già considerato vantaggio del miglioramento dell'affidabilità in quanto al collegamento complessivo (che combina le caratteristiche complementari degli apparati FSO e RF) le seguenti migliorie rispetto alle configurazioni tipiche di cui sopra: i) una riduzione notevole della frequenza di commutazione (rispetto ad una configurazione tipica hard switching); ii) l'assenza di un dispositivo che irradi continuamente campo RF, che potrebbe interferire nell'ambiente circostante, oltre a causare un maggiore dispendio energetico (rispetto ad una configurazione soft switching); iii) i massimi benefici che si possono trarre da un collegamento FSO, come un alto data-rate, mantenuti per la maggior parte del tempo disponibile (sempre in relazione ad una configurazione soft switching, la quale prevede il livellamento del data-rate del collegamento FSO per poi ricombinarlo adeguatamente con il flusso parallelo proveniente dal collegamento RF). Si tratta di uno schema che rappresenta pertanto una soluzione di compromesso evidente tra le due configurazioni tipiche di switching.

3. Sistema Ibrido FSO/RF: Analisi delle Prestazioni

Per quanto riguarda lo studio delle prestazioni del sistema ibrido FSO/RF, ci atteniamo alla valutazione di quei parametri che tradizionalmente vengono presi in considerazione per descrivere la qualità del collegamento, e, conseguentemente, dell'applicazione ad essa associata, cioè la probabilità di fuori servizio (outage probability), la Bit Error Probability (BER) e la capacità ergodica [9]. Procedendo secondo le assunzioni di un sistema ibrido FSO/RF standard, come quello illustrato in [10], in cui viene proposta un'architettura a bassa complessità (low-complexity) con schema di commutazione hard switching che impiega un collegamento FSO in combinazione con uno RF alle onde millimetriche (che trasmette alla frequenza di 60 GHz), ne ripercorriamo l'analisi, al fine di mostrare piuttosto chiaramente, a titolo di esempio, i vantaggi che derivano da una tecnica trasmissiva composita, nei confronti del solo collegamento ottico, a livello di prestazione.

In questo scenario di comunicazione, il collegamento FSO viene utilizzato finché il rapporto segnale-rumore istantaneo del canale ottico resta al di sopra di una data soglia γ_{th}^{FSO}. Quando l'SNR del collegamento FSO scende al di sotto della soglia, allora il sistema verifica la qualità del canale RF: se l'SNR di quest'ultimo è a sua volta al di sopra di una specifica soglia γ_{th}^{RF}, il collegamento RF viene attivato per la trasmissione. Ma se entrambi i rapporti segnale-rumore sono al di sotto delle rispettive soglie, il sistema dichiara di essere fuori servizio (outage). Gli autori di [10] definiscono σ_x come la varianza della distribuzione log-normale che descrive il comportamento delle fluttuazioni del segnale ottico dovute alla turbolenza e indicano con m lo shape parameter della variabile Nakagami che descrive l'andamento del canale RF.

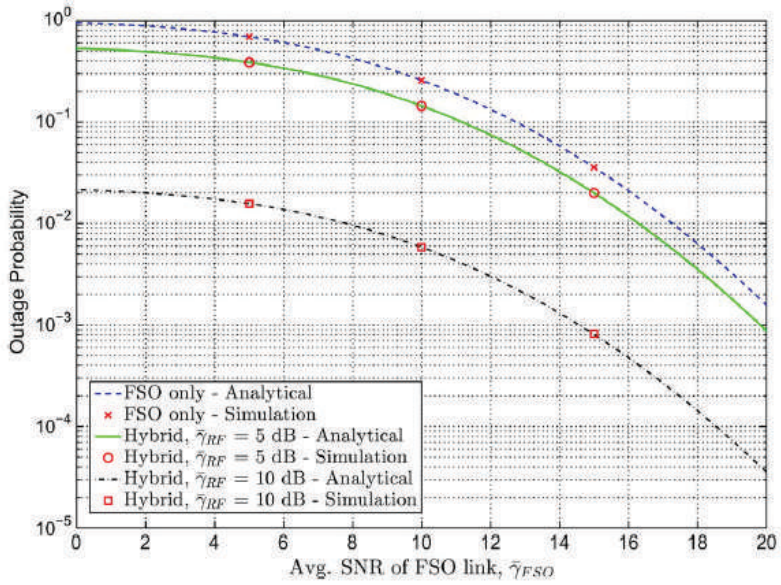


Figura 3. Probabilità di fuori servizio (outage probability) in funzione del rapporto segnale-rumore del collegamento FSO, quando le soglie $\gamma_{th}^{FSO} = \gamma_{th}^{RF} =$ 5 dB, m = 5 e $\sigma_x = 0.25$.

La Figura 3 mostra l'andamento della probabilità di fuori servizio al variare del rapporto segnale-rumore del collegamento FSO (γ_{FSO}) in tre differenti scenari applicativi: i) il solo collegamento FSO; ii) un collegamento ibrido FSO/RF con rapporto segnale-rumore del canale RF basso (γ_{RF} = 5 dB); iii) un collegamento ibrido FSO/RF con SNR del canale RF alto (γ_{RF} = 10 dB). Viene dimostrato (attraverso un modello analitico suffragato da risultati di simulazione) come un collegamento ibrido FSO/RF permetta di ridurre la probabilità di fuori servizio rispetto al solo sistema FSO: naturalmente, quanto più sarà alto il rapporto segnale-rumore del canale RF, tanto più sarà bassa la probabilità di outage che l'intera configurazione sperimenterà.

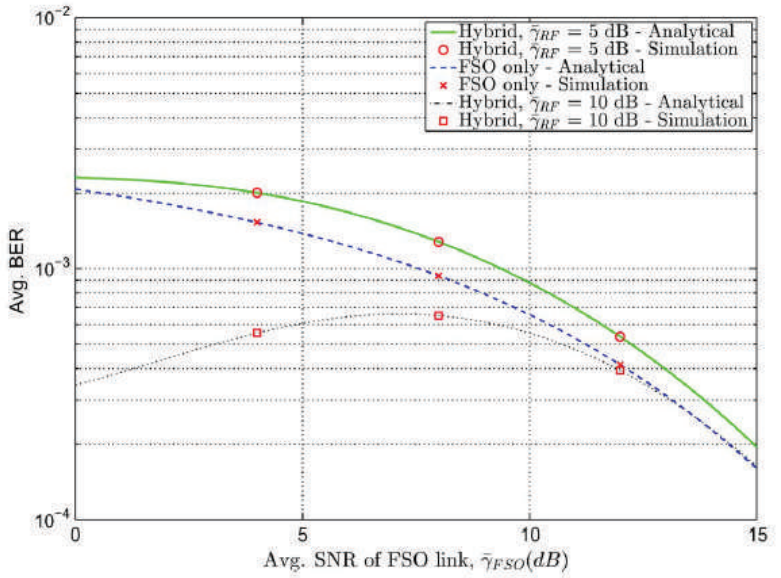


Figura 4. Probabilità d'errore (Bit Error Rate - BER) in funzione del rapporto segnale-rumore del collegamento FSO, quando le soglie $\gamma_{th}^{FSO} = \gamma_{th}^{RF} =$ 5 dB, m = 5 e $\sigma_x = 0.25$.

La Figura 4 mostra le curve di BER al variare del rapporto segnale-rumore del collegamento FSO negli stessi scenari applicativi sopra descritti. Come si nota, in materia di probabilità d'errore, che viene

valutata sulla sezione dati in cui il collegamento è attivo (o in servizio), quando viene impiegato un collegamento ibrido FSO/RF con basso SNR per il canale RF (5 dB), si ha un leggero deterioramento nelle prestazioni rispetto al solo sistema FSO: questo accade perché il servizio non viene sospeso come nel caso del singolo FSO, ma nella trasmissione viene utilizzato il più delle volte un canale RF di bassa qualità che finisce per intaccare il livello medio di BER. Infatti, quando l'SNR del canale RF sale a 10 dB, le prestazioni complessive del collegamento ibrido FSO/RF migliorano notevolmente: in particolare, al crescere dell'SNR del canale FSO accade che, quando tale valore è ancora basso, laddove viene impiegato più frequentemente il canale RF ad alto SNR, si ha un deterioramento graduale delle prestazioni per il collegamento complessivo fintantoché il canale FSO non comincia ad essere utilizzato con maggiore frequenza (il sistema FSO diviene più affidabile: cresce il suo SNR) e il valore medio di BER corrispondente torna a scendere.

La Figura 5 rappresenta un confronto delle prestazioni dei tre sistemi prima considerati a livello di capacità ergodica: si nota come l'impiego di un collegamento ibrido FSO/RF permetta di migliorare la capacità complessiva del sistema rispetto al singolo canale ottico, in particolare per bassi valori di γ_{FSO}. Oltretutto, se la qualità del collegamento RF è alta (γ_{RF} = 10 dB), la capacità complessiva, quando viene valutata per bassi valori dell'SNR del canale ottico, decresce leggermente fino a toccare un minimo, dal momento che in questo intervallo sono più frequenti le commutazioni al canale RF, per poi risalire, al crescere di γ_{FSO}.

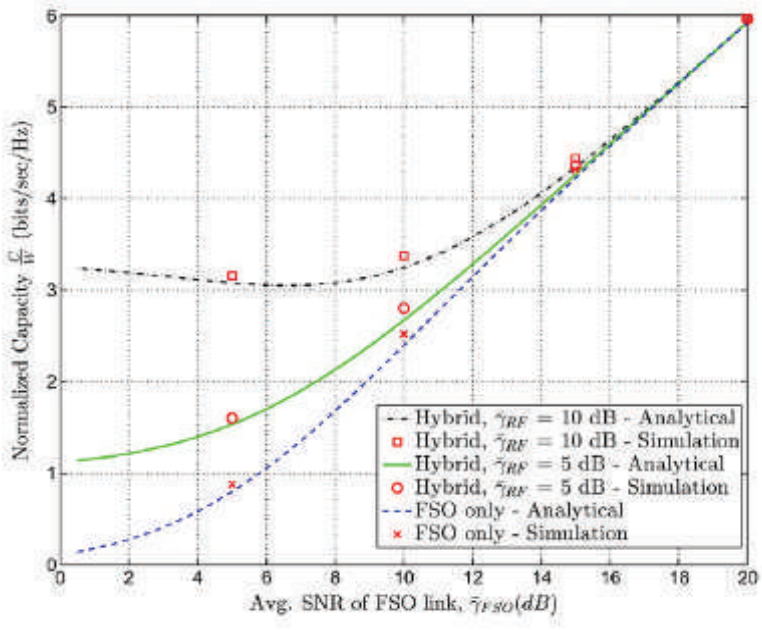


Figura 5. Capacità ergodica in funzione del rapporto segnale-rumore del collegamento FSO, quando le soglie $\gamma_{th}^{FSO} = \gamma_{th}^{RF}$ = 5 dB, m = 5 e σ_x = 0.25

Gli autori di [10] propongono anche un modello di commutazione a due soglie per il collegamento FSO, onde abbassare la frequenza delle transizioni on/off [11], che riducono il tempo di vita del sistema di comunicazione ottico: in questa configurazione, il collegamento FSO

continua a trasmettere finché il suo SNR non scende al di sotto di una determinata soglia; poi resta inattivo fintantoché il suo SNR non supera una seconda soglia, più alta della prima. Il sistema RF verrà impiegato quando il suo SNR supererà la soglia corrispondente mentre il canale FSO risulta inattivo. E' semplice intuire che maggiore è la differenza tra le due soglie usate per il canale FSO, minore la frequenza di transizione on/off del sistema di trasmissione ottico. Gli autori di [10] dimostrano, svolgendo un'analisi comparativa delle prestazioni – sempre in termini di probabilità di outage, BER e capacità ergodica, che il comportamento del sistema ibrido FSO/RF a soglia doppia per il canale FSO non differisce sostanzialmente da quello a soglia singola e risulta dunque più vantaggioso da un punto di vista pratico-implementativo.

Gli autori di [12], d'altro canto, riprendono il medesimo percorso di studio del sistema ibrido FSO/RF analizzato in [10], con l'aggiunta di un diverso modello di turbolenza per il canale FSO (la distribuzione Gamma-Gamma al posto della log-normale) e di fading per il collegamento RF (Rice al posto di Nakagami), derivando un'espressione in forma chiusa del BER per il sistema FSO in presenza di attenuazione da turbolenza combinata agli errori di puntamento (ribattezzata come condizione di combined fading) e dimostrando infine come un apparato ibrido FSO/RF possa superare di gran lunga in prestazioni il singolo dispositivo ottico in uno scenario di forte turbolenza.

4. Efficienza nei costi di dimensionamento del fronthaul

In quanto ai vantaggi economici derivanti dall'impiego di una simile tecnologia all'interno di un sistema di comunicazione radiomobile (concettualmente estendibile ai sistemi 5G), gli autori di [5] considerano il problema della minimizzazione del costo di rete attraverso la scelta di collegamenti in fibra ottica o in spazio libero, della tipologia FSO/RF, come illustrato in Figura 6, arrivando a dimostrare come tale soluzione ibrida di trasmissione sia in grado di garantire una certa efficienza in termini di costo e rappresenti pertanto un buon candidato per l'aggiornamento di molti segmenti della rete attualmente in funzione. Infatti, la scelta di impiegare la tecnologia più adeguata nel contesto progettuale delle reti di fronthaul (nel caso di architetture 5G) o più genericamente di backhaul, risulta oggi, a livello internazionale, di grande interesse, in special modo per quanto attiene ai costi di dispiegamento, che, nel caso di architetture di rete 4G, possono ammontare approssimativamente fino al 50 % dei costi totali [5]; col dispiegamento di piccole celle multiple e capillarmente diffuse atteso nel paradigma 5G, è realistico credere che i costi di implementazione siano destinati a crescere.

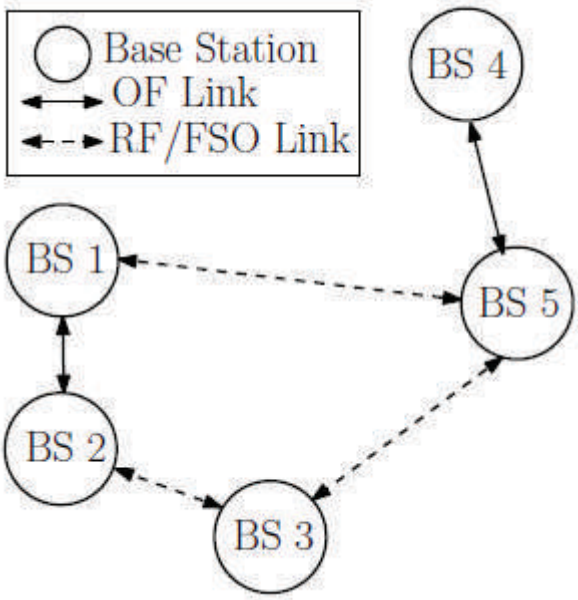


Figura 6. Esempio di rete composta da 5 stazioni radio-base connesse via fibra ottica (OF) o collegamenti ibridi FSO/RF.

Sempre attenendoci a [5] ma trasferendo il piano del discorso nel contesto 5G, come è possibile osservare dalla Figura 7, prendendo in considerazione tre sistemi di fronthaul, il primo ottimale ma interamente realizzato in cavo ottico (OF), il secondo derivante da una soluzione "euristica" (approssimazione analitica del caso ottimale) che può includere sia collegamenti OF che ibridi del tipo FSO/RF, il terzo ottenuto mediante algoritmo di ottimizzazione (che include, come il precedente, tanto segmenti di rete OF quanto collegamenti FSO/RF), notiamo che l'ammontare medio dei costi totali della rete si riduce quando i costi medi dei collegamenti FSO/RF risultano inferiori ($\pi^{(h)}$ = 10000/20000 dollari) al cosiddetto termine di cut-off ($\pi^{(h)}$ = 40000 dollari), il quale corrisponde al costo di un singolo collegamento in fibra ottica che soddisfa, a differenza di quelli in spazio libero, determinati requisiti di data-rate e affidabilità.

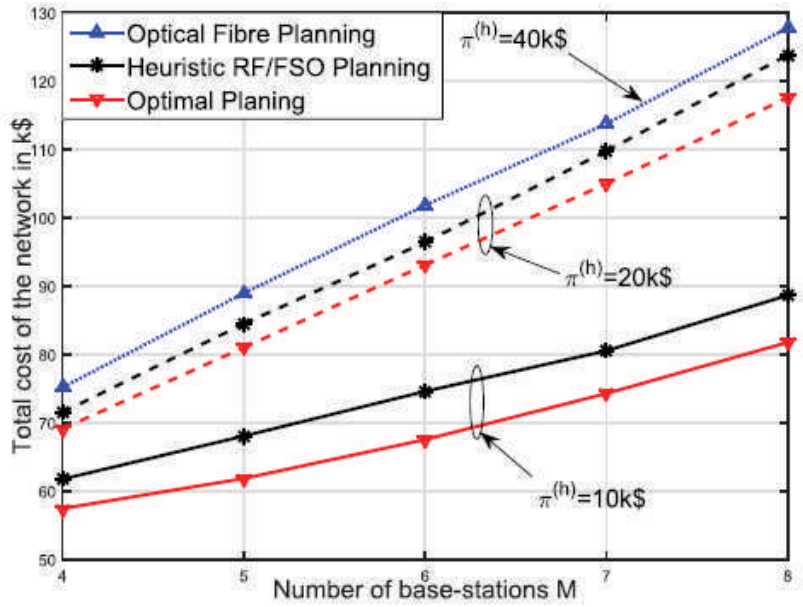


Figura 7. Costo medio della rete in funzione del numero delle stazioni radio-base M impiegate nella costruzione del fronthaul.

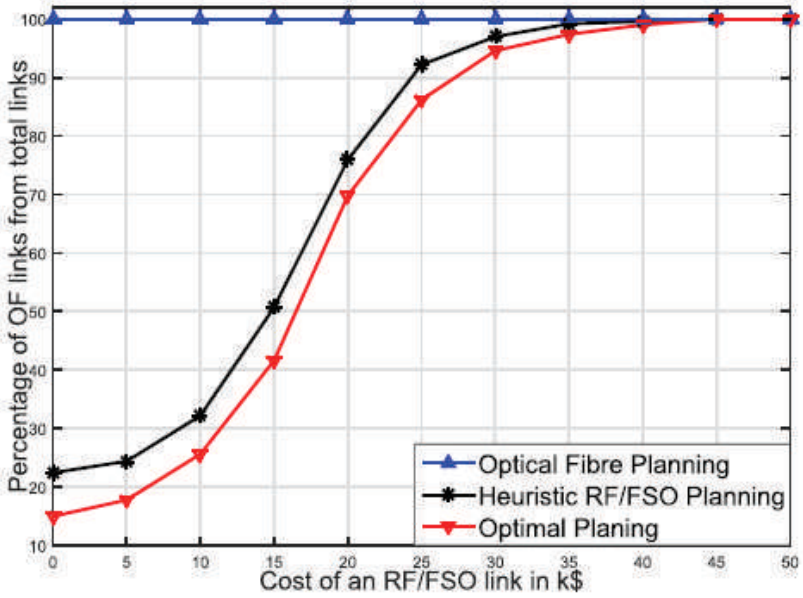


Figura 8. Percentuale di connessioni OF in funzione del costo dei collegamenti ibridi FSO/RF per una rete costituita da 7 nodi.

Dalla Figura 8 è possibile notare come la percentuale dei collegamenti OF all'interno di una rete ottimale di fronthaul composta da 7 nodi tende a crescere piuttosto rapidamente quando i costi medi dei collegamenti FSO/RF sono superiori ai 10000 dollari.

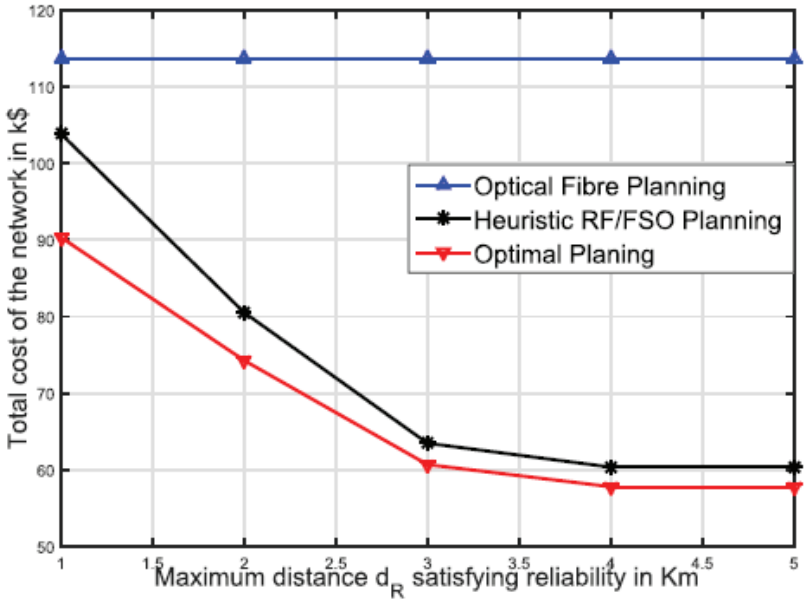


Figura 9. Costo medio della rete in funzione della massima distanza che soddisfi un requisito di affidabilità α per un sistema costituito da 7 nodi.

La Figura 9 mostra invece come il costo medio della rete ottimale mista di fronthaul (seconda e terza soluzione prima elencate) decresce all'aumentare della distanza massima (espressa in Km) che soddisfa un determinato requisito di affidabilità α.

Gli autori di [5] finiscono per dimostrare, in sostanza, che una rete come quella di fronthaul/backhaul, costituita da connessioni realizzate tramite sistemi ibridi FSO/RF e collegamenti in fibra, può trovare il suo assetto ottimale a seconda delle specifiche di progetto e certamente garantisce, laddove possibile, un più economico dispiegamento delle risorse. Questa, infatti, è una valutazione che tiene conto solo degli aspetti tecnico-economici relativi al dispiegamento di una architettura di fronthaul/backhaul; per una valutazione completa occorre tener presente anche i requisiti di rete imposti dalla tecnologia 5G che andranno valutati per ogni scenario applicativo.

5. Conclusioni

L'adozione dei sistemi ibridi FSO/RF può risultare vantaggiosa, alla luce dei risultati raggiunti in letteratura e qui riassunti per ragioni di spazio, all'interno del paradigma di rete che si sta profilando come di futura generazione, ovvero il sistema 5G. Infatti, tale complesso strutturale si articolerà attendibilmente, per soddisfare ad esempio determinati requisiti di data-rate e sostenere una gestione flessibile del carico di rete, in una forma di interconnessione varia tra le più disparate tecnologie che la ricerca va raffinando da decenni. Un posto speciale è riservato all'integrazione dell'ottica di spazio libero in soluzione ibrida con RF, se non altro per la sua evidente compatibilità con la tecnologia più consolidata a livello di rete per le trasmissioni ad alto flusso-dati, ovvero la fibra ottica, la quale mantiene tuttavia il suo primato nelle percentuali di utilizzo. Come sopra dimostrato, a questo si aggiunge un altro importante vantaggio: il potenziale alleggerimento dei costi

infrastrutturali che si può ricavare nel dispiegamento di collegamenti ibridi FSO/RF all'interno di una sezione della rete come il fronthaul, aperta al dialogo di più tecnologie. E non bisogna dimenticare infine il pieno adempimento di questo dispositivo di trasmissione ai requisiti previsti negli accordi europei per quanto concerne le tratte in spazio libero, come quelli che stanno recentemente spostando il piano tecnologico verso una tipologia di rete radiomobile sempre meno impattante sull'ambiente e più "green".

Bibliografia

[1] X. Ge, S. Tu, G. Mao, C. X. Wang, T. Han, "*5G Ultra Dense Networks*", IEEE Wireless Communications, vol. 23, no. 1, pp. 72-79, Feb. 2016.

[2] M. Jaber, M. A. Imran, R. Tafazolli, A. Tukmanov, "*5G Backhaul Challenges and Emerging Research Directions: A Survey*", IEEE Access, vol. 4, pp. 1743-1766, April 2016.

[3] Y. Niu, Y. Li, D. Jin, L. Su, A. V. Vasilakos, "*A Survey of millimeter Wave Communications (mmWave) for 5G: Opportunities and Challenges*", Wireless Networks, vol. 21, no. 8, pp. 2657-2676, April 2015.

[4] M. A. Khalighi, M. Uysal, "*Survey on Free-Space Optical Communication: A Communication Theory Perspective*", IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2231-2258, June 2014.

[5] A. Douik, H. Dahrouj, T. Y. Al-Naffouri, M. S. Alouini, "*Hybrid Radio/Free-Space Optical Design for Next Generation Backhaul Systems*", IEEE Transactions on Comm., vo. 64, no. 6, June 2016.

[6] E. Zedini, M. S. Alouini, "*Multihop Relaying Over IM/DD FSO Systems with Pointing Errors*", J. Lightwave Technol., vol. 33, no. 23, pp. 5007-5015, 2015.

[7] M. A. A. Ali, "*Free Space Optical Wireless Communications under Turbulence Channel Effect*", IOSR J. Electron. Commun. Eng., vol. 9, no. 3, pp. 1-8, 2014.

[8] T. Rakia, H. C. Yang, M. S. Alouini, F. Gebali, "*Outage Analysis of Practical FSO/RF System with Adaptive Combining*", IEEE Comm. Letters, vol.19, no. 8, pp. 1366-1369, Aug. 2015.

[9] S. Choudhury, J. D. Gibson, "*Information Transmission over Fading Channels*", IEEE GLOBECOM, pp. 3316-3321, 2007.

[10] M. Usman, H. C. Yang, M. S. Alouini, "*Practical Switching-Based Hybrid FSO/RF Transmission and Its Performance Analysis*", IEEE Photonics Journal, vol. 6, no. 5, Oct. 2014.

[11] H. Moradi, M. Falahpour, H. Refai, P. LoPresti, M. Atiquzzaman, "*On the Capacity of Hybrid FSO/RF Links*", Proc. IEEE GLOBECOM, pp. 1-5, Dec. 2010.

[12] A. Touati, A. Abdaoui, F. Touati, M. Uysal, A. Bouallegue, "*On the Effects of Combined Atmospheric Fading and Misalignment on the Hybrid FSO/RF Transmission*", J. Opt. Comm. Net. , vo. 8, no. 10, Oct. 2016.

Massimo Amendola, Giancarlo Gaudino
(Istituto Superiore CTI)

I progetti di alternanza scuola-lavoro dell'Istituto Superiore C.T.I.

School at Work projects of Higher Institute of Communications and Information Technology

***Sommario**: Con l'introduzione dei progetti di Alternanza Scuola-Lavoro (ASL), l'Istituto Superiore ha esteso i suoi programmi formativi, tradizionalmente destinati in ambiti caratterizzati da un alto livello di specializzazione, anche verso platee estremamente variegate, ma certamente interessate al mondo delle tecnologie dell'informazione, come lo sono quelle delle scuole medie superiori.*

Proprio per coprire esigenze formative così eterogenee, le iniziative ASL di ISCTI si sono sviluppate attraverso percorsi didattici ideati in modo tale da offrire agli studenti l'opportunità di fare scuola in un contesto lavorativo e di apprendere attraverso momenti di studio alternati da esperienze di laboratorio in cui, educazione formale, informale e pratica si combinano in un unico progetto.

***Abstract**: The introduction of the School at Work (ASL) projects, the Institute has extended its training programs, traditionally designed for high level of specialization, also towards extremely varied audiences, but certainly interested in the world of information technologies, as are those of high schools.*

To cover such heterogeneous training needs, ISCTI's ASL initiatives have been developed through educational courses designed to offer students the opportunity to do schooling in a work context and to learn through moments of study alternated with laboratory experiences in which, formal, informal and practical education are combined in a single project.

L'Alternanza Scuola-Lavoro (ASL), obbligatoria per tutti gli studenti degli ultimi tre anni delle scuole superiori, licei compresi, è una delle introduzioni più significative della legge 107 del 2015 (meglio nota come "La Buona Scuola").

Si tratta di una di una nuova visione della formazione che attraverso l'esperienza pratica aiuta a consolidare le conoscenze acquisite nella scuola, a provare sul campo le attitudini delle studentesse e degli studenti, ad arricchirne la formazione e a orientarne sia i percorsi di studio, sia quelli di lavoro in futuro grazie a progetti coerenti con i loro piani di studio.

I percorsi di Alternanza si basano su una convenzione stipulata tra scuole e aziende sia pubbliche che private. Nella convenzione si fa riferimento alle finalità del percorso formativo con particolare attenzione alle attività da svolgersi durante l'esperienza di lavoro, alle

norme e alle regole da osservare, al rispetto della normativa sulla privacy e sulla sicurezza dei dati, alla sicurezza nei luoghi di lavoro.

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) ha nella formazione e nell'istruzione specializzata nel campo delle telecomunicazioni e delle tecnologie dell'informazione una delle sue attività istituzionali che svolge in primo luogo con la Scuola Superiore di Specializzazione (SSST) e con la promozione di convegni, seminari e giornate informative a tema. Tra l'altro, alcuni dei seminari e dei corsi di formazione erogati dall'Istituto sono rivolti alla formazione continua e permanente degli ingegneri e vengono riconosciuti dal Consiglio Nazionale Ingegneri (CNI) e, in accordo all'ordinamento professionale nazionale e comunitario, consentono il rilascio dei crediti formativi.

Un ambito caratterizzato da un alto grado di competenza che per tale natura è dunque indirizzato a soggetti ed istituzioni coinvolti in modo più o meno diretto nel settore. Tuttavia, le opportunità innescate dalla nuova normativa hanno permesso all'Istituto, con l'avvio di alcuni progetti di Alternanza, di estendere i suoi servizi didattici rimodulati sulle esigenze specifiche delle scuole superiori, rivolgendosi così ad una platea indubbiamente meno esperta ma sicuramente interessata e più numerosa.

I percorsi di formazione ASL che l'Istituto ha attivato e che attiverà, poggiano di conseguenza su una metodologia didattica costruita in modo tale da offrire agli studenti la possibilità di fare scuola in una situazione lavorativa e di apprendere attraverso l'esperienza, alternando periodi di studio e di pratica, in cui educazione formale, informale ed esperienza di lavoro si combinano in un unico progetto.

Pertanto, questi progetti ideati in sinergia con le scuole coinvolte puntano a:

- attuare modalità di apprendimento flessibili che colleghino sistematicamente la formazione in aula con l'esperienza pratica;
- arricchire la formazione acquisita dagli studenti nei percorsi scolastici e formativi, con l'acquisizione di competenze spendibili anche nel mercato del lavoro;
- favorire l'orientamento dei giovani per valorizzarne le vocazioni personali, gli interessi e gli stili di apprendimento individuali.

Il perseguimento di queste finalità si concretizza attraverso:

- un sistema tutoriale assieme a uno o più tutor/referenti tra i docenti della scuola e dell'ISCTI che accompagnano gli studenti durante tutto il percorso di formazione;
- la progettazione integrata dei percorsi di formazione di ulteriore approfondimento, nell'ottica di favorire e supportare l'acquisizione di specifiche competenze e conoscenze, coerenti con il percorso di studi intrapreso dagli studenti;
- la valutazione e la certificazione delle competenze acquisite dagli studenti che hanno intrapreso i percorsi di approfondimento;
- la certificazione e il riconoscimento dei crediti formativi attraverso un attestato finale.

Intenti e fini che si saldano in modo naturale alle *mission* dell'Istituto Superiore le cui professionalità e la qualità dei propri laboratori sono messe al servizio dei giovani studenti per offrire a loro un credibile punto di contatto tra il mondo del lavoro e il mondo della scuola.

I progetti di alternanza dell'ISCTI hanno visto l'adesione di studentesse e di studenti provenienti da diverse tipologie di scuola come l'istituto Tecnico "E. Fermi" di Roma che ha in corso una convenzione triennale, l'Istituto di Istruzione Superiore "L. Pirelli" sempre di Roma, oppure il liceo Scientifico con indirizzo in informatica "G. Berto" di Mogliano Veneto (TV). Negli ultimi anni poi, altre scuole di Roma, i licei scientifici "S. Cannizzaro" e "C. Cavour", il liceo classico "I. Kant", l'istituto di istruzione superiore "F. Magellano" e l'istituto paritario "A. Nobel" hanno stipulato nuove convenzioni con l'ISCTI. È giocoforza quindi che i contenuti formativi siano ogni qualvolta calibrati e mirati a secondo delle necessità didattiche connesse alla scuola di provenienza e ai livelli di apprendimento raggiunti dai singoli studenti.

Nella fattispecie, nei percorsi di studio si prevedono attività focalizzate sulle discipline di informatica e di telecomunicazioni e vengono normalmente condotti attraverso seminari e pratiche di laboratorio su:

- la presentazione da parte di un referente del Servizio Prevenzione e Protezione per illustrare le procedure di sicurezza che i visitatori della sede devono intraprendere durante la loro permanenza;
- la sicurezza informatica con particolare interesse verso i pericoli e le minacce sia su PC sia su mobile in modo da sensibilizzare gli studenti ad un uso responsabile della rete e delle nuove tecnologie;
- le procedure per la certificazione di software di misura della Qualità dei Servizi su reti a larga banda nel laboratorio "Test Plant" che effettua monitoraggi, prove e sperimentazioni di servizi su tali reti;
- l'accessibilità e l'usabilità dei siti web incentrato sulla conoscenza delle tecnologie assistive per le persone disabili e sulle prove che esegue il laboratorio "valutazione della Qualità dei Servizi multimediali" per verificare l'accessibilità e l'usabilità dei siti web pubblici e privati;
- la qualità dell'audio e dei video con particolare riguardo alle tecniche per rendere accessibile la produzione multimediale;
- il controllo del mercato con l'obbiettivo di far conoscere le attività connesse alle prove compiute dal laboratorio "eurolab radio" per la sorveglianza ed il controllo di apparati e terminali di comunicazioni elettroniche;
- le attività della Sala Nautica in cui è possibile simulare le comunicazioni tra navi e tra navi e terra, oppure la generazione di tutte le chiamate comprese quelle di soccorso e tramite ciò, consentire il sostenimento degli esami pratici

per il rilascio del certificato di operatore radio marittimo o di stazione costiera;
- le modalità di progettazione, implementazione e controllo di un Sistema di Gestione Aziendale secondo quanto previsto dalla norma ISO 9001/2015;
- l'organizzazione di un meeting, esposto prevalentemente in lingua inglese, con la finalità di far conoscere le fasi di preparazione e di gestione di riunioni di gruppi di lavoro nazionali o internazionali.

I progetti di formazione di ulteriore approfondimento a cui si è fatto cenno, hanno invece l'obiettivo di ampliare le competenze dello studente coinvolgendolo in un vero e proprio corso di formazione fortemente qualificato da pratiche ed esperienze di laboratorio. Nel caso del liceo "L. Pirelli" ad esempio, un gruppo di studenti hanno potuto progettare e realizzare un proprio sito web che è stato migliorato grazie ai test di accessibilità e di usabilità che loro stessi hanno effettuato presso i laboratori dell'Istituto.

Gli studenti del "Cannizzaro" invece, hanno avuto modo di approfondire i contenuti dei seminari non solo con le valutazioni di accessibilità del sito della loro scuola, ma anche con la preparazione di meeting internazionali su argomenti di interesse, la stesura di articoli redazionali (con titoli spesso evocativi come "Alternanza al MISE: ogni passione può diventare un lavoro") e di video clip dedicati alle attività svolte durante la loro permanenza al Ministero.

Abbiamo dunque a che fare con vere e proprie esperienze di lavoro in cui lo studente ha avuto l'opportunità di conoscere non solo le professionalità necessarie alla ideazione e realizzazione di un prodotto finito. ma anche di cogliere il valore di tutti quegli aspetti multidisciplinari e cooperativi che quelle attività comportano.

La sfida ultima è che le positività scaturite dall'innesco dei processi di Alternanza Scuola-Lavoro possano veramente condurre ad una reale alleanza tra scuola e territorio, come ci si auspica nel sito web del MIUR. Un investimento per tutto il mondo che circonda la scuola, per chi crede nell'inserimento dei ragazzi all'interno dei luoghi di lavoro come motore della formazione di studenti qualificati e preparati ad affrontare, dopo gli studi, la realtà lavorativa. E per dare alle nostre studentesse e ai nostri studenti più competenze, più sapere e con ciò, più opportunità di lavoro e più potere di scelta.

Giancarlo Butti
Europrivacy

Il rispetto delle normative in tema di sicurezza e le opportunità per il business

Compliance with regulations on security and business opportunities

Sommario: *Le normative di carattere settoriale (relative al mondo finanziario, telco, infrastrutture critiche…) o applicabili a qualunque organizzazione (GDPR) che hanno fra i loro obiettivi diretti o indiretti la regolamentazione della sicurezza di un'organizzazione sono sempre più numerose.*

Gli adempimenti previsti per essere conformi a tali normative sono spesso considerati dalle organizzazioni solo come un costoso adempimento per essere compliance con la normativa, ma in realtà le misure di sicurezza richieste offrono alle aziende rilevanti vantaggi competitivi.

Abstract: *The sectorial set of rules (relating to the financial world, telco, critical infrastructures ...) or applicable to any organization (GDPR) that have among their direct or indirect objectives the regulation of the security of an organization are more and more increasing.*

The formalities required to comply with these regulations are often considered by the organizations only as an expensive formality to comply with the legislation, while the required security measures also offer to the companies significant competitive advantages.

1. Il perimetro di tutela

Sono solito iniziare i miei corsi in ambito privacy o sicurezza con la seguente espressione: "non esiste alcuna normativa che obbliga un'azienda a tutelare i propri asset, ma esistono normative che obbligando le aziende a tutelare altri asset, quali i dati personali, i propri collaboratori, gli stakeholder, tutelano indirettamente anche l'azienda".

Il concetto è chiaro ed immediato, tanto che diversi colleghi lo hanno fatto proprio.

Basta una semplice rassegna delle principali normative alle quali devono sottostare tutte le organizzazioni per verificarne la veridicità.

La normativa sulla **safety** (D.Lgs.81/08 e successive integrazioni) obbliga le organizzazioni a dotarsi, fra le altre, di misure antincendio, che ovviamente tutelano non solo i lavoratori, ma anche tutti gli **asset materiali** (e quelli immateriali in essi eventualmente contenuti) dell'azienda.

Le normative **privacy**, fra le quali il recente GDPR, obbligano le aziende a dotarsi di adeguate misure di sicurezza tecniche ed organizzative per tutelare i diritti e le libertà fondamentali delle persone

fisiche, con particolare riferimento al diritto alla protezione dei dati personali.

Per fare questo le aziende devono tutelare in particolare gli asset informativi nei quali sono presenti o transitano i dati personali dei soggetti interessati e sebbene questi siano un sottoinsieme (molto cospicuo) delle informazioni gestite da un'organizzazione, ne risultano tutelate di norma anche tutte le altre informazioni gestite dall'azienda e gli asset materiali che le contengono.

Già da soli questi due esempi costituiscono una valida dimostrazione dell'immediato ritorno economico per le organizzazioni derivante dall'applicazione della normativa.

È facile obiettare che il ritorno è esclusivamente di tutela; sono cioè protetti gli asset e le informazioni rispetto ad eventuali incidenti che nella realtà potrebbero non accadere mai e che le organizzazioni potrebbero mettere in atto altrimenti altre soluzioni, magari meno costose, quali un trasferimento di rischio ad una assicurazione.

2. Valutare i costi di un incidente di sicurezza

Le considerazioni espresse al precedente paragrafo potrebbero essere considerate valide se ci si limitasse ad una mera valutazione del rapporto fra i costi sostenuti per le misure di sicurezza implementate ed i costi derivanti dalla perdita di asset materiali/immateriali o peggio ancora in conseguenza di un infortunio di un collaboratore.

Tale valutazione dovrebbe inoltre tenere in debito conto il fatto che i costi delle implementazioni sono certi, mentre i costi di perdita/infortunio sarebbero da considerare solo nel caso in cui un evento avverso abbia luogo.

Tale valutazione è tuttavia non corretta.

In primo luogo, anche se non sarebbe del tutto corretto inserirlo nel nostro conteggio di costi e benefici, la corretta implementazione delle misure di sicurezza mette al riparo dalle sanzioni previste dalle specifiche normative di riferimento.

Tali sanzioni non sono da intendersi solo di natura economica o penale, ma ad esempio, nel caso della normativa privacy, potrebbero altresì comportare il blocco dei trattamenti dei dati personali e, nel caso più estremo, il blocco delle attività di un'organizzazione se questa dipende da tali trattamenti (si consideri ad esempio una società di mkt che si vede bloccare i database dei propri prospect).

Un incidente derivante dalla mancanza delle misure di sicurezza potrebbe portare alla perdita di informazioni importanti o vitali per l'azienda, al blocco dei server che erogano un servizio, al blocco di una linea di produzione.

Oltre al danno di natura prettamente materiale, si deve aggiungere il probabile danno di immagine per l'organizzazione, la cui quantificazione sebbene difficile è comunque possibile mediante tecniche reperibili in letteratura.

Se il danno subito ha come conseguenza il blocco temporaneo o definitivo della fornitura di un prodotto/servizio questo potrebbe

comportare conseguenze nella relazione con i clienti e all'attivazione di cause per inadempimento contrattuale.

Vanno inoltre aggiunti i costi di ripristino/riparazione derivanti dall'incidente che sono a loro volta condizionati dalle eventuali misure di sicurezza presenti (si pensi alla rottura di un disco fisso e alla conseguente perdita di dati il cui effettivo ripristino è condizionato dalla disponibilità di un backup o, in mancanza di questo, da una reimputazione manuale dei dati se questi sono disponibili su carta ovvero dal loro eventuale recupero presso terzi, se disponibili).

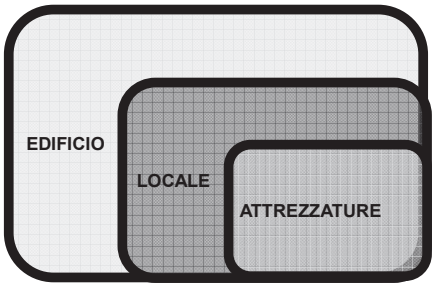


Figura 1 – Correlazione fra asset ai fini della valutazione dei rischi e delle relative contromisure (Fonte: Sicurezza totale, G. Butti ITER)

Descrizione bene	**Disco fisso**
Evento	Rottura
Impatti diretti	Perdita di dati Interruzione del servizio Costi di ripristino
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Descrizione bene	**Sito**
Evento	Distruzione
Impatti diretti	Inaccessibilità dei beni materiali ed immateriali presenti nell'edificio Distruzione parziale o totale dei beni presenti nell'edificio Costi di ripristino o attivazione di misure alternative
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Tabella 1 – Esempi delle conseguenze dirette, indirette di eventi avversi (Fonte: Sicurezza totale, G. Butti ITER)

Descrizione bene	**Materie prime**
Evento	Furto
Impatti diretti	Perdita economica Interruzione della produzione
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Eliminare il rischio	
Ridurre il rischio	Ridurre l'impatto Ridurre la probabilità
Trasferire il rischio	Assicurativo Non assicurativo
Accettare il rischio	

Tabella 2. IL trattamento del rischio residuo (Fonte: Sicurezza totale, G.Butti ITER)

3. La tutela delle informazioni riservate

La tutela delle informazioni riservate dovrebbe essere una delle principali preoccupazioni di un'azienda. Con tale termine si intendono le informazioni che consento all'azienda di mantenere un vantaggio competitivo sul mercato e sono costituite sia da informazioni di natura tecnica (ad esempio lo svolgimento di un processo industriale) sia di natura commerciale (ad esempio l'elenco dei propri clienti arricchito con informazioni che li caratterizzano dal punto di vista dell'azienda).

L'importanza di queste informazioni per le aziende è tale che il legislatore ha introdotto una loro autonoma tutela legale.

Al riguardo ci sono diversi motivi per cui il rispetto di normative come il GDPR consentano alle aziende di tutelare le proprie informazioni riservate e quindi il proprio know how.

In primo luogo è necessario mappare dettagliatamente le proprie informazioni, sia che queste siano presenti in database strutturati o in file destrutturati quali la posta elettronica o prodotti di produttività individuale.

Tale mappatura è infatti propedeutica alla individuazione dei dati personali trattati dalle aziende al fine della loro successiva protezione.

Inoltre questa attività, se effettuata con riferimento ai processi aziendali, consente di individuare anche le informazioni necessarie all'azienda per lo svolgimento della propria attività, ma che non sono formalizzate, ovvero quella componente del know how aziendale che è patrimonio implicito dei collaboratori[1].

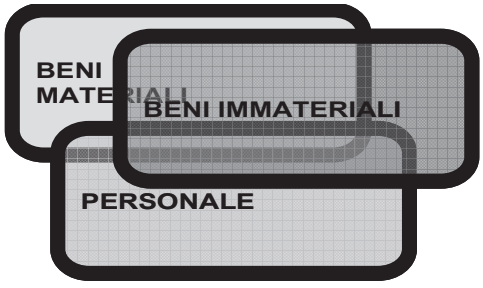


Figura 2. Relazione fra asset immateriali e gli asset materiali che li contengono (Fonte: Sicurezza totale, G.Butti ITER)

Gli strumenti di tutela dei dati personali, come già espresso in precedenza, portano a tutelare anche le informazioni che costituiscono il

[1] G. BUTTI, *La tutela del capitale intellettuale,* Il Mondo dell'intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2016,

know how aziendale; difficilmente infatti le misure tecniche ed organizzative messe in atto dall'azienda saranno limitate in modo puntale alla protezione dei dati personali (si pensi a firewall, antivirus, IDS, backup, credenziali di accesso differenziate…).

Ma c'è un secondo aspetto meno evidente che deriva da questa protezione "ereditata" dalle informazioni nel loro complesso.

L'articolo 98 del Codice di Proprietà Industriale (Legge n. 30/2005) che tutela i *segreti commerciali* (in precedenza *informazioni aziendali riservate*) così recita:

1) *Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
   a) *siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;*
   b) *abbiano valore economico in quanto segrete;*
   c) ***siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.***

In altre parole tali informazioni per essere tutelate dalla legge devono essere protette da misure di sicurezza tali per cui possano rimanere segrete.

Appare quindi evidente che un database o una cartella di rete ai quali siano stati applicati dei criteri di sicurezza, in quanto contenenti dati personali, garantiscono che anche le altre informazioni, considerate segrete dall'azienda, siano automaticamente tutelate dalla legge.

Al riguardo è importante ricordare che altrimenti, un'informazione considerata segreta dall'azienda, ma non protetta mediante misure tecniche e/o organizzative, non è tutelata dal Codice di Proprietà Industriale.

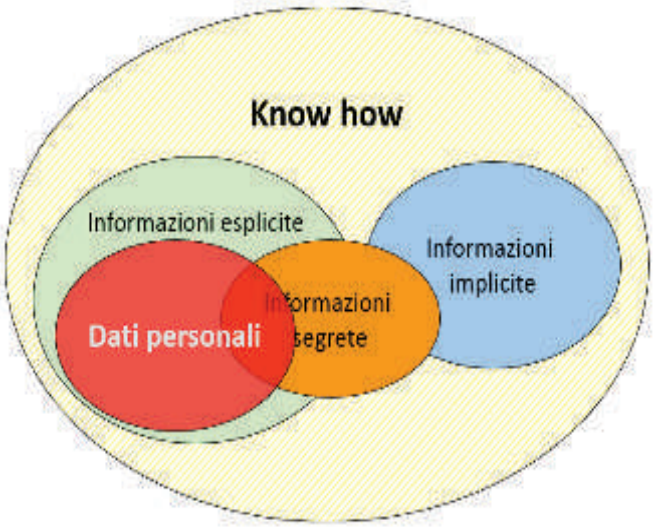


Figura 3. Relazione fra know how, informazioni segrete e dati personali

Anche la normativa safety tutela indirettamente le informazioni riservate, in quanto tutela i lavoratori (oltre agli asset aziendali rispetto al rischio indicendio…). Come più sopra specificato le informazioni implicite sono patrimonio dei singoli collaboratori ed un loro infortunio o decesso può portare ad una temporanea o definitiva indisponibilità di tali informazioni con conseguenze che difficilemente le aziende sono in grado di valutare preventivamente.

4. La continuità del business

In questo paragrafo verrà presentata una rassegna delle normative che obbligano le aziende a garantire la continuità nella erogazione dei loro servizi (l'argomento è particolarmente significativo, per cui per una trattazione più dettagliata si rimanda all'articolo **Aziende resilienti** su questo stesso numero della rivista **La Comunicazione - Note, Recensioni & Notizie**).

Tali normative possono riguardare settori specifici, quali le banche o le PA, oppure indistintamente tutti i soggetti che trattano dati personali, quali il GDPR.

Recente è inoltre l'attivazione della **DIRETTIVA (UE) 2016/1148 (NIS)** il cui recepimento in Italia è operativo dal 26 giugno del 2018 tramite il **DECRETO LEGISLATIVO 18 maggio 2018, n. 65**.

Nelle tabelle seguenti sono riportati gli articoli delle principali normative che hanno attinenza alla resilienza ed alla continuità operativa.

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Articolo 32 Sicurezza del trattamento 1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: … b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Tabella 3. Regolamento (UE) 2016/679 - GDPR

Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 4 – Il sistema informativo** **Sezione IV – La gestione della sicurezza informatica**
7. La disponibilità delle informazioni e delle risorse ICT *…* *— in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di backup (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;* *— le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del no single point of failure) volte a garantire l'alta disponibilità delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di disaster recovery;* *— in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo denial of service o distributed denial of service), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;*
Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 5 – La continuità operativa** **Allegato A – Requisiti per la continuità operativa** **Sezione II – Requisiti per tutti gli operatori**
1. Ambito del piano di continuità operativa **2. Analisi di impatto** **3. Definizione del piano di continuità operativa e gestione delle crisi** *3.1 Ruolo degli organi aziendali* *3.2 I processi critici* *3.3 La responsabilità del piano di continuità operativa* *3.4 Il contenuto del piano di continuità operativa* *3.5 Le verifiche* *3.6 Le risorse umane* *3.7 Esternalizzazione, infrastrutture e controparti rilevanti* *3.8 Controlli* *3.9 Comunicazioni alla Banca d'Italia e alla Banca centrale europea*

Tabella 4. Circolare 285 Banca d'Italia

Articolo abrogato dal D.LGS. 26 Agosto 2016, n. 179
Art. 50-bis. Continuità operativa. *1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.* *2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.* *3. A tali fini, le pubbliche amministrazioni definiscono:* *a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;* *b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità*

operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione. *4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.*

Tabella 5. CAD – Codice dell'amministrazione digitale

DECRETO LEGISLATIVO 18 maggio 2018, n. 65. **Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.**
Art. 12. **Obblighi in materia di sicurezza e notifica degli incidenti** *…* *2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.* *Art. 14.* **Obblighi in materia di sicurezza e notifica degli incidenti** **…** *3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.*

Tabella 6. Direttiva (UE) 2016/1148 - NIS

DECRETO LEGISLATIVO 18 maggio 2018, n. 65. **Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.**
Art. 12. **Obblighi in materia di sicurezza e notifica degli incidenti** *…* *2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.* *Art. 14.* **Obblighi in materia di sicurezza e notifica degli incidenti** **…** *3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.*

Tabella 7. Decreto Legislativo 18 maggio 2018, n° 65

5. il presidio dei processi

Sebbene non sia strettamente connesso al tema della sicurezza, il GDPR introduce una serie di obblighi che costringono le aziende a migliorare la loro capacità nella gestione dei processi.

Innanzi tutto la compilazione del **Registro delle attività di trattamento**, che è di fatto un obbligo per qualunque organizzazione (le eccezioni previste dal comma 5 dell'art. 30 del GDPR sono di fatto inapplicabili in quanto tutti i titolari effettuano quantomeno trattamenti non occasionali) costringe le organizzazioni a mappare i propri processi, valutando se gli stessi comportano un trattamento di dati personali. Tale registro deve inoltre essere mantenuto costantemente aggiornato al fine di dimostrare la conformità alla norma.

Il registro non contiene solo informazioni sui dati personali, ma anche sulle misure di sicurezza; la corretta documentazione di queste ultime comporta di fatto anche la necessità di procedere ad una adeguata mappatura del proprio sistema informativo e delle misure di sicurezza in essere.

Si ottiene così un presidio sui propri processi e sul proprio livello di sicurezza, rafforzato dalla necessità di garantire il rispetto di altri due principi base del GDPR:

- la privacy by design
- l'accountaility

Il rispetto della privacy by design impone alle aziende un costante presidio su una serie di eventi che possono modificare il proprio modello privacy *(Articolo 25* ***Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita****):*

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Articolo 25 ***Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita***
1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Tabella 8. Regolamento (UE) 2016/679 - GDPR

L'obbligo di svolgere tali attività preventivamente ed il fatto che in realtà, al di là di quanto individuato dalla normativa (variazioni in ambito

applicativo, servizi, prodotti), qualunque evento accada in azienda (nuovi prodotti/servizi offerti o acquisiti, variazioni al sistema informativo o al modello organizzativo, variazioni nel personale…) costringono l'azienda ad effettuare una valutazione degli impatti privacy fa sì che venga mantenuto un costante presidio sui processi aziendali.

Il titolare inoltre, non solo ha l'obbligo di rispettare la normativa, ma anche di essere in grado di dimostrarlo in ogni momento, documentando le azioni messe in atto per farlo.

Sebbene può sembrare paradossale, il fatto che le aziende non abbiano una piena consapevolezza né dei processi in atto, né delle informazioni di cui dispongono, è dimostrato dall'impegno necessario per l'adeguamento al GDPR.

6. La qualità dei dati

Anche il tema della qualità dei dati, sebbene solo indirettamente connesso al tema della sicurezza, viene ampiamente trattato sia dal GDPR, sia dalla Circolare 285 di Banca d'Italia.

Limitandoci al solo GDPR, in quanto valido per qualunque organizzazione, il tema della qualità dei dati trova riscontro nell'art. 5, il cui mancato rispetto comporta le sanzioni di fascia maggiore (20 milioni di euro o 4% del fatturato annuo mondiale).

Avere dati di qualità, in particolare dati esatti ed aggiornati, consente alle aziende di ridurre gli errori nell'ambito della produzione, nella gestione degli ordini, degli incassi e dei pagamenti, nella erogazione dei servizi e quindi in ultima analisi di ridurre i reclami ed i contenziosi con le varie controparti.

Il tutto si traduce quindi in un risparmio (si evitano rilavorazioni, nuove spedizioni, rimborsi, spese legali…) e in un incremento del livello di fiducia dei vari stakeholder nei confronti dell'azienda.

Nell'attuale contesto iper competitivo dove ai clienti basta un click su un sito on line per cambiare fornitore, garantire un servizio di qualità è fondamentale e questo molto spesso dipende dalla qualità dei dati che l'azienda e la sua intera filiera è in grado di garantire.

Anche quest'ultimo aspetto, per nulla scontato, è specificatamente previsto dal GDPR, che impone ad esempio al titolare che in caso di richiesta di aggiornamento dei propri dati da parte di un interessato, tale richiesta sia portata a conoscenza anche degli altri soggetti, esterni al titolare, che partecipano al trattamento.

Si pensi nella pratica ad un'azienda che fornisce un prodotti/servzio la cui manutenzione è affidata ad aziende terze sul territorio. Una variazione ad esempio del recapito telefonico del cliente/interessato da questi correttamente inoltrato all'azienda fonitrice del prodotto/servizio, ma da questa non comunicata ai suoi fornitori sul territorio può comportare la mancata assistenza anche per periodi prolungati (caso realmente accaduto), con grave disagio e disappunto dei clienti…

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Articolo 5 ***Principi applicabili al trattamento di dati personali*** *1. I dati personali sono:* *a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);* *b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);* *c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);* *d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);* *e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);* *f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).* *2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*

Tabella 9. Regolamento (UE) 2016/679 - GDPR

7. L'analisi dei rischi

Sebbene solo nella Circolare 285 di Banca d'Italia vi sia uno specifico paragrafo dedicato a questo argomento, nelle altre normative quali il GDPR o il NIS tale adempimento risulta citato o implicitamente necessario come propedeutico alla implementazione di adeguate misure di sicurezza.

Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 4 – Il sistema informativo** **Sezione III – L' analisi del rischio informatico**
L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario. *Il processo di analisi è svolto con il concorso dell'utente responsabile (1), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'audit, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:* *la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (2).* *Tale fase prende l'avvio con la classificazione delle risorse ICT (3) in termini di rischio informatico (4);* *il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.* *L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (5). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (6), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.* *Per le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo, è comunque prevista una valutazione integrativa, al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile.* *I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza dell'organo con funzione di gestione.* *Il processo di analisi del rischio è ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi e, comunque, in presenza di situazioni che possono influenzare il complessivo livello di rischio informatico.*

Tabella 10. Circolare 285 Banca d'Italia

Le varie normative tutelano ambiti diversi e quindi l'oggetto dell'analisi dei rischi varia.

Rispetto ai tradizionali asset aziendali ad esempio, l'oggetto di tutela del GDPR sono i diritti e le libertà delle persone fisiche e quindi l'analisi dei rischi deve essere effettuata rispetto a questo particolare asset

(anche se i dati personali degli interesati sono presenti negli asset aziendali e quindi le misure di tutela da implementare in conseguenza del risultato dell'analisi dei rischi avrà impatti positivi per la sicurezza dell'azienda).

Conclusioni

Sarebbe possibile continuare questo articolo con molti altri esempi, quali la riduzione dei costi di storage derivanti dall'obbligo (sanzionato) di limitare la conservazione dei dati al tempo strettamente necessario, o al rispetto della minimizzazione…

Quanto qui riportato evidenzia comunque che il rispetto "intelligente" delle normative citate permette alle aziende di essere:

- più consapevoli circa i propri processi, sistemi, informazioni, dati trattati
- più consapevoli rispetto ai rischi che incombono sui propri asset
- costantemente aggiornate e documentate in merito a quanto sopra esposto
- più consapevoli rispetto alla tutela del proprio know how e delle informazioni segrete
- più resilienti rispetto a eventi avversi quali eventi naturali, "attacchi" da parte di soggetti interni/esterni all'azienda, errori ed incidenti
- più competitive, grazie alla qualità delle informazioni gestite ed alla relativa riduzione dei costi derivanti da errori e contenziosi
- più appetibili per i vari stakeholder, in quanto l'immagine dell'azienda risulta consolidata.

Una valutazione costi/benefici che in ultima analisi pende decisamente a favore di questi ultimi e che dovrebbe portare le aziende a modificare radicalmente il loro approccio all'adeguamento normativo, cogliendone le opportunità.

Gianpaolo Susanna, Vincenzo Attanasio, Silvia Di Bartolo, Luigi Salamandra, Angelo Pizzoleo, Domenico Carleo
(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

(Università degli Studi di Roma "Tor Vergata", Dipartimento di Ingegneria Elettronica)

Valentina Lucli
(Università degli Studi di Roma "Tor Vergata", Dipartimento di Ingegneria Elettronica)

Influenza meteorologica sui sistemi di trasmissione in spazio libero "Free Space Optics" (FSO)

Weather influence on Free Space Optics (FSO) transmission systems

Sommario: *Nell'ambito delle telecomunicazioni, la crescita esponenziale delle infrastrutture e delle tecnologie ad oggi presenti, ha portato inesorabilmente ad una estrema necessità di reti di comunicazione adeguate, soprattutto a causa del crescente numero di persone che popolano le città. L'approssimarsi della commercializzazione dei nuovi dispositivi di rete 5G, crea l'esigenza della creazione di una infrastruttura di rete a supporto dell'interfaccia radiomobile che presenti adeguate caratteristiche in termini di capacità, latenza, risparmio energetico, etc. Risulta quindi sempre più mandatorio l'apporto di tecnologie che supportino la richiesta di una banda sempre più ampia per la fornitura di servizi e per lo smistamento dei dati. In questo articolo viene trattata una tecnologia laser che sta emergendo negli ultimi anni, in parte presente sul mercato, ma ancora in fase di esplorazione in ambito di ricerca per le possibili applicazioni. Nei laboratori di comunicazioni ottiche dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione viene effettuato questo tipo di ricerca su sistemi di trasmissione ottici in aria senza necessità di guide d'onda, denominato Free Space Optics (FSO). La funzionalità e l'utilità di questi sistemi è già stata ampiamente discussa e dimostrata in precedenti articoli; di seguito vengono indagate le questioni legate all'influenza dei fattori ambientali sul link ottico, che impattano pesantemente sulla qualità del collegamento, analizzate con l'ausilio di una stazione meteo collegata al set-up FSO. Viene quindi discussa l'influenza delle variabili legate al tempo atmosferico e dimostrata la stabilità di tali sistemi anche quando perturbati, a meno di condizioni che portano ad oscuramento totale (anche se al più queste ultime, risultano essere passeggere e di breve durata).*

Abstract: *In the field of telecommunication, the exponential growth of the infrastructures and technologies to date, have inexorably led to an extreme need for adequate communication networks, mainly due to the growing number of people that populate the cities. The contribution of technologies that support the demand for an increasingly broadband for the provision of services and for the sorting of data is therefore increasingly mandatory. This article deals with the topic of a laser technology emerging in recent years, technology already partially present on the market, but still under exploration in the field of research of possible applications. In the laboratories of the Ministry of the*

Economic Development, this type of research is carried out on optical transmission systems in air without the need for waveguides, called Free Space Optics (FSO); the functionality and usefulness of these systems has already been widely discussed and demonstrated in the previous papers. In this work, the issues related to the influence of environmental factors on the optical link are investigated, impacting heavily on the link quality, analyzed with the aid of a weather station connected to the FSO set-up. The influence of the variables related to the weather is then discussed and the stability of these systems is demonstrated even when perturbed, unless conditions that lead to total obscuration (even if at most the latter are transient and of short duration).

1. Introduzione

La nascita di servizi ICT di nuova generazione, quali ad esempio *Video Streaming* e *Cloud Storage*, insieme alla crescita esponenziale degli utenti ed alla possibilità di avere più dispositivi per singola persona, determinano un continuo aumento della richiesta di banda. Molti dei servizi di nuova generazione richiedono inoltre una connessione sempre attiva e quindi una copertura di rete pervasiva. Le tecnologie basate sull'utilizzo della fibra ottica ben si prestano a fornire la capacità di canale richiesta, nonché a soddisfare le necessità future. Le reti ottiche d'accesso proposte negli anni passati spaziano dalle reti punto-punto (*Point-to-Point*, PtP), alle reti ottiche attive (*Active Optical Network*, AON), fino a quelle passive (*Passive Optical Network*, PON). Le AON fanno uso di apparati elettricamente alimentati (attivi appunto), quali *router* e *switch*, mentre le PON gestiscono il segnale ottico all'interno della rete utilizzando ripartitori ottici (*splitter*) puramente passivi. Le PON sono quelle che suscitano più interesse, in quanto flessibili e particolarmente adatte all'uso nelle reti d'accesso metropolitane. La rete di accesso di nuova generazione (*Next Generation Access Networks*) dovrà essere in grado di fornire una singola architettura adattabile a servizi multipli, con *bitrate* e modulazioni differenti, mantenendo al contempo i consumi energetici più bassi possibili. La PON è attualmente l'architettura di riferimento che permette di soddisfare i requisiti di queste nuove reti di accesso, in quanto presenta dei costi di messa in esercizio (*capex*) molto più bassi rispetto alle altre tipologie; le attuali politiche messe in atto dal Governo permettono di affrontare i costi molto elevati da sostenere per l'installazione capillare delle fibre ottiche portando l'Italia ad essere in linea con i tempi di sviluppo delle tecnologie di futura generazione. Il tratto di rete cosiddetto verticale, dalla prossimità dell'edificio alla borchia d'utente, essendo la proprietà di natura privata, rimane scoperto da questa azione. Diverse sono le tecnologie che si stanno mettendo in campo per sostenere la capacità di rete offerta dalla fibra e raggiungere gli utenti nei loro appartamenti con connessioni ad elevato bit rate. Tra queste *XG.fast* promette *bitrate* oltre il Gigabit al secondo su distanze inferiori ai cento metri.

Una soluzione possibile per ovviare agli elevati costi di cablaggio o per raggiungere zone in cui è difficile realizzare opere civili (scavi, posa pali, etc.) può essere invece rappresentata da una rete ibrida cablata-wireless, in cui l'ottica in spazio libero, *Free Space Optics* (FSO), si sostituisce al collegamento cablato tra due punti di interesse, permettendo, laddove possibile, di abbattere i costi di messa in esercizio. Il sistema FSO è già una realtà presente in commercio anche se, per ora, ricopre solo applicazioni in piccoli settori all'avanguardia; i motivi per i quali non vi è ancora diffusione di tale tecnologia sono soprattutto le questioni legate al mezzo di propagazione in cui viene inserito e le perturbazioni che appunto, a seconda del mezzo, questa va incontro. Il sistema FSO infatti ha un potenziale di applicabilità molto esteso, praticamente in tutte quelle condizioni in cui la luce è propagabile e quindi in ambienti aperti e chiusi (aria), scenari subacquei (acqua) e spazi extraterrestri (vuoto) per applicazioni satellitari ad esempio; risulta quindi necessario uno studio sulle influenze che il segnale FSO riceve durante la trasmissione in questi ambienti. In spazi chiusi (*indoor*) l'applicabilità risulta molto più semplice in quanto la staticità del mezzo non va a perturbare la propagazione, a meno di forti variazioni dovute al tipo di contesto; ad esempio in un precedente lavoro [1] è stata investigata e dimostrata l'applicazione di tale tecnologia in ambienti data center, grandi sale di server dedicati alla gestione ed allo smistamento dei dati, in cui a seconda dei casi vi possono essere cause di diversa natura che hanno ripercussioni sulla trasmissione [1]. Risulta invece assai più oneroso lo studio a riguardo dell'applicabilità in spazi aperti (*outdoor*), essendo molteplici le variabili climatiche in gioco. Il presente articolo si focalizza appunto sul comportamento dei sistemi FSO nelle suddette condizioni, quando appunto esposti al variare delle condizioni atmosferiche ed all'azione degli agenti climatici.

2. Il sistema FSO outdoor

Per *Free Space Optics* (FSO), ovvero "comunicazioni ottiche in spazio libero", si intende la trasmissione di segnali tra due punti a formare un ponte ottico, effettuata tramite l'utilizzo di una sorgente luminosa, tipicamente laser. Il sistema FSO opera a lunghezze d'onda comprese tra 780-1600nm (tipiche delle telecomunicazioni in fibra), ed attualmente può trasportare dati, voce e video ad una velocità fino a 2.5Gbps [2-7] e 128Gbps a tecnologia ibrida, ovvero sfruttando le risorse e componentistiche di altre tecnologie (es. fibra ottica) [3]; inoltre, alcuni lavori presenti in letteratura, ognuno con un diverso setup sperimentale, hanno raggiunto velocità dell'ordine dei Tbps [4-5].

Un sistema FSO si compone fondamentalmente di tre blocchi: trasmettitore, canale atmosferico e ricevitore. Il link FSO deve essere realizzato in linea di vista (*Line of Sight*, LOS), ovvero in modo che il trasmettitore ed il ricevitore si vedano direttamente, senza la presenza di ostacoli interposta. Per la tecnologia FSO, questo rappresenta forse l'unico importante svantaggio, ma risulta anche un punto a favore,

laddove, ad esempio, vi siano necessità e problemi di sicurezza informatica, in quanto il segnale per poter essere catturato, deve venire interrotto o deviato; di conseguenza è immediatamente rilevabile la falla di sicurezza. Viceversa, nei sistemi a radiofrequenze non vi è possibilità di sapere chi altro stia "captando" il segnale trasmesso, essendo questo propagato in tutto l'ambiente circostante.

Il trasmettitore è costituito da un laser, il che permette collegamenti a grande distanza e ed alta velocità. I collegamenti tipici coprono distanze tra 300m e 5km, ma è possibile spingersi fino a 8÷11km [3]. Rispetto ad un sistema a radio frequenza convenzionale, il sistema FSO presenta numerosi vantaggi che scaturiscono dalle alte frequenze utilizzate (nell'ordine dei THz), disponendo di un ampio spettro di lunghezze d'onda che vanno dai 780nm (vicino infrarosso, *near-IR*) ai 1600nm (infrarosso, *IR*) senza considerare anche la possibilità di trasmettere nel visibile (*Vis* 390÷700nm) il quale però soffre di attenuazioni maggiori [6]. Gli spettri utilizzati inoltre non sono licenziati e cioè non vi sono restrizioni al momento, sull'uso di tali bande di frequenze che interessano la luce visibile ed infrarossa appunto, a differenza invece della banda radio che è ormai satura di trasmissioni.

L'FSO grazie a tali spettri, permette alti *bitrate* di trasferimento superiori ai 100Gbps cosa impossibile con le radiofrequenze; sono stati dimostrati in letteratura 128Gbps di trasferimento su 11Km con tecnologia FSO ibrida [3]. Essendo fuori dallo spettro di interesse delle radiofrequenze, l'FSO presenta un'immunità alle interferenze elettromagnetiche ed essendo il link ottico di una precisione nanometrica, non vi è rischio di *crosstalking* o interferenze di altro genere.

Parlando dei costi invece, questi sono notevolmente ridotti; difatti essendo un link in aria (o più in generale in un mezzo trasparente), non sono necessari i costi dovuti a scavi per interrare linee fisiche che invece risultano essere molto costosi. Questo è anche un vantaggio notevole rispetto alla fibra ottica insieme con il basso BER (*Bit Error* Rate) e la bassa latenza; infatti la luce risulta essere 1.5 volte più veloce in aria che in fibra (la velocità *v*, viene calcolata come *c* velocità della luce*/n*).

Le dimensioni di un sistema FSO sono decisamente ridotte; le testine laser di per sé, sono molto piccole, ma anche considerando la struttura che le contiene insieme con il resto della componentistica, il tutto risulta essere di dimensioni minori rispetto alle antenne a radiofrequenza. L'ingombro generale, dato dall'elettronica circostante di alimentazione e fotorilevazione per il puntamento e dell'involucro di incapsulamento, è meno voluminoso rispetto ad altri sistemi convenzionali, arrivando a dimensioni non oltre quelle di un "piede" cubo (circa $33cm^3$). Questo ne comporta facilità e velocità di installazione, che è un aspetto molto importante soprattutto se si pensa a situazioni di *disaster recovery* (terremoti, alluvioni, ecc.) dove vi è necessita di installare link temporanei, efficienti ed a bassa manutenzione in poco tempo.

C'è da discutere però, anche di alcuni svantaggi che i sistemi FSO presentano; essenzialmente due. Il primo è dovuto all'alta direttività del fascio trasmesso, che rende molto difficile l'acquisizione ed il puntamento del laser, ma questo è vero solo per sistemi FSO passivi non

dotati di elettronica aggiuntiva; gli apparati presenti in commercio, infatti, possiedono elementi atti alla conversione elettro-ottica che rendono fattibile l'auto-puntamento ed allineamento, ovviando così a questo problema. Rimane quindi l'altro dei due principali problemi e cioè la sensibilità a fattori atmosferici quali caligine, nebbia, pioggia e turbolenza, che sono appunto argomento del presente articolo.

3. Applicazioni FSO

Le applicazioni pratiche dei sistemi FSO sono innumerevoli, e riguardano i più svariati ambiti, da quello militare a quello satellitare. Nelle applicazioni militari le comunicazioni ottiche in spazio libero permettono di espandere la connettività all'interno delle basi militari, mantenendo al contempo gli standard di sicurezza necessari ed abbattendo i costi legati alle connessioni in fibra; i sistemi FSO si rivelano preziosi soprattutto nel caso in cui la base militare si trovi su terreni impervi ed ostili, essendo spesso campi provvisori (fig. 1a). Nelle applicazioni di tipo WSP (W*ireless Service Provider*), i sistemi FSO possono essere utilizzati per permettere le comunicazioni wireless in gallerie, aree shopping e/o sotterranee e metropolitane (fig. 1b). La facilità di implementazione dei link FSO permette inoltre il loro utilizzo in ambiti per la connettività d'impresa, per la connessione dei segmenti di LAN ubicati in edifici distinti e li rende particolarmente utili nel caso in cui il sito presso il quale sono installati, debba essere spostato (fig. 1c).

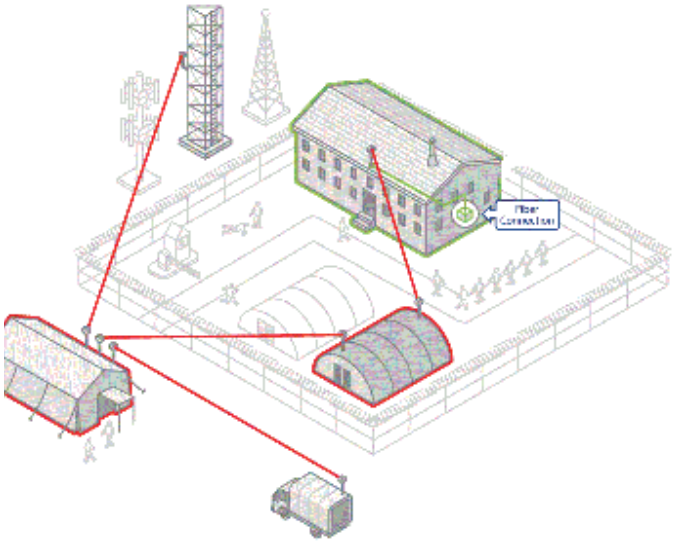


Figura 1a. *Alcuni esempi di applicazioni di link FSO: militari.*

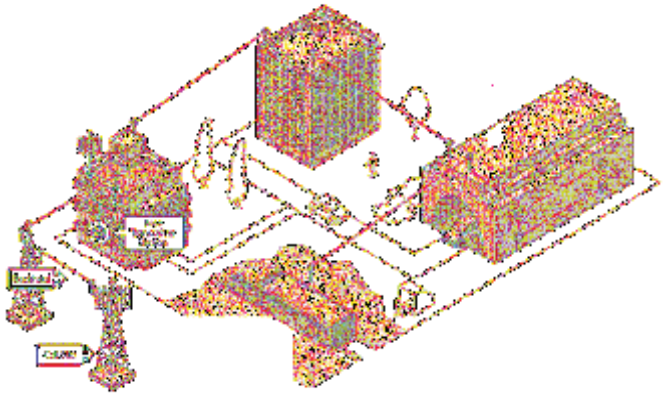


Figura 1b. *Alcuni esempi di applicazioni di link FSO: WSP.*

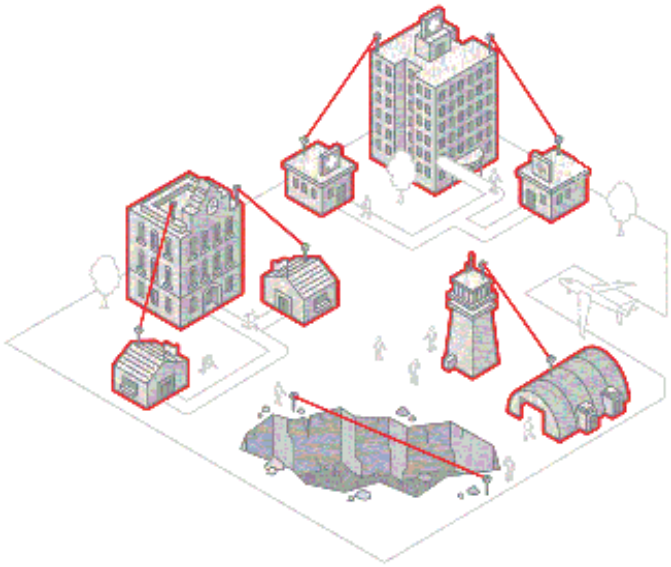


Figura 1c. *Alcuni esempi di applicazioni di link FSO: Connettività d'impresa.*

I collegamenti FSO possono essere utilizzati per risolvere il problema dell'"ultimo miglio", ovvero il calo di risorse che si ha nella rete di accesso; i sistemi FSO, infatti, si prestano all'integrazione con la fibra ottica e possono quindi fornire un collegamento ad alta velocità alle abitazioni non raggiunte direttamente dalla fibra. Sempre in ambito terrestre, un esempio eclatante delle potenzialità dei sistemi ottici in spazio libero è costituito dal drone "Aquila", progettato da Facebook (fig. 2); questo drone ha le dimensioni di un Boeing 737 (come apertura alare), è provvisto di pannelli solari, ed in grado di volare ad un'altezza di 27.000 metri. L'utilizzo di questo drone, è volto a fornire la connettività a banda larga in zone abitative "rurali" dove le tradizionali infrastrutture di rete non possono arrivare (per difficoltà oggettive di realizzazione, o semplicemente per i costi proibitivi). Il cuore del sistema di collegamento è proprio basato sulla tecnologia FSO, tramite una serie di laser che comunicano a terra con dei ricevitori, raggiungendo velocità fino a 10 Gbit/s.

Figura 2. *Il drone di Facebook "Aquila"*

In ambito satellitare è noto che le comunicazioni richiedano lo scambio di una grande mole di dati ad elevate velocità; i sistemi FSO, data l'elevata direzionalità dei fasci ottici e l'elevato *bitrate* ben si prestano ad essere usati in applicazioni di questo tipo. Un esempio attuale è l'uso dei sistemi FSO per i collegamenti nello spazio profondo e per le comunicazioni tra stazioni base e satelliti geo-stazionari.

4. Fenomeni atmosferici e criteri di valutazione di interesse in un sistema FSO

L'attenuazione atmosferica rappresenta una delle maggiori sfide per il canale FSO, in quanto può portare a perdite di segnale, o peggio al "crollo" del collegamento. L'atmosfera, infatti, non provoca solo un effetto di attenuazione del segnale, ma per via delle varie dimensioni delle particelle presenti nella stessa, e quindi vari cambi di indici di rifrazione, si verificano vere e proprie deviazioni del fascio laser. I principali fenomeni atmosferici che influenzano le prestazioni di un canale ottico sono:

- Nebbia e foschia: idrometeore che si formano dal vapore acqueo, che condensandosi formano delle piccolissime gocce d'acqua (5-10µm di diametro). Si parla di nebbia nel caso in cui la visibilità sia inferiore ai 1000m e di foschia se la visibilità è tra i 1000 ed i 5000m; la formazione di queste avviene in caso di umidità relativa della massa d'aria del 100%.
- Fumo: dispersione di particelle solide, solitamente di diametro inferiore a 2µm, risultante dalla condensazione del vapore che scaturisce da reazioni chimiche (quali, ad esempio, la combustione).

- Neve: acqua ghiacciata cristallina, formata da una moltitudine di minuscoli cristalli di ghiaccio, tutti aventi di base una simmetria esagonale, aggregati tra loro in maniera casuale a formare fiocchi di neve che vanno dal 1 ai 5mm di dimensioni.
- Caligine: fenomeno atmosferico in cui polvere, fumo ed altre particelle secche oscurano la limpidezza del cielo.
- Pioggia: insieme di goccioline d'acqua in atmosfera, variabili in numero e forma nel tempo e nello spazio. La forma di queste particelle dipende dalla loro dimensione: sono considerate sfere fino ad un raggio di 1 mm; oltre il mm sono considerate sferoidi oblati.
- Aerosol: sospensione in un gas di particelle di piccole dimensioni, liquide o solide generalmente di diametro inferiore ad 1µm. Gli aerosol sono diversi in natura, forma, dimensioni e concentrazione; data la variabilità di tali particelle, l'interazione tra aerosol e luce può avere una dinamica piuttosto ampia, in termini di lunghezze d'onda ed "importanza" del fenomeno di *scattering*. Poiché gli aerosol hanno origine sulla superficie terrestre, essi raggiungono la maggior concentrazione nello strato limite planetario dell'atmosfera (uno strato fino a 2km sopra la superficie terreste) e decrescono rapidamente al di sopra di esso. A quote più elevate, a causa delle attività atmosferiche e dell'azione combinata dei venti, la concentrazione di aerosol diventa spazialmente uniforme e più indipendente dalla collocazione geografica. L'interazione principale tra aerosol e raggio laser è rappresentata dallo *scattering*, il quale, data la dimensione delle particelle comparabile alle lunghezze d'onda d'interesse nelle comunicazioni ottiche, è descritto matematicamente dalla teoria dello *scattering* di Mie [8]. Secondo tale teoria il coefficiente di *scattering* degli aerosol è funzione della loro distribuzione dimensionale, sezione trasversa, densità e lunghezza d'onda "operativa".

In generale, l'insieme di tutte le particelle, solide o liquide, disperse in atmosfera, con diametro compreso tra qualche nanometro e decine/centinaia di micrometri, viene chiamato "particolato". Le dimensioni dei vari costituenti atmosferici e le relative concentrazioni sono riportate in Tabella 1 [9].

Tipo	**Raggio (μm)**	**Concentrazione (cm^{-3})**
Molecole d'Aria	10^{-4}	10^{19}
Aerosol	10^{-2}	da 10 a 10^{3}
Nebbia	da 1 a 10	da 10 a 100
Nuvole	da 1 a 10	da 100 a 300
Gocce di pioggia	da 10^{-4} a 10^{-2}	da 10^{-5} a 10^{-2}
Neve	da 10^{3} a $5x10^{3}$	N/A
Caligine	da $5x10^{3}$ a $5x10^{4}$	N/A

Tabella 1. Dimensioni e concentrazione dei costituenti atmosferici (particolato). I dati sono presi dallo studio condotto da X et al. [9].

Per la caratterizzazione del *link* ottico, in base ai fenomeni enunciati precedentemente, vi sono molteplici parametri d'interesse; questi risultano essere più o meno importanti a seconda dell'applicazione richiesta. Ad esempio, le condizioni cambiano su lungo o breve raggio a seconda della possibilità di potenze di emissione utilizzabili; di seguito verranno elencate e discusse le singole variabili da considerare per un *set-up* ottico FSO.

La **visibilità** è il primo dei parametri da considerare. In generale, è la misura della distanza alla quale un oggetto (o una luce) possono essere distinti chiaramente; dal punto di vista meteorologico, la visibilità è riferita alla trasparenza dell'aria, definita come portata ottica meteorologica MOR (*Metereological Optical Range*), ovvero la distanza atmosferica alla quale un oggetto di colore nero può essere visto e riconosciuto quando osservato contro uno sfondo chiaro oppure, analogamente, la distanza alla quale la potenza di riemissione luminosa (di un oggetto illuminato da un fascio collimato generato da una lampada ad incandescenza a 2700K), viene ridotta del 5% della sua intensità d'origine. La scarsa visibilità abbassa l'efficacia e la disponibilità dei sistemi FSO: tale condizione può verificarsi durante uno specifico periodo dell'anno o in specifici momenti della giornata. Si ha anche scarsa visibilità quando la concentrazione e la dimensione delle particelle è più alta rispetto alla visibilità media.

L'**attenuazione** atmosferica: è definita come quel processo per il quale la totalità o una parte delle onde elettromagnetiche viene persa nell'attraversamento dell'atmosfera. Sono diversi gli effetti che la determinano e sono variabili nel tempo, oltre ad essere dipendenti dalle condizioni locali e dalle condizioni metereologiche; in generale, l'attenuazione atmosferica è data dalla legge di Beer-Lambert [8] e viene misurata in dB/Km. Tra i fenomeni più importanti che causano attenuazione atmosferica ci sono l'assorbimento e lo *scattering*. L'assorbimento è causato dalle collisioni dei fotoni con particelle allo stato liquido o solido in aria (vapore acqueo, polvere, ghiaccio e

molecole organiche), a cui i fotoni cedono energia; il coefficiente di assorbimento dipende dal tipo di molecole gassose e dalla loro concentrazione. Dipende dalla lunghezza d'onda ed è perciò selettivo; per tale motivo l'atmosfera ha delle zone "trasparenti", ovvero dei *range* di lunghezze d'onda in cui l'assorbimento è minimo, chiamate "finestre" di trasmissione. Le lunghezze d'onda utilizzate in ambito FSO vengono fatte coincidere con queste finestre, ragion per cui il coefficiente di assorbimento è trascurabile ed il fenomeno di attenuazione è quindi principalmente dato dallo *scattering*. Lo *scattering* è la dispersione di un raggio in un insieme di direzioni in seguito all'interazione fisica tra particella ed onda elettromagnetica; nel momento in cui avviene l'interazione, i fotoni del fascio luminoso vengono deviati in ogni direzione, provocando la variazione della traiettoria del fascio incidente, che risulta quindi in una perdita del segnale utile, in quanto parte del fascio non riesce a raggiungere il ricevitore. Ci sono tre tipi principali di *scattering*: di Rayleigh, di Mie e "non selettivo". Il primo interessa gas molecolari e atmosferici di dimensioni molto minori rispetto alla lunghezza d'onda del raggio incidente. Ne risulta che lo *scattering* di Raylegh è trascurabile nell'infrarosso, mentre è significativo nelle bande dall'ultravioletto al visibile [11]. Lo *scattering* di Mie invece si ha nel caso in cui il diametro della particella sia uguale o maggiore di un decimo della lunghezza d'onda del raggio laser incidente; questo tipo di *scattering* interessa aerosol di dimensioni maggiori delle molecole di gas ed è la causa principale dell'attenuazione alle lunghezze d'onda d'interesse per le comunicazioni FSO. Lo *scattering* di Mie è perciò, il fenomeno da tenere maggiormente in conto quando si parla di ottica in spazio libero, in quanto l'attenuazione può raggiungere valori di centinaia di dB/km, le cui attenuazioni massime si hanno in presenza di nebbia; le particelle di nebbia sono infatti più piccole e permangono più a lungo nell'atmosfera causando un'attenuazione maggiore rispetto alla pioggia. Lo *scattering* dovuto alle piogge invece, viene denominato "non selettivo", poiché il raggio delle gocce (100-1000 μm) è molto maggiore rispetto alla lunghezza d'onda tipica di un sistema FSO; il raggio laser può quindi passare attraverso le particelle d'acqua. Le caratteristiche delle gocce di pioggia sono ben descritte dal modello di Best [12].

Tra le altre variabili vi sono poi le **turbolenze**; questo fenomeno influenza la propagazione del raggio ottico producendo una fluttuazione spaziale e temporale dell'indice di rifrazione, dovuta alle variazioni di temperatura, pressione e vento. La turbolenza atmosferica causa lo sfasamento del segnale ottico, ovvero la distorsione del fronte d'onda; tali aberrazioni ottiche causano anche distorsioni dell'intensità del segnale (fenomeni di scintillazione). Le variazioni di umidità, temperatura e pressione producono variazioni di densità, le quali portano alla variazione dell'indice di rifrazione in aria; tali variazioni vengono dette vortici ed hanno un effetto "lente" sul raggio che si propaga attraverso essi [12]. Se la dimensione dei vortici è maggiore del diametro del raggio, l'intero fascio del laser viene curvato; se invece la dimensione dei vortici è inferiore, il raggio viene distorto. Piccole variazioni nel tempo di arrivo dei vari componenti del fronte d'onda del

raggio producono interferenze costruttive e distruttive, che provocano fluttuazioni temporali dell'intensità del raggio in ricezione.

Se si considera, invece, l'atmosfera come un fluido viscoso si possono distinguere due diversi moti: il flusso laminare ed il flusso turbolento. Il flusso laminare è caratterizzato da uno scorrimento di strati di fluido gli uni sugli altri senza nessun rimescolamento; le caratteristiche della velocità del flusso laminare si mantengono quindi uniformi o variabili in maniera regolare. Nel caso del flusso turbolento, invece, il moto delle particelle di fluido avviene in maniera caotica, poiché le forze viscose non riescono a contrastare le forze d'inerzia e si creano quindi i cosiddetti vortici; per valutare se il flusso segue un regime di scorrimento laminare o turbolento si utilizza il numero di Reynolds, che risulta proporzionale al rapporto tra le forze d'inerzia e le forze viscose. Nel caso di regime laminare si avrà un numero di Reynolds alto, mentre nel caso di regime turbolento il numero di Reynold (*Re*) assumerà un valore più basso [6]. Per comprendere la struttura della turbolenza atmosferica è conveniente adottare la teoria della cascata di energia di Richardson, il quale ipotizza che in un fluido ad alto numero di Reynolds, i disturbi a piccola scala siano approssimativamente isotropi. Secondo la teoria di Richardson, un aumento del numero di Reynolds di un fluido in moto laminare provoca il passaggio al regime turbolento e la comparsa non simultanea di disturbi di diverse dimensioni (ordini). Nello specifico non appena *Re* supera il valore critico appaiono i disturbi a grande scala (disturbi del primo ordine), i quali, data la loro instabilità, generano disturbi del secondo ordine, che prelevano energia dai primi. A loro volta i disturbi del secondo ordine generano disturbi del terzo ordine e così via. Si viene quindi a creare una gerarchia in cui avviene un trasferimento di energia tra i disturbi a scala superiore a quelli a scala inferiore (cascata energetica), fino ad arrivare al punto in cui la viscosità trasforma tutta l'energia in calore. A partire dal concetto di cascata di energia di Richardson, Kolmogorov formula la prima teoria statistica della turbolenza, che permette di quantificare il fenomeno descritto qualitativamente da Richardson [13]. La teoria di Kolmogorov si applica alla turbolenza omogenea e isotropa, condizione di fatto irrealizzabile nei sistemi reali e che quindi costituisce un'astrazione concettuale volta alla semplificazione della trattazione teorica (si osserva comunque che tutti i sistemi reali sono localmente isotropi e omogenei).

La turbolenza ha in sé due effetti principali, quali la scintillazione e la diffusione del fascio. Per scintillazione del fascio si intende la variazione della densità di potenza ricevuta, causata dalle interferenze distruttive dei disturbi di piccola scala; la scintillazione è uno degli effetti da tenere in maggiore considerazione quando si parla di FSO. Le fluttuazioni di intensità della luce infatti, sono descritte dall'indice di scintillazione come la varianza normalizzata dell'intensità delle fluttuazioni [10]. La diffusione invece, descrive l'allargamento della dimensione del fascio a causa della diffrazione nell'atmosfera turbolenta [14]. In presenza di turbolenza atmosferica è bene descrivere le prestazioni di un collegamento FSO in termini di probabilità di "mancata rilevazione", la quale descrive la percentuale di tempo in cui l'irradianza dell'onda ricevuta si trova al di sotto della soglia prestabilita;

quindi, se il rapporto segnare rumore SNR (*Signal Noise Ratio*) nello spazio libero è sufficientemente alto, la probabilità di mancata rilevazione è determinata dai soli effetti atmosferici e viene espressa in funzione della soglia dell'irradianza [6].

Vi sono poi perdite dovute alla geometria definite come ***path-loss* geometrico**, che dipendono dalla larghezza del fascio (*beam-width*) del trasmettitore [15]. Le perdite geometriche devono sempre essere tenute in conto quando si parla di collegamenti FSO, in quanto tali perdite non sono variabili nel tempo come quelle provocate dall'attenuazione atmosferica, ma sono fisse per ogni specifico collegamento FSO.

Infine troviamo l'**attenuazione totale**, ovvero la somma di tutti i parametri suddetti considerati però ad alto livello.

5. Descrizione del setup FSO

Il sistema FSO è stato allestito su un banco ottico stabilizzato situato al piano terra del Ministero dello Sviluppo Economico di Roma, presso i laboratori dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), quale direzione del ministero stesso. In particolare, la stanza è dotata di una finestra che affaccia direttamente sul cortile interno dell'edificio; dirimpetto, ad una distanza di 40 metri circa, in un'altra stanza affacciata al medesimo cortile, vi è uno specchio, di diametro 6cm.

Tramite quest'ultimo, il percorso ottico totale in *back-to-back* (ovvero il segnale viene generato, trasmesso e ricevuto nella stessa stanza) risulta quindi essere di circa 80m, considerate anche le varie riflessioni all'interno delle stanze (fig. 3).

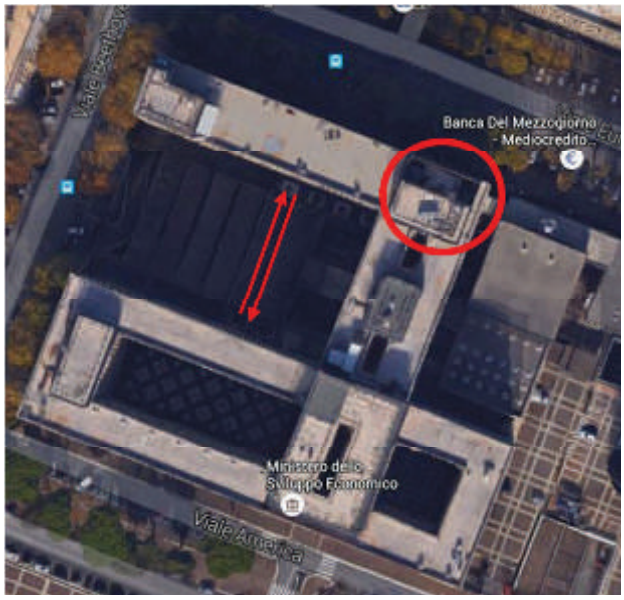


Figura 3a. Setup FSO: visuale dall'alto del percorso ottico e stazione meteo (cerchiata).

Figura 3b. Setup FSO: finestra su cortile.

Figura 3c. Setup FSO: banco ottico.

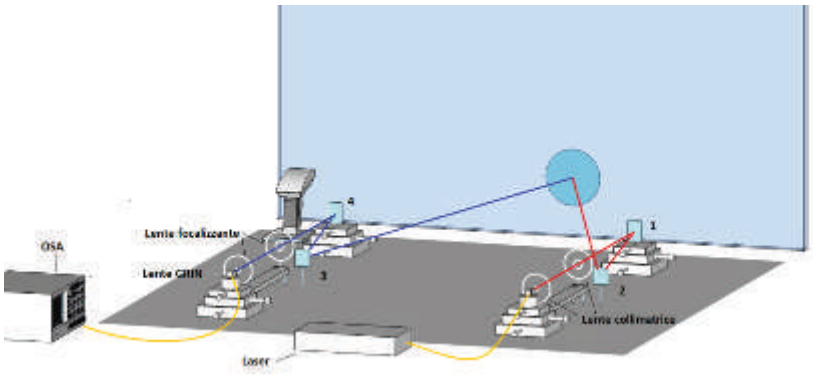


Figura 3d. Setup FSO: schema del setup sul banco ottico.

Il setup FSO in oggetto è di tipo completamente passivo, ovvero la sorgente laser viene trasportata in fibra e fatta emettere direttamente dalla fibra e riaccoppiata di ritorno in fibra (senza conversioni elettro-ottiche). Il setup è frutto dell'investigazione che è stata concordata di intraprendere; ovvero sono state individuate le grandezze significative da misurare e sono stati inseriti nei setup gli opportuni strumenti. Le grandezze in analisi sono elencate in seguito.

In Figura 3d viene riportato lo schema di principio del set-up FSO. Questo è diviso in sezione trasmittente e sezione ricevente che sono perfettamente simmetriche tra loro così da poter essere interscambiabili. Sulla parte trasmittente, a partire dalla terminazione della fibra, è posta una lente GRIN, ovvero una lente ad indice di rifrazione graduato che funziona in questo caso da *beam expander*, cioè permette di defocalizzare il fascio allargandolo; il raggio emesso dal laser quindi viene espanso dalla GRIN ed arriva su un'altra lente asferica (modello AL1020-C Thorlabs) che lo collima in un pacchetto simmetrico di fasci paralleli (le lenti collimatrici hanno quest funzione di rendere i raggi paralleli tra loro). A distanza di 30cm dalla prima lente collimatrice è posta una seconda lente collimatrice di diametro pari a 30mm. Il raggio incide quindi sullo specchio indicato in figura con il numero 1 e viene riflesso sullo specchio indicato con il numero 2. Quest'ultimo è orientato in modo tale che il raggio da esso riflesso attraversi la finestra chiusa ed incida sullo specchio che si trova al di là del cortile; questo riflette il raggio, che va ad incidere sullo specchio numero 3 e successivamente sullo specchio 4. Da questo punto parte la sezione ricevente; il raggio laser incide quindi su di una lenta focalizzante di diametro pari a 30 mm ed in seguito su di un'altra lente GRIN, che in questo caso è posizionata in modo tale da focalizzare il fascio in fibra; questa raggiunge quindi l'Optical Spectrum Analyzer (OSA), che fornisce la misura in potenza del segnale ricevuto. Completa il setup la termocamera (FLIR E50) che ha lo scopo di misurare la temperatura del vetro della finestra nella zona in cui attraversano i raggi diretto e riflesso; la termocamera misura inoltre la temperatura della meccanica del banco ottico. La termocamera è uno strumento che rileva la radiazione infrarossa (invisibile all'occhio umano) e la converte in un'immagine visibile. La radiazione infrarossa è emessa da ogni oggetto che si trovi ad una temperatura superiore allo zero assoluto ed aumenta in intensità con l'aumentare della temperatura. Una telecamera ad infrarossi calibrata è in grado di restituire le immagini termografiche dell'oggetto e di fornire misure in temperatura accurate senza la necessità di un contatto diretto. Tale strumento è dotato di puntatori che permettono di selezionare i punti o le aree di interesse e di uno spotmeter in grado di effettuare la misura della temperatura (massima, minima e media) nell'area selezionata. Il *range* di temperatura è selezionabile dall'utente.

Per poter utilizzare in modo efficiente il sistema FSO e quindi ridurre al minimo le perdite per disallineamento del sistema, è necessario ottimizzare il setup posizionando in modo opportuno gli specchi e le lenti.

6. Stazione meteo ed analisi dati

Il setup FSO è direttamente interfacciato, mediante piattaforme software, ad una stazione meteo situata sul terrazzo del Ministero (Fig.3a). Le strumentazioni utilizzate per la misura dei dati meteorologici sono molteplici, quali:

- **Anemometro** *Campbell Scientific* 05103-L: è uno strumento in grado di misurare velocità del vento comprese tra 0 e 100m/s, con un'accuratezza di ± 0.3m/s, e direzione del vento a 360°. La velocità del vento viene misurata mediante un'elica a quattro pale di forma elicoidale, la cui rotazione produce un segnale sinusoidale AC, con frequenza proporzionale alla velocità del vento. La direzione del vento, invece, viene ricavata dall'orientazione dell'anemometro; in uscita si ha una tensione che risulta direttamente proporzionale all'angolo di *azimuth*.

- **Pluviometro** *Sianmicros* a bascula con sensore SIAP UM 7505: è uno strumento per la misura dei parametri riguardanti le precipitazioni piovose. Il sensore è composto da un'area di raccolta di 720cm^2 e da una bascula a doppia vaschetta collegata ad un magnete che genera un impulso in uscita ad ogni commutazione.

- ***Combilog*** 1020 di Theodor Friedrichs & Co. con interfacce seriali (RS232 e RS485) che permettono la comunicazione via ASCII, PROFIBUS o MODBUS: gli strumenti fin qui descritti sono collegati a questo *datalogger* progettato appositamente per sistemi di misura meteorologici, idrologici e ambientali. È dotato di 8 canali di misura analogici e 6 digitali e supporta tutti i più comuni tipi di sensori, che possono essere connessi simultaneamente; lo strumento è in grado di calcolare valori medi, minimi, massimi, deviazione standard e altre funzioni aritmetiche collezionabili via software. I sei input/output digitali possono essere usati per raccogliere segnali di *feedback*, misurare frequenze o per ricevere segnali seriali in codice di *Gray* a 8 bit.

- **Disdrometro**-visibilimetro PWS100 (*Present Weather Sensor*) della Campbell Scientific: è uno strumento per stazioni meteorologiche in grado di misurare parametri di pioggia e visibilità. Il dispositivo può lavorare a temperature ambientali che vanno dai –25°C ai 50°C, in presenza di vento con velocità fino a 60m/s.

Il PWS100 è costituito da un'unità laser e due sensori posizionati ad angoli di 20° rispetto all'asse ottico del laser, di cui uno sul piano verticale e l'altro sul piano orizzontale; l'unità laser (Figura 2.8) è costituita da vari componenti ottici che permettono di creare una sorta di piano di luce.

Il laser opera ad una lunghezza d'onda di 830nm ed è modulato in frequenza a 96Hz. Questa struttura permette di definire un volume adatto a rivelare particelle di varie dimensioni, costituito da quattro piani di luce di 0.4mm di profondità ed equi-spaziatura. Quando una particella attraversa l'area di rivelazione emette un segnale dal quale è possibile ricavare la natura del fenomeno in atto; la velocità delle particelle viene ricavata calcolando il tempo che intercorre tra due picchi di segnale consecutivi. Il diametro invece è calcolato combinando le

informazioni sulla velocità con il ritardo che intercorre tra la rivelazione del picco da parte dei due sensori.

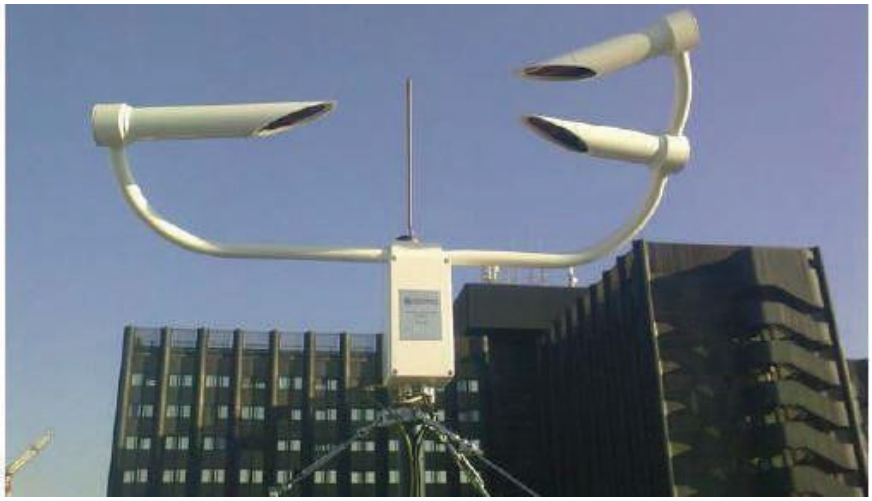


Figura 4. Disdrometro-visibilimetro

La visibilità viene misurata mediante tecniche di *scattering* che permettono di stimare il *range* ottico meteorologico (MOR). La quantità di particelle scatterate in corrispondenza dei sensori è proporzionale alla visibilità per quanto concerne le piccole particelle di nebbia. Nel caso in cui le particelle siano di dimensioni maggiori (come pioggia ad esempio), il PWS100 stima la visibilità utilizzando come fattore di calibrazione la propria capacità di discriminare le particelle. Le informazioni che il disdrometro-visibilimetro è in grado di fornire sono numerose, tra queste si ricordano: visibilità media (in m); intensità di pioggia (in mm/h); pioggia accumulata; distribuzione delle gocce di pioggia; velocità media delle particelle (in m/s); dimensioni medie delle particelle (in mm) e tipo di precipitazione. L'intervallo di visibilità misurabile dallo strumento va da 0 a 20000m, con un'accuratezza del 10%. Le particelle rilevabili dallo strumento hanno un diametro che va da 0.1mm a 30mm (con accuratezza del 5%) ed una velocità da 0.16m/s a 30m/s. Le tipologie di precipitazione che il PWS100 è in grado di riconoscere sono: pioviggine (gocce di pioggia di diametro inferiore a 0.5mm), pioggia, neve, caligine (nebbia, foschia, fumo, polvere, ecc.), grandine, neve tonda (è una precipitazione costituita da granelli di ghiaccio di diametro tra 2 e 5mm); pioggia e pioviggine congelantesi, ovvero precipitazioni liquide che ghiacciano al contatto con un oggetto).

Per l'identificazione del tipo di fenomeno e della relativa intensità vengono forniti i codici WMO (*World Meteorological Organization*); facendo uso del software *PWSViewer* di Campell Scientific è possibile connettersi allo strumento e scegliere i dati da includere nel messaggio che il PWS100 invia periodicamente. Nel caso in esame, i dati di maggiore interesse risultano essere: visibilità; tipologia di precipitazione; dimensione delle particelle. Il software di acquisizione creato è provvisto di una sezione per la lettura dei dati provenienti dal disdrometro-visibilimetro.

- **Mediaconverter Moxa** Moxa NPort IA5450A: è uno strumento che permette la connessione seriale-Ethernet; è provvisto di due porte

Ethernet a 10/100 Mbps e quattro porte seriali RS-232/422/485 con *baudrate* da 50 a 921.6kbps.

Gli strumenti meteorologici sono alimentati mediante un pannello fotovoltaico, realizzato con sei moduli di silicio policristallino, in grado di sviluppare una potenza di picco di 150W. Al pannello è connesso un modulo batterie a ricombinazione, in grado di fornire 48V con una capacità di 200Ah. In Figura 5 viene mostrato uno schema riassuntivo delle attuali interconnessioni tra gli strumenti meteorologici e l'isola fotovoltaica.

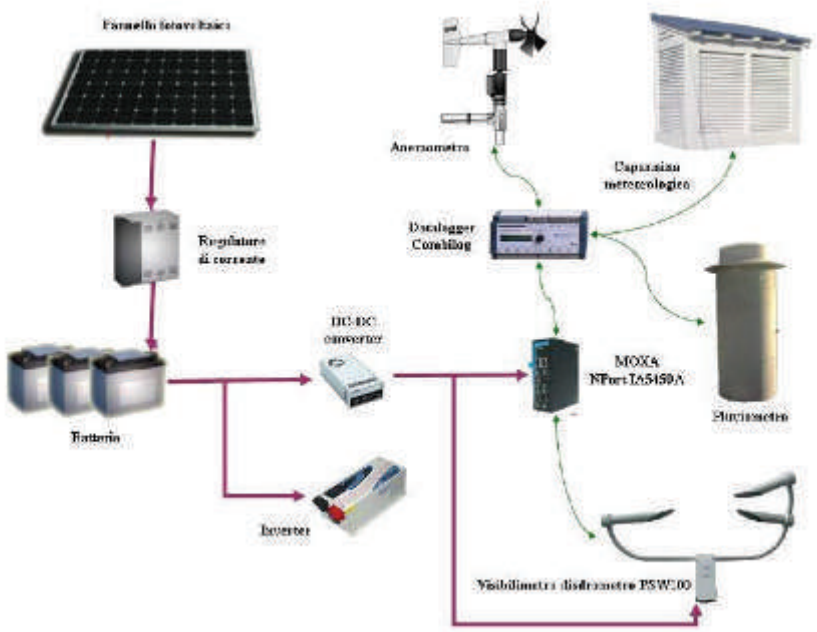


Figura 5. Schema a interconnessioni tra gli strumenti della stazione meteo.

I dati provenienti dalla stazione metereologica e le misure di potenza registrate dall'OSA (*Optical Spectrum Analyzer*) sono stati utilizzati per studiare il comportamento del sistema FSO al variare delle condizioni atmosferiche. Per effettuare l'analisi dei dati si è fatto ricorso all'ambiente per il calcolo numerico *MATLAB*, al software di *data-analysis Origin* ed all'ambiente di programmazione di tipo grafico *LabVIEW*, il quale consente di realizzare programmi in forma di diagrammi a blocchi. I dati sono stati raccolti impostando un intervallo di acquisizione pari a 1 secondo.

Le prime analisi effettuate hanno lo scopo di comprendere quali siano le grandezze che influenzano più significativamente l'andamento della potenza del segnale ottico ricevuta nel tempo. I parametri presi in considerazione sono i seguenti:

- Potenza del segnale (dBm); differenza tra potenza di lancio e ricevuta di ritorno.
- Temperatura esterna (°C);
- Temperatura del vetro della finestra del laboratorio (°C); deviazioni del fascio dovute alle variazioni termiche del vetro della finestra in uscita.

- Temperatura della componentistica meccanica strutturale interna del laboratorio (°C); deviazioni del fascio dovute all'escursione termica dei materiali e banchi ottici in uso.
- Temperatura del vetro della finestra del laboratorio (°C);
- Umidità (%);
- Pressione atmosferica (hPa);
- Velocità e direzione del vento (m/s e gradi di rotazione);
- Intensità ed accumulo della pioggia (mm/h).

In figura 6 è possibile osservare l'andamento delle variabili relative alla temperatura in un periodo di tempo di misure consecutive di 5 giorni (lo stesso andamento è risultato anche su scale maggiori di 15-20 giorni ripetute in più sessioni di misura).

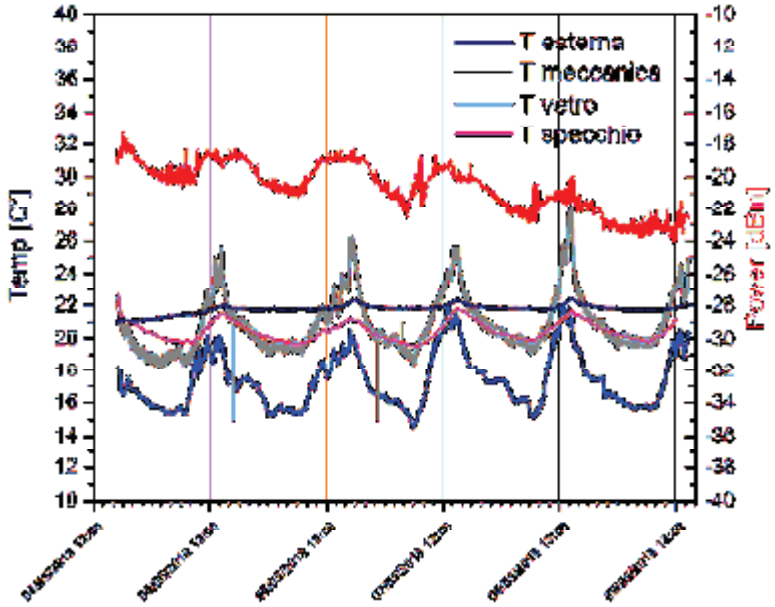


Figura 6. *Correlazione tra potenza e temperature componentistica*

Già da una prima analisi del grafico è evidente l'elevato grado di similitudine esistente tra la curva rappresentativa dell'andamento della potenza nel tempo e la curva delle diverse temperature in gioco; vi è infatti la temperatura esterna che influenza gran parte del segnale e la temperatura delle stanze di laboratorio da cui proviene il segnale stesso. Le temperature registrate dalla termocamera presentano un andamento fortemente correlato all'andamento della temperatura esterna registrata dalla stazione meteo. Queste vanno ad influenzare le dilatazioni termiche della strumentazione e componentistica meccanica, causando disallineamenti e defocalizzazioni. La temperatura del vetro delle finestre attraverso le quali passa il segnale va anch'essa ad influenzare di molto la potenza ricevuta; vi sono infatti 4 attraversamenti sui vetri (essendo due le stanze in oggetto ed essendo doppi gli attraversamenti per l'andata ed il ritorno del segnale) e questi, essendo soggetti ad irraggiamento solare, ombreggiamento e sbalzi di temperatura tra notte e giorno, sono chiaramente anch'essi soggetti a dilatazione. Potenza e temperatura risultano direttamente proporzionali

quindi; laddove c'è una variazione della temperatura si verifica anche una variazione del valore di potenza registrato. Si viene a formare un ciclo di isteresi non ideale che ne determina quelle oscillazioni in un periodo di 24h. L'affezione dell'isteresi sul segnale non è ideale in quanto le varie dilatazioni e latenze menzionate sopra, meccanicamente non tornano alle stesse condizioni di partenza; ne risulta quindi che il segnale di potenza ricevuto, complessivamente tende a decrescere al passare dei giorni.

In figura 7 sono riportati gli andamenti relativi all'umidità esterna, pressione atmosferica e velocità del vento.

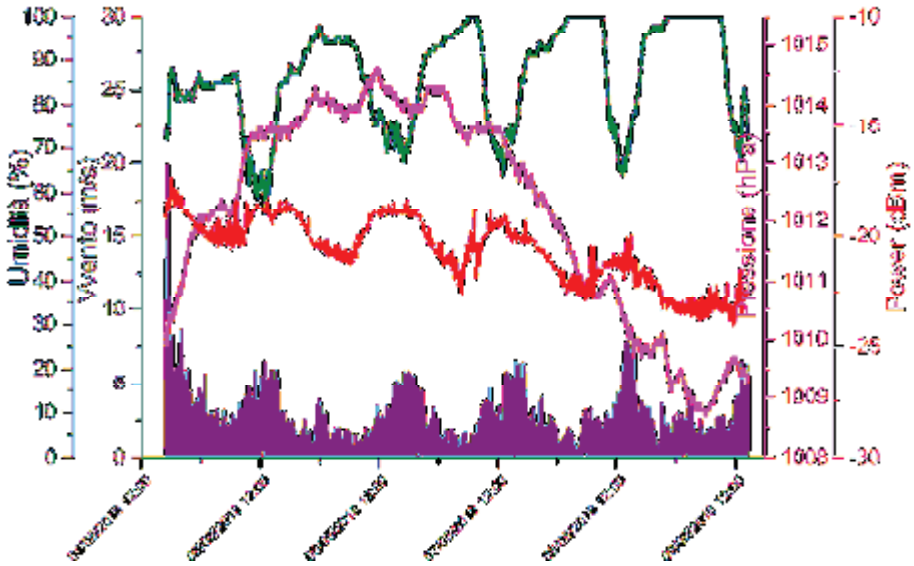


Figura 7. Correlazione tra potenza ed umidità esterna, pressione atmosferica e velocità del vento

Si osserva come la curva dell'umidità (in verde) abbia un andamento quasi perfettamente complementare rispetto alla curva di potenza, nonché, per quanto detto prima, complementare anche alla temperatura, come effettivamente ci si aspetta che sia. Le due grandezze di temperatura e umidità risultano quindi essere inversamente proporzionali; si vede come ad un aumento dell'umidità corrisponda una diminuzione della potenza ed a un abbassamento dell'umidità corrisponda invece un aumento della potenza del segnale ricevuto. Questo fenomeno ribadisce esattamente quanto detto nella trattazione teorica ovvero che un'elevata percentuale di umidità indica una maggiore concentrazione di particelle di vapore acqueo nell'atmosfera, le quali alimentano i fenomeni di *scattering*, che provocano una pesante attenuazione del segnale, quindi una diminuzione sostanziale della potenza ricevuta. Il sistema risulta comunque strettamente correlato anche agli altri fattori atmosferici. La velocità del vento per esempio (curva viola) contribuisce anch'essa ai fattori d'influenza sulla potenza ricevuta; infatti risulta chiaro ed intuitivo che all'aumentare del vento decresca l'umidità e di conseguenza aumenti la potenza ricevuta. Questo accade perché la ventilazione favorisce la vaporizzazione delle particelle d'acqua allo stesso modo in cui agisce l'innalzarsi della temperatura; all'aumentare

del vento inoltre, aumenta anche la variazione istantanea della potenza per effetto delle turbolenze.

Per quanto concerne invece la pressione in figura 7 (curva magenta), non è stato ancora possibile evidenziare un legame con l'andamento della potenza ricevuta, ragion per cui nel seguito dell'analisi ci si focalizzerà prettamente su temperatura e umidità. Ripetute misure nell'arco di due anni circa, hanno mostrato una forte incoerenza negli andamenti di pressione rispetto a quelli della potenza; non vi è evidenza sperimentale del legame diretto tra le due grandezze. Questa mancanza di legame è però ragionevole in quanto la pressione non è una variabile "diretta" come la temperatura e l'umidità e cioè non va ad influenzare in tempo reale l'attenuazione del segnale FSO; è invece una variabile "indiretta" ovvero dipendente anche essa dagli stessi fattori di umidità e temperatura. Non è risultato quindi produttivo analizzare variabili indirette come questa in quanto richiederebbe strumentazioni più sofisticate ed uno studio assai più oneroso; anche la direzione del vento insieme con la pressione è stata scartata come variabile d'interesse in quanto determinata dall'accumulo e dispersione di zone di aria calda e fredda in regioni di territorio molto vaste.

Analizzando più in dettaglio gli sbalzi di potenza tra la mattina e la sera, andando a vagliare le ore più calde del giorno, è stato osservato (figura 8) come la potenza presenti variazioni molto evidenti, fino anche a 30dBm, tra le 08:00 e le 20:00.

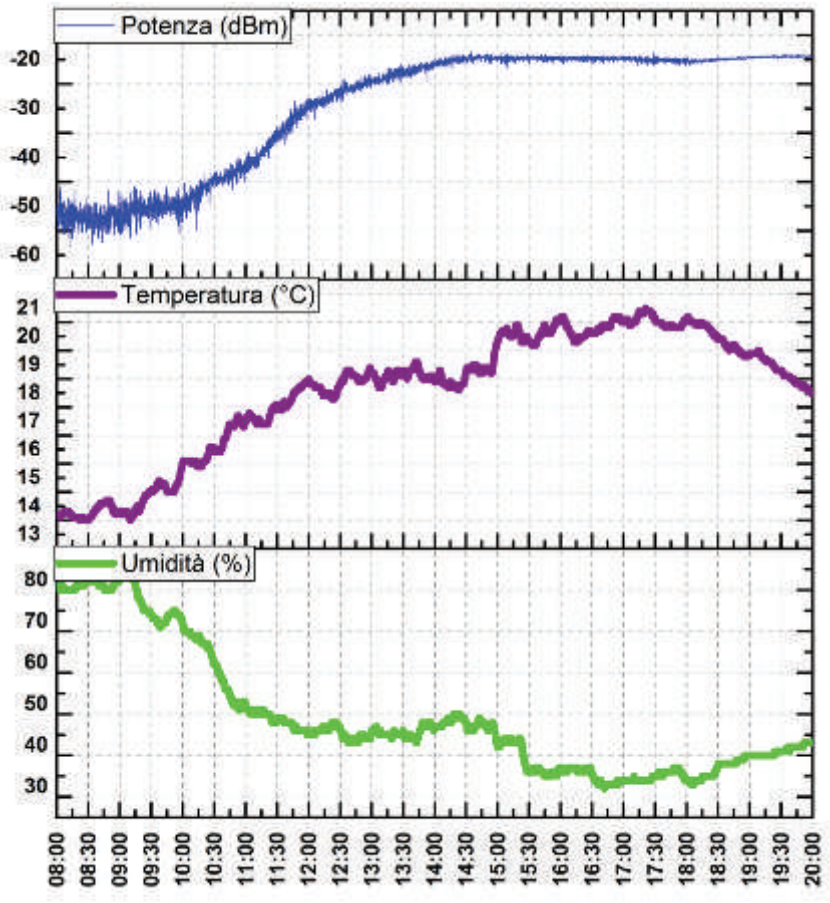


Figura 8. Andamento di potenza diurno tipico in relazione a temperatura e umidità

Si osserva inoltre come le oscillazioni puntuali di potenza maggiori si verifichino nei periodi in cui l'umidità è più alta e la temperatura più bassa, il che è in linea con la quantità di particelle di acqua nell'aria che generano *scattering*. Per studiare la variazione complessiva della potenza del segnale nelle ore diurne e nelle ore notturne si è calcolata, mediante gli algoritmi di calcolo del software *Origin*, la deviazione standard della potenza, la quale esprime proprio la variabilità dei valori registrati intorno al valor medio. Dal grafico di figura 9a si osserva in media una maggiore variabilità della potenza nelle ore diurne rispetto a quelle notturne, sempre e comunque effetto diretto di temperatura e umidità.

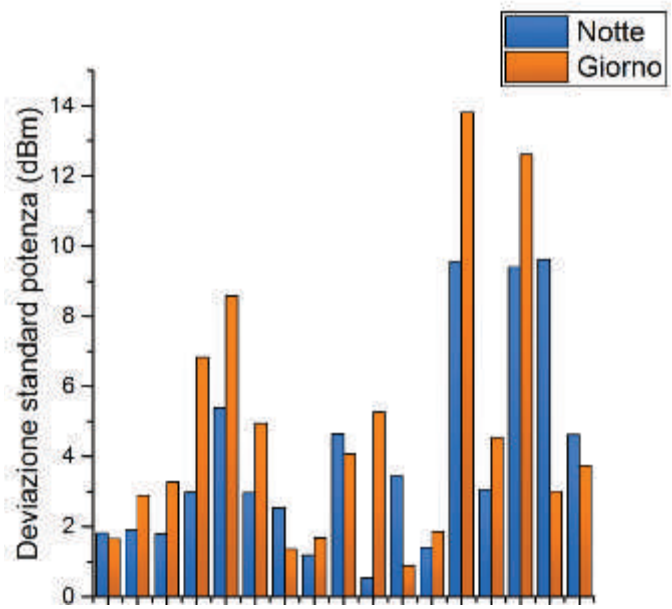


Figura 9a. Deviazione standard giorno/notte di potenza.

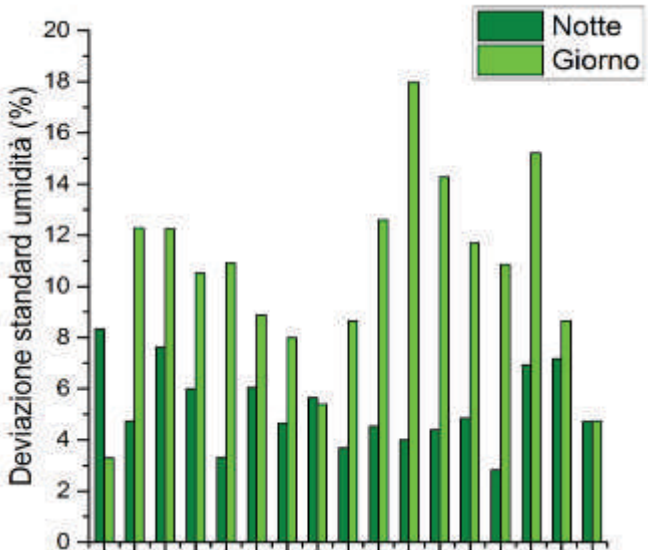


Figura 9b. Deviazione standard giorno/notte umidità.

È interessante confrontare la variabilità della potenza appena osservata con la variabilità di giorno e di notte, dell'umidità (figura 9b) è

quindi possibile vedere come anche l'umidità presenti una maggiore variabilità di giorno rispetto alla notte. Il confronto dei grafici testimonia ulteriormente la correlazione tra umidità e potenza evidenziata nel paragrafo precedente. Per analizzare in modo approfondito la variazione istantanea della potenza è tuttavia stato necessario calcolare la deviazione standard in un intervallo molto più piccolo rispetto alle 12 ore considerate nei grafici precedenti.

Si è quindi realizzato uno script in *MATLAB* in grado di analizzare un numero ristretto di campioni di potenza e umidità calcolandone rispettivamente deviazione standard e valor medio. Si è scelto di calcolare la deviazione standard e media ogni quarto d'ora ed è risultato di nuovo che la potenza subisce maggiori oscillazioni intorno al valor medio in corrispondenza di valori elevati di umidità. In particolare per umidità compresa tra il 60% e 80% si verificano variazioni di potenza da 1dBm fino a circa 2.2dBm. Le variazioni scendono notevolmente nelle ore della giornata in cui l'umidità di mantiene al di sotto del 50%; le variazioni istantanee di potenza di maggiore entità si sono registrate più e più volte nel corso di due anni di misure, confermando quanto detto, in corrispondenza di valori elevati di umidità.

Per quanto riguarda invece le precipitazioni, il discorso cambia notevolmente; la pioggia è in questo caso da considerarsi un "particolato" di grandi misure, ovvero particelle d'acqua di dimensione molto al di sopra dell'umidità. In caso di piogge leggere il segnale viene pressoché lasciato inalterato garantendo una comunicazione del sistema, ma in casi di temporali improvvisi e massicci, si oltrepassano i casi di attenuazione e *scattering* menzionati nei paragrafi precedenti, fina al raggiungere fenomeni di oscuramento (figura 10).

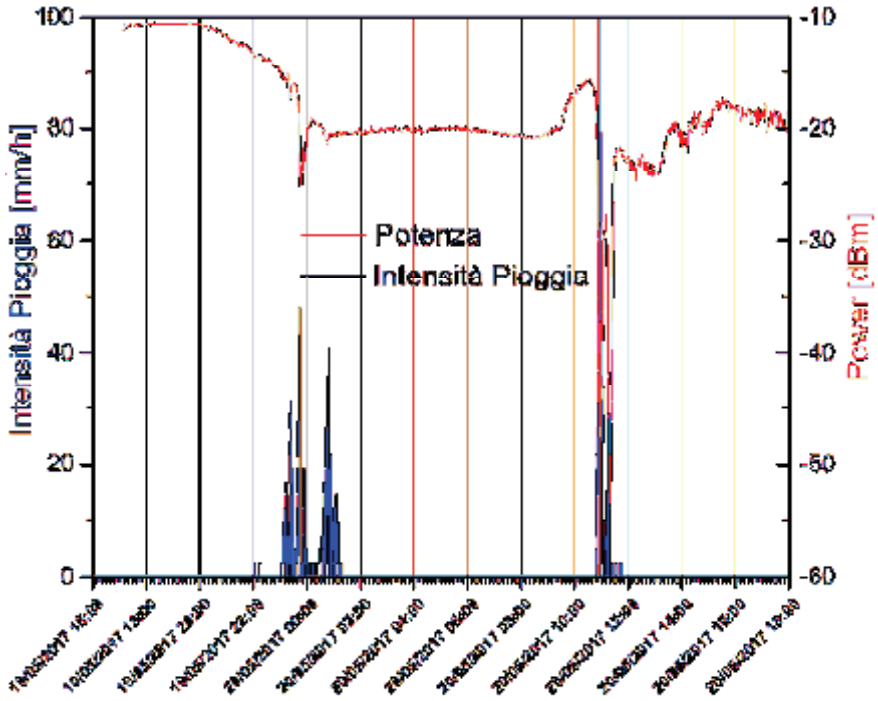


Figura 10. Effetto di un improvviso temporale sul segnale ottico.

Si può facilmente osservare come il segnale diminuisce in presenza di pioggia fitta fino anche a crollare quando oscurato da frequenza massiccia e dimensioni delle gocce che superano il mm di diametro. Per entità di pioggia contenute invece, il collegamento viene mantenuto, a meno chiaramente di effetti dovuti all'aumento di livelli di umidità atmosferica considerevole che ne consegue, di cui già parlato in precedenza. Si può quindi concludere che la pioggia non ha effetti "diretti" sul sistema nella maggioranza dei casi; può provocare un crollo repentino, ma temporaneo, del collegamento solo in circostanze di improvvisi temporali e che quindi in linea di massima viene a ripristinarsi nel giro di pochi minuti.

7. Conclusioni

Il presente lavoro è stato volto all'acquisizione di dati da un sistema ottico in spazio libero prototipale FSO in grado di trasmettere e ricevere segnali ottici viaggianti nello spazio libero, ed all'integrazione di questi con i dati provenienti da una stazione meteo. È stato studiato il comportamento del sistema al variare delle condizioni atmosferiche, analizzando le interdipendenze tra le grandezze in gioco, focalizzandosi soprattutto sulla relazione tra potenza ricevuta, temperatura ambientale, umidità atmosferica e piogge. Sebbene trovare una legge che leghi l'andamento del segnale ottico con le variazioni atmosferiche sia piuttosto complesso, si è riusciti comunque ad ottenere dei risultati preliminari di rilevante importanza. Si è visto come l'andamento della potenza sia fortemente influenzato della temperatura e dell'umidità nel tempo e come le fluttuazioni della potenza siano legate al livello di particelle di acqua sospese nell'aria. Dati più elaborati ed esaustivi saranno collezionati nel prossimo futuro con la reintegrazione nella stazione meteo del disdrometro-visibilimetro, il quale è stato fuori uso per molto tempo; questo, essendo espressamente dedicato alla misura della concentrazione di particolato in sospensione nell'aria, permetterà un'analisi più approfondita dei fenomeni d'interazione tra fenomeni atmosferici e segnale FSO. Sarà quindi possibile acquisire dati sulla visibilità ed avere informazioni più dettagliate circa le precipitazioni atmosferiche; nel dettaglio sarà anche possibile correlare l'andamento della potenza ricevuta con gli effetti delle polveri sottili di varia natura e dimensione. Gli studi sono stati condotti presso i laboratori di ottica della Divisione II dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), con sede presso il Ministero dello Sviluppo Economico in Roma, quartiere EUR.

Si ringraziano i colleghi del laboratorio ed in particolare Valentina Lucli, tesista in ISCOM laureatasi sotto la supervisione del Prof. Silvello Betti dell'Università degli Studi di Roma "Tor Vergata".

Bibliografia

[1] G. Susanna et al., Applicazione di sistemi di trasmissione in spazio libero "Free Space Optics" (FSO) in ambienti "Data Center" (DC) dedicati alla gestione ed allo smistamento dati, La Comunicazione, 2016.

[2] W. Ghuman et al., *Free Space Optics: Enabling optical connectivity*, Indianapolis: SAMS publishing, 2002

[3] M. A. Shemis et al., Broadly Tunable Self-Injection Locked InAs/InP Quantum-dash Laser Based Fiber / FSO / Hybrid Fiber-FSO Communication at 1610 nm, IEEE, 2018

[4] E. Ciaramella et al., "1.28-Tb/s (32 \times 40 Gb/s) Free-Space Optical WDM Transmission System", Photonics Technology Letters, IEEE, 2009

[5] G. Parca et al., Optical wireless transmission at 1.6-Tbit⁄s (16 × 100 Gbit⁄s) for nextgeneration convergent urban infrastructures, Optical Engineering 52(11), 2013.

[6] R. L. P. Larry C. Andrews*, Laser beam propagation through random media*, Bellingham, Washington: SPIE, 2005.

[7] "fSONA unveils 2-5-Gbps free-space optical systems", 2012, Online.

[8] H. Hemmati, *Near-Earth Laser Communication*, CRC Press, 2008.

[9] S. M. I. a. Z. S. Roberto Ramirez-Iniguez, *Optical Wireless Communications IR for Wireless Connectivity,* Taylor & Francis Group, Book, CRC Press, 2007.

[10] G. Willebrand, Fiber optic Without Fiber, 2001.

[11] S. G. N. a. S. K. Nayar, *Vision and the Atmosphere*, 2007.

[12] A.C.Best, *The size distribution of raindrops*, 1950: Quarterly Journal Royal Meteorological Society, 1950.

[13] A. N. Kolmogorov, The local structure of turbulence in incompressible viscous fluids for very large reynolds numbers, Compt. Rend. Acad. Sci. (SSSR), 1941.

[14] L. C. A. a. R. L. Phillips, *Laser Beam Propagation through Random Media*, SPIE Optical Engineering, 1998.

[15] I. I. a. E. K. Kim, Availability of Free Space Optics (FSO) and Hybrid FSO/RF Systems, Optical Access, Incorporated, 2002.

Giacomo Assenza, Luca Faramondi, Roberto Setola
(Complex System & Security Lab Università Campus Bio-Medico di Roma)

Peculiarità e problematiche della cyber security per gli Industrial Control System

Peculiarities and challenges of cyber security for the Industrial Control Systems

Sommario: *Gli Industrial Control System (ICS) sono una parte integrante delle moderne Infrastrutture Critiche (IC) in quanto sovrintendono a tutte le operazioni connesse con la gestione e il controllo di settori vitali come quello elettrico, petrolchimico, energetico, ecc.. Tuttavia, tali sistemi espongono le IC alla minaccia cyber, e i recenti attacchi informatici hanno dimostrato che è possibile, attraverso delle manipolazioni malevoli dei processi produttivi, provocare danni cinetici con conseguenze potenzialmente catastrofiche. Questo articolo illustra i problemi di sicurezza che scaturiscono dall'integrazione negli ICS di elementi e prodotti standardizzati e connessione Internet. Verranno, inoltre, analizzati gli attacchi cyber più rilevanti e si fornirà una profilazione della minaccia cyber suggerendo alcuni aspetti difensivi.*

Abstract: *ICS have become an integral component of CI, facilitating operations in vital sectors such as electricity, nuclear, energy and petrochemical manufacturing. However, these systems expose CI to the cyberthreat, and recent attacks demonstrated that targeting industrial process via cyberspace for inducing mechanical break points and provoking kinetic impacts has become possible. This paper will illustrate how ICS business-driven trends such as adopting IT elements, employing standard products and increasing Internet connectivity, have affected the security of industrial processes. Also, the paper will analyse the most relevant ICS cyberattacks and will provide a profiling of the cyberthreat and suggest defensive aspects.*

1. Introduzione

Gli Industrial Control System (ICS) sono ormai parte integrante delle infrastrutture critiche moderne in quanto sovrintendono a tutte le operazioni connesse con la gestione e il controllo. Questi sistemi di controllo, che rientrano nella più amplia categoria delle OT (operational technologies) e che vengono impiegati fina dagli anni '60, hanno subito profonde trasformazioni tutte orientate verso la massimizzazione della loro efficienza. Gli ICS infatti, che erano un tempo isolati dall'ambiente esterno e che si servivano di sistemi di legacy propri, si servono oggi di soluzioni IT, *off-the-shelf* e sono connessi a Internet. Queste trasformazioni, oltre ad avere consentito significativi progressi tecnologici e riduzione dei costi di

esercizio, hanno introdotto vulnerabilità importanti negli ambienti OT che potrebbero comprometterne la sicurezza. Infatti, data la grande quantità di dati scambiati e il vincolo di *hard real-time* che caratterizza le OT risulta difficile integrare in questi sistemi le classiche soluzioni di sicurezza del mondo IT rendendoli suscettibili ad attacchi cyber.

L'aspetto più critico delle vulnerabilità degli ICS è che gli attacchi cyber potrebbero indurre un impatto cinetico con drammatiche conseguenze sulla salute delle persone e sull'ambiente oltre che produrre danni con costi e tempi di ripristino significativi. Infatti un aggressore può volontariamente alterare il normale operato di un processo fino a portare il sistema a un punto di rottura meccanico. Bisogna infatti considerare che gli ICS costituisco dei target strategici e rilevanti non solo per la funzione che svolgono nella società ma anche perché spesso maneggiano impianti e processi intrinsecamente pericolosi, e una loro manomissione potrebbe provocare danni ambientali e alla popolazione, oltre che meramente economici.

Questi timori si sono concretizzati a partire dal 2011 con la scoperta di Stuxnet, il primo malware in grado di "deteriorare" fisicamente una apparecchiatura meccanica (nel caso in specie le centrifughe per l'arricchimento dell'uranio in un impianto nucleare Iraniano). Ad oggi, si sono verificati almeno altri quattro attacchi con conseguenze cinetiche: Irongate (2014) che ha comportato il danneggiamento di un impianto metallurgico in Germaia, BlackEnergy3 (2015) e Crashoverride (2016) che hanno provocato l'uno a distanza di un anno dall'altro due blackout in Ucraina, e Trisis (2017) che ha causato lo shutdown di uno stabilimento petrolchimico in Medio Oriente. Sebbene tali attacchi abbiano avuto un impatto limitato, o comunque ben lontano da catastrofico, hanno dimostrato che operazioni offensive immateriali, dunque una sequenza di zeri e uno, sono potenzialmente in grado di ottenere i medesimi risultati di una carica esplosiva, con il vantaggio che l'azione può essere sferrata da migliaia di chilometri di distanza e, soprattutto, che la possibilità di attribuzione, ossia di risalire all'autore dell'attacco, sono ridotte o comunque non immediate.

Quest'articolo affronterà l'argomento e la trattazione è sviluppata come segue: le sezioni 1, 2 e 3 illustrano il ruolo che svolgono gli ICS nelle IC e illustrano, anche a seguito delle recenti trasformazioni, i loro punti di vulnerabilità; la sezione 4 traccia le caratteristiche della minaccia cyber per gli ambienti industriali e la 5 passa in rassegna i principali attacchi informatici contro le OT; infine, la sezione 6 introduce alcuni elementi che giocano a favore della difesa degli ICS.

2. ICS e Infrastrutture critiche

L'acronimo ICS si riferisce a un insieme di tecnologie, sia software che hardware, che si interfacciano direttamente con i processi industriali e che svolgono attività di produzione, trasporto e trasformazione dei beni. Gli ICS, come gli SCADA (*Supervisor Control and Data Acquisition*), e i DCS (*Distributed Control Systems*) rientrano nella più amplia categoria delle Operational Technologies (OT), ossia quegli apparati e sistemi che impiegano network, protocolli di comunicazione ed elementi fisici per svolgere tre funzioni principali: l'acquisizione dei dati, le attività di controllo e supervisione, e l'esecuzione di comandi (Stouffer & Al., 2011).

Le società moderne dipendono in modo sempre più radicale dai dispositivi ICS. Infatti, tra i clienti dei principali fornitori di soluzioni OT (Rockwell Automation, Siemens, ABB, Mitsubishi) figurano soggetti che operano in campi quali il settore energetico, delle comunicazioni e dei trasporti. Tali campi sono considerati dalla maggior parte degli stati come settori critici, e i soggetti che vi operano sono identificati come infrastrutture critiche (IC) (Brunner & Suter, 2009). Sebbene non esista una caratterizzazione universale di infrastruttura critica, riflettendo questa l'identità geografica storica e culturale dei singoli soggetti (Setola, 2011), queste possono essere identificate come tutti quei sistemi e assetti, tanto fisici che virtuali, il cui malfunzionamento o interruzione avrebbe un impatto diretto e significativo sull'economia, sicurezza e salute nazionale, provocando un effetto domino di imprevedibili reazioni a catena in grado di compromettere la stabilità stessa di un paese (EPCP, 2005).

Le IC eseguono le funzioni essenziali della società moderna e costituiscono il loro cuore pulsante. Proprio come il cuore non può mai smettere di battere, gli assetti critici devono essere sempre disponibili, affidabili e operativi. Questo bisogno primario di disponibilità e performance ha comportato nel mondo degli ICS, presenti negli impianti industriali e manufatturieri già dagli anni '60, delle trasformazioni significative. Nel corso del tempo, infatti, le OT che tradizionalmente si affidavano a sistemi di legacy con protocolli proprietari e fisicamente isolate dall'ambiente esterno (Brunner & Suter, 2009; Galloway & Hancke, 2013), hanno fatto ricorso in modo sempre più massiccio alle tecnologie IT e a prodotti *off-the-shelf*. Inoltre, molti componenti di questi sistemi, che comunicavano un tempo attraverso network chiusi, sono stati integrati nel più generale trend del "*Industrial Internet of Things* (IIoT) con il risultato che gli odierni Cyber-Physical Sistems (CPS), ossia dispositivi informatici che controllano processi fisici, sono dotati non solo di un accesso diretto attraverso il corporate

network, ma anche di connessione internet (Sadeghi, Wachsmann & Waidner, 2015).

Da una parte, questo trend ha portato degli indubbi benefici che abbiamo potuto osservare nella nostra quotidianità in termini di miglioramenti generali della qualità della produzione e della sua efficienza ed economicità. Dall'altra, questo connubio ha implicato l'introduzione delle tradizionali vulnerabilità e minacce del settore IT nel dominio OT che, per le sue particolarità intrinseche, è un ambiente dove le misure di cyber-security risultano di difficile applicazione creando un problema di sicurezza non trascurabile (Nicholson & Al., 2012).

3. Sicurezza negli ambienti OT, il limite della disponibilità

Gli ambienti OT sono caratterizzati da peculiarità proprie che proiettano la necessità di proteggere questi apparati su un trade-off che vede l'opposizione di due elementi: la security e la safety. In primo luogo, gli ambienti ICS si caratterizzano per lo scambio di grandissime quantità di informazioni che vengono continuamente inviate e ricevute da una pletora complessa di fonti e soggetti, nel formato di pacchetti dalle piccole dimensioni dell'ordine di pochi byte.

Questo si lega all'altro aspetto essenziale degli ICS, ossia quello di dover rispondere a un vincolo di *hard real-time*. Infatti, gli impianti OT sono disegnati per interfacciarsi con "sistemi fisici" come reazioni chimiche, flussi di liquidi, processi di riscaldamento e raffreddamento, movimenti di oggetti etc. Gli impianti OT devono dunque operare ed adattarsi alle dinamiche e ai tempi richiesti dalla logica del processo supervisionato. Questo implica un alto livello di determinismo dove il meccanismo deve necessariamente passare attraverso una precisa sequenza di input, e in un intervallo di tempo ben determinato, per produrre l'output desiderato.

Ne consegue che l'applicazione di misure classiche di cyber-security quali cifratura, antivirus, firewalls e firma digitale, risulterebbe particolarmente problematica in quanto introdurrebbe controlli di routine che rischiano di compromettere il fluido funzionamento delle attività, generando un elevato overhead che, anche a causa della natura asincrona di tali processi, rischia di compromettere il normale ciclo di funzionamento introducendo pericolosi e inaccettabili ritardi dell'elaborazione del dato.

Infine, un altro fattore che limita l'introduzione di misure di sicurezza, è la difficoltà di operare azioni di manutenzione del sistema. Gli ICS infatti sono disegnati per operare a ciclo continuo

24x365, o almeno fino a quando il processo controllato è attivo. Ne consegue che gli interventi di aggiornamento, upgrade e patching, che richiedono un periodo di downtime dell'infrastruttura, devono essere pianificati con largo anticipo e non possono seguire pedissequamente le innovazioni in ambito di sicurezza (Cook & Al., 2017). Inoltre, tali attività sono considerate rischiose in quanto qualsiasi modifica del sistema, in un ambiente complesso e caratterizzato dal requisito di hard real-time, potrebbe creare effetti inaspettati. Gli interventi sul software dunque richiedono intense attività di testing, generalmente indicate come processo di convalida, il cui costo in termini monetari e di tempo è significativo oltre che, in molti casi, imposto e regolato da specifiche norme e procedure pensate in modo quasi esclusivo con un'ottica di salvaguardia dell'integrità e tracciabilità del processo e della safety dei lavoratori e degli utenti (McLaughlin & Al., 2016).

In altre parole, una volta istallati e certificati, gli ICS rimangono operativi per più di 20 anni con interventi di manutenzione sui sistemi controllo ridotti al minimo, il che implica in molti casi l'utilizzo di software obsoleti sui quali il processo di patching e aggiornamento non è effettuato in modo sempre tempestivo. Per esempio uno studio condotto alcuni anni fa da una società specializzata negli USA ha evidenziato che il tempo medio per l'applicazione di una patch di sicurezza era di 350 giorni con alcuni episodi nei quali l'istallazione era stata effettuata solo 3 anni dopo il rilascio della patch. Una diversa ricerca ha, addirittura evidenziato, che solo il 10% degli operatori installa patch e aggiornamenti mentre il restante lascia i propri sistemi suscettibili di essere attaccati (Bodenheim, 2014). Inoltre la maggior parte dell'apparecchiature presenti in ambito industriale a non è in grado di gestire misure di sicurezza sofisticate, infatti la maggior parte dei PLC (*Programmable Logic Controller*) istallati sono dimensionati rispetto al ciclo di funzionamento proprio del processo da controllare e non hanno capacità di calcolo per elaborare ulteriori informazioni (Higgins & Jan, 2013). Infine, nel 2011 Symantec ha pubblicato un report in cui evidenziava 129 vulnerabilità che interessano i prodotti ICS (Symantec, 2011), mentre solo un anno dopo ne sono state individuate 171, mostrando un trend di crescita di oltre il 40% in un sol anno e che difficilmente subirà delle inversioni in futuro.

4. Una crescente superficie di attacco

In questo contesto di vulnerabilità intrinseche, l'unica barriera che ha garantito per un lungo periodo di tempo un livello accettabile di protezione era costituita dalla così detta *security through obscurity*. Tale concetto fa della complessità dei sistemi OT un elemento di difesa volto a dissuadere un eventuale attaccante dall'agire. Infatti, per compromettere un ICS basato su protocolli propri e senza connettività esterna erano necessari non solo una conoscenza estensiva del software utilizzato, ma anche un punto di accesso fisico all'ambiente industriale. A questo andava aggiunta la necessità di conoscere il processo sotteso al fine di individuare qurgli elementi e quelle azioni atte a indurre rischio significativi al processo. Di conseguenza, le OT erano viste ragionevolmente immuni da attacchi esterni, e la minaccia principale era considerata quella interna (Byres & Lowe, 2004) proveniente da "addetti ai lavori" scontenti e mossi da motivi personali (Galloway & Hancke, 2013).

Non è un caso che fino al 2010 l'unico episodio di cui si ha notizia riguarda un attacco portato contro i sistemi di gestione delle acque nella cittadina di Maroochy Shire (una provincia australiana) che provocò la dispersione di 800.000 litri di liquami grezzi con significativi danni ambientali ed economici. In questo caso l'autore dell'attacco era uno degli sviluppatori del sistema che aveva poi cercato di mettere in piedi una estorsione (Slay & Miller, 2007).

È evidente che oggi, come diretta conseguenza della maggiore connettività e dell'utilizzo di soluzioni predefinite, la strategia di *security through obscurity* non è più ragionevole.

Da una parte, questi cambiamenti hanno dato la possibilità di sferrare attacchi da remoto, scavalcando quindi il vincolo della necessità di accesso fisico (Drias & Al., 2015), dall'altra hanno significativamente facilitato le attività di *reconnaissance*. La *reconnaissance* costituisce uno step propedeutico essenziale nella preparazione delle operazioni cyber (Assante & Lee, 2015) nel quale gli attaccanti raccolgono intelligence e informazioni riguardo al target prescelto al fine di identificarne le debolezze e i punti di rottura da sfruttare per compromettere il sistema e indurlo in una configurazione non-safe. Oggi, gli attori malintenzionati possono soddisfare in buona parte le loro esigenze di raccolta di informazioni e documentazione impiegando strumenti di intelligence open source (OSINT). La piattaforma Shodan, per esempio, è un motore di ricerca liberamente utilizzabile e dai costi limitati, in grado di tracciare tutte le porte di comunicazione connesse a Internet, incluse quelle dei dispositivi OT. Gli utenti possono facilmente individuare quale specifico ICS è utilizzato in

un impianto e, una volta identificato, posso mappare il sistema al fine di individuarne le vulnerabilità e i punti di ingresso sfruttabili (Bodenheim, Butts, Dunlap & Mullins, 2014; Bodenheim, 2014).

5. Evoluzione della minaccia

Gli sviluppi del mondo delle OT hanno portato anche a una trasformazione effettiva del panorama delle minacce cyber. Infatti, se tra il 1982 e il 2000 il 70% degli attacchi era di natura interna, tra il 2000 e il 2003 si è verificata una progressiva inversione del trend che ha portato l'ammontare delle azioni con origine esterna fino al 70% degli attacchi totali (Byres & Lowe, 2004; Iversen, 2004), ed è improbabile che questa tendenza diminuisca in futuro.

Questi dati, accompagnati da un aumento generale della frequenza degli attacchi informatici (Kaspersky lab ICS-CERT, 2017) hanno sollevato una grande preoccupazione per le minacce derivanti dal cyberspazio. Nel 2009, un sondaggio che coinvolgeva oltre 600 IT security manager di imprese operanti in settori critici ha evidenziato che la maggior parte degli intervistati riteneva probabile, se non imminente, un'operazione cyber di larga scala in grado di degradare le IC del paese (McAfee, 2009). Lo stesso anno, l'ex presidente americano Barack Obama, ha definito gli attacchi cibernetici "*una delle più gravi minacce alla sicurezza statale ed economica che le nostre nazioni stanno affrontando*" (Napolitano, 2009) e, secondo uno studio recente, le minacce informatiche detengono la quarta posizione dopo quelle legate al terrorismo, vandalismo e furto fisico (Moreno & Al., 2018).

L'aspetto più critico delle vulnerabilità degli ICS è che gli attacchi informatici potrebbero avere non solo un impatto economico, ma anche uno cinetico. Un aggressore può introdurre guasti e alterare il normale operato di un processo fino a portare il sistema a un punto di rottura meccanico. A questo timore è stato dato fondamento pratico nel 2007 con il progetto Aurora, condotto dall'Idhao National Lab, nel quale una squadra di hacker etici simulò un attacco informatico per distruggere un gruppo elettrogeno da 27 tonnellate (Cárdenas, Amin & Sastry, 2008). L'esperimento Aurora dimostrò che un attacco immateriale ipoteticamente sferrabile da migliaia di kilometri di distanza è in grado di creare danni meccanici potenzialmente paragonabili a quelli ottenibili da una carica esplosiva, con il vantaggio che la possibilità di attribuzione, ossia di risalire all'autore dell'attacco, sono ridotte o comunque non immediate.

Questo comporta che un attacco informatico contro le IC potrebbe creare danni all'ambiente, problemi alla salute delle

persone e gravi disagi per la società (ARIA, 2015). Questo anche perché occorre considerare che il ripristino e la riparazione delle componenti meccaniche dei sistemi OT possono richiedere tempi dilatati dell'ordine di mesi se non addirittura di anni.

Oggi, la necessità di difendere le OT da attacchi cyber è riconosciuta a livello italiano e mondiale. In Italia la relazione dei Servizi di Intelligence al Parlamento del 2016 avverte della possibilità che un'operazione cyber può danneggiare oggetti fisici e, come affermato nel 2012 dall'ex Segretario alla Difesa statunitense Leon E. Panetta, un'operazione di successo potrebbe portare a un "cyber-Pearl Harbor" se un gruppo di aggressori acquisisse il controllo degli "interruttori critici" (Bumiller & Shanker, 2012).

6. I principali attacchi

Il Progetto Aurora era solo una simulazione e fu ampliamente considerato con scetticismo in quanto gli hacker avevano una conoscenza estensiva dell'impianto che gli ha concesso di eseguire una manipolazione mirata del processo, mentre, in uno scenario realistico, si riteneva improbabile che un avversario disponesse di informazioni tanto precise e dettagliate.

Tuttavia, l'apparizione del worm Stuxnet nel 2010, ha cambiato radicalmente non solo lo scenario, ma anche la percezione della minaccia cyber (Langner, 2011; 2013). Questo worm era specificatamente progettato per attaccare i PLC Siemens in uso in uno stabilimento nucleare nel Natanz, una regione dell'Iran. Nello specifico, Stuxnet era programmato per alterare la velocità di rotazione di alcuni motori facendoli girare in modo anomalo (Albright, Brannan, Walrond, 2011, Langner, 2011; 2013). L'attacco provocò la deteriorazione di circa 1,000 turbine che di conseguenza rallentò significativamente il programma nucleare iraniano (Lindsay, 2013).

Stuxnet non è stato un caso isolato, ma ha segnato il punto di inizio di una serie di operazione cyber volte a compromettere la sicurezza fisica dei processi industriali fra i quali è importante ricordare: Irongate (2014), Black Energy 3 (2015), Crashoverride (2016) e Trisis/Triton (2017).

L'attacco Irongate del 2014 prese di mira un'acciaieria tedesca. I malintenzionati ottennero l'accesso alla rete degli impianti e, impedendo il corretto spegnimento di una fornace, furono in grado di causare "danni fisici enormi" a vari componenti critici del sistema, comportando la sospensione della produzione e costi significativi per ripristinare l'operabilità (Lee & Al., 2014).

In Ucraina invece, due attacchi informatici importanti hanno preso di mira il settore energetico. BlackEnergy 3 è il primo attacco cyber conosciuto che è stato in grado di interferire con le operazioni di un operatore elettrico provocando un blackout il 23 dicembre del 2015 che è durato per 6 ore tenendo al buio circa 225,000 utenti nella regione. Il malware, dopo aver imparato il corretto funzionamento del sistema sfruttando le informazioni visualizzate tramite la HMI (*Human Machine Interface*), è stato capace di inviare comandi "leciti" con l'obiettivo di disconnettere alcune sottostazioni dalla rete elettrica e successivamente rendere non operativo l'apparato di telecontrollo cancellando alcuni file di sistema (Lee, 2017a; E-ISAC, 2016). A distanza di un anno, nel dicembre 2016, un secondo blackout ha colpito l'Ucraina, e in questo caso il gestore elettrico ha esplicitamente dichiarato che la causa è da ricercare in interferenze illecite nella rete di controllo industriale derivanti dall'esterno, ovvero in un attacco cyber condotto tramite il malware CrashOverride. Attraverso il malware, anche conosciuto come Industroyer, gli attaccanti hanno potuto prendere il controllo degli interruttori di alcune sottostazioni, che sono poi stati aperti provocando una perdita di energia di circa un'ora in vari sobborghi di Kiev (Lee, 2017a ESET, 2017).

Una peculiarità interessante di questi due attacchi è che i malware hanno funto da mero vettore per accedere e prendere controllo dei dispositivi di gestione delle operazioni, e soltanto la malevola interazione degli attaccanti con il sistema ha provocato i due blackout (Conway & Al., 2016; Lee, 2017a; Cherepanov, 2017). Questo indica che il focus principale dell'operazione non è tanto nella payload dei due malware, ma piuttosto nella conoscenza degli attaccanti e nella loro capacità di sfruttare il processo per portarlo in una condizione di malfunzionamento. Il che implica che questo tipo di attacchi non sono limitati a un particolare vendor o impianto ma possono essere riproposti altrove (Lee, 2017a). Per esempio, il CERT USA ha evidenziato che malware come BlackEnergy 3 e Crashoverride sono stati rinvenuti in diversi sistemi di controllo di utility americane (Larson, 2018) e che in alcuni casi sono rimasti latenti nei sistemi anche per più di cinque anni (Setola & Al., 2019).

Infine, l'ultimo attacco OT in ordine cronologico è il malware scoperto nel dicembre 2017 in un impianto petrolchimico in Medio Oriente, e conosciuto con il nome di Trisis o Triton. La particolarità di questo malware è che il suo target sono i sistemi SIS (Safety Instrumental System) ovvero quella porzione dei sistemi ICS, generalmente separata dai normali sistemi di gestione di processo, che sono utilizzati per prevenire eventi catastrofici (Lee, 2017b; Johnson & Al., 2017). I SIS supervisionano le

operazioni critiche assicurando che il processo industriale mantenga un livello minimo di sicurezza. Se la soglia necessaria non viene soddisfatta, i controllori SIS entrano in modalità *safe-failed* interrompendo le operazioni produttive (Higgins, 2018). In questo caso, gli aggressori sono riusciti a penetrare il dispositivo SIS e nel tentativo di riprogrammare il controller hanno involontariamente attivato lo stato di errore provocando l'arresto del processo industriale.

Prendere di mira i SIS è strategicamente rilevante in relazione a due scenari plausibili. Una prima strategia, classificabile come fake attack, consiste nel riprogrammare il SIS affinché il sistema rilevi dei falsi positivi. In altre parole, parametri o situazioni del tutto normali vengono segnalate come anomale e potenzialmente pericolose inducendo il sistema ad adottare misure di recovery, se non addirittura lo shutdown del processo. Una seconda tipologia di attacco, decisamente più critica e perniciosa, implica la riprogrammazione dei dispositivi SIS affinché il sistema non sia più in grado di rilevare situazioni di emergenza, e dunque di intraprendere le necessarie azioni di "protezione" per riportare i processi in configurazione di sicurezza. In tale scenario il processo produttivo perde la capacità di prevenire l'insorgenza di situazioni pericolose per cui un ulteriore evento anomalo, sia esso accidentale o indotto dall'attaccante, può degenerare in un incidente con impatti significativi in termini di danni fisici e ambientali (Johnson & Al., 2017; Assante, 2018).

L'impatto di questi attacchi, pur rimanendo limitato e ben al di sotto della soglia di un "cyber-Pearl Harbour", ha dimostrato che operazioni cibernetiche con conseguenze cinetiche non sono più una mera speculazione teorica o l'oggetto di esperimenti militare ma, al contrario, gli strumenti offensivi di questo genere sono diventati "possibili, accessibili, incisivi e capaci di interrompere il corretto funzionamento delle società sviluppate" (Tabansky, 2011). Non è un caso che anche il Global Risks Report del 2019 enfatizza il rischio cyber come una minaccia con un impatto potenziale non lontano da quello di calamità e disastri naturali maggiori (figura 1) (WEF, 2019). È tuttavia da considerare che gli attacchi informatici, a differenza delle catastrofi ambientali, sono minacce artificiali di cui la mano umana è la prima responsabile e, in quanto tali, sono più facilmente difendibili e mitigabili.

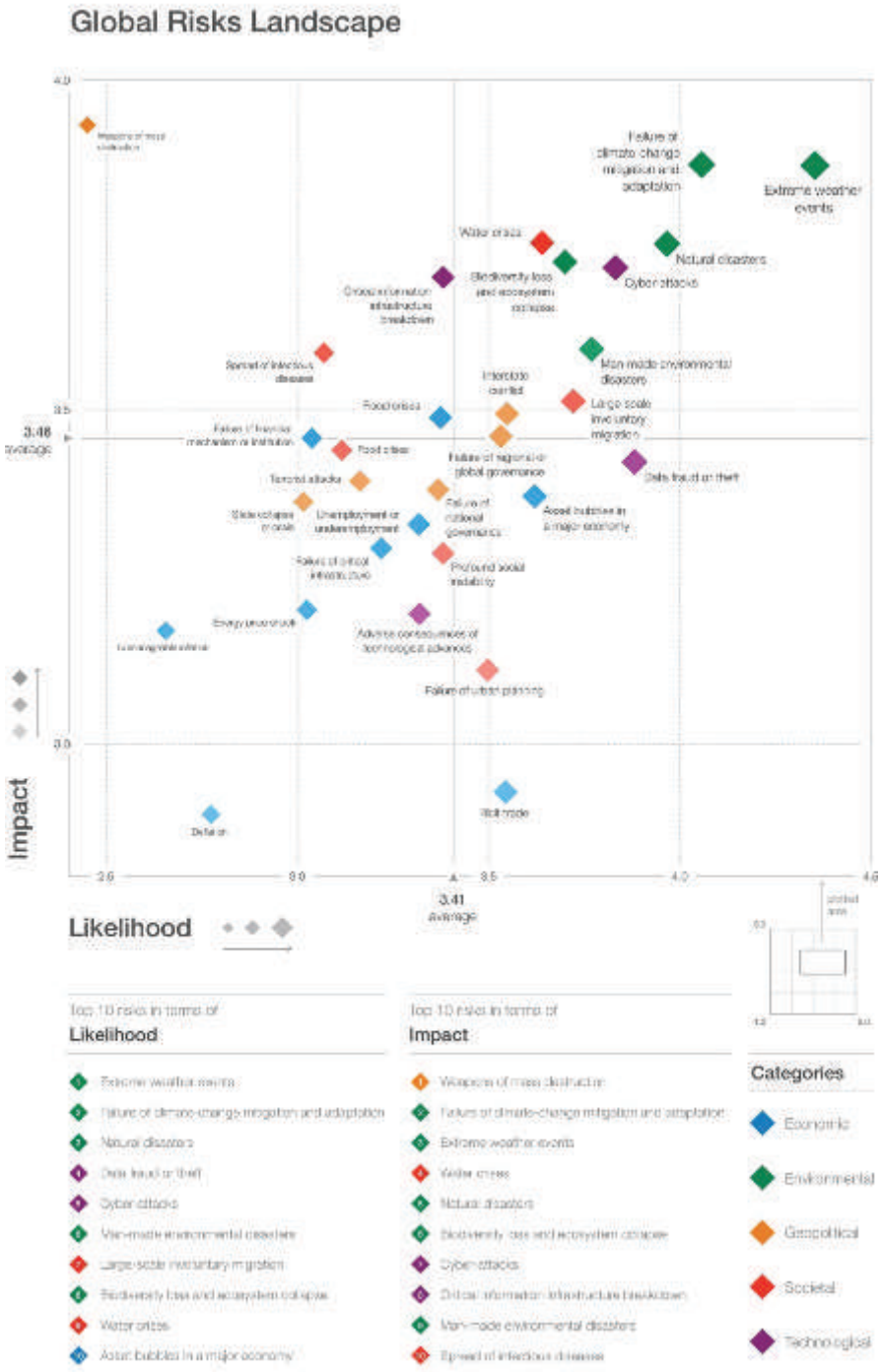


Figura 1 Thrath Landscape, Global Risk Report 2019

7. Aspetti difensivi degli ICS

Sebbene la loro intrinseca vulnerabilità e l'alta esposizione alla minaccia cyber, gli attacchi contro le OT sono risultati limitati sia in termini di frequenza (ad oggi se ne possono annoverare solo cinque che hanno avuto conseguenze fisiche), sia in termini di

impatto, e questo suggerisce che gli aggressori non hanno ancora sviluppato la capacità o l'intenzione di infliggere danni significativi.

In primo luogo, bisogna considerare che a partire dalla scoperta di Stuxnet sono state proposte varie misure difensive per proteggere gli ICS. Una delle strategie migliori è il così detto approccio a "cipolla" o *defence in depth*. Questo metodo è organizzato sulla base di una gerarchia di rilevanza delle minacce nei vari sistemi e mira a creare filtri e barriere che ostacolino l'attaccante nel tentativo di accedere ai settori critici del processo, ossia quei livelli del sistema che garantiscono la safety dell'intero ambiente. La *defence in depth*, introdotta con lo standard ANIS/ISA 99 (Byres & Al., 2012) e ripresa in modo più dettagliato dall'ICS Cyber Emergency Response Team statunitense (DHS, 2016), prevede di segmentare la rete ICS in zone, dove sono raggruppati gli asset logici e fisici che presentano requisiti di sicurezza comuni in termini di criticità e conseguenze in caso di un eventuale manomissione. Tutte le unità che compongono un settore sono considerate trust e possono dunque scambiare dati e informazioni senza restrizioni. Al contrario, il dialogo tra entità afferenti a zone diverse deve essere concentrato in un numero limitato di snodi, generalmente chiamati *conduits*, e in corrispondenza di ognuno di essi è bene che vengano inseriti sistemi di monitoraggio, come firewall o dispositivi analoghi, per verificare la correttezza e regolarità dei flussi. Inoltre, in un'architettura a cipolla si tende a raggruppare gli asset più critici nei settori più interni del sistema. In tale contesto, una misura che aumenterebbe notevolmente la sicurezza dell'intero sistema potrebbe essere quella di adottare soluzioni di comunicazioni data diode, ossia basate su device che consentono un flusso dell'informazione esclusivamente unidirezionalmente dall'interno (campo) verso l'esterno (rete aziendale). Tuttavia, limitare il flusso informativo risulta particolarmente problematico in quanto occorre sia ricevere informazioni dal campo sia definire set-point, strategie e attività di manutenzione. Questo impone la presenza di sistemi di by-pass del data diode con conseguente limitazione dell'efficienza di quest'ultimi rendendone l'adozione poco utile in tutti quei casi in cui le attività di controllo sono in volume paragonabili al flusso di monitoraggio.

Al di là delle misure difensive poste in essere, le operazioni cibernetiche sono *scale sensitive* e la difficolta di preparare e sferrare un attacco con successo aumenta in parallelo con la complessità del sistema preso di mira. I sistemi industriali sono tra i target più complessi e quindi tra i più ardui da compromettere. La grande difficoltà risiede nel fatto che un malintenzionato, per portare un processo al punto di rottura, deve essere in grado non

solo di comprendere e padroneggiare il linguaggio dell'ICS per mandare comandi legittimi, ma deve anche sapere quali comandi mandare, a quali componenti del sistema e quali reazioni fisiche provocare per mandare il processo in una configurazione erronea (Setola & Al., 2019). In altre parole, un attaccante deve combinare skills di diversa natura che comprendono non solo articolate abilità informatiche ma anche avanzate conoscenze ingegneristiche del processo che si vuole compromettere.

Oggi, gli attori che raggiungono questo livello di sofisticazione vengono definiti come *Advanced Persisten Threath* (APT) (NIST, 2011), ossia un team di avversari determinati e dotati di risorse consistenti (basti pensare che lo sviluppo di Stuxnet è costato oltre venti milioni di dollari) che trascendono il regno digitale comprendendo anche aspetti istituzionali ed organizzativi quali la capacità di acquisire conoscenze di intelligence precise e dettagliate, e la possibilità di mobilitare capitale umano di prima qualità (Rid & Mc Burney, 2012; Lindsay, 2013; Liff, 2012).

È evidente che la soglia di risorse necessarie per poter prendere di mira gli ambienti ICS è ben al di fuori della portata degli attori più deboli e, al contrario, rimane una prerogativa di attori di altissimo profilo probabilmente sponsorizzati e supportati da entità statali che usano le APT come *proxies* nel cyberspace (Maurer, 2018). Da una parte, questo aspetto taglia fuori gli attori più comuni, come i criminali o gli attivisti (Craig & Valeriano, 2018). Dall'altra suggerisce che le operazioni offensive contro gli OT sono volontariamente circoscritte nel loro impatto e sono progettate più per raggiungere vantaggi geopolitici, economici o militari, che per infliggere danni "economici" o reputazionali alla vittima.

8. Conclusioni

Negli ultimi anni si è assistito a una crescita non solo della frequenza, ma anche della qualità degli attacchi cyber contro gli ICS. Da una parte, questo è dovuto a un aumento sostanziale della vulnerabilità esposte da questi sistemi, che per ragioni di efficienza hanno integrato in modo sempre più massiccio strumenti e prodotti propri del mondo IT. Dall'altra, si è registrato un generale aumento e diffusione delle capacità offensive cyber che ha portato al verificarsi di almeno cinque attacchi informatici (Stuxnet, Irongate, BlackEnergy3, Crashoverride, Trisis) con conseguenze cinetiche.

L'impatto di questi attacchi è risultato limitato e distante dalle previsioni catastrofiche di un "Cyber Pearl-Harbour". Inoltre, le OT costituiscono i target più complessi e comprometterli richiedere il

lavoro delle APT, ossia team altamente sofisticati che dispongono di risorse tecnico organizzative al di fuori della portata degli hacker più comuni. Come riconosciuto dal summit NATO del 2016, che elegge il cyberspace come quinto dominio delle operazioni (NATO, 2019), si pensa che le APT vengano sponsorizzate da entità statali che se ne servono per avanzare i propri interessi geopolitici.

Tuttavia, è da notare come le capacità offensive cyber si stiano sviluppando più velocemente delle contromisure per arginarne la minaccia (WEF, 2018), è dunque urgente e necessario che gli operatori delle IC, in sinergia con i soggetti pubblici deputati, si preparino per ridurre le vulnerabilità delle OT e per proteggersi rispetto a questa classe di attacchi.

Bibliografia

[1] Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet malware and natanz: Update of isis december 22, 2010 report. *Institute for Science and International Security*, *15*, 739883-3

[2] ARIA - Analysis, Research and Information on Accidents database (2015). Ministry of Environment / General Directorate for Risk Prevention, the BARPI (Bureau forAnalysis of Industrial Risks and Pollutions). At: https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en

[3] Assante, M. (2018). Triton/TriSIS – In Search of its Twin. *SANS Industrial Control Systems*. 29 January. Available at: https://ics.sans.org/blog/2018/01/29/tritontrisis-in-search-of-its-twin

[4] Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*

[5] Bodenheim, R. C. (2014). *Impact of the Shodan computer search engine on internet-facing industrial control system devices* (No. AFIT-ENG-14-M-14). AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT

[6] Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, *7*(2), 114-123

[7] Brunner, E.M. & Suter, M. (2009). International CIIP Handbook 2008/2009, *CRN handbooks,* 4(1)

[8] Bumiller, E. and Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S, *The New York Times*, 11 October 2012 available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

[9] Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218)

[10] Byres, E., Eng, P., & Fellow, I. S. A. (2012). Using ANSI/ISA-99 standards to improve control system security. *White paper, Tofino Security*

[11] Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. In *HotSec*

[12] Cherepanov, A. (2017). WIN32/INDUSTROYER, A new threat for industrial control systems. *White paper, ESET (June 2017)*

[13] Conway, T., Lee, R. M., & Assante, M. J. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing and Analysis Center*. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[14] Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security*, *70*, 467-481

[15] Craig, A. J., & Valeriano, B. (2018) Realism and Cyber Conflict: Security in the Digital Age. *Realism in Practice*, 85

[16] DHS (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. *Industrial Control Systems Cyber Emergency Response Team*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [20/05/2019]

[17] Drias, Z., Serhrouchni, A., & Vogel, O. (2015). Analysis of cyber security for industrial control systems. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on* (pp. 1-8). IEEE

[18] E-ISAC (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.

[19] ESET, (2017). ESET discovers dangerous malware designed to disrupt industrial control systems. *ESET – Enjoy Safer Technology*. 12 June, Available at: https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-dangerous-malware-designed-to-disrupt-industrial-control-systems/

[20] European Commission (2005). Green Paper on a European programme for critical infrastructure protection, Com. 576 final. Available at: https://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:52005DC0576&from=BG

[21] Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, *15*(2), 860-880.

[22] Higgins, K. J., & Jan, D. (2013). The SCADA patch problem. *Information Week*. Available at: https://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979

[23] Higgins, K.J. (2018). FireEye Finds New Clue in TRITON/TRISIS Attack. Dark Reading, 6 August. Available at: https://www.darkreading.com/operations/fireeye-finds-new-clues-in-triton-trisis-attack/d/d-id/1332008

[24] Iversen, W. (2004). Hackers Step Up SCADA Attacks. AutomationWorld. 12 october. Available: https://www.automationworld.com/article/technologies/networking-connectivity/switches-gateways-routers-modems/hackers-step-scada

[25] Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., Glyer, C., (2017). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. FireEye. 14 December. Available at: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[26] Kaspersky lab ICS-CERT, (2017). Threat Landscape for Industrial Automation Systems In The Second Half Of 2016, Kaspersky Lab. Available: https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

[27] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49-51.

[28] Langner, R. (2013). To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. *The Langner Group*

[29] Larson, S. (2018). Threats to Electric Grid are Real; Widespread Blackouts are Not. Dragos, 6 August. Available at: https://dragos.com/blog/20180806ElectricGridThreats.html

[30] Lee, R. (2017 a). CRASHOVERRIDE: Analysis of the threat to electric grid operations. *Dragos Inc., March*

[31] Lee, R. (2017 b). TRISIS Malware: Analysis of Safety System Targeted Malware. Dragos Inc. available at: https://dragos.com/blog/trisis/

[32] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber-attack. *Industrial Control Systems*, *30*, 62

[33] Liff, A. P. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401-428

[34] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404

[35] Maurer, T. (2018). *Cyber Mercenaries*. Cambridge University Press

[36] McAfee, (2009). In the Crossfire: Critical Infrastructure in the Age of Cyber War. McAfee report. Available at: https://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf

[37] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039-1057

[38] Moreno, V. C., Reniers, G., Salzano, E., & Cozzani, V. (2018). Analysis of physical and cyber security-related events in the chemical and process industry. *Process Safety and Environmental Protection*, *116*, 621-631

[39] Napolitano, J. (2009) A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack. Department of Homeland security. 20 October. Available: https://www.dhs.gov/news/2009/10/20/secretary%E2%80%99s-web-address-cybersecurity

[40] NATO (2019). NATO's role in cyberspace. *NATO Review Magazine*, 2019. Available: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

[41] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418-436

[42] NIST (2011). *Managing Information Security Risk: Organization, Mission, and Information System View* (No. Special Publication (NIST SP)-800-39)

[43] Rid, T., & McBurney, P. (2012). Cyber-weapons. *the RUSI Journal*, *157*(1), 6-13

[44] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE* (pp. 1-6). IEEE

[45] Setola, R. (2011), *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*, Centro Militare di Studi Strategici CEMISS, At: http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/Lastrategiaglobalediprotezione.aspx

[46] Setola R., Faramondi L., Salzano E., & Cozzani, V.(2019). An overview of Cyber Attack to Industrial Control System. *Chemical Engineering Transactions vol.75,2019*

[47] Slay, J., & Miller, M. (2007, March). Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection* (pp. 73-82). Springer, Boston, MA

[48] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security, NIST special publication 800-82, *National Institute of Standards and Technology*

[49] Symantec (2011). Symantec. "SCADA (Supervisory Control and Data Acquisition) security threat landscape". Available at: https://www.symantec.com/security-center/threat-report

[50] Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. *Military and Strategic Affairs*, *3*(2) 61-68

[51] World Economic Forum (2018), The Global Risks Report 2018, https://www.weforum.org/reports/the-global-risks-report-2018

[52] World Economic Forum (2019). Global Risks Report 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Fabio Paternò, Antonio Giovanni Schiavone
(*CNR-ISTI, Human Interfaces in Information Systems Laboratory)*

Valutazione dell'usabilità di applicazioni web su dispositivi mobili tramite individuazione di "bad usability smells"

Evaluation of web applications' usability on mobile devices through "bad usability smells" detection

Sommario: *Il Web è lo strumento più diffuso e pervasivo per comunicare informazioni, stimolare la crescita di comunità o fornire servizi interattivi. Oggigiorno, i dispositivi più comuni per la navigazione Web sono gli smartphone, che ormai da tempo hanno superato i personal computer nelle statistiche relative all'accesso in rete. Conseguentemente, nell'ambito dello sviluppo di applicazioni e siti web è diventato fondamentale garantire una buona usabilità per l'accesso tramite dispositivi mobile. Nel corso degli anni sono stati proposti vari strumenti automatici per la valutazione dell'usabilità di applicazioni web, molti dei quali non consentono di effettuare un'analisi dell'usabilità basata sul comportamento degli utenti nei loro contesti quotidiani.*

Il nostro laboratorio ha sviluppato un nuovo metodo di valutazione dell'usabilità, basato sull'analisi delle interazioni degli utenti, allo scopo di identificare specifici comportamenti degli utenti (detti "bad usability smells"), che spesso vengono manifestati per gestire situazioni problematiche nell'uso di una applicazione. Il metodo consiste nell'analizzare i log delle interazioni degli utenti ed identificare la presenza di queste interazioni problematiche, che sono descritte e formalizzate tramite un linguaggio specifico realizzato ad hoc. Tale metodo è stato applicato, tramite il relativo strumento automatico di supporto, in un caso di studio relativo ad una applicazione Web italiana di largo uso: attraverso tale approccio è stato possibile identificare alcune parti dell'interfaccia utente dell'applicazione che erano problematiche dal punto di vista dell'usabilità.

Abstract: *The Web is the most widespread and pervasive way for communicating information, stimulating community growth or providing interactive services. Nowadays, the most common devices for Web browsing are smartphones, which have long since surpassed personal computers in network access statistics. Consequently, in the development of applications and websites it has become essential to guarantee good usability for access via mobile devices. Over the years, various automatic tools have been proposed for the evaluation of the usability of web applications, many of which do not allow usability analysis based on user behavior in their daily contexts.*

Our laboratory has developed a new usability evaluation method, based on the analysis of user interactions, in order to identify specific

user behaviors (called "bad usability smells"), which are often manifested to handle problematic situations during the use of a web application. The method consists in analyzing the log of user interactions and identifying the presence of these problematic interactions, which are described and formalized through a specific language created for this pourpose. This method has been applied, through the relative automatic support tool , in a case study of a widely used Italian Web application: through this approach it was possible to identify some parts of the user interface of the application that were problematic from the usability point of view.

1. Introduzione

Il World Wide Web è un mezzo globale indispensabile di comunicazione per persone, aziende e pubbliche organizzazioni. Lo sviluppo di applicazioni Web di semplice uso è diventato ormai un elemento cruciale per chiunque voglia promuovere servizi o trasmettere informazioni. Questa necessità è resa ancora più stringente dall'uso diffuso di dispositivi mobili, i quali oggigiorno sono le piattaforme più utilizzate per svolgere attività di svago (come effettuare ricerche online[1] o usufruire di contenuti multimediali) e il loro utilizzo nelle attività professionali è in costante crescita[2].

Difatti, l'uso di tali dispositivi mobili ha cambiato il modo in cui le persone navigano nel Web ed usano i servizi online: lo svolgimento di tali attività non è più rilegato in ambienti definititi quali ad esempio uffici o case, ma può essere effettuato praticamente in qualunque luogo, come ad esempio sui mezzi di trasporto pubblico, in ambienti all'aperto, all'interno di locali pubblici, etc).

Per diversi anni, i ricercatori hanno condotto studi relativi all'analisi e il miglioramento dell'usabilità delle applicazioni Web[3][4], proponendo diversi strumenti, metodologie e tecniche per questo scopo. In particolare, gli studi si sono concentrati sullo sviluppo di strumenti di valutazione automatica dell'usabilità [5], il cui utilizzo consente di ridurre i tempi e i costi necessari all'analisi dell'usabilità, liberare i valutatori da compiti ripetitivi e noiosi, e che le valutazioni siano possibili anche per applicazioni complesse senza aumentare i costi di valutazione eccessivi. Gli strumenti di valutazione automatica dell'usabilità possono essere classificati in due gruppi principali: quelli che usano il codice sorgente delle pagine Web (cioè la loro struttura e / o contenuto) come fonte di dati per il rilevamento di problemi di usabilità, e quelli che si concentrano sull'analisi dei dati di interazione dell'utente reale. Il primo gruppo include alcuni strumenti commerciali come Google Mobile Friendly Test Tool [6] o Bing's Mobile Friendliness Test Tool [7]. A partire dalla struttura della pagina Web, questi strumenti cercano di valutarne l'usabilità nello specifico contesto della navigazione web effettuata tramite dispositivi mobili. Nel secondo gruppo, invece, i dati di utilizzo possono essere recuperati dai log del server (contenente principalmente le sequenze cronologiche delle pagine web visitate) o dalla registrazione lato client delle attività degli utenti mentre stanno navigando (registrando così sia la sequenza di pagine Web visitate che interazioni

infra-pagina, come ad esempio selezioni con il mouse, uso della barra di scorrimento, ecc.).

L'ascesa di dispositivi come smartphone e tablet ha portato all'ampia adozione di tipi di interazioni utente che sono significativamente diversi da quelli sui dispositivi desktop. Le differenze nascono dai molti possibili contesti d'uso, dalle limitazioni tecniche dei dispositivi mobili (ad es. Connettività non sempre ottimale, dimensioni dello schermo minori, con risoluzioni diverse, capacità di elaborazione talvolta limitata), e dal modo in cui gli utenti interagiscono con loro (ad esempio, alcuni utenti preferisco interagire con gli smartphone con entrambe le mani, gli altri preferiscono interagire con una sola mano [8]). Variazioni in ciascuno di questi fattori (ad esempio il cambiamento della dimensione dello schermo [9]) può quindi portare a diverse percezioni di usabilità. Al fine di comprendere e analizzare meglio questi tipi di interazioni degli utenti è quindi necessario definire criteri specifici e sviluppare nuovi strumenti di valutazione per garantire poi un'adeguata valutazione dell’usabilità anche in contesti mobili. Per venire incontro a tale esigenza, presso l’HIIS Laboratory dell’Istituto di Scienza e Tecnologie del Consiglio Nazionale delle Ricerche è stato elaborato una metodologia basata sul rilevamento automatico di indicatori di problemi di usabilità (definiti "Bad Usability Smells") nei dispositivi mobili durante l’accesso alle applicazioni Web. Per mettere in pratica tale metodologia è stato inoltre sviluppata una piattaforma di valutazione dell'usabilità, chiamata M.U.S.E. (Mobile Usability Smell Evaluator)[10], che è in grado di registrare l'utente comportamento durante l'interazione con qualsiasi applicazione Web attraverso qualsiasi tipo di dispositivo abilitato per il browser. Le interazioni utente così ottenute vengono elaborate da un algoritmo per l'identificazione di specifici pattern di interazione che indicano la presenza potenziale di problemi di usabilità.

2. Formalizzazione dei Bad Usability Smell

I Bad Usability Smell rappresentano degli indicatori della potenziale presenza di qualche problemi di usabilità all'interno di un'applicazione web.

Nello sviluppo di un approccio basato sull’individuazione di tali indicatori, un ruolo fondamentale è ricoperto dagli utenti di tali applicazioni, che, tramite le loro interazioni con l’applicazione, sono la fonte dei dati utili al rilevamento di tali criticità dal punto di vista dell’usabilità. Al fine quindi di garantire la qualità dei dati acquisiti, il rilevamento delle interazioni dovrebbe essere effettuato in modo non invadente, in modo da non influire sul comportamento dell'utente durante l'esecuzione dei suoi compiti. Le strategie adottate per svolgere compiti possono variare da utente per utente in base a vari aspetti, ad esempio contesti d'uso diversi, dispositivi diversi, diversa personalità, ecc. Anche di fronte allo stesso problema di usabilità, gli utenti possono adottare varie strategie (e di conseguenza, comportamenti) volte a superare eventuali situazioni problematiche. Nonostante tale variabilità, è possibile definire un piccolo sottoinsieme di comportamenti più

frequentemente adottati dagli utenti per far fronte a specifici problemi di usabilità. Questo sottoinsieme è quindi la base per la definizione dei Bad Usability Smell. Vari ricercatori hanno condotto negli anni alcuni studi volti a catturare tali "comportamenti più frequenti", o in relazione a particolari tipologie di dispositivi (ad esempio nei confronti di applicazioni desktop) oppure rivolti a diverse finalità (ad esempio il supporto all'adattamento automatico delle pagine web). A causa delle limitate dimensioni dello schermo, della scarsa precisione di puntamento del tocco basato sulle dita umane, gli utenti, navigando tramite dispositivi mobili, possono incontrarne delle difficoltà se la progettazione dell'interfaccia utente non tiene conto delle peculiarità di tali dispositivi.

Una prima fase del nostro lavoro è stato definire un insieme di problemi di usabilità che possono essere rivelati tramite l'analisi del comportamento dell'utente. Per identificare questo set ci siamo basati sui lavori presenti in letteratura scientifica (ad es. [11]), informazioni fornite da software commerciali, come ad esempio [12], importanti studi relativi all'usabilità mobile [13] e nostre analisi sullo sviluppo di vari siti Web e di come gli utenti interagiscono con essi in ambiente mobile. Alla fine di questa fase di studio, abbiamo identificato sei diversi problemi di usabilità:

- **Elementi troppo piccoli o vicini**: questo bad smell è caratterizzato da elementi interattivi nella pagina Web che sono eccessivamente piccoli o vicini. (ad es. Figura 1)
- **Links troppo vicini**: corrisponde a una selezione dell'utente che implica il caricamento di una pagina sbagliata.
- **Contenuto distante**: quando l'utente è forzato ad eseguire molti scroll in alto ed in basso.
- **Sezione Troppo Piccola**: una sezione troppo piccola richiede specifiche azioni di ingrandimento.
- **Cattiva leggibilità**: quando vi sono testi con font troppo piccoli o spaziature troppo ridotte (ad es. Figura 2 – lato sinistro)
- **Form lunghe**: quando vi è un numero di elementi in una form che può essere considerato eccessivo per una buona usabilità su dispositivo mobile (ad es. Figura 2 – lato destro)

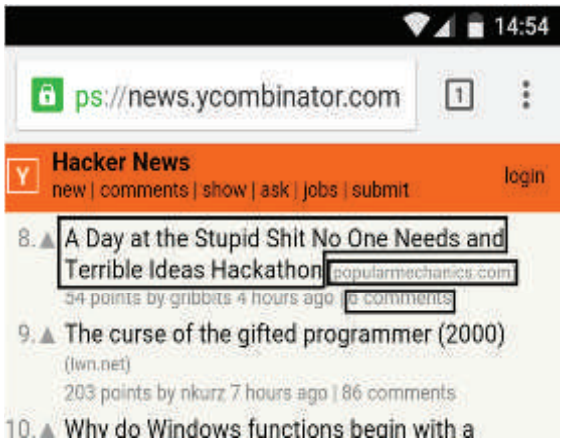


Figura 1. Esempio di elementi troppo vicini

Figura 2.. Esempio di cattiva leggibilità (a sinistra) e di form lunghi (a destra)

Un passo necessario al fine di sviluppare un sistema automatico per il rilevamento dei bad smell è stato lo sviluppo di un linguaggio utile per formalizzare tali indicatori. Poiché le sessioni utente sono registrate come sequenze di eventi, anche tali indicatori sono stati formalizzati come pattern di eventi. Quindi, il rilevamento di bad usability smell si ottiene controllando, all'interno delle sequenze di eventi registrate, la presenza di pattern di eventi che rappresentano uno o più cattivi odori di usabilità. Durante la fase di sviluppo di tale approccio, abbiamo notato come sia molto difficile individuare sequenze di eventi esattamente precise per rilevarli. Infatti, i comportamenti degli utenti possono variare in molti modi, anche minimi, e quindi è impossibile associare un problema di usabilità con una sequenza di eventi esatta. Questo aspetto ha portato all’ introduzione di una serie di operatori per definire le tipologie di sequenze di eventi rilevanti, e quindi destinati a facilitare il rilevamento di sequenze simili tra loro, anche se non esattamente identiche, in modo da introdurre una certa flessibilità nel meccanismo di rilevamento. Ad esempio abbiamo introdotto:

- Operatori per indicare il numero di ripetizioni di un evento (o per indicare la presenza di nessun limite di ripetizioni, indicate tramite il carattere speciale *).
- Operatori per indicare una direzione negli eventi per cui l'informazione ha senso (ad esempio lo scroll), oppure lasciare indefinita tale informazione (indicate tramite il carattere speciale $).
- Operatori per definire un'intervallo temporale, inteso come tempo massimo che può trascorrere tra l'evento precedente e quello corrente.

In Tabella 1 è possibile osservare alcuni esempi di formalizzazione astratta dei bad smell. Per esempio, nel primo caso abbiamo una sequenza di eventi di pinch, seguita da una sequenza di eventi pan in qualunque direzione, e conclusa da un evento tap su un elemento con conseguente cambio di focus.

Bad Usability Smell	Pattern di Eventi
Too Small or Close Elements	[*] Pinch(out) + [*]Pan($) + Tap + Focus(in)
Too Close Links	[*]Tap + Beforeunload + Pageview + Beforeunload + Pageview
Distant Content	[5]Pan(down)

Tabella 1. Pattern comportamentali per alcuni bad smell

Per l'implementazione concreta del linguaggio definito, utile per consentirne l'applicazione in un sistema automatico, seguendo l'esempio di numerosi altri lavori in letteratura (ad esempio [14]), abbiamo utilizzato un semplice linguaggio XML. I vantaggi nell'uso di XML per formalizzare tali pattern sono che la loro descrizione è facilmente comprensibile sia da esseri umani che da sistemi informatici, può essere facilmente estesa e/ o modificata e può essere convalidata definendo un appropriato Schema XSD.

3. Il validatore di usabilità M.U.S.E.

Al fine di implementare concretamente l'approccio proposto, abbiamo sviluppato uno strumento automatico di valutazione dell'usabilità web chiamato M.U.S.E. (Mobile Usability Smell Evaluator), la cui architettura è illustrata in Figura 3.

Tale strumento è basato su di un proxy che è in grado di registrare il file con gli eventi generati durante da un utente durante l'interazione con qualsiasi Web applicazione tramite dispositivi desktop o mobili.

I dati sul comportamento degli utenti sono raccolti attraverso un Logger JavaScript iniettato nella pagina Web dal proxy: lo strumento è quindi in grado di registrare le interazioni dell'utente con qualsiasi sito Web, e quindi senza la necessità per il proprietario del sito Web di installare manualmente gli script di registrazione dei dati.

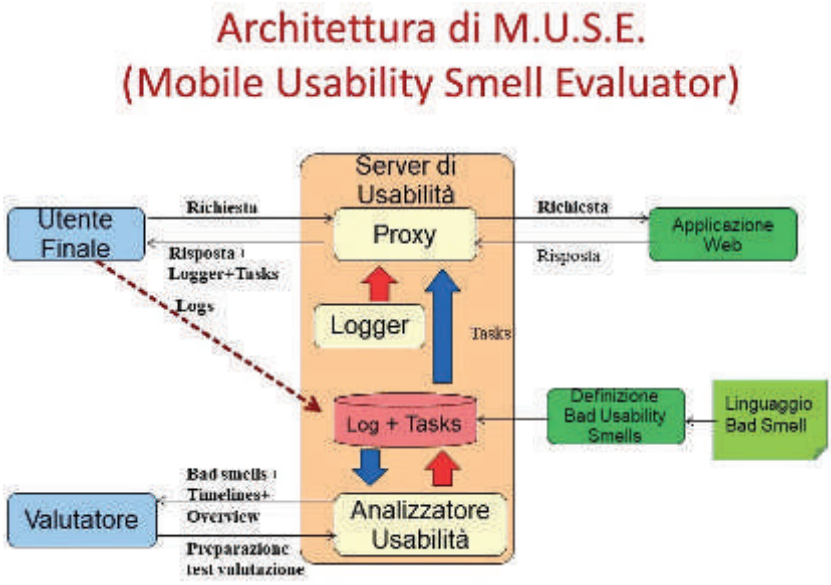


Figura 3 . L'architettura di M.U.S.E.

M.U.S.E. include anche un pannello di gestione attraverso il quale un esperto di usabilità, oltre ad associare la piattaforma ad un particolare sito, può definire dei compiti specifici che gli utenti possono completare al fine di testare una particolare pagina o una particolare funzionalità di un'applicazione web. Ogni interazione dell'utente è registrata come sequenza di eventi, che include sia quelli generati direttamente dall'utente (ad es. click, tap, movimento del mouse) che quelli generati dal browser in risposta alle azioni dell'utente (ad esempio ridimensionamento della pagina, cambiamento di orientamento di un dispositivo mobile).

Una volta catturati tali sequenze di eventi, il validatore consente agli esperti di usabilità di analizzare le interazioni dell'utente, graficamente rappresentate tramite delle timeline [15]: ognuna di esse può essere fatta scorrere temporalmente in avanti ed indietro, ed inoltre una coppia di timeline può essere sovrapposta per consentire di confrontare visivamente il comportamento di due distinti utenti nell'esecuzione dello stesso compito. Sempre tramite lo stesso pannello, l'esperto può attivare la funzionalità di riconoscimento automatico dei bad smell, precedentemente formalizzati e caricati sulla piattaforma. La Figura 4 mostra una timeline in cui è stata rilevata la presenza di un sottoinsieme di eventi corrispondente ad un bad smell, evidenziato in rosso.

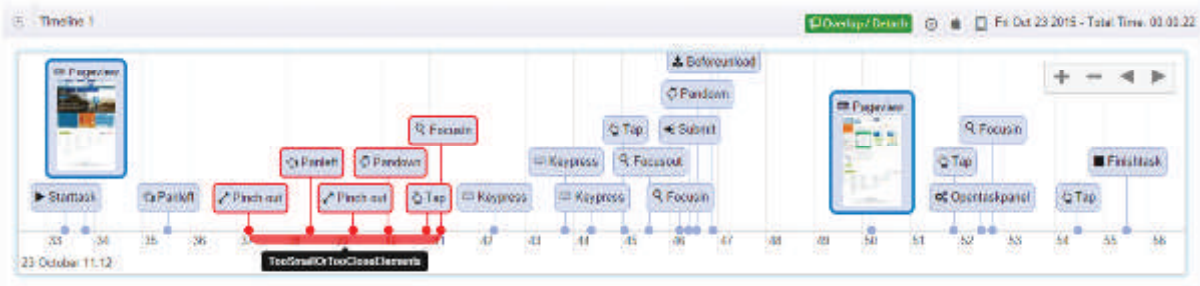


Figura 4. Esempio di timeline all'interno della quale è stato rilevato un bad smell

4. Test Utenti

Al fine di testare il nostro approccio, fu creata una sessione di valutazione dell'usabilità, composta da quattro diversi compiti, da svolgersi sulla versione inglese di un sito relativo alle autostrade italiane, che fornisce servizi di pubblica utilità e che presentava problematiche di usabilità. A tale test hanno partecipato circa 40 utenti (età media 28) di entrambi i sessi, che hanno eseguito i compiti previsti dalla sessione di test tramite il loro smartphone senza vincoli di luogo e di tempo. L'esecuzione di tale test ha portato alla generazione di più di 14000 eventi, in cui MUSE ha trovato 51 istanze di bad usability smells.

I risultati dei test evidenziarono alcuni problemi di usabilità riguardanti la struttura dell'interfaccia utente, avente troppi elementi e non bene organizzati: in particolare, i più comuni bad usability smells rilevati nell'applicazione considerata furono "Elementi Troppo Piccoli o Vicini" e "Contenuto Distante".

5. Conclusioni

Abbiamo presentato un nuovo approccio per la valutazione dell'usabilità delle applicazioni web, con particolare riferimento all'usabilità in ambito mobile. Tale metodologia, basata sulla raccolta di dati relativi all'interazione di alcuni utenti all'interno di una applicazione web e sul successivo rilevamento di bad usability smell, è stata implementata uno strumento automatico di valutazione, chiamato M.U.S.E.

La soluzione proposta consente la valutazione di applicazioni Web mobile senza obbligare il possessore dell'applicazione a modificarla manualmente per seguire tali test. Inoltre, secondo l'approccio proposto, gli utenti che partecipano al test possono operare "in the wild", ossia senza l'obbligo dell'uso di dispositivi specifici, di svolgere i test in luoghi o in tempi predefiniti.

L'insieme dei bad usability smells, definiti all'interno della nostra metodologia, è stata formalizzata tramite linguaggio XML, in modo che tale insieme sia facilmente modificabile ed espandibile, senza richiedere cambiamenti nell'implementazione del validatore di usabilità. Pianifichiamo ulteriori studi per migliorare le funzionalità di M.U.S.E. e di effettuare ulteriori studi volti a migliorare e raffinare le definizioni dei bad usability smells.

Bibliografia

[1] Google's AdWords official blog (May 2015) http://adwords.blogspot.com/2015/05/building-fornext-moment.html.
[2] ComScore's Global Mobile Report (July 14, 2015). http://www.comscore.com/Insights/Presentations-andWhitepapers/2015/The-Global-Mobile-Report
[3] J. Grigera, A. Garrido, and J. M. Rivero "A tool for detecting bad usability smells in an automatic way" in Web Engineering, ser. Lecture Notes in Computer Science. vol. 8541 pp. 490–493, 2014.
[4] V. F. de Santana and M. C. Calani Baranauskas "WELFIT: A Remote Evaluation Tool for Identifying Web Usage Patterns through Client-Side Logging" in International Journal of Human-Computer Studies, vol. 76 no. C pp 40-49, 2015.
[5] M. Y. Ivory and M. A. Hearst "The state of the art in automating usability evaluation of user interfaces" in ACM Computing Surveys (CSUR) vol. 33 no. 4 pp. 470-516, 2001.
[6] Google Mobile Friendly Test Tool. https://www.google.com/webmasters/tools/mobilefriendly/
[7] Bing's Mobile Friendliness Test Tool. https://www.bing.com/webmaster/tools/mobilefriendliness
[8] S. Boring, D. Ledo, X. Chen, N. Marquardt, A. Tang and S. Greenberg, "The fat thumb: using the thumb's contact size for single-handed mobile interaction" in Proc. 14th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'12), 2012, pp. 39-48.
[9] D. Raptis, N. Tselios, J. Kjeldskov and M. Skov "Does size matter? investigating the impact of mobile phone screen size on users' perceived usability, effectiveness and efficiency" in Proc. 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI 2013), 2013, pp. 127-136).
[10] F. Paternò, A. G. Schiavone, A. Conti: "Customizable Automatic Detection of Bad Usability Smells in Mobile Accessed Web Applications", Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI 2017)
[11] J. Grigera, A. Garrido, and J. M. Rivero "A tool for detecting bad usability smells in an automatic way" in Web Engineering, ser. Lecture Notes in Computer Science. vol. 8541 pp. 490–493, 2014.
[12] Google Search Console. Retrieved February 6, 2017 from https://www.google.com/webmasters/tools/
[13] J. Nielsen and R. Budiu. Mobile Usability. New Riders (2013)

[14] A. G. Schiavone, F. Paternò: “An extensible environment for guidelinebased accessibility evaluation of dynamic Web-applications“, Universal Access in the Information Society v. 14, no. 1

[15] F. Paternò, A. G. Schiavone, P. Pitardi. “Timelines for Mobile Web Usability Evaluation”, in Proc. of the International Working Conference on Advanced Visual Interfaces (AVI 2016), 2016, pp. 88-91.

Sergio Pompei,
Edion Tego,
Elena Mammi,
Francesco Matera
(Fondazione Ugo Bordoni)

Elio Restuccia,
Vincenzo Attanasio,
Emanuele Nastri,
Anna Stefania Michelangeli
(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Verso il LAB ISCOM 5G: Il segmento XHAUL

Towards the 5G LAB ISCOM: the XHAUL segment

Sommario: *In questo articolo è descritta la piattaforma che è stata realizzata presso l'ISCOM per avere un laboratorio compatibile con gli ambienti 5G che si presenteranno nel giro dei prossimi tre anni. Come vedremo questa piattaforma si basa su una rete sperimentale che rappresenta una rete di trasporto ottimizzata proprio per le connessioni alle base station degli apparati wireless, segmento che oggi viene indicato con il termine* ***XHaul****, con una serie di strumenti analitici e simulativi per studiare tutte le possibili architetture di rete ibride wireless. In questo articolo in particolare descriviamo questa piattaforma con le sue modalità per la creazione di percorsi logici, denominati slice, per la connessione delle antenne degli apparati wireless e la modalità per la gestione dinamica delle risorse con tecniche Software Defined Networks (SDN). Riportiamo inoltre diversi risultati sperimentali che mostrano l'eccellenza delle scelte fatte.*

Abstract: *This article describes the platform that has been built at ISCOM to have a laboratory compatible with 5G environments that will be present within the next three years. As we will see, this platform is based on an experimental network that represents a transport area optimized for connections to the base stations of wireless devices, a segment that today is referred to as* ***XHaul****, with a series of analytical and simulative tools to study all the possible hybrid network architectures. In this article in particular we describe this platform with its modalities for the creation of logical paths, called slices, for the connection of the antennas of the wireless devices and the mode for the dynamic management of resources with Software Defined Networks (SDN) techniques. We also report various experimental results that show the excellence of our choices.*

1. Introduzione

La progressiva crescita esponenziale del traffico dati sta spingendo verso una rivoluzione della rete caratterizzata da una crescente capacità, dall'evoluzione del wireless verso il cosiddetto paradigma 5G [1] e, soprattutto, dalla cooperazione tra diversi sistemi cablati e wireless [2] , con una adeguata convergenza tra le reti in fibra ottica, spesso denominate come Next Generation Networks (NGN) e quelle radio con particolare rilevanza per quel mondo che va sotto il nome di

Internet delle cose (Machine to Machine, M2M e Device to Device, D2D) [3]. Inoltre, l'evoluzione RAN (Radio Access Network) sfrutterà sempre di più una combinazione di tecniche di virtualizzazione, centralizzazione e coordinamento, che interagiscono tra di loro in diversi modi all'interno di un nuovo concetto definito come C-RAN [4].

Tale evoluzione stimolerà anche la domanda di servizi e applicazioni coinvolgendo sempre più il mondo dei *verticals*. Così la rete dovrà essere sempre più abile a soddisfare, in ogni segmento logico (o fisico), quei requisiti specifici in termini di QoS, larghezza di banda e affidabilità. Questo approccio è stato visto recentemente come una nuova strategia di telecomunicazione denominata *Network Slicing as a Service* (NsaS) [5], che aiuterà gli operatori ad offrire reti ad hoc end-to-end adattate ad ogni esigenza per essere offerte come un servizio. Per tale scopo, nelle reti in fibra ottica la multiplazione di lunghezza d'onda (WDM) e quella Optical-Orthogonal Frequency Division Multiplexing (O-OFDM), utilizzate dalle reti core alle reti di accesso, ed in particolare sulle reti passive ottiche (PON), garantiranno enormi capacità [6]. I processi di slicing saranno permessi da tecniche di inoltro che consentono l'implementazione di percorsi virtuali all'interno della stessa infrastruttura [7-10]. Da questo punto di vista il Carrier Ethernet (CE) sembra essere uno dei candidati più interessanti, in particolare per connettere l'unità di base band (BBU), grazie alla sua capacità di gestire reti private VPN di Layer 2 (L2), permettendo connessioni point-to-multipoint e trasmissioni di tipo multicast e broadcast [11-13]. Inoltre CE abilita i processi di virtualizzazione di rete (NFV) [14].

In questo articolo mostriamo come il laboratorio ISCOM NGN è stato configurato per realizzare una infrastruttura in grado di rispondere alle caratteristiche descritte sopra, descrivendo la nostra visione di *slicing*, tenendo conto degli approcci dello strato 2-3 che operano dal segmento di accesso domestico a quello metro e core, con alcuni test sperimentali in merito al nostro approccio CE basato sulla tecnica Backbone Bridge-Traffic Engineering (PBB- TE) all'interno di una rete GMPLS [1] che include sia una parte regionale che una di accesso che dovrebbe connettersi alle Base Station (BS) con connessioni di tipo backhauling o fronthauling. In pratica le sperimentazioni riguarderanno quel segmento di rete oggi definito come **Xhaul** [15]**,** che parte dalle antenne radio fino a raggiungere i punti di presenza (PoP) nelle reti core di uno o più service provider, attraversando elementi di instradamento ad alta capacità e connessioni eterogenee (ad esempio, fibra ottica o wireless, rame ad alta capacità, o onde millimetriche) che collegano le celle radio (sia macro che micro, pico e femto) anche con mini data center.

In particolare mostriamo i vantaggi di avere degli accessi basati sugli apparati NG-PON2 che risultano particolarmente importanti per avere basse latenze. Inoltre riportiamo anche la nostra modalità per la gestione dinamica delle risorse con un approccio Software Defined Network (SDN).

Questo articolo è strutturato nella seguente maniera. Dopo questa introduzione nel Par. 2 è riportata una breve panoramica sui servizi 5G. Nel Par. 3 descriviamo l'ambiente di studio che abbiamo realizzato per affrontare le svariate dinamiche sul 5G, con particolare rilevanza per le

tecniche riguardanti l'XHaul. Nel Par. 4 riportiamo i risultati per le tecniche di backhaling e di slicing, nel Par. 5 descriviamo il nostro approccio SDN con test riguardanti aspetti di disaster recovery. Nel Par. 6 descriviamo l'ambiente per i test di QoS per apparati wireless con alcune misure su smartphone in modalità Wi-Fi. Le conclusioni sono riportate nel Par. 7.

2. I servizi di tipo 5G

Prima di procedere alla descrizione dell'infrastruttura del laboratorio riportiamo alcune caratteristiche essenziali che riguarderanno i servizi 5G, che ci aiuteranno anche a capire le scelte che sono state fatte in questa attività. In particolare in questo articolo ci interessiamo solo degli aspetti del 5G che riguardano le ricadute che possono avere sulla realizzazione della rete di trasporto (accesso-metro-core), e questo proprio per definire le configurazioni da attuare sulla rete NGN ISCOM per renderla idonea alla connessione con apparati di tipo 5G.

In particolare facciamo riferimento al raggruppamento di industrie, operatori e centri di ricerca che hanno formato la *Next Generation Mobile Network Alliance* [8] e che ha cercato di evidenziare tutte le trasformazioni che la rete NGN, sia di tipo Core che di accesso, dovrà subire per rendersi adeguata alle reti 5G.

In realtà tale documento presenta diverse disamine dei servizi 5G, senza mai entrare del dettaglio delle tecnologie delle reti access-core, ed in particolare di come queste possono essere utilizzate. Tuttavia proprio la disamina dei servizi 5G ci permetterà di avere una accurata conoscenza delle prestazioni necessarie, permettendoci di fare le nostre proposte per la rete access-core e di sperimentarle sul test bed ISCOM.

Il white paper **NGMN White paper** [8] distingue otto use cases che individuano dei gruppi di servizi con specifiche richieste prestazionali; riportiamo tale elenco descrivendo tra le parentesi il servizio più caratteristico:

* Broadband access in dense area (pervasive video);
* Broadband access everywhere (50 Mb/s per tutti);
* Higher user mobility (High speed train);
* Massive Internet of things (sensor networks);
* Extreme real-time communications (tactile internet);
* lifeline communications (natural disaster);
* Ultra reliable communications (E-Health services);
* Broadcast-like services (Broadcast-like services).

Nella tabella 1 riportiamo i principali Key Performance Indicators (KPI's) per gli 8 case studies elencati.

Use case category	User Experienced Data Rate	E2E Latency	Mobility
Broadband access in dense areas	DL: 300 Mbps UL: 50 Mbps	10 ms	On demand, 0-100 km/h
Indoor ultra-high broadband access	DL: 1 Gbps, UL: 500 Mbps	10 ms	Pedestrian
Broadband access in a crowd	DL: 25 Mbps UL: 50 Mbps	10 ms	Pedestrian
50+ Mbps everywhere	DL: 50 Mbps UL: 25 Mbps	10 ms	0-120 km/h
Ultra-low cost broadband access for low ARPU areas	DL: 10 Mbps UL: 10 Mbps	50 ms	on demand: 0-50 km/h
Mobile broadband in vehicles (cars, trains)	DL: 50 Mbps UL: 25 Mbps	10 ms	On demand, up to 500 km/h
Airplanes connectivity	DL: 15 Mbps per user UL: 7.5 Mbps per user	10 ms	Up to 1000 km/h
Massive low-cost/long-range/low-power MTC	Low (typically 1-100 kbps)	Seconds to hours	on demand: 0-500 km/h
Broadband MTC	See the requirements for the Broadband access in dense areas and 50+Mbps everywhere categories		
Ultra-low latency	DL: 50 Mbps UL: 25 Mbps	<1 ms	Pedestrian
Resilience and traffic surge	DL: 0.1-1 Mbps UL: 0.1-1 Mbps	Regular communication: not critical	0-120 km/h
Ultra-high reliability & Ultra-low latency	DL: From 50 kbps to 10 Mbps; UL: From a few bps to 10 Mbps	1 ms	on demand: 0-500 km/h
Ultra-high availability & reliability	DL: 10 Mbps UL: 10 Mbps	10 ms	On demand, 0-500 km/h
Broadcast like services	DL: Up to 200 Mbps UL: Modest (e.g. 500 kbps)	<100 ms	on demand: 0-500 km/h

Tabella 1. Key Performance Indicators (KPI's) per gli 8 case studies elencati [8]

Use case category	Connection Density	Traffic Density
Broadband access in dense areas	200-2500 /km^2	DL: 750 Gbps / km2 UL: 125 Gbps / km2
Indoor ultra-high broadband access	75,000 / km^2 (75/1000 m^2 office)	DL: 15 Tbps/ km2 (15 Gbps / 1000 m2) UL: 2 Tbps / km2 (2 Gbps / 1000 m2)
Broadband access in a crowd	150,000 / km^2 (30.000 / stadium)	DL: 3.75 Tbps / km2 (DL: 0.75 Tbps / stadium) UL: 7.5 Tbps / km2 (1.5 Tbps / stadium)
50+ Mbps everywhere	400 / km^2 in suburban 100 / km^2 in rural	DL: 20 Gbps / km2 in suburban UL: 10 Gbps / km2 in suburban DL: 5 Gbps / km2 in rural UL: 2.5 Gbps / km2 in rural
Ultra-low cost broadband access for low ARPU areas	16 / km^2	16 Mbps / km^2
Mobile broadband in vehicles (cars, trains)	2000 / km^2 (500 active users per train x 4 trains, or 1 active user per car x 2000 cars)	DL: 100 Gbps / km^2 (25 Gbps per train, 50 Mbps per car) UL: 50 Gbps / km^2 (12.5 Gbps per train, 25 Mbps per car)
Airplanes connectivity	80 per plane 60 airplanes per 18,000 km^2	DL: 1.2 Gbps / plane UL: 600 Mbps / plane
Massive low-cost/long-range/low-power MTC	Up to 200,000 / km^2	Non critical
Broadband MTC	See the requirements for the Broadband access in dense areas and 50+Mbps everywhere categories	
Ultra-low latency	Not critical	Potentially high
Resilience and traffic surge	10,000 / km^2	Potentially high
Ultra-high reliability & Ultra-low latency* (*) the reliability requirement for this category is described in Section 4.4.5	Not critical	Potentially high
Ultra-high availability & reliability* (*) the reliability requirement for this category is described in Section 4.4.5	Not critical	Potentially high
Broadcast like services	Not relevant	Not relevant

Tabella 2. Principali caratteristiche in termini di densità e traffico

3. L'ambiente per gli studi sul 5G realizzato da ISCOM-FUB

Nella figura 1 descriviamo la nostra piattaforma con molteplici funzioni per esser utilizzate in molti degli ambienti che caratterizzeranno le reti 5G dei prossimi anni; essa consiste di:

- una infrastruttura di rete core-metro-access, con l'introduzione di una nuova rete NG-PON2, che è stata configurata per gestire il trasporto delle informazioni verso le

reti wireless disponibili nei prossimi anni in ambito 5G, con specifici KPI richiesti dalle release dei nuovi sistemi wireless;

- di un insieme di tool analitici e simulativi che permettono di studiare le prestazioni di reti wireless con topologie complesse, sia in termini di copertura che di consumi energetici, considerando sia le bande radio oggi disponibili che quelle di prossima utilizzazione;
- di metodologie per la caratterizzazione del canale, specialmente per quelle ad alte frequenze su cui il comportamento della propagazione ha ancora degli aspetti non facilmente descrivibili per la presenza di molti aspetti con comportamento aleatorio.

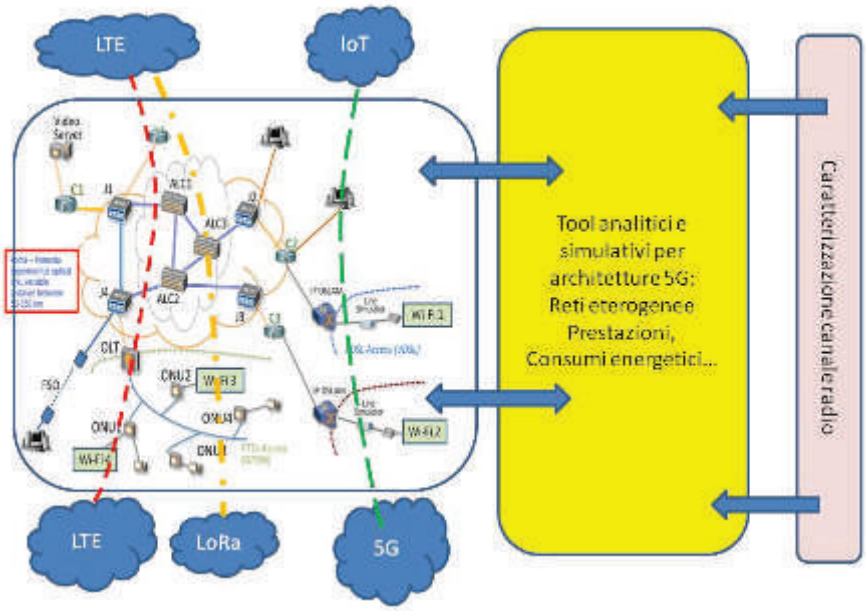


Figura 1. L'ambiente 5G realizzato da FUB e ISCTI. Le linee tratteggiate rappresentano i circuiti logici e fisici implementati in questo progetto per garantire i parametri KPI tipici del 5G

Il laboratorio Core-Metro-Access, riportato a sinistra della Figura 1, dovrà poi essere connesso con apparati wireless che al momento non sono presenti. Si spera inoltre che questo *LAB 5G ready* diventerà un punto di attrazione per future sperimentazioni regionali e nazionali, specialmente perchè questo lab può mettere a disposizione tutta una serie di apparati che non sono facilmente reperibili tra enti pubblici e terzi, a cominciare proprio dalla rete NGPON2, che proprio in questo progetto si è rivelata come una fondamentale infrastruttura per la connessione di reti eterogenee costituite da macro e micro cell.

Tramite questa piattaforma, oltre ai casi che riportiamo in questo articolo, saranno possibili tutta una serie di studi che possono coprire una serie di argomenti tipici delle tematiche sul 5G che vengono in genere suddivise in tre diverse categorie: **Enhanced Mobile Broadband (eMBB), Massive machine type communications (mMTC) e Ultra-reliable and low latency communications (URLLC)**.

4. Connessioni logiche e fisiche per celle: backhauling

L'utilizzo della porzione di spettro a più alte frequenze e bande sempre maggiori, insieme a una maggiore richiesta di copertura comportano come ricaduta la **densificazione** delle infrastrutture wireless con dispiegamento di smallcell per l'offloading della rete di macrocelle. Questo determinerà però un aumento dei collegamenti (fibra e ponti radio) per rilegare le celle con un conseguente aumento dei costi infrastrutturali. La nuova rete di quinta generazione però si mostra flessibile sull'impiego di qualsiasi tecnologia per la sezione di accesso, con l'obiettivo però di rispettare i parametri di rete preposti tra cui throughput e latenza.

L'architettura base che abbiamo preso in considerazione per reti ultrabroadband mobile è quella riportata in Figura 2, dove a livello di accesso le reti in fibra di tipo P2P e GPON, verranno gestite con tecniche slicing atte a creare circuiti logici e fisici a bassissima latenza. La configurazione tipica utilizzata per HetNet sarà basata su backhauling con P2P per macrocelle e GPON e NGPON2 per small cell, e la rete sarà in grado di gestire in modo dinamico (secondo schemi tipici delle SDN) le risorse disponibili (essenzialmente connessioni ottiche GbE) sfruttando le conoscenze che possono provenire da una rete di monitoraggio per la valutazione della QoS presso gli utenti o per la conoscenza del traffico in rete.

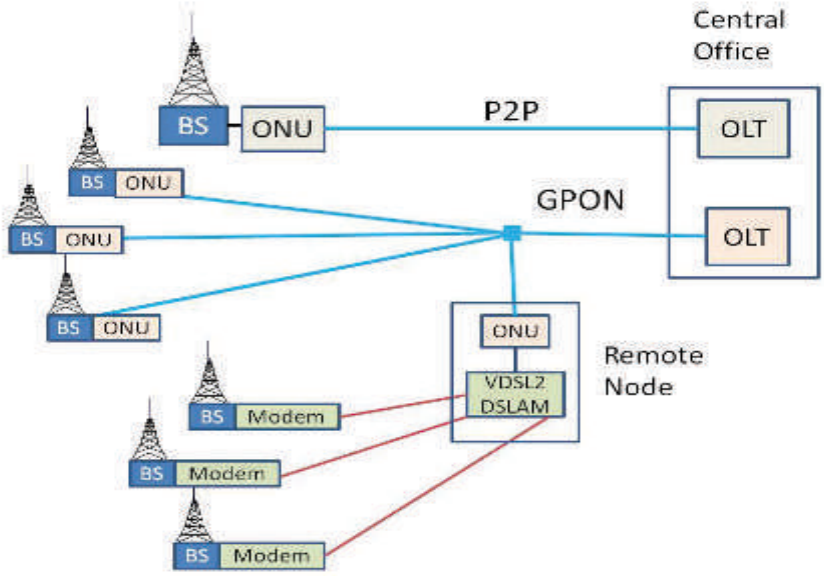


Figura 2. Configurazione backhauling per copertura con Macro-Micro celle

Nella **Errore. L'origine riferimento non è stata trovata.** si riporta la configurazione utilizzata nel LAB NGN per studiare le prestazioni di queste reti specialmente dal punto di vista della latenza.

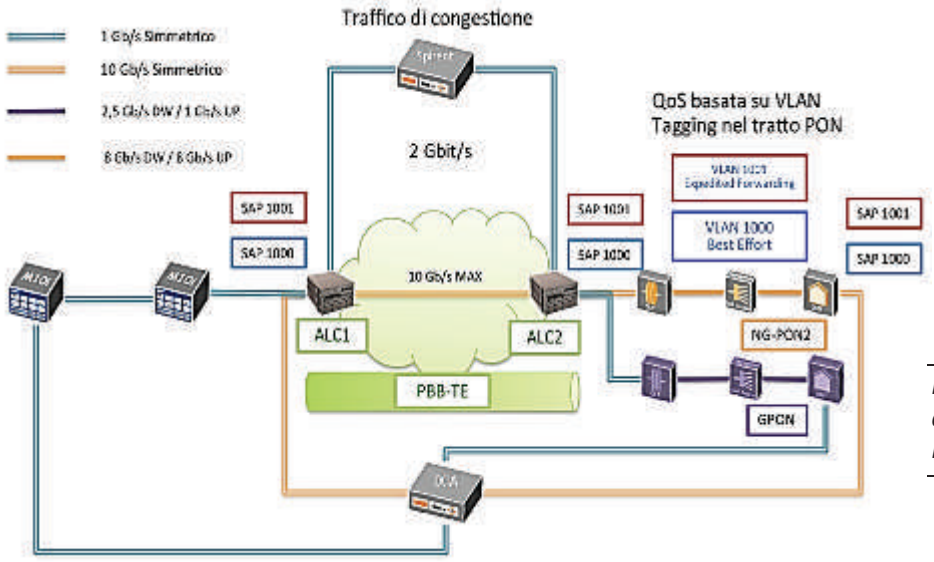


Figura 3. Configurazione rete di test (caratterizzazione NG-PON2)

In particolare per ricreare condizioni di carico reale della rete e per simulare situazioni di congestione critiche ci si è avvalsi di due generatori di traffico come lo Spirent e l'Ixia dotati di interfacce a 10 Gb/s, anche per valutare le tecniche di slicing per la differenziazione dei servizi.

4.1. Struttura dei Test Upstream e Downstream

Per poter dimostrare l'obiettivo preposto, inizialmente, affinché l'architettura di rete considerata sia compatibile con i parametri del 5G si sono scelti tre tipi di test da applicare sia in downstream che in upstream. Prima di analizzare la struttura di ciascuno si illustra nel prossimo paragrafo il tipo di Latenza scelta per tali test.

4.2. Algoritmo di calcolo della latenza

Il software IXIA mette a disposizione per l'ambiente di testing diversi algoritmi di calcolo della latenza, i principali sono:

- Store and Forward Latency: E' definito dallo standard RFC 1242 e considera l'intervallo di tempo che inizia quando l'ultimo bit del frame lascia la porta di invio e finisce quanto il primo bit del frame è visto sulla porta di ricezione(LIFO).
- Cut Through Latency: E'definito dallo standard RFC 1242 e considera l'intervallo di tempo che inizia quando il primo bit del frame lascia la porta di invio e finisce quando il primo bit del frame è visto sulla porta di ricezione(FIFO).

Per l'esecuzione dei test si è scelto come algoritmo di calcolo della latenza, il Cut Through Latency, ampiamente diffuso e compatibile con le nostre scelte di Testing.

Di seguito si illustra la costruzione dei tre Test realizzati in downstream/upstream che si eseguono inizialmente a "router scarico" per poi portare a "stressare" la rete, testandola in condizioni peggiori.

Test 1

Il primo Test viene effettuato utilizzando il software del generatore di traffico IXIA e si articola nei seguenti passi:

1. Si attiva singolarmente il traffico residenziale (1Gb/s) e si testa la rete in uno scenario "ideale" per verificarne i parametri di latenza e di throughput a rete scarica.
2. Si esegue singolarmente il traffico mobile a 10Gb/s e si attendono risultati che esprimano sia parametri minimi di latenza e sia di throughput tali da poter dimostrare l'effettivo utilizzo dell'NG-PON2 come infrastruttura di backhauling per small cell anche in questo caso a rete scarica.

Entrambe le componenti di test si eseguono in upstream/downstream, in una rete dove i singoli dispositivi vengono "stressati" in maniera minima, cercando di ottenere cosi i primi parametri iniziali da cui partire per effettuare le successive considerazioni.

Il test è stato eseguito facendo partire i singoli traffici per una media di tempo di 20 s ciascuno e per ogni flusso considerato si è scelto opportunatamente un line rate tale da comportare una packet Loss prossima allo 0%.

I parametri scelti per ciascun flusso sono stati quelli di seguito riportati sia per il primo test che per i successivi:

- Per il flusso a 10Gb/s sia in upstream che in downstream, si è impostato il line rate circa all'80% poiché fissando valori più alti si è notata una notevole perdita di pacchetti dovuta sia alla trama che all'overhead dell'NG-PON2 che ha determinato quindi un payload utile di circa 8Gb/s.
- Per il flusso a 1Gb/s sia in upstream che in downstream, si è configurato una line rate circa del 99.6% determinando un flusso nella rete di circa 1Gb/s.

Per il test 1 in analisi sono stati impostati i flussi sopra citati senza nessuna classe di servizio.

In seguito analizzando i risultati, si osserverà il comportamento delle due infrastrutture di rete di accesso quali la GPON e la NG-PON2 sia in downstream che in upstream, dove ci si aspetta una latenza più alta determinata dall'accesso TDMA.

Test 2

Per il secondo test, si decide di analizzare il comportamento dei traffici in una situazione di "carico" della rete. Il test è stato effettuato sul generatore di traffico IXIA facendo partire in background anche il traffico del generatore SPIRENT.

Tale Test è stato realizzato per analizzare i parametri di latenza e throughput dei traffici in una situazione di saturazione del canale.

Per ottenere il maggior carico nella rete, il test è stato articolato nel seguente modo:

1. Sono stati eseguiti insieme sia il traffico GPON (1Gb/s) sia il traffico mobile virtualizzato in 4 flussi da 2Gb/s e sia i due flussi generati da SPIRENT da 1Gb/s l'uno per un totale di 11 Gb/s sul ramo tra i due Alcatel 7750 connessi tramite interfaccia ethernet 10 Gb/s.

Il punto 1 è stato effettuato sia in downstream che in upstream, inserendo nella rete un totale di flussi di circa 10 Gb/s. Ci si aspettano quindi parametri elevati sia in downstream che in upstream, in ambito di latenza e throughput, che indichino la necessità di trattare in maniera distinta nella nostra architettura di rete il traffico mobile per il 5G.

Il secondo test è durato per una media di tempo di circa 20 s e i line rate per i flussi considerati sono:

- Flusso residenziale: 99.6 % line rate.
- 2 Flussi aggiuntivi dello SPIRENT: 100% line rate.
- 4 Flussi mobile da 2Gb/s: 80% line rate.
- Flussi eseguiti considerati in modalità Best Effort.

Test 3

L'ultimo test, effettuato sia in upstream che in downstream si pone l'obiettivo di dimostrare come il traffico mobile gestito con un'opportuna qualità del servizio può ottenere parametri di latenza e throughput inferiori.

Il test 3 si articola così in tal modo:

- Sono eseguiti come nel test 2 tutti i traffici compreso il residenziale a 1 Gb/s, i 4 traffici mobile a 2Gb/s e i due traffici SPIRENT per caricare la rete.
- Solo un traffico mobile a 2Gb/s considerato in un contesto 5G ad ultra-low-latency è stato modificato al fine di ottenere una qualità del servizio maggiore rispetto agli altri traffici mobile generici a 6 Gb/s. Tale cambiamento è stato effettuato scegliendo una priorità IP di tipo DiffServ con PHB di tipo EF in modo da ottenere una priorità maggiore rispetto agli altri traffici della rete.

Questo Test, vuole simulare una reale architettura 5G dove non tutto il traffico mobile ma solo quello per un determinato servizio viene gestito in un ambiente di rete "carico" in modalità differente. Il test è stato eseguito per una media di 20 s con gli stessi line rate applicati in precedenza.

4.3. Risultati del Testing

In questa sezione si analizzano i risultati di testing, confrontando l'evoluzione dei parametri di latenza e throughput in base alle diverse strutture di test eseguiti.

Test 1

Considerando il traffico mobile a 10 Gb/s in downstream si mostrano i risultati in Figura 4:

Traffic Item	Cut-Through Avg Latency (ns)	Cut-Through Min Latency (ns)
10G	74.539	73.700

Figura 4. Latenza 10Gb/s downstream

Dalla Figura 4 in esame si può notare come la latenza media ottenuta sia di 74.539 ns. Tale risultato ci mostra le potenzialità della rete di accesso NG-PON2, la quale dimostra di poter essere impiegata come rete di backhauling 5G, ottenendo parametri di latenza < 1 ms. L'esito sostenuto rientra pienamente nei requisiti di utente 5G.

Analizzando il test in termini di throughput:

Name	Tx Rate (Mbps)	Rx Rate (Mbps)
10G	8.092.105	8.092.105

Figura 5. Throughput 10Gb/s downstream

Si nota come la velocità di trasmissione e ricezione sia circa di 8 Mbps considerando come citato in precedenza un line rate del 80% sul flusso a 10Gb/s analizzato.

Focalizzandosi invece sulla Figura 6, i risultati ci mostrano una notevole differenza di latenza in ambito upstream per il traffico mobile a 10 Gb/s:

Traffic Item	Cut-Through Avg Latency (ns)	Cut-Through Min Latency (ns)
10G – UPStream	150.598	96.560

Figura 6. Latenza upstream 10Gb/s

Come previsto si nota una latenza media di 150.598 ns superiore rispetto alla latenza media in downstream. Tale incremento è dovuto

all'accesso TDMA della NG-PON2 dove le ONT possono trasmettere in un determinato intervallo di tempo.

Per quanto riguarda il throughput si rispecchia il valore ottenuto in downstream.

Entrambi i flussi in up/downstream a 10 Gb/s presentano packet loss allo 0% e ciò si evince dai risultati in Figura 4, Figura 5 e Figura 6.

Analizzando invece la rete di accesso GPON per il traffico residenziale si ottiene una latenza media di 244.506 ns in downstream, notando, come la NG-PON2, un notevole incremento nella direzione upstream.

Da questo primo test possiamo affermare come il traffico mobile generato da una "base band unit" nella rete di accesso in esame risponda in maniera ottima ai requisiti del 5G in una configurazione di rete NG-PON2 "ideale".

Test 2

Tale Test, secondo la struttura spiegata in precedenza ci mostra come i traffici a 2Gb/s per il mobile e il traffico residenziale subiscono un notevole aumento di perdita di pacchetti e una latenza spropositata dovuta alla congestione nella rete.

La Figura 7 ci mostra il test in upstream, e si può vedere come i diversi traffici mobile reagiscono alla saturazione del canale:

Traffic Item	Cut-Through Avg Latency (ns)	Cut-Through Min Latency (ns)
1G GPON UPStream	75.991.450	1.405.060
2 Gb/s BE3 UPStream	68.353.045	584.840
2 Gb/s BE2 UPStream	68.353.061	584.770
2 Gb/s BE1 UPStream	68.353.176	584.190
2 Gb/s EF UPStream	68.353.000	582.020

Figura 7. Latenza upstream flussi da 2Gb/s BE

Analizzando uno dei traffici a 2Gb/s si nota una latenza massima di 68.840.530 ns convertita in ms ad un valore di 68, che sfora ampiamente i requisiti di utente 5G dove la massima latenza ammissibile è di 10 ms. Inoltre il packet loss si aggira intorno all'8 % **rendendo indispensabili** tecniche di qualità del servizio per tutelare i traffici mobile ad ultra latenza in caso di saturazione della rete.

Test 3

Il test 3 analizzato in Figura 8, ci evidenzia come l'intervento della qualità del servizio per il traffico a ultra-low-latency sia una tecnica fondamentale per preservare la priorità del traffico e garantire una certa banda.

Traffic Item	Cut-Through Avg Latency (ns)	Cut-Through Min Latency (ns)
1G GPON UPStream	79.965.743	3.134.080
2 Gb/s BE3 UPStream	92.258.985	542.210
2 Gb/s BE2 UPStream	92.250.685	541840
2 Gb/s BE1 UPStream	92.306.040	541.020
2 Gb/s EF UPStream	126.763	106.990

Figura 8. Latenza con qualità del servizio 2Gb/s upstream

Dalla Figura 8 in upstream, si nota come la latenza media per il traffico mobile destinato a servizi ultra-low-latency con classe di servizio EF, nonostante la saturazione della rete, mantenga una latenza media di 126.75 ns, rientrando interamente nei requisiti 5G.

Name	TX Frames	RX Frames	Loss %
2 Gb/s BE3 UPStream	15.384.616	13.187.354	14,282
2 Gb/s BE2 UPStream	15.384.616	12.966.931	15,715
2 Gb/s BE1 UPStream	15.384.616	14.690.002	4,515
2 Gb/s EF UPStream	15.384.616	15.384.616	0

Figura 9. Tabella con frame rate

Osservando la Figura 9 la packet loss mostrata per i traffici generici mobile a 2Gb/s sono intorno al 15% , mentre nel caso del traffico ad ultra low latency sono allo 0 % . Tale risultato evidenzia come il traffico mobile, gestito attraverso una determinata priorità, possa raggiungere la core Network attraverso una rete di accesso soddisfacente, che gli permette di ottenere parametri richiesti per il 5G.

4.4. Grafici

In tale paragrafo si mostrano i grafici ottenuti dalla fase di testing utilizzando il sistema di gestione ISAM5620 per i router Alcatel-Lucent.

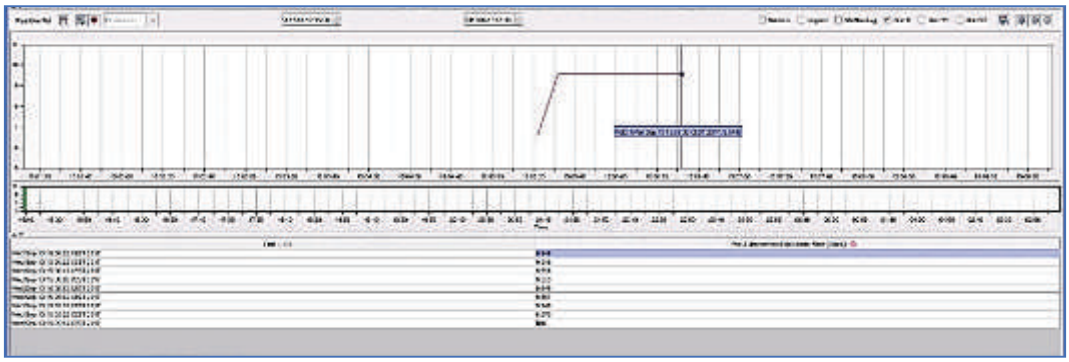


Figura 10. Grafico Saturazione del canale

La Figura 10 mostra il totale dei flussi trasmessi dalla porta due del router Alcatel-Lucent in fase di congestione. Si nota dalle statistiche un flusso totale di circa 10 Gbps che viene realizzato eseguendo sia il test 2 che il test 3.

Tale insieme di traffici porta quindi a saturare l'interfaccia a 10 Gb dei due router Alcatel-Lucent mostrando nei singoli test gli effetti di ciò che comporta.

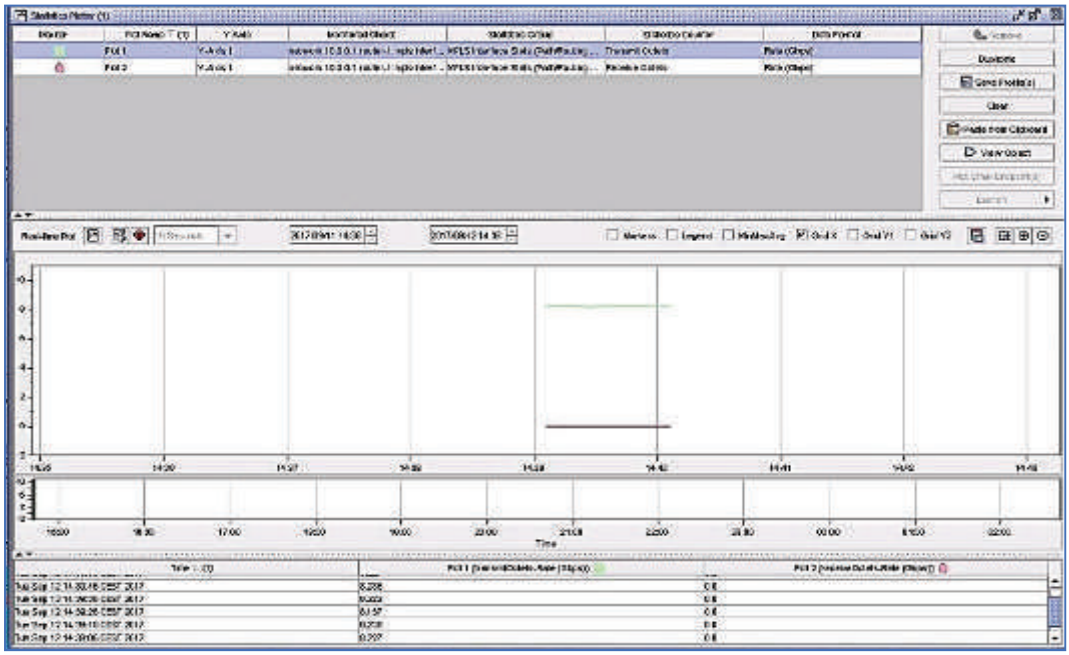


Figura 11. Grafico Tunnel MPLS

L'immagine in Figura 11 invece, è stata ottenuta mettendosi in ascolto sull'interfaccia dell'Alcatel-Lucent (router ingress MPLS) verso il successivo Alcatel in direzione downstream. Si può verificare come effettivamente nel Tunnel MPLS si trasmettano 8Gbps, che rappresentano quindi il traffico mobile presente nel tunnel che inizia sul Router Alcatel-Lucent e termina sulla OLT dell'NG-PON2. La medesima considerazione può essere effettuata in upstream.

4.5. Configurazione della qualità del servizio con Carrier Ethernet tipo PBB-TE

Per quanto riguarda la configurazione della qualità del servizio si è proceduto nella implementazione del PBB-TE (Provider Backbone Bridging – Traffic Engineer) nei 2 router Alcatel 7750. Il PBB-TE è un tipo di configurazione che permette di interconnettere due punti della rete come se facessero parte della stessa LAN ovvero come se fossero interconnessi attraverso un semplice switch di livello 2.

Il PBB-TE per funzionare correttamente ha bisogno dei seguenti protocolli implementati:

- OSPF (Open Shortest Path First), come IGP (Interior Gateway Protocol)
- RSVP (Reservation Protocol), come segnalazione (propedeutico all'MPLS)
- MPLS (Multi Protocol Label Switching), come protocollo di trasporto
- LDP (Label Distribution Protocol), come segnalazione per il tunnel SDP (Service Distribution Protocol)

Il PBB-TE è stato configurato implementando prima l'OSPF tra i due router Alcatel, successivamente l'RSVP, l'LDP e l'MPLS come base per poter creare il tunnel SDP su cui far convergere il traffico delle diverse VLAN d'ingresso (interfacce SAP).

Il tipo di convergenza del traffico può essere di due tipi:

- E-Line, servizio punto-punto
- E-LAN, servizio punto-multipunto

Per i nostri scopi è stato sufficiente configurare il servizio E-Line, in questo modo i due SAP in ingresso ai router seguono vie parallele tra i due endpoint.

La mappatura della qualità del servizio avviene a livello SAP, indicando le code assegnate a ciascun SAP. Nel caso in esame per il 1000 è Best Effort e per il 1001 è Assured Forwarding e 1002 è Expedited Forwarding.

Le tre code sono già presenti nei router poiché sono code di tipo Network.

I tre traffici così implementati seguono distintamente due percorsi logicamente separati, sebbene condividano la stessa infrastruttura. Seguono anche un trattamento relativamente alla priorità differente, caratterizzato dalle diverse code dello scheduler associate.

Si noti inoltre che il tipo di configurazione permette lo slicing di rete, nella fattispecie gli indirizzi IP configurati nelle due interfacce del generatore di traffic IXIA sono appartenenti alla medesima sottorete per ciascuna VLAN. Contestualizzando meglio, nel caso di una rete di backhauling è come se BBU ed EPC fossero direttamente connesse con un semplice cavo di rete, a fronte invece di una architettura di rete molto più complessa.

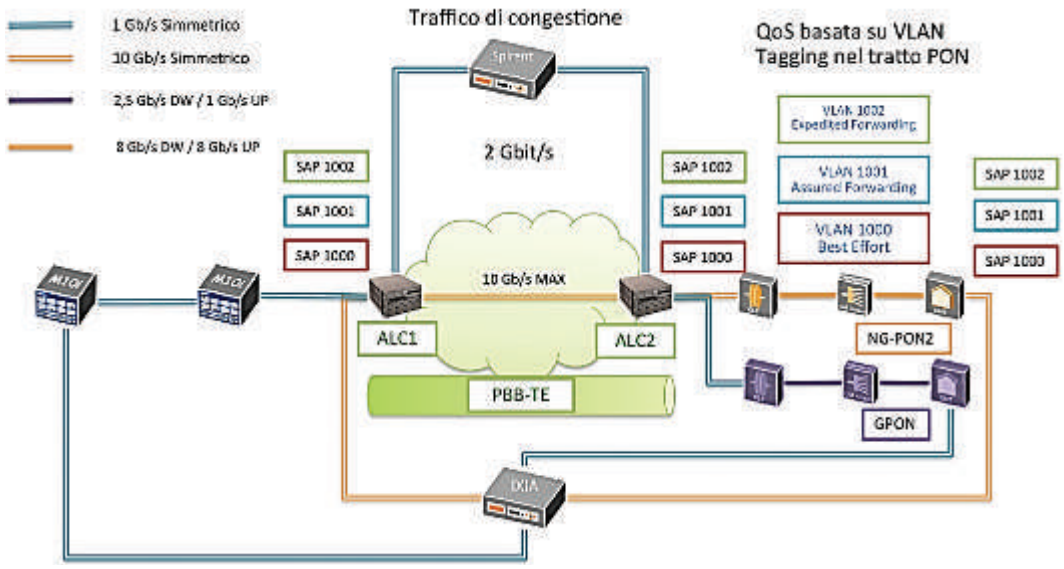


Figura 12 . Configurazione servizi per gestione qualità del servizio basata su VLAN tagging e PBB-TE

Ci siamo quindi messi nel caso peggiore di Uplink, con il traffico generato dall'interfaccia di IXIA collegata all'ONT verso quella collegata ad ALC1.

Il risultato ottenuto è quello mostrato in figura seguente.

Traffic Item	Tx Rate (Mbps)	Rx Rate (Mbps)	Loss %	Cut-Through Avg Latency (ns)
1 Gb/s BE UL - DL	1,973.688	1,824.420	12.658	61,101,091
2 Gb/s EF UL	1,973.688	1,973.664	0.000	140,969
2 Gb/s AF UL	1,973.688	1,970.610	0.179	791,274
4 Gb/s BE UL	3,947.364	2,596.788	31.683	143,038,658

Figura 13 . Statistiche di traffico generato in Uplink sull'architettura di rete in esame

In evidenza i tre traffici, due con gestione della qualità di tipo EF e AF da 2 Gb/s ed uno BE da 4 Gb/s. Le tre tipologie di traffico possono essere associate ai tre paradigmi del 5G:

- uRLLC – EF, nessuna perdita di pacchetti e latenza media di 0,140 ms;
- eMBB – AF, perdite minime e latenza media di 0,791 ms;
- mMTC – BE, perdite superiori al 10% e latenza di 143 ms.

Il quarto traffico in figura è solo di tipo BE per congestionare il percorso di rete.

4.6. Valutazioni finali

Dai Test effettuati in laboratorio è emerso sempre più l'affermarsi di tecnologie già esistenti impiegate in ambiti di sviluppo e innovazione come il 5G. La rete di accesso, nonché l'NG-PON2, hanno dimostrato di essere utilizzabili in uno scenario 5G, mostrando parametri di latenza soddisfacenti per coprire una vasta gamma di scenari di casi d'uso come

l'accesso broad-band in differenti modalità e come servizi di ultra-low latency. Simulando nel corso dei test l'effettivo carico della rete si è evidenziato, con le varie accortezze considerate, come i test mostrino esiti positivi e come la rete risponda correttamente nonostante l'effettivo "stress" sui parametri richiesti, avendo preventivamente configurato una QoS ad hoc.

5. Andamento dinamico della rete

Il tema delle SDN nei laboratori ISCOM è stato già affrontato in diverse sperimentazioni [16-22], e dopo una accurata analisi della letteratura scientifica e prendendo spunto da precedenti sperimentazioni nel LAB ISCOM sulle tecniche di gestione automatiche delle risorse, intese come connessioni GbE e percorsi logici di tipo VPLS-MPLS, ma soprattutto considerando gli apparati attualmente disponibili in LAB, si è deciso di utilizzare uno schema con un Orchestrator che comandava direttamente i router con messaggi SMNP. La principale innovazione per il nostro schema SDN è nella gestione della QoS, infatti l'orchestrator è comandato con messaggi provenienti dalla rete di monitoraggio mPlane, che la FUB realizzò nell'ambito del progetto EU FP7 mPlane; tale rete permette di conoscere lo stato degli accessi utilizzando sonde attive e il traffico mediante un monitoraggio passivo. Mediante l'analisi tra la correlazione dei dati delle sonde passive e attive è possibile vedere se un in punto della rete è presente una congestione o una riduzione del rapporto SNR. Le informazioni circa le criticità della rete sono passate da mPlane all'Orchestrator che provvederà ad esempio ad aumentare la capacità di un collegamento tra due router. Tutto questo processo è stato testato sperimentato in LAB e i dettagli di tutta questa metodologia sono riportati nel lavoro [18] presentato alla conferenza FOAN 2017 tenutasi nel 2017 a Monaco di Baviera.

Per aiutare il lettore possiamo riassumere che lo schema della rete di monitoraggio mPlane è costituita da un'infrastruttura distribuita per eseguire misure attive, passive e ibride a diversi livelli OSI. Un repository raccoglie, memorizza e analizza i dati raccolti tramite una elaborazione parallela e un reasoner che cerca in modo iterativo la causa di una degradazione nella rete, anche determinando le condizioni che portano ad alcuni problemi. In particolare lo strato di misura utilizza una serie di sonde programmabili (software e hardware) sia realizzate nel progetto stesso sia già disponibili ma adattate però all'architettura mPlane.

Uno degli obiettivi principali di mPlane è quello di assistere l'utente in tutte le sue esigenze relative all'accesso alla rete, in particolare per quanto riguarda i test di qualità del servizio (QoS) e per la verifica e la certificazione della SLA tra utente e ISP. Quindi, lo strato di misura di mPlane risulta fondamentale per le SDN in quanto fornisce un quadro di monitoraggio della rete distribuito e onnipresente per raccogliere misure eterogenee da un variegato numero di punti di misura diversi.

Per testare l'efficienza della nostra modalità SDN abbiamo deciso di prendere in considerazione la tematica delle *Next Generation Emergency Networks*, che oggi ha molto importanza, e su cui il Governo sta puntando molto, anche con un apposito decreto dell'aprile 2017 riguardante la protezione delle ***infrastrutture critiche*** materiali ***e*** immateriali. Quindi abbiamo voluto considerare lo studio della rete per *disaster recovery*. Per questo si sono messe a punto delle metodologie che simulano una situazione di disastro (terremoto, tempesta,...) che crea rottura di cavi e congestione nella rete, cercando di testare come il nostro approccio SDN può permettere il ripristino di una situazione di buona qualità delle trasmissioni con misure di throughput, latenza e tempi di ripristino tipici di quelli richiesti dalle reti 5G.

Quindi si considera l'ambiente riportato nella Figura 14 dove si suppone sostanzialmente di avere due reti distinte, una grigia che non è sotto il nostro controllo, e una gialla con il controllo delle prestazioni ottenute tramite il piano di misura mPlane. Improvvisamente un evento disastroso distrugge dei cavi di trasmissione (sia nella rete grigia che gialla), provocando una interruzione delle trasmissioni che è direttamente osservata nella rete gialla, ma anche un aumento del traffico che dalla rete grigia ora transita nella rete gialla, per l'indisponibilità di connessioni nella rete grigia.

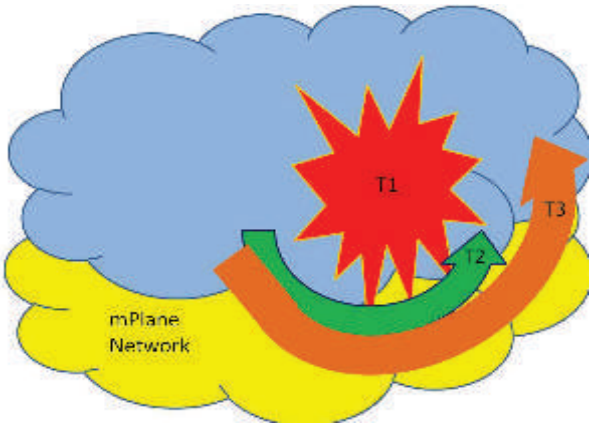


Figura 14 . Esempio di disaster recovery

L'ambiente sperimentale che abbiamo considerato è quello riportato nella figura sotto. Non descriviamo tutti i componenti che sono stati già illustrati in precedenti pubblicazioni [16-22]. Qui diciamo semplicemente che la restoration delle connessioni ottiche GbE è effettuata con la tecnica Standby Secondary Path technique (called VPLS SSP), dove noi implementiamo un link basato sullo Standby Secondary Path. Quando il collegamento primario si interrompe il router corrispondente instrada il traffico direttamente sul collegamento che era stato definito come secondario, senza calcolare nuove rotte. Nella Figura 15 il percorso primario riguarda i router J1-J2-J4, mentre il secondario J1-A1-A2-J4.

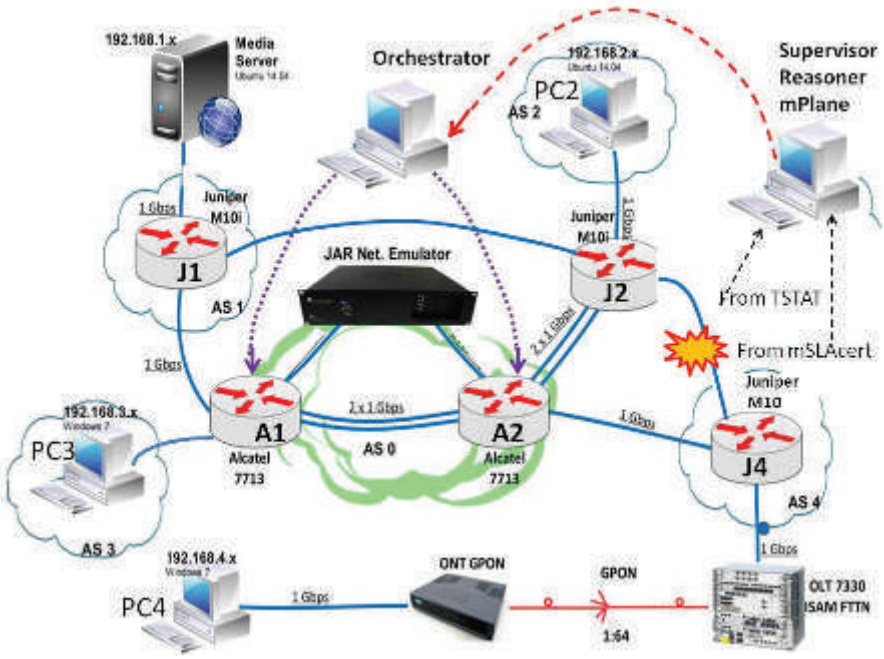


Figura 15 . Schema del laboratorio configurato per il Disaster Recovery con trestoration basata su VPLS Standby Secondary Path

Per quanto riguarda invece il controllo della congestione dovuta all'incremento del traffico (dalla rete grigia alla gialla) è stato adottato l'approccio SDN basato sulla procedura Dynamic Upper Fixed Lower (DUFL).

Vediamo come si comportano gli eventi illustrati nella figura. Prima di tutto a T1 il percorso primario si rompe tra J2 e J4. Tale danno è quasi istantaneamente ripristinato dall'approccio VPLS SSP che attiva il collegamento GbE tra A1 e A2; successivamente, in T2, il JAR induce due diversi livelli di congestione introducendo traffico spurio nel collegamento A1-A2 che quasi satura la capacità del collegamento considerando il traffico tra Media Server e PC4, che è sotto test, e che era stato fissato a 92 Mb / s.

Al tempo T3 il JAR introduce un traffico spurio di 1 GbE in A1-A2 che causa una forte congestione. L'effetto di tale congestione viene rilevato sia dalla destinazione dell'utente (PC4) sia dal mezzo di mSLAcert, e analizzando il traffico mediante TSTAT con la sua sonda passiva situata sull'uscita A2. La correlazione tra i dati di TSTAT e mSLAcert, eseguita nel supervisore-mplane, allarmerà l'orchestrator che gestirà A1 e A2 per attivare l'altro collegamento GbE tra A1 e A2.

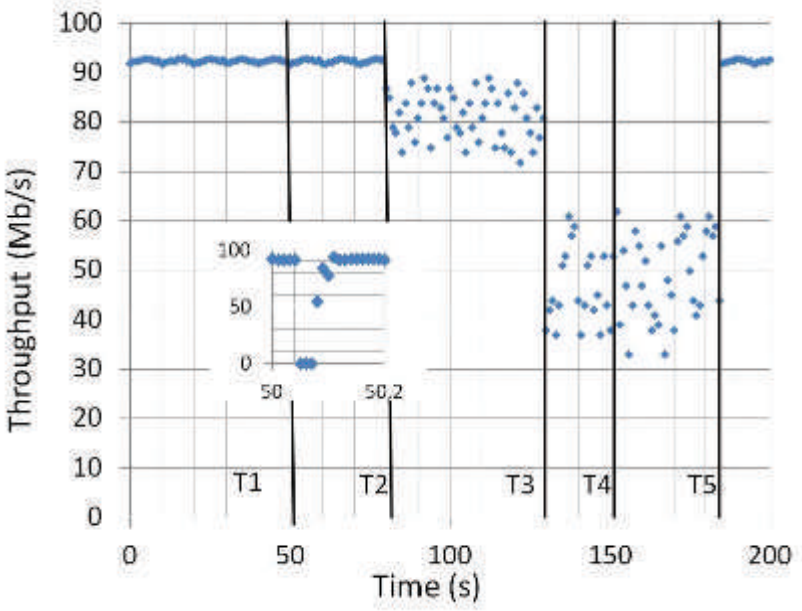


Figura 16 . Throughut vs time during the damages effects

Le conseguenze di tutti questi eventi sono chiaramente indicate in Figura 16 dove riportiamo il throughput misurato su PC4 tramite mSLAcert. In T1 il guasto del collegamento viene ripristinato immediatamente dalla procedura VPLS SSP in circa 40 ms. Nel riquadro della figura mostriamo i dettagli della procedura di restoration in una scala temporale più dettagliata. A T2 la prima congestione induce un piccola diminuzione del throughput, mentre a T3 l'effetto è rilevante. mPlane verifica sia il throughput del PC4 che il traffico che viaggia verso PC4, rilevando la presenza di anomalie nella trasmissione dei pacchetti che vengono analizzate secondo un approccio basato sulla correlazione di Pearson descritto in [17]. In particolare abbiamo preso in considerazione come parametri principali il Throughput medio (punti blu in Figura 16), il numero di segmenti ritrasmessi del flusso a causa di ritrasmissione veloce (Fast_retry) e quelli dovuti a timeout (Timeout_retry). Qui possiamo sintetizzare che il coefficiente di correlazione di Pearson esprime il grado di relazione tra due variabili, x e y, e varia da -1 a 1.

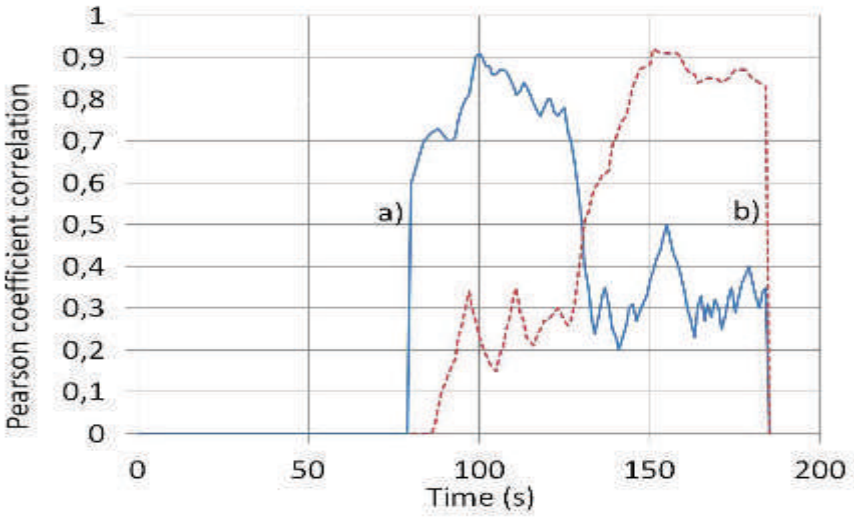


Figura 17 . Pearson correlation between Troughput and Fast_retry (a) and between Troughput and Timeout_retry (b)

Nella Figura 17 riportiamo le correlazioni di Pearson relativa ai valori tra Throughput e Fast_retry (a) e tra Throughput e Timeout_retry (b).

Come previsto, in assenza di congestione entrambe le correlazioni sono pari a zero. Finché abbiamo una leggera congestione, è presente solo la ritrasmissione rapida dei pacchetti, e questo è il motivo per cui, per un po ', la linea tratteggiata rimane zero mentre la linea continua cresce. Più aumenta la congestione, maggiore è il numero di segmenti prodotti dalla ritrasmissione rapida e dal timeout, e quando si verifica una pesante congestione i segmenti ritrasmessi a causa del timeout, saranno più numerosi di quelli provenienti dalla ritrasmissione veloce.

I valori di correlazione mostrano che, in caso di leggera congestione, abbiamo una prevalenza della correlazione tra throughput e ritrasmissione rapida e, viceversa, in caso di forte congestione abbiamo una correlazione più alta tra throughput e timeout del pacchetto.

La Figura 17 ci suggerisce di implementare algoritmi specifici che ci permettono di generare allarmi quando si presentano questi tipi di anomalie. Tali allarmi potrebbero essere importanti per la gestione della rete, e in particolare tali rilevamenti di anomalie potrebbero essere utilizzati per apportare modifiche adeguate alla configurazione di rete, in modo che parte del traffico possa essere instradata in alcuni collegamenti meno congestionati.

Nel nostro caso abbiamo definito una soglia pari a 0.8 riguardante solo la linea tratteggiata di Figura 17 per decidere quando il percorso tra A1 e A2 doveva raddoppiare la capacità, attivando un altro collegamento GbE.

I risultati mostrano quindi l'affidabilità del metodo proposto e sperimentato, che a nostro avviso potrà essere utilizzato anche in reti con terminazioni LTE.

6. Sperimentazioni e2e con WiFi.

Per studiare le prestazioni su rete wireless dal lato terminale è stata realizzata una apposita APP per Android sviluppata con IDE Android Studio 2.2.3. Tale App effettua un ciclo di test costituito dai seguenti KPI relativi alla qualità della rete ed alla qualità dei servizi (web browsing e video on-demand):

1. Ping delay tra end-point e server
2. Throughput in Download tra server e end-point
3. Throughput in Upload tra end-point e server
4. Web Page Download Speed: download di una pagina web di riferimento (ETSI Kepler)
5. First Frame Download Speed: velocità di download del primo frame di un video on-demand
6. Full Video Download Speed: campionamento valore del buffer ogni secondo per un servizio video-on demand.

Al fine di collaudare l'affidabilità dell'applicazione, sono stati svolti dei test di network performance su rete mobile pubblica 3G. Su tale rete è stata rilevata un'oscillazione del throughput in download pari a 2.5 - 6.1 Mbps in busy hour e un'oscillazione pari a 7.5 - 12.1 Mbps in off-peak hour.

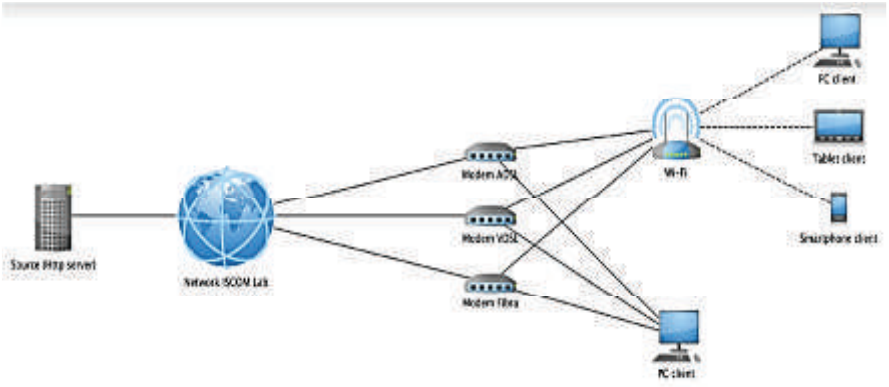


Figura 18 . Configurazione del LAB per misure su Wi-Fi con dispositivo Android

Al fine di effettuare dei test comparativi è stato configurato, quindi un test-bed opportuno riportato in Figura 18. Per il collegamento wi-fi del test-bed è stato utilizzato un protocollo di connessione Wi-Fi 802.11 e, con frequenza trasferimento dati a 2,4 GHz, e come end-point è stato utilizzato un dispositivo Samsung Galaxy S3, con sistema Operativo Android 4.3 Jelly Bean (API level 18).

Nelle figure che seguono riportiamo i KPI elencati precedentemente misurati sul dispositivo connesso alla rete Wi-Fi con access point connesso successivamente a modem appartenenti a diverse architetture di rete: ADSL (profilo download a 7 e 20 Mb/s), VDSL (profilo a 30 e 100 Mb/s) e fibra (100 Mb/s).

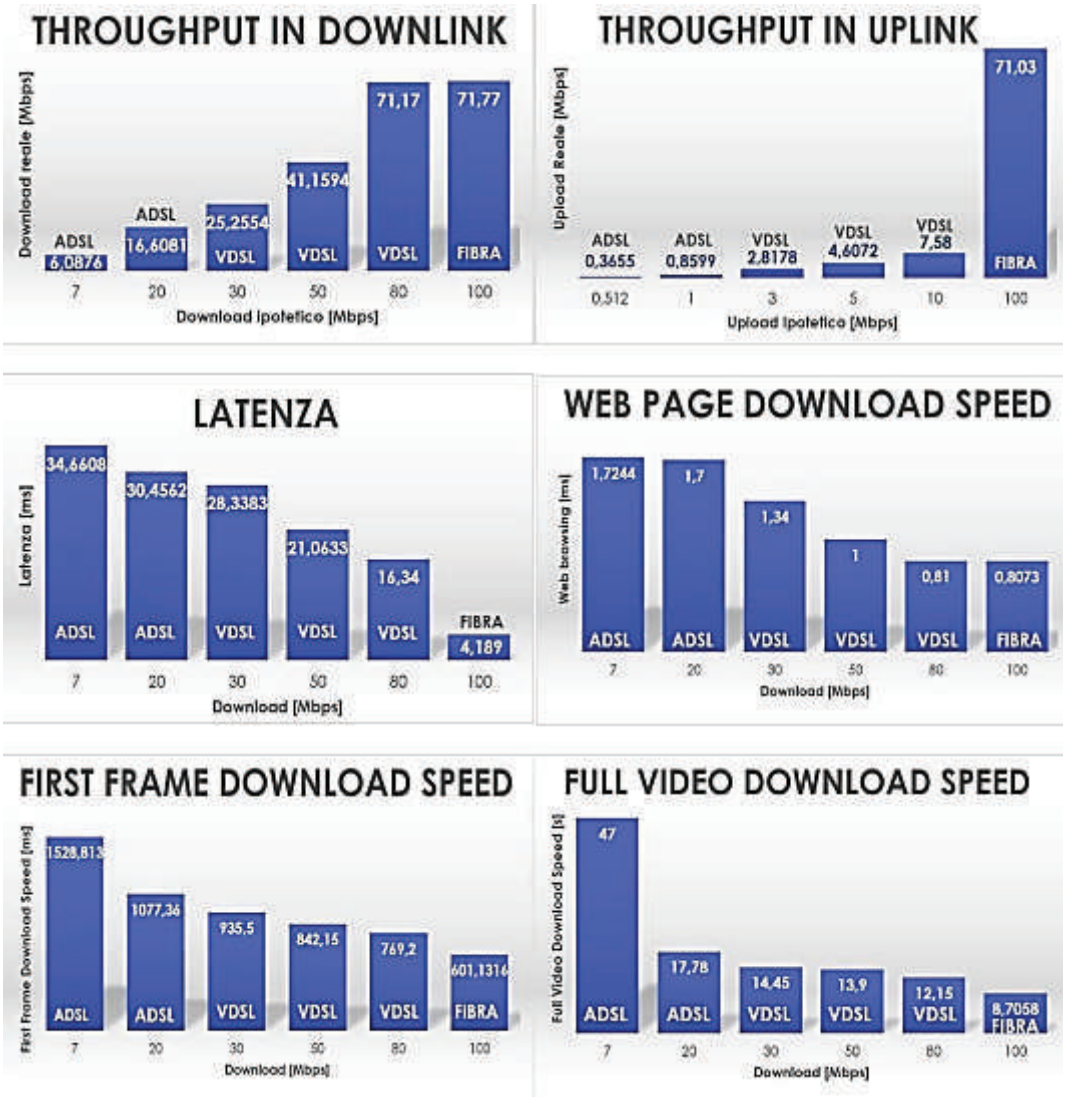


Figura 19 . Prestazioni del dispositivo Android in diverse architetture di connesione per la rete Wi-Fi

I risultati di Figura 19 mostrano la valità del prototipo software per la misura di KPI volti a caratterizzare le prestazione della rete e dei servizi come quelli presi in esame.

Inoltre questi risultati mostrano le potenzialità delle architetture delle reti di accesso anche ai fini della capillarità dei trasmettitori radio previsti nelle reti di prossima generazione (5G). Le architetture FTTC e FTTH presuppongono la presenza di fibra ottica almeno fino agli armadi stradali; la stessa fibra può essere efficentemente sfruttata per l'illuminazione delle BTS di nuova generazione (fetmocelle), la cui capillarità è compatibile con quella degli armadi stradali.

7. Conclusioni

In questo articolo abbiamo descritto l'ambiente che è stato realizzato dalla FUB e dall'ISCOM per gli studi sul 5G, con particolare rilevanza per gli aspetti che riguardano la rete XHaul, cioè la rete di trasporto (core-access) che connette le BS. In particolare è stata descritta la configurazione completa della rete ISCOM per uno scenario di tipo *Slicing* e cioè di una partizione logica della rete in tanti segmenti End-to-End (server-client), dove in ciascun segmento poteva esser definita una specifica classe di servizio (throughput, latenza, jitter). La sperimentazione ha riguardato tutti i principali dispositivi connessi alla rete e cioè i router Juniper e Alcatel e gli accessi GPON. Oltre ai test di QoS su PC connessi alle ONU GPON, sono stati considerati anche accessi di tipo Wi-Fi. Con questa configurazione, il laboratorio si presta come base per una rete completa di tipo 5G per la gestione di tante reti radio di tipo eterogeneo. Inoltre la suddivisione della rete in tanti segmenti logici è uno degli approcci fondamentali per la gestione di servizi multi-*verticals* con importanti sviluppi verso i programmi di Industria 4.0.

Nella stessa rete sono state anche sperimentate tecniche di tipo SDN basate, comunque, su una semplice comunicazione tra i router di tipo SNMP. Inoltre è stato proposto un nuovo modello di *Orchestrator* per reti SDN basato sull'utilizzo delle informazioni fornite dalla piattaforma mPlane e questa funzionalità è stata anche testata in laboratorio mostrando come la rete NGN si riconfiguri automaticamente durante le situazioni di congestione, aumentando il numero di connessioni tra i router per aumentare la capacità di trasporto.

Bibliografia

[1] Andrews, J., Buzzi, S. Choi, W., Hanly S. V., Lozano, A., Soon, A., Zhang, J. C., 2014 "What will 5G be?", IEEE Journal of Selected Area in Telecommunications, vol. 32, n.6, pp. 1065-82.

[2] Sun, S., Gong, L., Rong, B., Lu, K., "An Intelligent Framework for 5G Heterogeneous Networks" IEEE Comm. Magazine, Nov. 2015

[3] Settembre, M., "Towards a Hyperconnected world" Networks 2012, Rome, October 16-18, 2012.

[4] Fan, C., Zhang, C. F., Yuan, X., June 2016, "Advances and Challenges towards a Scalable Cloud Radio Access Network" IEEE Comm. Magazine, pp. 29-35.

[5] Zhou, Li, X., Chen, R., Zhang, H., May 2016" Network slicing as a Service: Enabling Enterprises' Own Software-Defined Cellular Networks" IEEE Communication Magazine, pp. 146-154.

[6] Mitchel, J. E., 2014 "Integrated Wireless Backhoul Over Optical Access Networks", J. of Lightwave Technology Vol. 32, n. 20, pp. 3373-3382.

[7] M. R. Sanna, S. Beker, W. Kiess, S. Thakolsri, "Service-based Slice Selection Function for 5G" GLOBECOM 2016, December 4-8, Washington DC. USA.

[8] "5G white paper" by NGMN Alliance, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf.

[9] T. Yoo,"Network slicing Architecture for 5G Networks" ICTC 2016, October 19-21, Jeju Island, Korea

[10] A.Nakao, P. Du, "Application-Specific Slicing for MVNO and Traffic Characterization" J. Opt. Comm. Networking, vol. 9, n. 2, 2017, pp.A256-A262.

[11] S. Pompei, L. Rea, Luca; F. Matera, A. Valenti, Experimental investigation on optical gigabit Ethernet network reliability for high-definition IPTV services Journal of Optical Networking, Vol. 7, n. 5, pp. 426-435, 2008

[12] A. Valenti, S. Pompei, L. Rea, F. Matera, G. Tosi-Beleffi, F. Curti, S. Di Bartolo, G. Incerti, and D. Forin "Experimental Investigation of Quality of Service in an IP All-Optical Network Adopting Wavelength Conversion" IEEE/OSA J. of Optical Communications and Networking, Vol. 1, Issue 2, pp. A170-A179, July 2009.

[13] A. Valenti, S. Pompei, N. Avallone, F. Matera, G. Tosi Beleffi, "Experimental implementation of efficient multicast processes: towards Carrier Ethernet networks and all-optical multicast IEEE ICTON 2011, Stoccolma June 26-30, 2011.

[14] Pulcini, L., Grazioso, P., Valenti, A., Matera, F., Del Buono, D., Attanasio, V., 2016 "Software Defined Networks over Carrier Ethernet for 5G: Tests from a GMPLS test bed" proceedings of Fotonica 2016, Rome June 6-8 2016

[15] De la Oliva, F. Cavaliere, P. Iovanna et al. "Xhaul: toward an integrated fronthaul/backhaul architecture in 5G networks". IEEE Wireless Communications, 22(5), pp. 32- 40, October 2015

[16] Tego, E., Matera, F., Del Buono, D., Attanasio, V., 2014 "Quality of Service Management based on Software Defined Networking Approach in wide GbE Networks" EuMed Telco 2014 Napoli, November 12-14 2014

[17] Tego, E., Rufini, A., Valenti, A., Matera, F., Mellia, M., Traverso, S.,"Software Defined Network approach driven by the mPlane Measurement Plane" AEIT International Conference, Capri (NA) October 5-7 2016

[18] E. Tego et al. "A Measurement Plane to Monitor and Manage QoS in Optical Access Networks" Proc. of FOAN 2017, Munich (GE) (2017).

[19] M. Giuntini, P. Grazioso, F. Matera, A. Valenti, V. Attanasio, S. Di Bartolo, and E. Nastri: "Enabling Optical Network Test Bed for 5G Tests", Fiber and Integrated Optics, published online Dec. 14th, 2016, Taylor & Francis, http://dx.doi.org/10.1080/01468030.2016.1262481

[20] Tego E., Idzikowski F., Chiaraviglio L., Coiro A., and Matera F., "Facing the reality: validation of energy saving mechanisms on a testbed", Journal of Electrical and Computer Engineering, Hindawi, 27 March 2014

[21] E. Tego, C. Carciofi, P. Grazioso, V. Petrini, S. Pompei, F. Matera, V. Attanasio, E. Nastri E. Restuccia "A Measurement Plane for Optical Networks to Manage Emergency Events" Fiber and Integrated Optics, On-line December 2017.

[22] S. Pompei, E. Mammi, D. Valeriani, F. Marini , E. Restuccia, E. Manca, V. Attanasio "GPON Architectures for 5 G services" Fotonica 2018, Lecce May 2018.

LA COMUNICAZIONE
Note Recensioni & Notizie
Pubblicazione dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Immagine di copertina:

Quadro di Claudio Lunghini
"Parlami…
Ancora…
Ti ascolto."

Claudio Lunghini ha lavorato presso
L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione