POLITECNICO DI MILANO

Facoltà di Ingegneria dell'Informazione

Corso di Laurea Magistrale in Ingegneria delle Telecomunicazioni

ANALISI DI METODOLOGIE BASATE SU INFORMAZIONI DI CONTESTO PER LA GESTIONE DI CHIAMATE DI EMERGENZA SU IMS

Relatore: Prof. Antonio CAPONE

Correlatore: Sara GRILLI

Tesi di Laurea di:

Valentina FRANCHI

matricola 708670

Anno Accademico 2009/2010

INDICE

Capitolo 1

Introduzione

Il problema della pubblica sicurezza è più che mai attuale, dato che tutt'oggi incidenti e catastrofi naturali sono all'ordine del giorno, presentando problemi di gestione non indifferenti.

All'interno di queste situazioni problematiche sono di fondamentale importanza le comunicazioni, che devono essere il più efficienti possibile per permettere la coordinazione delle operazioni di soccorso. Questo problema è ovviamente oggetto di interesse nel settore delle telecomunicazioni. In particolare, il Cefriel di Milano sta partecipando, in collaborazione al Politecnico di Torino, al progetto PICO, il cui scopo è la creazione di una piattaforma di controllo e distribuzione di servizi in uno scenario NGN[1](Next Generation Network) e ambisce a fornire servizi di

1Con la locuzione NGN si indica la futura evoluzione delle reti di telecomunicazioni verso una tipologia di rete che consenta il trasporto di tutte le informazioni ed i servizi (voce, dati, comunicazioni multimediali) incapsulando le stesse in pacchetti: nella maggior parte dei casi le reti di tipo NGN sono infatti basate su protocollo IP. La ITU-T (International Telecommunication Union - Telecommunication Standardization Bureau, ovvero il settore della Unione Internazionale delle Telecomunicazioni che si occupa di regolamentare le telecomunicazioni, fornendo delle specifiche standard riconosciute a livello internazionale) stessa la definisce come rete a commutazione di

telecomunicazione innovativi per utenti differenziati in situazioni d'emergenza, relativamente sia alla prevenzione che all'intervento in caso di necessità, sfruttando le potenzialità offerte dalle Internet Technologies (IT) [2].

All'interno del progetto PICO si colloca questo lavoro di tesi, il cui scopo è quello di individuare metodi di gestione delle chiamate d'emergenza che possano aumentare l'efficacia della comunicazione. Sfruttando nel modo adeguato le opportunità offerte dalle IT, è possibile instaurare canali di comunicazione che non si limitino alla comunicazione vocale, ma che possano coinvolgere l'uso di applicazioni ad-hoc volte ad arricchire il flusso di informazioni scambiate tra il chiamante (richiedente l'intervento di soccorso) al centro di smistamento delle chiamate, per raggiungere lo scopo di un'associazione client – server ottimale, che permetta di sfruttare appieno le potenzialità di entrambe le parti.

Più precisamente, si intende sfruttare la possibilità di trasportare più informazioni usando l'architettura di rete NGN di quanto sia possibile fare usando la tradizionale PSTN[2] (Public Switched Telephone Network) nello stesso intervallo di tempo.

Obiettivo di questo lavoro di tesi di ricerca è quindi la creazione di un algoritmo efficiente per la selezione del server più idoneo rispetto alle caratteristiche dell'utente che richiede il servizio.

Per svolgere il lavoro, si è partiti dalla considerazione di ciò che già esisteva. In particolare, sapendo dell'esistenza di gruppi di lavoro dedicati allo studio della gestione delle chiamate d'emergenza in NGN (in particolare ECRIT, facente parte di IETF) si sono studiati i protocolli già esistenti riguardanti il problema (in particolare LoST, di cui si parlerà nel capitolo 2, standardizzato appunto da ECRIT) e il sistema IMS, che si usa per l'implementazione del sistema ideato.

Per cominciare, si è analizzato con particolare attenzione l'aspetto di "contextawareness", poiché in base agli aspetti ritenuti caratterizzanti del contesto in cui si trova l'utente, per la scelta del server verrà elaborato l'algoritmo di selezione. In particolare, quali caratteristiche aggiuntive oltre all'informazione di localizzazione

pacchetto che fornisce servizi ed è in grado di far uso di tecnologie a banda larga multipla e di trasporto basato sulla QoS (Quality of Service, qualità del servizio percepito dall'utente), nella quale le funzionalità correlate alla fornitura dei servizi siano indipendenti dalle tecnologie di trasporto utilizzate. Offre un accesso non limitato agli utenti a diversi service provider, e supporta una mobilità generalizzata consentendo la fornitura consistente ed ubiqua di servizi agli utenti. [1]

2 La PSTN è la rete telefonica pubblica, la più grande rete per le telecomunicazioni esistente al mondo, che copre l'intero pianeta e alla quale chiunque può accedere.

possono risultare interessanti al fine di un instradamento più mirato delle chiamate d'emergenza.
Una volta stabiliti questi indicatori determinanti, sono state formulate alcune varianti di algoritmi decisionali, che verranno poi implementati su una piattaforma reale e funzionante. Si passerà infine alla fase di test per verificare la funzionalità dei metodi proposti. Sarà importante anche stabilire quali aspetti sono da tenere in considerazione per realizzare una valutazione realistica ed accurata delle prestazioni del sistema, che permetta di decidere quale metodo usare per soddisfare le proprie esigenze.
Nel Capitolo 2 verrà esposto lo stato dell'arte, spiegando più dettagliatamente il progetto PICO, ed illustrando gli organi esistenti, e i relativi protocolli prodotti, che stanno lavorando al problema della gestione delle chiamate d'emergenze nelle NGN.
Il progetto PICO prevede di lavorare in ambiente IMS (IP Multimedia Subsystem), un’architettura di rete per la convergenza di tutti i dispositivi di telecomunicazione (fissi e mobili) in un’unica rete IP, per offrire servizi voce e multimediali. Nel Capitolo 3 viene affrontata l'analisi del sistema IMS, compresa la sua implementazione OpenIMSCore, usata per creare l'apparato di simulazione che servirà a costruire la piattaforma di test di simulazione del progetto di tesi.
Nel Capitolo 4 Si passerà all'esposizione degli algoritmi formulati per risolvere il problema, mentre il Capitolo 5 tratta l'implementazione del sistema e l'analisi dei risultati ottenuti dalle simulazioni.
Nel Capitolo 6 vengono tratte le conclusioni, con alcune considerazioni sugli sviluppi futuri.

Capitolo 2

Stato dell'arte:
PICO, ECRIT e LoST

In questo capitolo introduttivo si analizzerà lo stato dell'arte, presentando il progetto PICO, all'interno del quale si inserisce il lavoro di tesi, e ciò che già esisteva in relazione all'argomento di chiamate d'emergenza in ambiente IP, i lavori di ricerca e i protocolli prodotti.

2.1 Introduzione al problema della pubblica sicurezza

La pubblica sicurezza è sempre stata un punto cruciale per ogni nazione. Attualmente, lo sviluppo delle tecnologie di comunicazione permette di rendere l'intero apparato dedicato a questo scopo più efficiente sfruttando le potenzialità dei sistemi di ultima generazione.

Il progetto PICO[3], nato dalla collaborazione di CEFRIEL e Politecnico di Torino, ha come obiettivoil raggiungimento di questa maggior efficienza sfruttando le IT (Internet Technologies). PICO ambisce a creare una piattaforma di controllo e distribuzione di servizi in uno scenario NGN[4](Next Generation Network) e ambisce a fornire servizi di telecomunicazione innovativi per utenti differenziati in situazioni d'emergenza, relativamente sia alla prevenzione che all'intervento in caso di necessità [2].

In questo lavoro, l'attenzione volge in particolare alla gestione delle chiamate d'emergenza usando comunicazioni SIP[5] (Session InitiationProtocol, [3]) in diversi scenari, quali emergenza medica, incidente stradale, incendio, o simili. Lo scopo del lavoro è quello di realizzare un sistema di comunicazione che, traendo vantaggio dalle possibilità offerte dalle IT, riesca a facilitare le operazioni di soccorso.

Più precisamente, si intende sfruttare la possibilità di trasportare più informazioni usando l'architettura di rete NGN di quanto sia possibile fare usando la tradizionale PSTN[6](Public Switched Telephone Network, [4]) nello stesso intervallo di tempo.

L'utilizzo del protocollo SIP in situazioni di emergenza è una tematica che viene

3 Il sito ufficiale del progetto, all'interno del quale si possono trovare l'elenco dei documenti stilati e i contatti dei responsabili all'interno di CEFRIEL e Politecnico di Torino, è http://softeng.polito.it/pico/index.html.

4 Con la locuzione NGN si indica la futura evoluzione delle reti di telecomunicazioni verso una tipologia di rete che consenta il trasporto di tutte le informazioni ed i servizi (voce, dati, comunicazioni multimediali) incapsulando le stesse in pacchetti: nella maggior parte dei casi le reti di tipo NGN sono infatti basate su protocollo IP. La ITU-T (International Telecommunication Union - Telecommunication Standardization Bureau, ovvero il settore della Unione Internazionale delle Telecomunicazioni che si occupa di regolamentare le telecomunicazioni, fornendo delle specifiche standard riconosciute a livello internazionale) stessa la definisce come rete a commutazione di pacchetto che fornisce servizi ed è in grado di far uso di tecnologie a banda larga multipla e di trasporto basato sulla QoS (Quality of Service, qualità del servizio percepito dall'utente), nella quale le funzionalità correlate alla fornitura dei servizi siano indipendenti dalle tecnologie di trasporto utilizzate. Offre un accesso non limitato agli utenti a diversi service provider, e supporta una mobilità generalizzata consentendo la fornitura consistente ed ubiqua di servizi agli utenti.

5 SIP è un protocollo basato su IP, definito dalla RFC 3261, impiegato principalmente per applicazioni di telefonia su IP, ovvero VoIP (Voice over IP).

6 La PSTN è la rete telefonica pubblica, la più grande rete per le telecomunicazioni esistente al mondo, che copre l'intero pianeta e alla quale chiunque può accedere.

analizzata anche da un gruppo di lavoro di IETF [7](Internet Engineering Task Force, [5]), ECRIT[8] (Emergency Context Resolution with Internet Technologies [6]), adibito allo studio delle chiamate d'emergenza in ambiente VoIP, che ha prodotto LoST, il protocollo descritto nel RFC 5222 [7],e che ha lo scopo di fornire una descrizione dei casi in cui è adeguato usare IT e come sfruttarle per gestire il routing delle chiamate d'emergenza.

LoST è l'acronimo di Location-to-Service Translation Protocol, un protocollo basato su XML che ha la funzione di effettuare il mapping tra identificativi di servizio e informazioni di localizzazione geografica o tramite indirizzo civico su contatti URI di servizio. In particolare, lo si usa per determinare la centrale telefonica adeguata da associare all'utente che effettua la chiamata d'emergenza.

2.2 Il progetto PICO

L'idea progettuale alla base di tutto il sistema PICO è la realizzazione di sistemi di telecomunicazione innovativi a larga banda per utenze differenziate in materia di sicurezza, prevenzione e intervento in caso di catastrofi naturali.

L'obiettivo del progetto è lo studio e sperimentazione della distribuzione di servizi innovativi in un ambiente IMS[9](IP Multimedia Subsystem, [8]), all'interno del quale la struttura della piattaforma architetturale IMS deve essere adattata ed estesa per adeguarsi al contesto di lavoro. Gli obiettivi specifici consistono nell'implementazione di prototipi e nell'analisi delle prestazioni dei servizi offerti

7 La IETF è una comunità aperta di tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Ciò che la differenzia dagli enti di standardizzarne più tradizionali è la sua struttura aperta: il lavoro viene svolto da gruppi di lavoro (workinggroups, come appunto ECRIT) che operano soprattutto tramite Mailing list (sistema organizzato per la partecipazione di più persone in una discussione asincrona tramite email), aperte alla partecipazione di chiunque sia interessato [5].

8 Tutta la documentazione e i contatti di questo gruppo di lavoro sono reperibili all'indirizzo internet http://www.ietf.org/dyn/wg/charter/ecrit-charter.html.

9 IMS è un'architettura di rete per la convergenza di tutti i dispositivi telecomunicazione (fissi e mobili) in un'unica rete IP, per offrire servizi e voce multimediali. Di IMS parleremo approfonditamente all'interno del cap. 2 [8].

dal sistema IMS in termini di streaming applicativo con proprietà di "context-awareness"[10] che, più in generale, si traducono nella disponibilità di applicazioni fruibili da remoto tramite infrastrutture virtuali in termini di protocolli, requisiti necessari, caratteristiche di compatibilità. Si dovrebbe quindi giungere all'allestimento di raccomandazioni e linee guida per la previsione delle prestazioni sulla piattaforma di distribuzione del servizio.

Lo svolgimento del lavoro è organizzato in fasi successive. La prima di queste prevede la studio degli scenari applicativi del progetto, con particolare attenzione ai dettagli tecnici che andranno ad influenzare le scelte progettuali all'interno dell'architettura di rete. E' da ricordare, infatti, che un aspetto fondamentale del progetto è proprio il "context-awareness". Questo aspetto verrà largamente sfruttato nello step successivo, che studia le problematiche relative alla fornitura di servizi che si adattino in modo continuo e trasparente al contesto dell'utente, definito in termini di locazione, dispositivo in uso, ed altre variabili da stabilire in sede progettuale. Il passo successivo sarà la realizzazione di un prototipo del sistema, per poi effettuare test che permettano di valutare le prestazioni della piattaforma realizzata.

In Fig.2.1 si ha un esempio schematico delle principali parti in gioco nel sistema di gestione delle situazioni d'emergenza.

10 Con la locuzione "context-awareness" si indica una modalità di computing che tenga conto dei cambiamenti dell'ambiente all'interno del quale si trova il sistema, che altrimenti è statico.

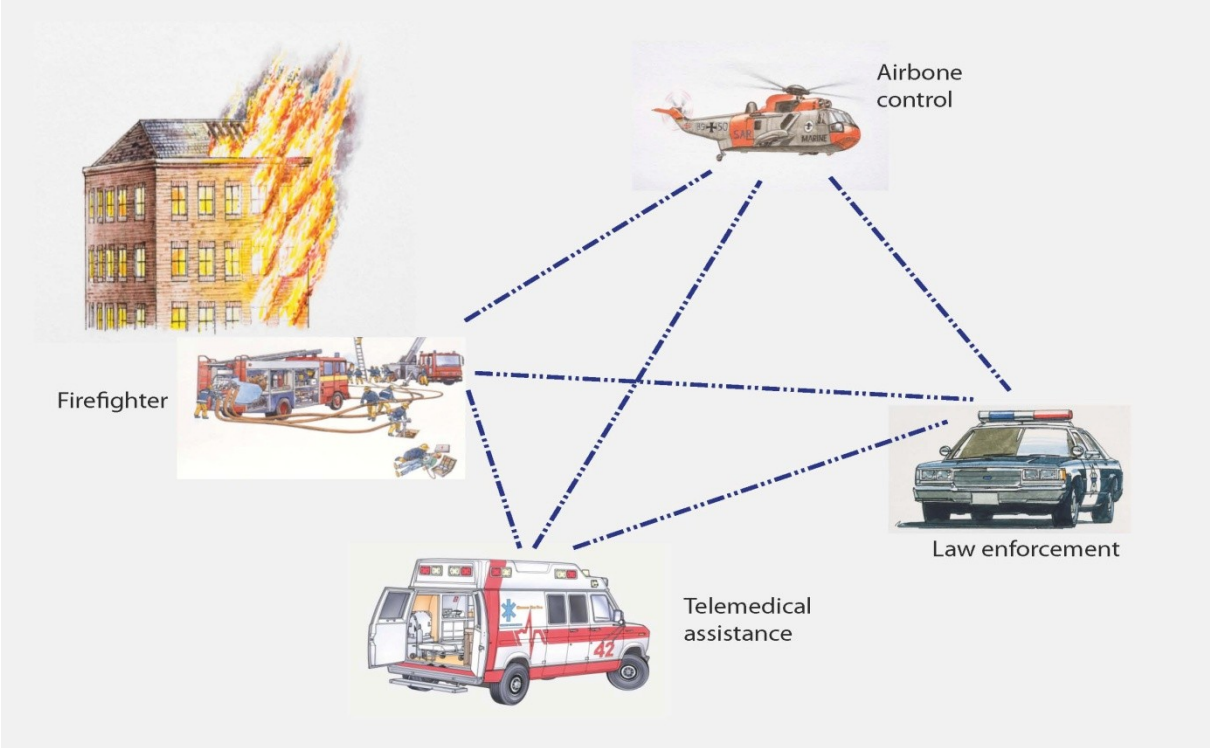


Fig.2.1: Panoramica delle entità in gioco

2.2.1 Scenari applicativi

Come si è accennato in precedenza, la prima fase del progetto consisteva nello studio degli scenari applicativi, ovvero nella stesura di descrizioni di situazioni reali all'interno delle quali sarebbe stato necessario effettuare interventi d'emergenza. Dalla descrizione minuziosa delle operazioni di soccorso da compiere per agire nel modo più efficiente possibile vengono estratti i dettagli che serviranno a stabilire le caratteristiche tecniche che il sistema di comunicazione dovrà possedere per costituire effettivamente un apparato che migliori la funzionalità dell'intervento.
Nello specifico, all'interno del progetto PICO sono state considerate tre entità adibite alla gestione della pubblica sicurezza: vigili del fuoco (internazionalmente conosciuti come Fire Fighter, e quindi denominati FF nella documentazione del progetto), forze di polizia (Law Enforcement, LE) e operatori di servizi di emergenza medica (Emergency Medical Services, EMS).
E' necessario tenere presente alcuni aspetti fondamentali per il funzionamento

efficiente della piattaforma di comunicazione: velocità di connessione, interoperabilità, funzionalità, sicurezza delle operazioni, fornendo larga banda per permettere il trasferimento di contenuti multimediali.

Prima di spiegare con maggiori dettagli gli scenari applicativi considerati, è necessario accennare alle caratteristiche che i dispositivi in uso dovrebbero possedere, per poter fare una stima realistica delle applicazioni implementabili.

I dispositivi devono avere diverse interfacce per adattarsi all'utente che li sta impiegando e per interagire con i sistemi di comunicazione già esistenti, e devono essere resistenti alle condizioni ambientali, spesso ostiche, all'interno delle quali verranno usati. Oltre all'uso di questi particolari apparati, si può ipotizzare la presenza sul luogo dell'emergenza di diversi sensori, il cui compito potrebbe essere il rilevamento delle condizioni atmosferiche, il monitoraggio di zone a rischio,la misurazione dei parametri vitali dei soccorritori, e così via. Tutti i dispositivi in uso, comunque, devono essere in grado di interfacciarsi con la piattaforma NGN che si intende implementare.

Per rendere realistici gli scenari si sono immaginate delle situazioni concrete, tenendo in considerazione in particolare le necessità e le capacità degli operatori di soccorso. Verranno descritti il caso di emergenza medica, incendio domestico, stop del traffico, e, per simulare un caso di interoperabilità tra tutte le forze di pubblica sicurezza, esplosione.

Prima di avere una panoramica delle diverse situazioni esemplificative, è necessario puntualizzare che ogni utente in possesso di PSCD (Public Safety Communication Device), ovvero il dispositivo che permette di comunicare con la centrale di soccorso, deve effettuare una determinata procedura di autenticazione all'accensione dell'apparato. Per motividi sicurezza, infatti, sarà necessario autenticarsi, fornendo il proprio profilo alla centrale operativa. Inoltre, è doveroso accennare al fatto che si suppone un'organizzazione gerarchica delle reti.

In Fig. 2.2 si ha una rappresentazione schematica dell'organizzazione gerarchica delle reti usate, che sono:

- PAN (Personal Area Network): è la rete formata dal dispositivo dell'operatore (anche più di uno, se presenti, dipende dal tipo di operatore) e dall'apparecchiatura a bordo del proprio mezzo di soccorso.
- IAN (Incident Area Network): è la rete formata sul luogo dell'incidente (con "incidente" si intende la situazione critica generica alla quale si sta prestando

soccorso) dai diversi operatori.

- JAN (Jurisdictional Area Network): è la rete che racchiude tutte le entità di soccorso all'interno di una certa giurisdizione.

- EAN (Extended Area Network): è la rete generica che comprende tutte le entità di soccorso, indipendentemente dalla giurisdizione di appartenenza.

Ovviamente, JAN ed EAN sono reti permanenti, mentre IAN viene creata all'occorrenza sul luogo del disastro. Un esempio di IAN è quello della rete formata dalla centralina a bordo dell'ambulanza collegata ai PSCDs dei paramedici di turno.

E' importante considerare il tipo di dispositivo in uso, infatti a seconda delle sue caratteristiche sarà possibile effettuare o meno certi tipi di comunicazioni e collegamenti. Questo aspetto verrà richiamato e chiarito più in seguito, quando si andrà a spiegare quali migliorie tecniche si apporteranno al sistema per renderlo più efficiente e funzionale.

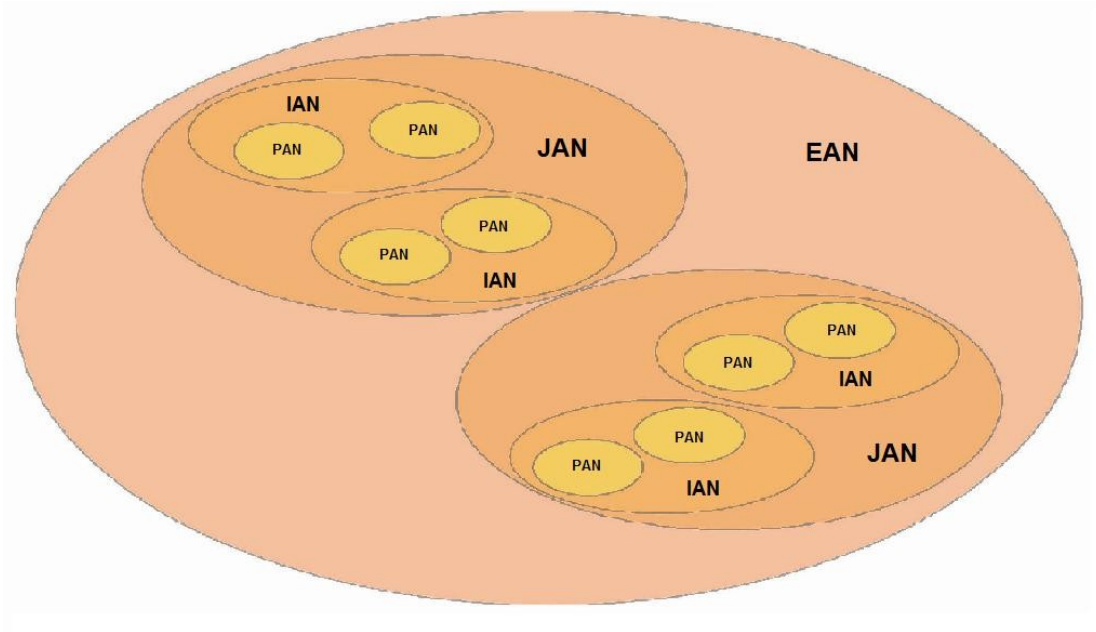


Fig.2.2: Organizzazione gerarchica delle reti

In questa sede non si riporteranno dettagliatamente tutte le descrizioni di scenari che sono contenute nei deliverables[11] del progetto, ma si limiterà la descrizione ad un quadro generale delle situazioni, con le relative operazioni da compiere, focalizzandosi sugli aspetti che risulteranno interessanti per il lavoro di tesi.

Scenario Emergenza Medica

Si suppone che con l'inizio del turno i paramedici effettuino tutte le procedure di identificazione necessarie. L'aspetto di identificazione dell'utente è importante in quanto in seguito vedremo come il suo ruolo possa essere determinante nella valutazione di certi parametri significativi all'interno dell'algoritmo di scelta del servizio. Inoltre, grazie all'identificazione dell'utente la centrale di servizio può recuperare il profilo associato, stabilendo il grado di accesso a dati ed iniziando il tracking di ciascuno, per avere un registro di tutte le operazioni compiute dai paramedici, delle istruzione a loro fornite dalla centrale operativa, ecc. Tutte queste informazioni possono risultare utili in un'eventuale successiva analisi dello svolgersi dei fatti.

Per quanto riguarda l'esempio di scenario applicativo di emergenza medica, all'interno del progetto PICO si è scelto di simulare un attacco di cuore.

Si ipotizza una chiamata al numero d'emergenza effettuata dal parente di un uomo che, tornato da una partita di tennis, accusa dolore al petto. La centrale operativa visualizza le ambulanze in zona, e confrontando i tempi previsti di percorrenza di ognuna per raggiungere il paziente sceglie quale contattare ed inviare. Si suppone che l'ambulanza abbia a bordo un sistema di navigazione. Per accelerare ulteriormente il viaggio, si potrebbe ipotizzare che l'andamento dei semafori lungo il percorso possa essere modificato in tempo reale per facilitare la guida.

Una volta arrivati sul posto, i paramedici cominciano le operazioni. Mentre uno inizia a controllare lo stato del paziente, l'altro raccoglie informazioni dalle altre persone, seguendo lo schema apposito. Queste informazioni raccolte verranno inviate alla centrale di soccorso e potranno essere sfruttate come componenti decisionali all'interno dell'algoritmo di scelta del server ospedaliero a cui connettere i paramedici.

Il paziente potrebbe anche indossare un braccialetto RF ID (Radio Frequency Identification Data), utile poiché con un veloce scan i paramedici verrebbero a

11 I deliverables sono consultabili sul sito http://softeng.polito.it/pico/deliverables.html [2].

conoscenza di eventuali allergie a medicinali del paziente. I paramedici iniziano poi il trasferimento dell'uomo verso l'ospedale scelto, avendogli prima attaccato il dispositivo per EKG (Elettrocardiogramma) wireless, in grado anche di inviare i risultati direttamente all'ospedale verso cui il paziente viene trasportato. In questo modo, il cardiologo dell'ospedale può capire di quali cure ha bisogno l'uomo e a predisporre il personale in modo adeguato. Durante il trasporto si misurano ed inviano all'ospedale anche altri parametri vitali, come la pressione sanguigna e la saturazione.

Si nota che attraverso tutta la ricostruzione, sia i paramedici che l'unità mobile di soccorso vengono seguite dalla rete, che conosce in tempo reale la localizzazione geografica di ognuno. Tutti i parametri vitali rilevati dal paziente vengono registrati, come avviene con le conversazioni tra paramedici e ospedale, che dovrebbero avvenire in modalità conference. Tutti i dispositivi dovrebbero essere wireless, per facilitare le operazioni di soccorso. Le caratteristiche che deve possedere il dispositivo in uso sono importanti poiché la caratterizzazione di quest'ultimo sarà parametro d'interesse nella selezione del server adeguato.

Scenario Emergenza Vigili del Fuoco

Come per i paramedici, e per gli stessi motivi, i vigili del fuoco devono eseguire la procedura di identificazione appena iniziano il turno. Per loro, però, sarebbe opportuno che la divisa in dotazione fosse integrata da alcuni sensori che possano rilevare le condizioni ambientali in cui l'operatore si trova e i parametri vitali dello stesso. Questo accorgimento potrebbe essere molto utile nel caso in cui il vigile sia impegnato in operazioni di soccorso in ambienti contaminati o pervasi da fumi tossici. In questo caso inoltre è ancora più importante potersi avvalere di una precisa localizzazione geografica dell'operatore, in caso di perdita di sensi durante un intervento. La rete di sensori della divisa, unita al PSCD, forma la PAN (Personal Area Network) del vigile, e le informazioni da essa rilevate vengono registrate, unitamente al codice identificativo della persona, all'interno del database della centrale operativa. Una volta che tutte le operazioni di identificazione e test dei dispositivi in uso sono ultimate, l'unità si considera disponibile per interventi.
Per simulare realisticamente un intervento, all'interno delle specifiche del progetto PICO si è ipotizzato un caso di incendio domestico.

Si suppone che alla centrale operativa giunga una chiamata d'emergenza da un civile che ha notato del fumo sospetto uscire da una finestra di un appartamento, tanto da far pensare ad un incendio.
Con lo stesso procedimento usato nel caso dell'ambulanza, la centrale invia sul posto l'unità di soccorso che impiega meno tempo ad arrivare. A seconda della descrizione della situazione che viene fornita dalla persona che fa la segnalazione, il centro direzionale può decidere di mandare più di una unità di soccorso.
Appena possibile, vengono fornite all'unità le piante dell'edificio, specialmente l'ubicazione di scale ed ascensori, e la localizzazione degli idranti nella zona.
Nel frattempo, la centrale invia chiamate di allerta a tutti gli occupanti l'edificio, con l'ordine di evacuare immediatamente la zona, e il centro di emergenza medico più adatto, ordinando di mandare un'unità di soccorso sul luogo e di prepararsi ad accogliere eventuali vittime.
Durante il percorso, il veicolo dovrebbe essere in grado di controllare i semafori allo stesso modo dell'ambulanza, e dovrebbe avere un sistema di navigazione che fornisca informazioni su eventuali strade chiuse o interrotte.
Una volta arrivati sul luogo, i pompieri confermano che è un incendio, e lo comunicano all'istante alla centrale. Questa dispone l'immediata sospensione dell'erogazione di gas nella zona, per evitare dannose conseguenze.
La centrale può visualizzare continuamente la posizione di ogni componente dell'unità di soccorso, mentre gli operatori sono in comunicazione continua tra loro, e si preparano ad intervenire seguendo le istruzioni del coordinatore.
Mentre alcuni parlano con le persone che hanno già lasciato l'edificio, registrandone i dati, altri cominciano ad entrare, per aiutare le persone che ancora sono dentro ad uscire. Possibilmente, il PSCD dovrebbe filmare continuamente ciò che ogni vigile vede e fa (ad esempio piazzando la videocamera sull'elmo della persona). I sensori delle divise rilevano continuamente temperatura, stato dell'aria e parametri vitali dei vigili. Questi ultimi vengono controllati continuamente dal personale dell'EMS intervenuta sul posto; non appena vengano riscontrate delle anomalie o dei segni di stress, la persona interessata viene richiamata fuori dall'edificio.
Anche la localizzazione precisa e continua dei vigili è molto importante: se uno di loro dovesse perdere il senso dell'orientamento (a causa del fumo, ad esempio), potrebbe chiedere aiuto e la centrale ordinerebbe ad un compagno di andarlo a recuperare, fornendo indicazioni precise su come trovarlo.

I vigili portano a termine la perlustrazione e scoprono dov'è l'incendio, estraggono gli eventuali intossicati, portandoli sulla EMS per curarli, e si occupano di spegnere le fiamme.
Il centro direzionale si occupa anche di verificare che siano state controllate tutte le stanze dell'edificio, confrontando i luoghi visitati dai vigili con la planimetria dell'edificio e le informazioni fornite dai condomini.
Una volta estinto il fuoco e controllato tutte le persone coinvolte, tutto l'equipaggio di soccorso può tornare alle rispettive basi.

Gli aspetti caratteristici di questo scenario sono, la necessità di accedere ad altri centri di soccorso o servizio (chiamata dell'ambulanza, sospensione dell'erogazione del gas, acquisizione delle planimetrie) e il controllo continuo della situazione sul posto, sia per quanto riguarda la posizione del personale, sia tramite i sensori, sia per mezzo di videocamere e microfoni. Questo controllo serve sia a prevenire incidenti che a tenere traccia di come sono state svolte le operazioni di soccorso.

Scenario Emergenza Stradale

Il personale coinvolto stavolta è l'ufficiale di polizia. Dopo aver completato il check in amministrativo, l'ufficiale porta il suo equipaggiamento sull'auto che gli è stata assegnata per il turno. Nel veicolo, inizia la procedura di identificazione biometrica con il proprio PSCD. Dopo l'autenticazione, il sistema imposta il profilo dell'agente sul PSCD e nella rete, stabilendo il livello di accesso ai dati a cui ha diritto e iniziando il tracking delle sue attività. L'ufficiale inizia il test dei dispositivi che userà all'interno del veicolo: terminali di dati, monitors, videocamere, displays, ecc.., il tutto integrato in una PAN. Tutte le attrezzature codificano le proprie informazioni attraverso l'ID dell'agente e inviano la propria registrazione e il proprio stato alla rete.
Quando l'ufficiale aziona il veicolo, il centro di raccolta wireless riconosce la sua PAN e carica i file dei database pertinenti, le ultime chiamate alle forze dell'ordine e l'attuale percorso, con relative condizioni atmosferiche, verso la stessa PAN. Dopo aver completato i self-test e ricevuto gli aggiornamenti, l'agente comunica il suo stato di attività al centro di rete. La rete della Polizia riporta l'informazione al centro direzionale, corredata di posizione dell'agente, identificazione dello stesso e delsuo

equipaggiamento.

L'emergenza immaginata in questo caso riguarda uno stop del traffico ad alto rischio. Si suppone che, mentre sta pattugliando il traffico, l'ufficiale veda un'auto che attraversa un incrocio nonostante la luce rossa del semaforo. Quindi preme il pulsante "*Veichle Stop*" sul proprio PSCD, il quale manda un messaggio alla centrale operativa, notificando l'inizio dell'operazione, l'ID dell'agente e la posizione della sua auto. Mentre l'agente guida verso il trasgressore, la targa del veicolo inseguito viene annotata e mandata al database della motorizzazione per effettuare le verifiche del caso. Nel frattempo, la videocamera a bordo del veicolo dell'agente ha cominciato a registrare tutto in una RAM apposita. Questo video, essendo in un dispositivo che fa parte della rete dell'auto, sarà accessibile dal centro operativo e da tutti gli autorizzati in qualsiasi momento, su richiesta. Intanto, altre pattuglie nelle vicinanze vengono informate di ciò che sta accadendo.

In breve tempo, la motorizzazione trova informazioni sul veicolo e le invia al PSCD dell'ufficiale, che entra così in possesso di dati e fotografia del possessore del veicolo; queste, fornite sia in forma audio che video dal PSCD, fanno sapere che l'auto non è segnalata.

Il veicolo accosta e si ferma. Quando l'ufficiale scende dalla propria auto, ha comunque accesso continuo ai dispositivi della PAN, che continuano a comunicare con il resto della rete.

Ipotizziamo che mentre il conducente comincia a fornire spiegazioni, l'ufficiale noti qualcosa di sospetto e per questo motivo decida di effettuare un'ispezione dell'auto. Per farlo chiama rinforzi, e il centro operativo, tramite l'‘informazione di localizzazione, visualizza i veicoli in zona usando un sistema che indichi il più vicino tenendo conto anche delle condizioni del traffico, delle interruzioni, ecc. Una volta identificata l'unità di rinforzo migliore, questa viene informata del da farsi e forma una rete con l'unità già attiva. Per sicurezza, anche le altre pattuglie nei paraggi vengono informate di ciò che sta accadendo.

Il supervisore acquisisce il video in real-time e lo guarda dalla sua postazione, controllando che non ci siano dettagli sospetti.

Nel caso in cui i sospetti dell'ufficiale siano fondati e il guidatore stia effettivamente compiendo qualche crimine, questi verrebbe messo in arresto e gli verrebbero fatte indossare delle manette con RF ID tag, da caricare poi con l'ID dell'agente, la natura del crimine e il codice del caso. L'ufficiale responsabile richiederebbe anche un

veicolo per il trasporto dell'uomo in arresto al centro operativo.
Dopo l'arresto, l'agente può prelevare un campione biometrico del guidatore attraverso il suo PSCD, che invia i dati al database per effettuare l'identificazione. In questo modo, sul PSCD si ottiene un'immagine corredata da nome, data di nascita e caratteristiche fisiche dell'individuo i cui tratti coincidono con quelli rilevati dall'agente, permettendo di verificare che i dati anagrafici presenti nel database rispecchiano quelli sulla patente.
Se quindi il guidatore viene arrestato, viene chiamato un carro attrezzi per portare via il veicolo, che da quel momento è sotto sequestro. Questa informazione viene immediatamente comunicata alla motorizzazione, che così può aggiornare il database in modo corretto.

Ciò che si nota, in particolare, all'interno di questo scenario, è che durante tutta la simulazione, il personale delle forze dell'ordine, il relativo equipaggiamento e il soggetto arrestato vengono seguiti dal sistema di localizzazione in tempo reale, per fornire alla centrale operativa gli aggiornamenti necessari. Inoltre, tutte le informazioni e le prove raccolte (attraverso monitor e sistemi di riconoscimento vocale) vengono memorizzate, corredate dell'ID dell'agente, senza necessità di supporto cartaceo.
Infine, tutti i database dei vari corpi delle forze dell'ordine possono essere consultati in ogni momento.

Scenario Multi - giurisdizione
Questo scenario si focalizza sul comando ed il controllo, ovvero su quegli aspetti che sono fondamentali per garantire la necessaria interoperabilità in caso di emergenza.
Lo scenario viene considerato dal punto di vista dei comandi di emergenza e per gli incidenti, senza includere quello delle persone coinvolte.
Si suppone che sia avvenuta una grande esplosione in uno stabilimento chimico: questo comporta alto rischio di fuga di gas tossici ed altre sostanze chimiche. L'unità IC ("Incident Command")arriva sulla scena e valuta la situazione. Dopo una breve ricognizione dell'area, la squadra avvia il centro di comando ed inizia a ricevere informazioni dalla rete temporanea creata in loco dalla prima unità di soccorso arrivata.

Nel frattempo, viene allertato l'EM ("Emergency Manager"), il quale attiva il terminale di comando all'interno dell'EOC ("Emergency Operation Centre") per monitorare la situazione. Tutte le parti attive nella zona sono a disposizione per le richieste dell'EM.

Il display mobile del centro di comando registra tutte le unità presenti, incluse EMS, LE ("Law Enforcement") e Vigili del Fuoco.

L'IC può osservare sul suo display tutte le unità coinvolte nell'operazione di soccorso, le aree contrassegnate a seconda delle caratteristiche momentanee (incendi, incidenti..). Le informazioni sono disponibili nel sistema dell'EM non appena vengono acquisite dall'IC, e vengono fornite sia in formato mappa GIS sia in formato testo.

Quando nuove unità raggiungono il luogo dell'incidente, vengono immediatamente autenticate ed inserite nella lista di unità disponibili in possesso dell'IC.

La sezione di Vigili del Fuoco controlla lo stato della situazione valutata dalla relativa unità che si trova sul posto, e coordina tutto come necessario. Ogni dato rilevato da qualsiasi delle unità sul luogo ritenuto rilevante per una diversa sezione di appartenenza viene immediatamente inviato al centro di comando interessato.

Dopo aver completato tutte le incombenze relative al particolare tipo di incidente, l'IC inizia a coordinarsi con le varie sezioni di sicurezza pubblica: Forze dell'Ordine, Vigili del Fuoco ed Emergenza Medica. Appena l'IC inizia a dare le prime direttive, la sezione dei pompieri informa della necessità di altre unità di soccorso, a causa della vastità dell'area incidentata. L'IC provvede subito a chiamare rinforzi; quando questi arrivano si registrano alla rete ed iniziano a coordinarsi con le squadre già presenti.

L'unità di emergenza medica crea un' area di triage/treatment ed inizia a coordinare le risorse mediche disponibili nell'area incidentata, allertandole e informandole della situazione.

L'unità dei Vigili del Fuoco riceve da uno dei sensori di uno dei suo pompieri l'avviso di presenza di sostanze chimiche rischiose nell'area incidentata, perciò allerta tutte le unità di soccorso di tutti i tipi presenti nella zona del pericolo riscontrato. Per questo motivo, l'EM chiama sul luogo tutto il personale disponibile relativo alla sezione Sostanze Pericolose e lo pone sotto il controllo dell'IC, che dispone un secondo perimetro di sicurezza attorno al luogo interessato.

Vedendo il cambio di disposizione, l'EM informa tutte le sue unità affinché si

adeguino, e intanto le allerta di limitare la ventilazione esterna dato il rilevamento delle sostanze pericolose.

L'unità LE si dirige verso l'IC per coordinarsi e configurare le modifiche alla viabilità necessarie a deviare il traffico dalla zona informando del pericolo.

L'EM comincia a coordinarsi con le altre organizzazioni per attuare le necessarie misure di sicurezza , come ad esempio la chiusura delle linee del gas e l'intervento sulla fornitura di energia elettrica. Inoltre, è ancora l'EM che coordina le nuove unità di LE giunte sul luogo in seguito all'ordine dell'IC.

Dopo alcune investigazioni da parte di LE e Vigili del Fuoco, l'IC potrebbe stabilire che non si è trattato di un incidente, e quindi disporre che l'area sia considerata scena del crimine ed ordinare ad alcune unità LE di indagare sull'accaduto, in collaborazione con l'adeguata divisione di pompieri ed informando immediatamente l'EM.

Se necessario, verrebbero allertate unità apposite per neutralizzare problemi o rischi di vario genere.

A seconda dei tag RF ID apposti dal personale medico, i vari pazienti vengono trasportati nei centri ospedalieri più vicini in base al grado di gravità individuale.

L'EM chiama anche altre unità di rinforzo sul luogo, le quali appena arrivano si uniscono alla rete creata, per ricevere le informazioni scambiate tra le varie unità.

I Vigili del Fuoco informano l'IC che tutti gli incendi sono stati posti sotto controllo, mentre tutte le fughe di sostanze tossiche sono state contenute ed eliminate. Tute le squadre relative alle sostanze tossiche vengono rilasciate, tranne una, trattenuta per sicurezza.

Quando anche tutti i fuochi sono stati sedati, anche tutte le unità di pompieri vengono rilasciate, tranne una, sempre per precauzione.

L'EM informa l'IC che tutti i pazienti sono stati trasportati ai centri ospedalieri più adeguati.

Ovviamente, in un caso di emergenza reale le cose sarebbero diverse da un esempio di pura simulazione. Per questo, le caratteristiche dei sistemi di comunicazione dovranno essere tali da permettere gli adattamenti necessari alle diverse situazioni. E' importante ricordare che nei casi simili a quello appena analizzato, ovvero quando si trovano a cooperare più forze di sicurezza pubblica contemporaneamente, è molto importante la coordinazione tra le diverse unità, per garantire un'azione efficiente e

veloce. Si potrebbero riscontrare anche casi in cui oltre alla multidisciplinarietà sia necessaria una collaborazione tra forze appartenenti a nazioni diverse. Per questo motivo, nel progetto del sistema sarà necessario tenere in conto anche questo aspetto.
L'idea di una piattaforma basata su standard condivisi è quella alla base del sistema IMS, che analizzeremo più nel dettaglio di seguito, e che verrà impiegato nello sviluppo del progetto.
All'interno del progetto PICO è stato rilasciato anche un documento che definisce le caratteristiche tecniche che dovrebbe avere il dispositivo in dotazione agli operatori, ma questo aspetto non è rilevante per il lavoro di tesi qui presentato.
Risulta invece più interessante avere una visione d'insieme delle strutture che si intendono usare all'interno della piattaforma (architetture, gerarchie, protocolli ed interazioni) e discutere le proprietà del contesto che caratterizzeranno il sistema.

2.2.2 Organizzazione della piattaforma PICO

Tutte le forze di pubblica sicurezza sono raggruppabili in tre macrocategorie, come si può vedere dalla figura (Fig.2.3), ed ogni operatore è rappresentabile genericamente come PSCDU (PSCD User).
Sarà poi in fase di autenticazione e identificazione che l'utente fornirà le informazioni sulla propria categoria di appartenenza, permettendo la sua classificazione e l'assegnazione di un certo livello di autorizzazione nell'accesso ai dati.
Sia gli utenti appena citati che il centro di coordinamento si dovranno poi interfacciare con la piattaforma IMS, con la quale interagiranno tramite il dispositivo in dotazione (PSCD).
In Fig.2.4 si possono vedere degli esempi di operazioni elementari che l'utente di pubblica sicurezza può compiere: Autenticazione, Identificazione, Scelta dell'applicazione che si vuole usare (scegliendola tra una lista di applicazioni disponibili in streaming dalla centrale operativa), Esecuzione dell'applicazione selezionata, Rimozione dell'applicazione una volta terminato l'uso. La rimozione

dell'applicazione viene fatta per evitare di occupare memoria del dispositivo inutilmente.

In Fig.2.5 si ha una visione generale della struttura del sistema. Si vede che il PSCD è composto da due parti principali: la sezione applicativa e l'interfaccia IMS, necessaria per interagire col sistema. Nella parte applicativa sono racchiuse l'interfaccia web usata dall'utente,il sistema per gestire le applicazioni on demand e il blocco che si occupa di autenticazione e autorizzazione. Nell'interfaccia è racchiuso il vero e proprio client SIP, che è in relazione con l'Application Server (il database che racchiude tutte le applicazioni fruibili dall'utente) e con la piattaforma IMS, il quale gestisce tutta la parte di comunicazione vera e propria: le registrazioni al sistema, le chiamate, il routing, ecc.

Il protocollo usato dalla piattaforma IMS è SIP. Di IMS e SIP si parlerà con maggior dettaglio nel prossimo capitolo.

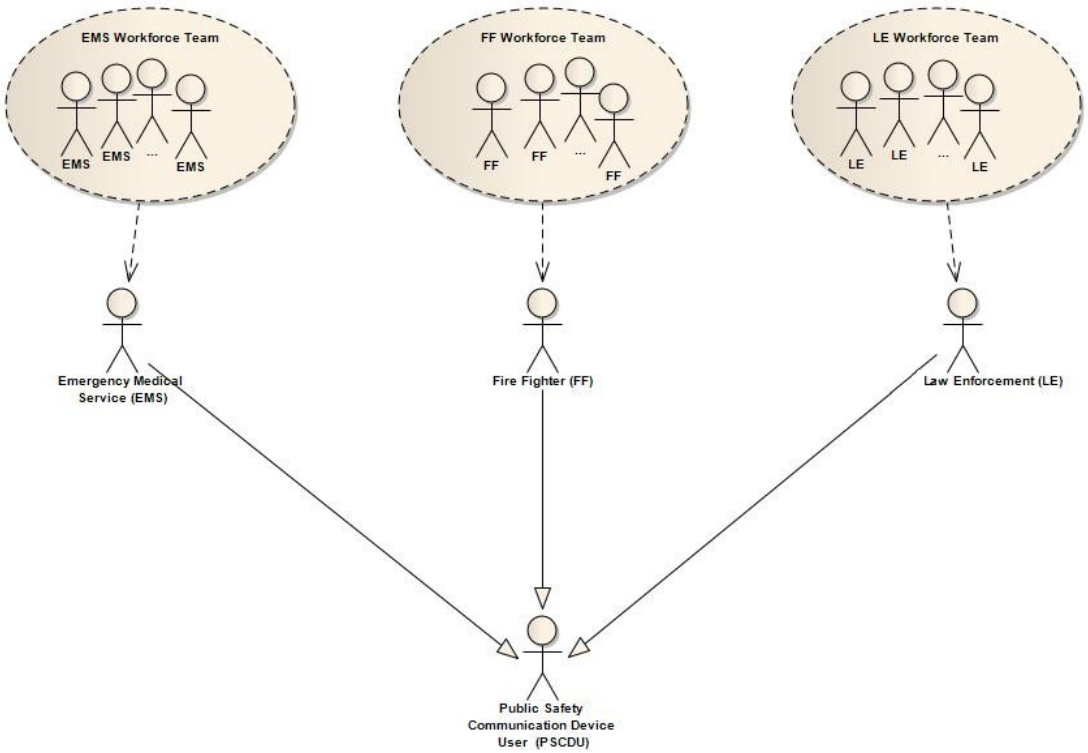


Fig.2.3 : Attori del sistema PICO

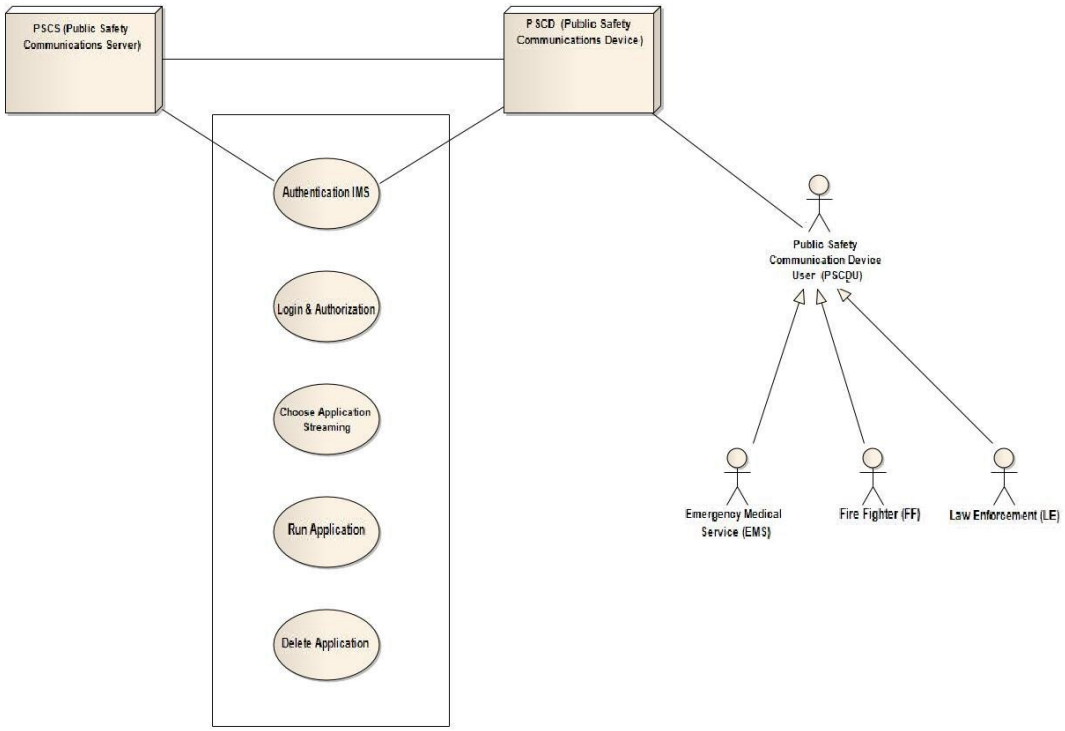


Fig. 2.4: Principali azioni possibili tramite PSCD

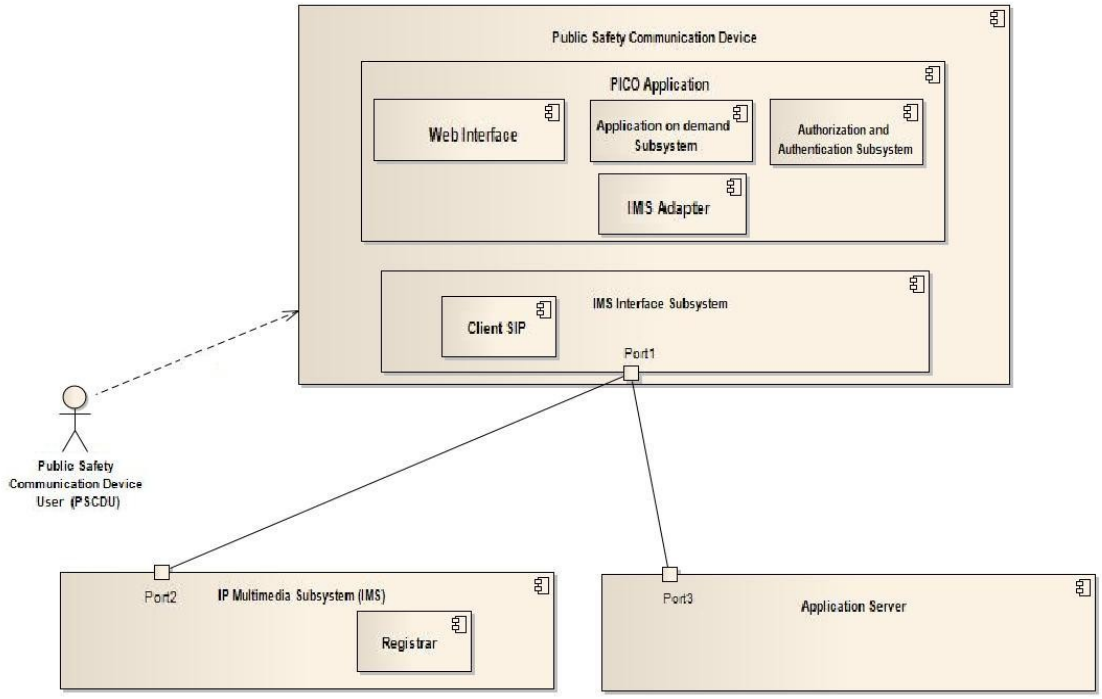


Fig.2.5: Architettura logica del sistema

2.3 ECRIT

ECRIT è un gruppo di lavoro IETF che ha come obiettivo la definizione di specifiche tecniche che esplicitino le caratteristiche che deve possedere il sistema di gestione delle chiamate d'emergenza nelle reti di nuova generazione.

La rete PSTN [4] è banalmente configurata per riconoscere un numero specificato esplicitamente (ad esempio 118, 911, ecc.) come chiamata d'emergenza. Questi numeri, che variano a seconda dello stato in cui ci si trova e di cui abbiamo una rappresentazione in Fig.2.6, sono rapportati ad un contesto di servizio d'emergenza e dipendono da una configurazione regionale dei metodi di servizio di connessione e da un sistema di distribuzione dei servizi basato sulla localizzazione geografica.

Queste chiamate vengono inoltrate a speciali call centers attrezzati per gestire gli episodi d'emergenza. La distribuzione del servizio di gestione delle chiamate d'emergenza attraverso questi sistemi richiede sia un'associazione della localizzazione fisica del chiamante con l'appropriato centro di servizio che un idoneo routing delle chiamate per connettere le chiamate al centro direzionale.

Le chiamate eseguite usando Internet technologies non usano gli stesi sistemi per raggiungere l'obiettivo, ovvero la connessione più vantaggiosa possibile. Inoltre, l'impiego diffuso di reti stratificate e tunnel rende il tutto più difficoltoso. Ci sono tuttavia delle Internet technologies adatte per descrivere la localizzazione e gestire il routing delle chiamate.

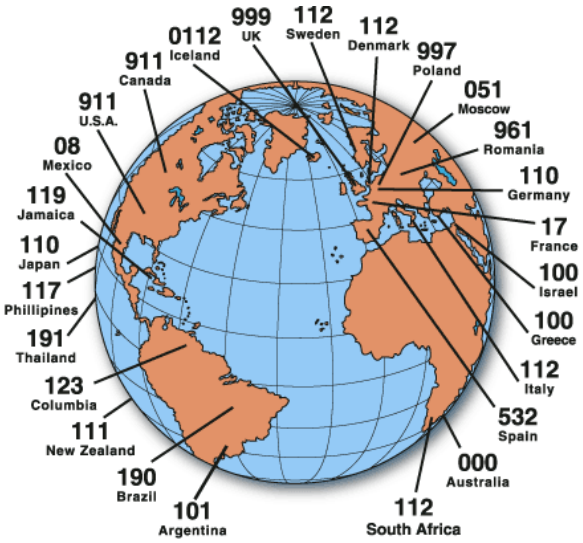


Fig.2.6 Numeri d'emergenza in diversi stati del mondo

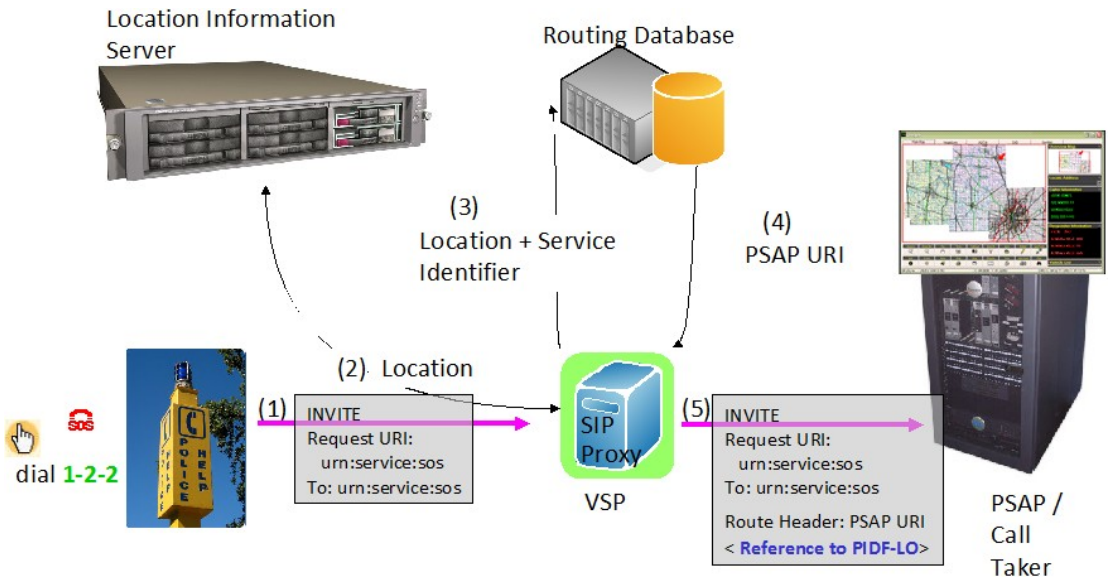


Fig.2.7 : Scambio di messaggi iniziale di chiamata di richiesta di soccorso nel sistema ECRIT

ECRIT mira a descrivere quando queste tecnologie sono appropriate e come vanno usate. Non si occupa invece della questione della gestione delle priorità all'intero del traffico telefonico. Si suppone che le chiamate provengano da utenti qualsiasi di

Internet, mentre il traffico generato da enti militari o governativi viene gestito in modo diverso, poiché richiede livelli di sicurezza ed autenticazione non necessari altrimenti.

In Fig.2.7 si vedono le parti in gioco previste da ECRIT: l'utente effettua la chiamata al numero d'emergenza del proprio stato (1) tramite il comando INVITE di SIP (per la struttura completa dei messaggi SIP si veda il par.3.3.1), la chiamata passa per il SIP Proxy (P-CSCF, si veda cap.3) che la inoltra al Location Information Server (nella piattaforma OpenIMSCore descritta nel cap.3 è LRF, vedere il cap.3 per i dettagli) e al Routing Database (che in OpenIMSCore è chiamato LoST Server, vedi cap.3), ottenendo alla fine l'URI del PSAP (Public Safety Answering Point, è il termine generico con cui ci si riferisce al centro di soccorso in questione) più vicino all'utente che richiede soccorso. Il PSAP scelto viene poi informato dal SIP Proxy e viene instaurata la connessione tra esso e l'utente chiamante.

Il gruppo di lavoro mostra come la disponibilità di dati di localizzazione e informazioni di routing delle chiamate possano abilitare comunicazioni tra utente e relativo centro di risposta alla chiamata d'emergenza effettuata. Si usa sempre il termine "chiamata", ma va ricordato che il flusso informativo in gioco può essere di diversi tipi (ad esempio voce, testo, ecc.), non solo voce.

Tutte le soluzioni presentate da ECRIT devono essere fruibili a prescindere dalla giurisdizione all'interno della quale vengono implementate, senza che sia necessaria la presenza di una singola autorità centrale. Inoltre, deve essere possibile gestire le diverse entità di soccorso indipendentemente, dato che il routing delle varie chiamate deve essere autonomo.

All'interno del lavoro del gruppo, vengono considerati anche gli aspetti di privacy e sicurezza.

Nell'Ottobre 2009 il gruppo ha raggiunto la sottoscrizione di LoST, nel documento "Synchronizing Location-to-Service Translation (LoST) Protocol based Service Boundaries and Mapping Elements" [9], che verrà affrontato nel dettaglio in seguito (paragrafo 2.4).

2.4 LoST (Location-To-Service Translation Protocol)

LoST è il protocollo definito all'interno del documento IETF RFC 5222 [7]. LoST sta per Location-to-Service Translation, ed è un protocollo basato su XML che serve a mappare identificatori di servizio e informazione di localizzazione (geografica o indirizzo civico) su contatti di servizio URI (Uniform Resource Identifier). In particolare, può essere usato per determinare il PSAP appropriato per servire l'emergenza in questione. In Fig.2.8 si ha una rappresentazione schematica della sua funzione.

Non verrà esaminato nel dettaglio l'intero documento, ci si limiterà a delineare un quadro generale e a riportare gli script XML in esso definiti interessanti per gli scopi della tesi.

Nel documento RFC 5222 ci si focalizza sulla descrizione del protocollo tra il mapping del client e quello del server. Le altre funzioni, come la scoperta dei server, la replica dei dati e l'architettura di mapping dei server sono descritti in documenti separati.

I messaggi di richiesta trasportano informazioni di localizzazione e un identificativo di servizio codificato come URN (Uniform Resource Name) dal client LoST al LoST server. Il server LoST usa il suo database per mappare i valori in ingresso su uno o più URIs e restituisce quegli URIs arricchiti di informazioni opzionali (come ad esempio cenni sui limiti di servizio) come risposta al client LoST.

Se il server non può risolvere la richiesta da solo, può interrogare un altro server o restituire l'indirizzo di un altro LoST server. Inoltre, il protocollo permette di recuperare i limiti di servizio e fare una lista dei servizi disponibili per una particolare posizione geografica osupportati da un certo server.

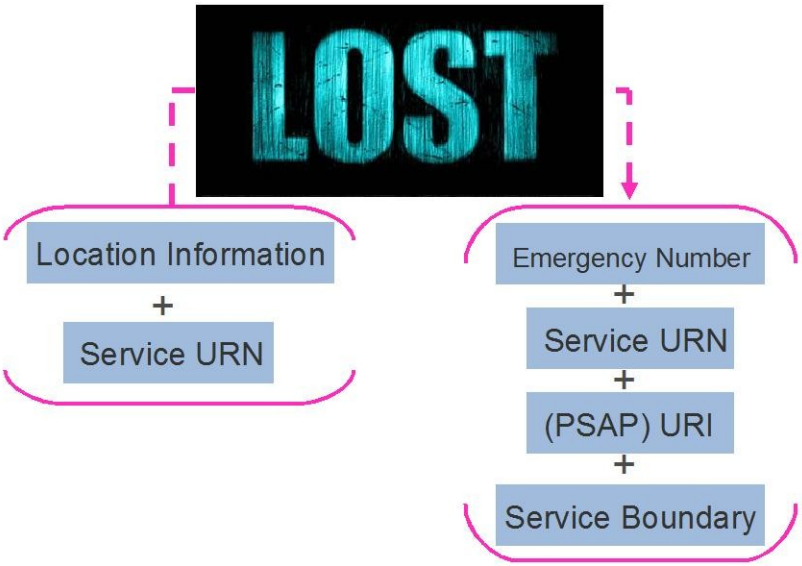


Fig.2.8: Schematizzazione del funzionamento di LoST

I server LoST sono identificati da una stringa univoca U-NAPTR/DDDS (URI-Enabled NAPTR/Dynamic Delegation Discovery Service), in forma di nome DNS.
Si riporta ora in Figura 2.9 un esempio di mapping usando coordinate geografiche, supponendo una richiesta di servizio alla polizia. Questo messaggio, facendo riferimento alla Fig.2.7, verrà incluso nel messaggio di INVITE inviato dall'utente al SIP Proxy.

```
<?xml version="1.0" encoding="UTF-8"?>
<findService
xmlns="urn:ietf:params:xml:ns:lost1"
     xmlns:p2="http://www.opengis.net/gml"
serviceBoundary="value"
recursive="true">

<location id="6020688f1ce1896d" profile="geodetic-2d">
<p2:Point id="point1" srsName="urn:ogc:def:crs:EPSG::4326">
<p2:pos>37.775 -122.422</p2:pos>
</p2:Point>
</location>
<service>urn:service:sos.police</service>

</findService>
```

Fig. 2.9: Una richiesta <findService> geografica

Data questa richiesta, un server risponderà con un servizio ed una informazione ad esso relativa. I questo esempio, il server ha mappato la localizzazione fornita dal client come riguardante un servizio di polizia del dipartimento di New York City, e dirà quindi al richiedente che può contattare il servizio desiderato attraverso l'URI "sip:nypd@example.com" e "xmpp:nypd@example.com". La forma della risposta sarà quella riportata in Fig. 2.10:

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponsexmlns="urn:ietf:params:xml:ns:lost1"
     xmlns:p2="http://www.opengis.net/gml">
<mapping
expires="2007-01-01T01:44:33Z"
lastUpdated="2006-11-01T01:00:00Z"
source="authoritative.example"
sourceId="7e3f40b098c711dbb6060800200c9a66">
<displayNamexml:lang="en">
         New York City Police Department
</displayName>
<service>urn:service:sos.police</service>
<serviceBoundary profile="geodetic-2d">
<p2:PolygonsrsName="urn:ogc:def::crs:EPSG::4326">
<p2:exterior>
<p2:LinearRing>
<p2:pos>37.775 -122.4194</p2:pos>
<p2:pos>37.555 -122.4194</p2:pos>
<p2:pos>37.555 -122.4264</p2:pos>
<p2:pos>37.775 -122.4264</p2:pos>
<p2:pos>37.775 -122.4194</p2:pos>
</p2:LinearRing>
</p2:exterior>
</p2:Polygon>
</serviceBoundary>
<uri>sip:nypd@example.com</uri>
<uri>xmpp:nypd@example.com</uri>
<serviceNumber>911</serviceNumber>
</mapping>
<path>
<via source="resolver.example"/>
<via source="authoritative.example"/>
</path>
<locationUsed id="6020688f1ce1896d"/>
</findServiceResponse>
```

Fig. 2.10: Risposta a richiesta di servizio con coordinate geografiche <findServiceResponse>

Se invece l'utente invia un indirizzo, la sua richiesta sarà in questa forma (Fig.2.11):

```
<?xml version="1.0" encoding="UTF-8"?>
<findServicexmlns="urn:ietf:params:xml:ns:lost1"
recursive="true" serviceBoundary="value">
<location id="627b8bf819d0bad4d" profile="civic">
<civicAddress
xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
<country>DE</country>
<A1>Bavaria</A1>
<A3>Munich</A3>
<A6>Otto-Hahn-Ring</A6>
<HNO>6</HNO>
<PC>81675</PC>
</civicAddress>
</location>
<service>urn:service:sos.police</service>
</findService>
```

Fig.2.11: Richiesta di servizio tramite indirizzo <findService>

In questo caso la risposta del server sarà quella riportata in Fig.2.12.

A queste forme base di richiesta e risposta possono essere applicate delle varianti, come ad esempio la richiesta di validazione dell'indirizzo, di specifica dei limiti di servizio, della lista dei servizi disponibili a seconda della posizione attuale, di verifica dell'interoperabilità.

Nel documento vengono analizzati nello specifico tutti i campi e tutti i casi, e anche tutti gli errori che si potrebbero incontrare. Vengono analizzate ed esposte anche le procedure di registrazione al server e gli aspetti relativi alla sicurezza.

Nel lavoro di tesi, vengono rielaborati gli XML qui definiti in forma base per adattarli agli scopi prefissati.

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponsexmlns="urn:ietf:params:xml:ns:lost1">
<mapping
expires="2007-01-01T01:44:33Z"
lastUpdated="2006-11-01T01:00:00Z"
source="esgw.ueber-110.de.example"
sourceId="e8b05a41d8d1415b80f2cdbb96ccf109">
<displayNamexml:lang="de">
MuenchenPolizei-Abteilung
</displayName>
<service>urn:service:sos.police</service>
<serviceBoundary
profile="civic">
<civicAddress
xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
<country>DE</country>
<A1>Bavaria</A1>
<A3>Munich</A3>
<PC>81675</PC>
</civicAddress>
</serviceBoundary>
<uri>sip:munich-police@example.com</uri>
<uri>xmpp:munich-police@example.com</uri>
<serviceNumber>110</serviceNumber>
</mapping>
<path>
<via source="esgw.ueber-110.de.example"/>
<via source="polizei.muenchen.de.example"/>
</path>
<locationUsed id="627b8bf819d0bad4d"/>
</findServiceResponse>
```

Fig. 2.12: Risposta alla richiesta di servizio tramite localizzazione con indirizzo <findServiceResponse>

Capitolo 3

IMS (IP Multimedia Subsystem)

3.1 Introduzioneal sistema

Nel corso degli ultimi anni, lo sviluppo delle Next Generation Network (NGN) ha dato agli utenti la possibilità di accedere ad un grande numero di applicazioni basate sul trasferimento e la condivisione di contenuti multimediali con ampia versatilità. La definizione ufficiale di NGN [1], fornita dalla ITU-T nel documento "Terms of Reference NGN-GSI" del 13-08-2009, è quella di una rete a pacchetto capace di fornire servizi di telecomunicazione facendo uso di tecnologie di trasporto a banda larga e con controllo di QoS (Quality of Service), nella quale le funzioni relative al servizio sono indipendenti dalle tecniche di trasporto di livello inferiore. Le reti NGN implementano l'Internet Protocol Multimedia Subsystem, che è un'architettura di rete per la convergenza di tutti i dispositivi di telecomunicazione (fissi e mobili) in un'unica rete IP, per offrire servizi voce e multimediali.

Nel seguito IMS verrà brevemente introdotta, fornendo le definizioni principali, qualche cenno storico ed in particolare la sua architettura ed i suoi elementi costitutivi.

Definizioni di IMS e benefici

IMS è un'architettura di rete per la distribuzione di servizi IP multimediali. IMS permette un'esperienza multimediale più ricca rispetto alla tecnologia basata su commutazione di circuito, realizzando una tecnologia e terminali con molteplici tipologie di accesso alla rete, localizzazione geografica delle utenze e un'alta personalizzazione di servizi offerti a seconda delle esigenze degli utenti finali.

Come conseguenza della scelta di IMS come architettura di convergenza, diversi enti di standardizzazione vengono coinvolti nella definizione del sistema, sia da rete fissa che mobile.

IMS è stato definito originariamente da 3G.IP (forum industriale formatosi nel 1999), che ha sviluppato l'architettura iniziale. Questa venne presa dal 3GPP[12](3rd Generation Partnership Project) come parte del proprio lavoro di standardizzazione per supportare le reti GSM e l'evoluzione delle tecnologie cellulari. IMS apparse inizialmente nella release 5 di 3GPP (evoluzione da 2G a 3G)[13], nella quale SIP

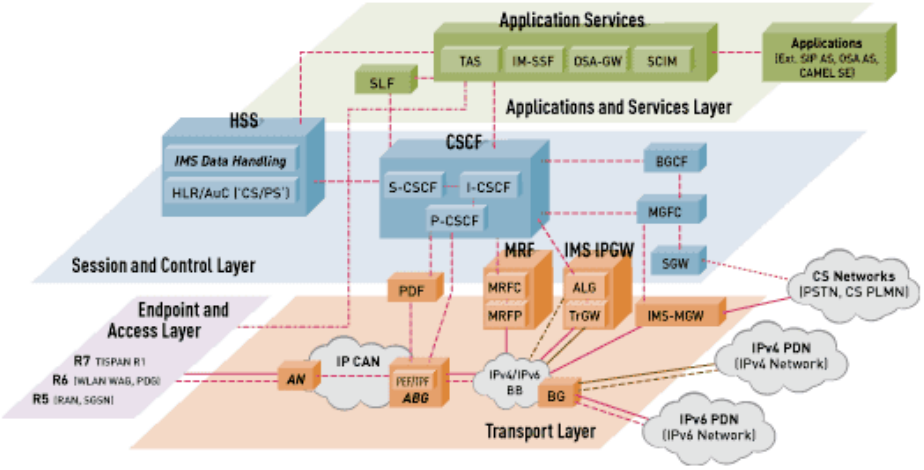


Fig. 3.1: Architettura IMS completa secondo la definizione fornita da 3GPP - TISPAN.

12 3GPP è una collaborazione tra gruppi di associazioni di telecomunicazione per creare specifiche di sistema globalmente applicabili per sistemi telefonici di terza generazione [.

13 3G (conosciuta anche come IMT-2000, ovvero International Mobile Telecommunications-2000) è una famiglia di standard per telecomunicazioni mobili definita da ITU (International Telecommunication Union) che include specifiche e definizioni per GSM EDGE, UMTS, CDMA2000, WiMax e DECT. Rispetto a 2G (standard per telefonia di seconda generazione) fornisce uso simultaneo di traffico voce e dati e maggiora rate di dati [11].

(Session Initiation Protocol, definito dall'IETF, del quale parleremo nei prossimi paragrafi) venne scelto come protocollo principale per il set up delle telefonate . Nelle releases6 e 7 di 3GPP fu ulteriormente migliorato includendo caratteristiche aggiuntive, come l'interworking con WLAN[14]e il supporto per reti fisse, lavorando assieme a TISPAN[15].
IMS può essere pensata come un modo per offrire ovunque servizi Internet indipendentemente dalla tecnologia di accesso.
In Fig.3.1 troviamo la rappresentazione schematica dell'intera architettura IMS fornita da 3GPP e TISPAN.

IMS può offrire alcuni importanti valori aggiunti rispetto alle attuali architetture di rete di core:

- IMS fornisce servizi multimediali abilitando il *controllo della QoS* (Quality of Service)[16]. Nelle odierne tecnologie 3G, nonostante l'accesso a Internet sia molto più veloce di prima, non ci sono garanzie sulla QoS percepita dall'utente; viene seguito il principio del "best effort"[17]: la rete farà del proprio meglio per assicurare un buon livello di servizio, ma se durante un trasferimento multimediale la disponibilità di banda ha un brusco calo, non si può fare nulla per mantenere il livello del servizio. IMS invece regola il livello di QoS all'interno della rete IP e trae vantaggio dai meccanismi di misura della QoS per verificare e garantire la

14 WLAN è l'acronimo di Wilreless Local Area Network, ed indica appunto una rete locale che sfrutta tecnologia wireless. Con questa sigla si indicano genericamente tutte le reti locali di computer che non utilizzano dei collegamenti via cavo per connettere fra loro gli host della rete [12].

15 TISPAN è l'acronimo di Telecoms & Internet converged Services & Protocols for Advanced Networks. TISPAN è un corpo di standardizzazione di ETSI (European Telecommunications Standard Institute, organizzazione di standardizzazione indipendente nell'ambito delle telecomunicazioni), specializzato in reti fisse e convergenza Internet [13].

16 Nell'ambito delle reti di telecomunicazione a commutazione di pacchetto, la locuzione "Quality of Services" indica il meccanismo di controllo delle risorse attraverso cui si raggiunge una determinata qualità del servizio. Qualità del servizio è l'abilità di fornire diversi livelli di priorità a diverse applicazioni, utenti o flussi di dati o di garantire un certo livello di performance a determinati flussi di dati [14].

17 La consegna "best effort" descrive un servizio di rete nel quale la rete non fornisce alcuna garanzia sull'effettiva consegna dei dati o sulla qualità del servizio percepita dall'utente [15].

qualità della trasmissione. Per offrire questo servizio, i providers di servizi di rete IMS dovranno avere la possibilità di misurare, regolare e distribuire un certo livello di rate di trasmissione, ritardo dei gateway e rate d'errore.

- IMS consente agli operatori di realizzare *un'adeguata tariffazione delle sessioni multimediali*. Nei sistemi 3G, l'utente paga il numero di byte trasferiti. Una videoconferenza necessita di una grande quantità di bytes trasferiti, perciò è molto costosa per l'utente. Se l'operatore potesse fornire una tariffazione diversificata a seconda del tipo di servizio impiegato dall'utente, l'utente potrebbe trarne beneficio. Questo è concretizzabile usando tecnologia IMS, la quale fornisce informazioni all'operatore circa il tipo di servizio richiesto al momento dall'utente, in modo che il provider possa applicare la tariffazione adeguata.
- IMS fornisce una *piattaforma comune per ogni tipo di servizio*. Elemento essenziale per un'efficiente offerta di servizi convergenti è rendere possibile l'introduzione nuovi servizi facilmente e velocemente. Questa caratteristica di integrazione tipica di IMS ridurrà il cosiddetto "time-to-market" (tempo di immissione sul mercato) per il rilascio di nuovi servizi multimediali. I providers di servizi sono molto interessati a questa caratteristica, poiché una delle maggiori sfide nelle reti di comunicazione attuali è il miglioramento del lungo e costoso processo che la creazione di un nuovo servizio richiede. IMS supporta lo sviluppo di nuovi servizi e un ricco scenario d'affari: costruito su interfacce accuratamente progettate, consente agli operatori di lanciare nuovi servizi o di espandere quelli già esistenti. Inoltre, per facilitare lo sviluppo di servizi nuovi e creativi, le caratteristiche standardizzate del mass-market[18] possono essere esposte attraverso pubbliche interfacce a clienti, che possano fare il download, e a servers di rete: le interfacce standard e le caratteristiche comuni fornite dall'infrastruttura IMS abilitano i providers di servizi ad adottare facilmente un servizio creato da terze parti e a creare un servizio che si integra efficientemente con molti altri. Per questo, i nuovi servizi hanno il potenziale di arrivare rapidamente sul mercato con portata globale e senza intaccare l'infrastruttura. In IMS, il controllo e la gestione delle sessioni

18 Mass market: categoria di servizi standardizzati che vengono supportati da un vasto range di terminali e che interagiscono all'interno della community globale dell'operatore. Questi servizi sono caratterizzati da scalabilità, disponibilità e performance; la crescita funzionale viene definita dalla standardizzazione. Questa categoria di servizi è l'alternativa ai "non standardized services", che gli operatori individualmente possono fornire ai propri clienti con breve time-to-market e flessibilità [16].

multimediali vengono realizzati usando SIP (Session Initiation Protocol) come protocollo standard. Questo protocollo permette add/drop[19] dinamico di contenuti multimediali durante una sessione, a seconda del tipo di applicazione in uso. IMS abilita l'implementazione di una piattaforma comune di controllo del servizio, esecuzione e interazione per tutti i servizi e per tutti gli abbonati che accedono alla propria rete.

- IMS permetta agli utenti di sfruttare ogni tipo di servizio *indipendentemente dalla propria localizzazione*. IMS usa tecnologia Internet per far sì che l'utente possa girovagare in diversi Paesi ed avere ovunque l'opportunità di accedere a qualsiasi tipo di servizio. Per rendere questo possibile, IMS fornisce elementi di informazione di localizzazione e di registrazione degli utenti che abilitano la mobilità, uniti a set-up e gestione delle sessioni e inoltro di messaggi a reti IMS e non.
- L'architettura IMS ha la peculiarità di essere *access-independent,*ovvero di essere fruibile indipendentemente dalla tecnologia con cui si effettua l'accesso. Questo aspetto è chiaramente fondamentale nell'ottica di una migrazione verso la convergenza globale. Ogni tipo di accesso può interagire col nucleo IMS, sia che si tratti di DSL, WLAN, GPRS, WiMAX[20], e così via. Questa possibilità è molto importante poiché la maggioranza dei dispositivi attualmente in commercio non sono IMS. A tempo debito, tutti i terminali e le reti di accesso lo saranno, ma fino ad allora ci sarà un mix. Questa caratteristica di IMS, molto preziosa in un sistema di comunicazione orientato alla convergenza, facilita lo sviluppo di nuovi servizi, ma implica la creazione di specifiche interfacce standard.

19 Il termine add/drop, ovvero letteralmente aggiungi/togli, fa riferimento alla caratteristica di rete che consente di spillare o inserire direttamente singoli contenuti multimediali senza dover manipolare l'intero flusso aggregato [17].

20 DSL (Digital Subscriber Line), WLAN (Wireless Local Area Network), GPRS (General Packet Radio Service) e WiMAX (Worldwide Interoperability for Microwave Access) sono diverse tecnologie di accesso a sistemi telefonici [18].

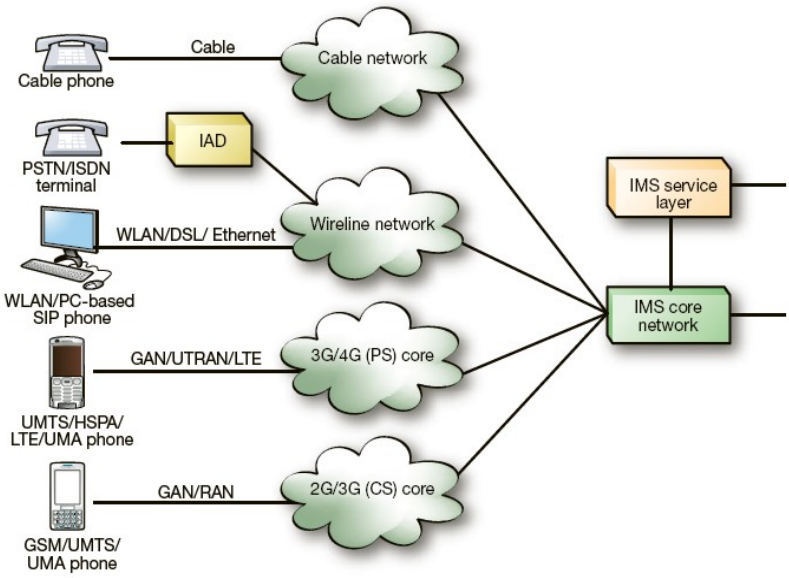


Fig.3.2 Rappresentazione di rete IMS con tecnologia di accesso multiplo.

In Fig.3.2 si ha una rappresentazione schematica della piattaforma IMS e dei diversi tipi di accesso possibili.

IMS hagli strumenti e le funzioni per manipolare numerosi servizi non standardizzati in modo standardizzato: interoperabilità, conoscenza del tipo di accesso, tipo di supporto, sicurezza, qualità del servizio, interworking con reti esistenti. I servizi offerti all'utente finale da IMS sono il frutto della combinazione di servizi elementari come presenza (inclusa disponibilità di persona e terminale, preferenze di comunicazione, capacità del terminale, attività e posizione correnti, ecc.), messaggi (instantmessaging, session-based messaging, consegna ritardata dei messaggi, MMS, voce-video messaggi), conferencing (con contenuti multimediali additivi) e streaming multimediale. Dallacombinazione di questi servizi elementari, IMS può fornire diversi tipi di servizi complessi, come il Push to talk Over Cellular (POC) per usare il tradizionale servizio walkie-talkie su rete mobile attraverso dispositivi mobili, o tutte le possibili applicazioni derivate dalla mobilità offerta da IMS: si può iniziare la chiamata su un dispositivo fisso (come ad esempio il telefono di casa) e continuarla su un dispositivo mobile senza interromperla; cominciare a vedere un film in TV, interromperlo e continuare la visione sul proprio PDA in giardino. Si può anche sfruttare un mix di servizi, come ad esempio mandare un MMS dalla propria auto e farlo apparire sullo schermo TV; durante una conversazione tra amici fare uno sharing del video di cui si sta parlando, e così via.

3.2 Architettura IMS

IMS è stata progettata per usare un'architettura stratificata. E' stato detto in precedenza che IMS lavorerà su qualsiasi tipo di architettura di rete sottostante: questo significa che i servizi ditrasporto devono essere separati dalla rete di segnalazione IMS e dai servizi di gestione della sessione.
Un beneficio di questo tipo di architettura è la scalabilità, ovvero la possibilità di aggiungere nuove reti in seguito.
Analizzando la figura 3.1, dal basso verso l'alto, nell'architettura stratificata IMS si hanno: piano di Accesso, piano di Controllo e piano Applicativo.
Il piano di Accesso realizza la connessione di tutti gli utenti alla rete IMS core. Ciò viene fatto direttamente se l'utente usa un terminale IMS, attraverso gateways se il dispositivo non è IMS. I gateways usano interfacce standard che rendono possibile la comunicazione con tutte le entità esistenti. Questo livello è quindi direttamente responsabile del trasporto del traffico tra endpoints.
Il piano di Controllo ha come occupazione principale la Call Session Control Function (CSCF). Questa funzione è compiuta dividendo il controllo tra tre diverse entità: Proxy, Serving and Interrogating, che verranno analizzate nel dettaglio in seguito. Questo insieme di server e proxy ha la funzione di processare e gestire i pacchetti di segnalazione SIP all'interno di IMS, effettuando il controllo dell'andamento della sessione ed il routing dei messaggi.
Il piano applicativo contiene ed esegue i servizi (applicazioni IP), e li distribuisce usando SIP per interfacciarsi con il livello di Controllo.
Ora si può andare oltre questa generica panoramica, analizzando ogni parte dell'architettura IMS nel dettaglio.

3.2.1 HSS – Home Subscriber Server

Questo è il principale database che supporta le entità dell'architettura IMS, responsabile della gestione di chiamate e sessioni multimediali. L'HSS contiene tutte le informazioni sul profilo utente, gestisce autenticazioni e autorizzazioni a livello IMS e può fornire informazioni sulla posizione fisica dell'utente. Le informazioni sul profilo utente includono identità, nome del S-CSCF associato (vedi paragrafo su S-CSCF), profilo di roaming, parametri di autenticazione e informazioni di servizio. L'identità privata dell'utente è assegnata dall'operatore di rete di residenza ed è usato per operazioni come registrazione e autorizzazione, mentre quella pubblica può essere usata da altri utenti per richiedere la comunicazione con l'utente finale. L'HSS inoltre fornisce la tradizionali funzioni di Home Location Register (HLR) e Authentication Centre (AUC), richieste dai domini PS[21]e CS[22]. In base a diversi fattori, come il numero di abbonati mobili, la capacità delle strutture e l'organizzazione di rete, ci possono essere molteplici HSS per ogni home network. In questo caso, serve un Subscriber Location Function (SLF) per mappare gli indirizzi degli utenti ed abilitare così I-CSCF, P-CSCF e AS a trovare l'indirizzo dell'HSS che contiene i dati user-specific richiesti. Entrambi HSS e SLF comunicano attraverso il protocollo Diameter[23].

21 PS, acronimo di Packet Switching, è un metodo di comunicazione proprio delle reti digitali, che raggruppa tutti i dati trasmessi in pacchetti, facilitandone la trasmissione su reti a data-stream variabile [19].

22 CS, acronimo di Circuit Switching, è un tipo di rete che stabilisce un circuito (o canale) tra nodi e terminali prima che gli utenti possano comunicare, come se i nodi fossero fisicamente connessi tramite un circuito elettrico [20].

23 Diameter è un protocollo AAA (Authentication, Authorization and Accounting) successivo a RADIUS, ma non direttamente compatibile. Diameter è un protocollo peer-to-peer, e consiste in un protocollo di base esteso con applicazioni specifiche di Diameter stesso. Il protocollo base da solo è inutilizzabile, ma può sempre essere associato con qualsiasi applicazione Diameter specifica di un servizio. E' supportato da TCP o SCTP e richiede obbligatoriamente l'uso di IPsec [21].

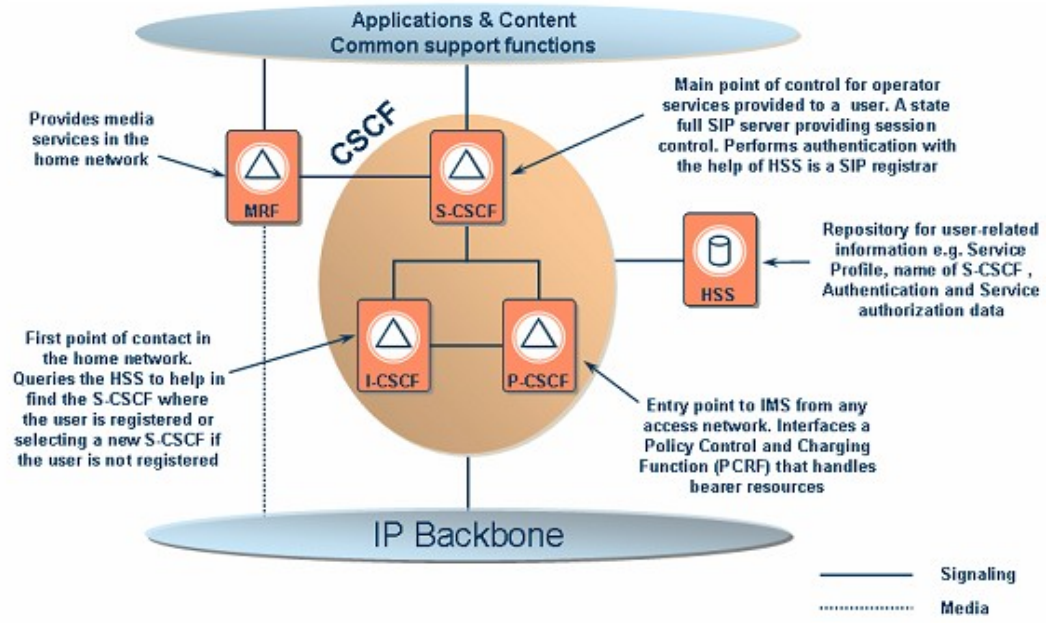


Fig. 3.3 Panoramica dell'IMS core

3.2.2 CSCF - Call Session Control Function

I pacchetti di segnalazione SIP in IMS vengono processati usando un gruppo di entità che si potrebbero definire "la famiglia di session management e routing". Questa famiglia consiste di tre entità: Proxy CSCF (P-CSCF), Interrogating CSCF (I-CSCF), e Serving CSCF (S-CSCF). In Fig.3.3 è rappresentata una panoramica del sistema.

3.2.2.1 P-CSCF (Proxy CSCF)

Il primo punto di contatto per gli utenti all'interno di IMS è il P-CSCF. Questo costituisce un Proxy SIP stateful[24], tutto il traffico da/verso gli utenti finali passa attraverso questa entità. Il P-CSCF valida le richieste, le inoltra verso selezionate destinazioni e processa e inoltra la risposta. Esegue l'autenticazione utente, può stabilire una sessione sicura IPsec con terminali IMS e supporta funzionalità RAC

24 Con il termine "stateful" si indica un sistema che si basa su uno "state", ovvero una configurazione unica di informazioni su una certa struttura.

(Resource Admission Control). Inoltre, si può comportare come User Agent, il cui ruolo è necessario per rilasciare le sessioni in condizioni anomale e per generare transazioni SIP indipendenti. Nella rete di un operatore ci possono essere uno o più P-CSCF. Il terminale trova il suoP-CSCF usando DHCP[25] o, in reti GPRS, PDP[26]Context. Quando un terminale IMS viene assegnato ad un P-CSCF questa associazione non cambia durante la validità del periodo di registrazione. Si elencano ora tutte le funzioni fornendo una breve spiegazione:

- Inoltro delle richieste di registrazione SIP all'I-CSCF a seconda dell'home domain name fornito dall'utente nella richiesta, e di altre richieste e risposte ricevute dall'utente verso il S-CSCF.
- Rilevamento di richieste di instaurazione di sessioni d'emergenza.
- Invio di informazioni relative alla contabilità all'entità CCF (Charging Collection Function).
- Fornitura di protezione dell'integrità della segnalazione SIP e mantenimento di associazione di sicurezza IPsec con l'utente.
- Possibilità di comprimere i messaggi SIP per ridurre il round trip time su links critici.
- Esecuzione dell'organizzazione dei media, controllo del contenuto del payload SDP (SDP: Session Description Protocol) per assicurarsi che il contenuto media sia adatto all'utente.
- Mantenimento di timers nelle sessioni. Questo può rilevare risorse libere esaurite da sessioni sospese.
- Interazione con l'entitàresponsabile del controllo delle autorizzazioni sul piano delle informazioni media ottenute dal P-CSCF. Questa funzione prende la richiesta di controllo a livello di servizio dal livello applicativo e lo traduce in un parametri IP QoS.
- Possibile fornitura di difesa contro attacchi alla segnalazione SIP.

25Dynamic Host Configuration Protocol: protocollo usato dal client per ottenere i parametri per operare nella rete IP. Riduce il carico di lavoro, dividendolo tra dispositivi distinti [22].

26 Packet Data Protocol: contiene informazioni sull'utente e sulla sessione mentre il client sta funzionando [23].

3.2.2.2 I-CSCF (Interrogating CSCF)

E' un Proxy SIP stateless posto ai confini di ogni dominio amministrativo ed è il punto di contatto per tutte le connessioni destinate a utenti che si stanno effettivamente muovendo nella rete di un diverso operatore. E' l'entità capace di determinare il S-CSCF presso il quale un utente si deve registrare, e realizza questa associazione interrogando l'HSS. Il I-CSCF può essere rimosso dal percorso di segnalazione una volta che è stato usato per stabilire quale S-CSCF usare. L'indirizzo IP del I-CSCF viene pubblicato nel Domain Name System (DNS) del dominio, in modo che i servers remoti lo possano trovare ed usare come punto di inoltro.

3.2.2.3 S-CSCF (Serving CSCF)

E' il cervello di IMS. Questa entità registra gli utenti e fornisce loro i servizi. Esegue il set up delle sessioni multimediali e le modifiche dei loro attributi e rilasci, routing, traduzioni, fornitura delle informazioni di fatturazione al sistema dei media, interrogazioni all'HSS per ottenere le autorizzazioni, informazione sull'innesco del servizio e sul profilo utente, usando il protocollo Diameter. Non memorizza in locale i dati utente. E' un server SIP, sempre posizionato nelle rete home. Durante il set up delle sessioni controlla SDP per assicurarsi che la sessione rispetti i confini d'uso del profilo utente in questione. Neldettaglio, le funzioni svolte da S-CSCF sono:

- Manipolazione delle richieste di registrazione; conosce l'indirizzo IP dell'utente e quale P-CSCF sta usando un punto d'accesso IMS.
- Registrazione e de-registrazione dell'utente (con supervisione del timer della registrazione) e autenticazione attraverso lo schema IMS "Authentication and Key Agreement".
- Download delle informazioni utente e dei dati relativi al servizio dall'HSS (se necessario).
- Routing del traffico destinato a dispositivi mobili verso P-CSCF e del traffico generato da dispositivi mobili verso I-CSCF, BGCF o AS.
- Controllo delle sessioni con capacità di decidere quando una richiesta deve esser ulteriormente processata facendo routing verso un AS, cioè interagendo con la

piattaforma dei servizi.

- Traduzione di numeri E.164[27]in URI SIP necessari per il routing di segnalazione SIP.
- Controllo della disposizione dei media nel payload SDP.
- Supporto per sessioni d'emergenza.
- Invio di informazioni al Charging Collection Function (CCF).

3.2.3 AS(Application Servers)

E' un server SIP che contiene ed esegue i servizi, interfacciandosi con S-CSCF per ottenere informazioni sull'utente tramite SIP. L'AS è normalmente impiegato per supportare diversi tipi di servizi telefonici e per gestire le sessioni multi-client che includono risorse multimediali. A seconda del servizio, l'AS può lavorare in diversi modi: SIP proxy, SIP UA o SIP B2BUA (back-to-back user agent, cioè come user agent verso entrambe le terminazioni della chiamata SIP, responsabile della manipolazione di tutta la segnalazione SIP tra le estremità). Un AS può essere nella home network o in una rete esterna. Nel primo caso userà interfaccia Diameter, nel secondo invece un'interfaccia Mobile Application Part (MAP)[28] . "AS" è il termine usato per riassumere il comportamento di AS SIP, OSA – SCS (Open Service Access – Service Capability Server) o IM-SSF (IP Multimedia Service Switching Function) per offrire accesso ai servizi in base alla Customized Applications for Mobile network EnhancedLogic (CAMEL). Ci possono essere uno o più AS per ogni subscriber e uno o più AS coinvolti nella stessa sessione, con l'obiettivo di fornire servizi multipli allo stesso utente nello stesso tempo.

27 Un numero E.164 è un numero usato in PSTN e in alcune altre reti, definito da raccomandazioni ITU-T, che definisce il piano di numerazione internazionale delle pubbliche telecomunicazioni [24].

28 MAP è un protocollo di livello applicativo SS7 che costituisce il livello applicativo per i vari nodi in reti mobili GSM e UMTS e reti GPRS per comunicare gli uni con gli altri, fornendo così servizi agli utenti di telefonia mobile [25].

3.2.4 MRF (Media Resource Function) e Gateways

Queste entità non vengono analizzate nel dettaglio in quanto non sono utili per gli scopi della tesi, ma menzionate per completezza.
Il MRF si occupa della gestione dei media nella home network. E' usata per processare i dati multimediali,per realizzare conferenze multimediali di chat con sessioni di lavoro collaborative, conversioni Text-To-Speech (TTS) e riconoscimento del parlato, conversione in tempo reale di dati multimediali con codifiche diverse. Ogni MRF è diviso in due unità funzionali.
I gateways sono tutte le entità che permettono alla piattaforma di interfacciarsi con il resto della rete.

3.3 Implementazione e servizi IMS

Si analizzano ora altri aspetti di IMS. Per cominciare, si vedranno i protocolli impiegati,inclusi alcuni accenni alle procedure di identificazione e tariffazione, e poi un sommario dei principali servizi forniti da IMS.
I protocolli usati in IMS possono essere organizzati in tre principali gruppi: protocolli di Segnalazione, di Sicurezza, e di gestione dei Media. Ai fini del lavoro di tesi sono interessanti solo quelli di segnalazione e di gestione dei media, per cui non verrà fatta l'analisi di Diameter, usato per la Sicurezza, mentre ci si soffermerà brevemente su SIP e SDP per quanto riguarda la segnalazione e su RTP [17] per la gestione dei Media. In figura 3.4 si ha una rappresentazione dell'uso di SIPin una piattaforma IMS.

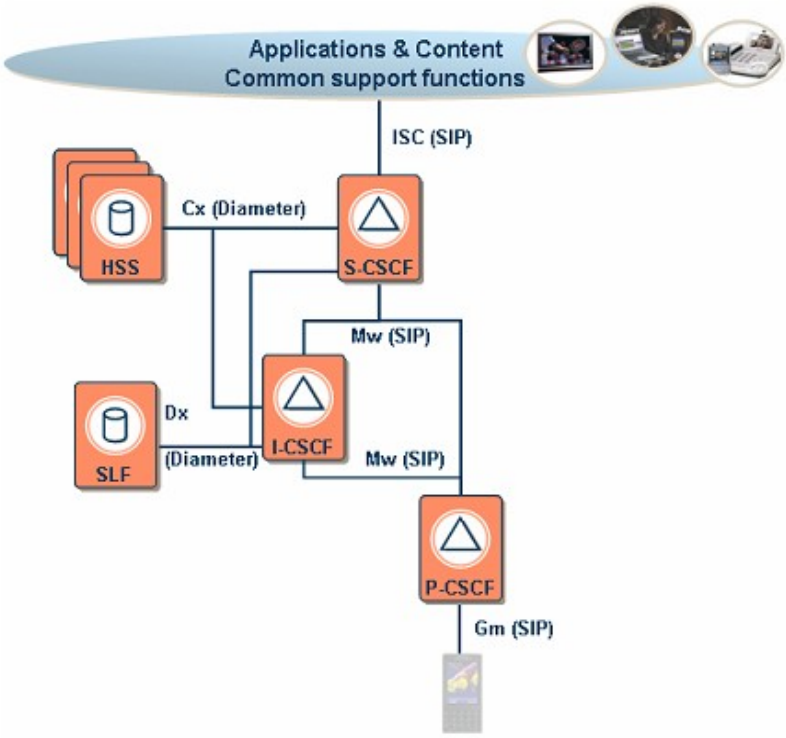


Fig.3.4: Uso del protocollo SIP in IMS

3.3.1 Protocolli di Segnalazione

I protocolli di segnalazione vengono usati per identificare il metodo di "encapsulation" delle segnalazioni che identificano lo stato delle comunicazioni tra due terminali.

3.3.1.1 SIP – Session InitiationProtocol

SIP [3] è uno standard IETF ed è usato unitamente ad altri protocolli quali il Session DescriptionProtocol (SDP) e il Real Time Streaming Protocol (RTSP [17]). SIP è un protocollo di segnalazione di chiamata e gestisce il set up delle sessioni multimediali, il loro tear down e la supervisione. In teoria, SIP può essere usato con qualsiasi protocollo di trasporto di dati real time, ma in pratica si usa sempre RTP.
SIP definisce due categorie di entità: client (User Agent client, un'applicazione che invia richieste SIP) e server (un'applicazione che risponde alle richieste). E' quindi

chiaramente basato sulla classica architettura a logica distribuita client/server.
Nelle stessa unità fisica ci possono essere sia client che server. In SIP ci sono quattro tipi di servers: proxy server (riceve le richieste e le gestisce, inoltrandole al corretto server o endpoint, abilitando funzioni quali call forwarding, time-of-dayrouting, follow me..), redirect server (riceve richieste SIP ed effettua traduzione di indirizzo), user agent server (tipicamente in terminali utente, riceve le richieste di chiamata e risponde ad esse) e registro (un server che accetta le richieste di registrazione).
SIP è molto semplice e flessibile. Non gestisce direttamente i media; lo fanno gli utenti attraverso gli appositi campi personalizzabili. I messaggi SIP sono in formato testo: questo lo rende più chiaro, ma richiede un maggiore impiego di banda. I messaggi SIP hanno un campo, chiamato "message body", che viene lasciato libero per SDP o altro protocollo. Per esempio, può essere usato per trasportare messaggi ISUP per interoperare con reti PSTN.
Metodi SIP di base sono:

- INVITE per aprire una sessione, specificando identità dell'utente e tipo di media;
- ACK per rispondere ad una richiesta;
- OPTIONS per conoscere le capacità del server, che tipo di funzionalità e media supporta, ecc.;
- BYE per chiudere una sessione;
- CANCEL per terminare una transazione in corso;
- REGISTER per realizzare la registrazione di un client US presso un server SIP;
- INFO per trasferire informazioni quali toni multifrequenza, informazioni di tariffazione, messaggi di segnalazione non - SIP durante una sessione.

Si può vedere un esempio di setup di chiamata mediante SIP in Fig. 3.5.
Dopo l'inizio della sessione, che può essere un po' più complessa se la chiamata passa attraverso uno o più proxies, in SIP generalmente si ha l'assegnazione della descrizione della sessione (usando SDP), la gestione della sessione (una volta che la connessione viene stabilita, gli endpoints scambiano direttamente i media streams), e la terminazione della sessione.

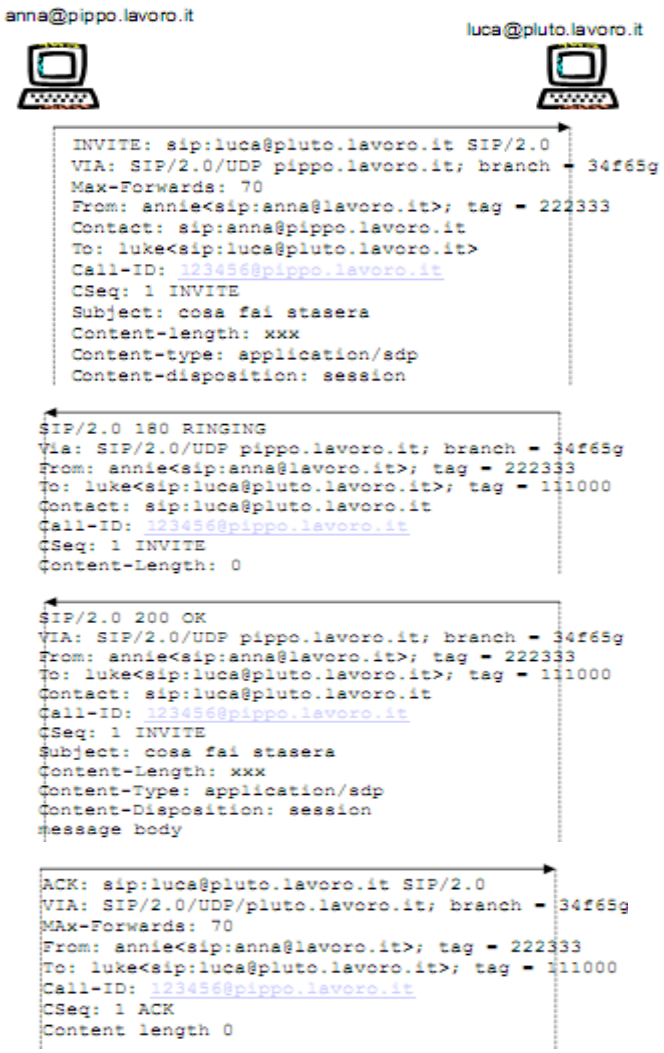
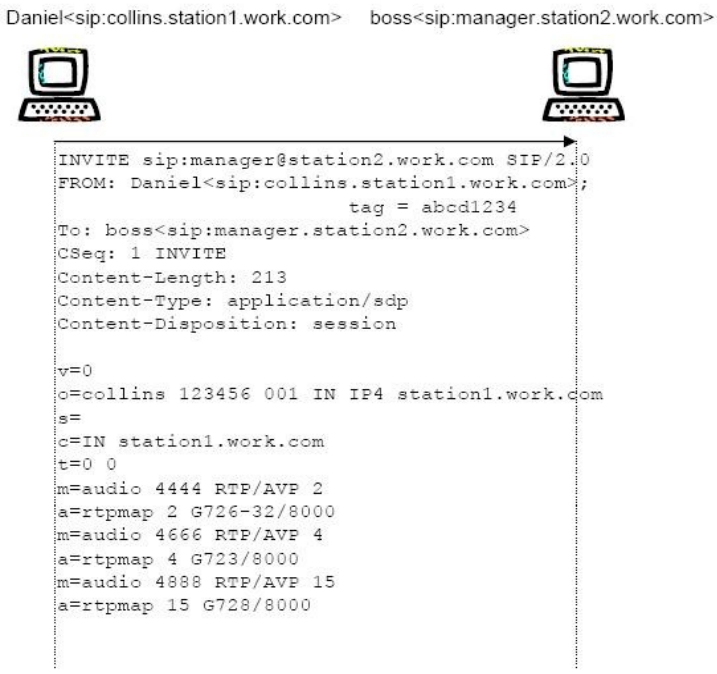


Fig.3.5: Esempio di chiamata SIP.

3.3.1.2 SDP – Session DescriptionProtocol

SDP [18] è un protocollo per la descrizione dei media, che non gestisce il loro trasporto, quindi deve essere usato con un protocollo adatto al trasporto dei media sul piano utente, per esempio RTP. Per SDP una sessione è formata da uno o più media streams. La descrizione fornita riguarda ogni stream della sessione. SDP, come SIP, usa messaggi in formato testo.

In Fig.3.6 si ha un esempio di chiamata SIP con SDP:



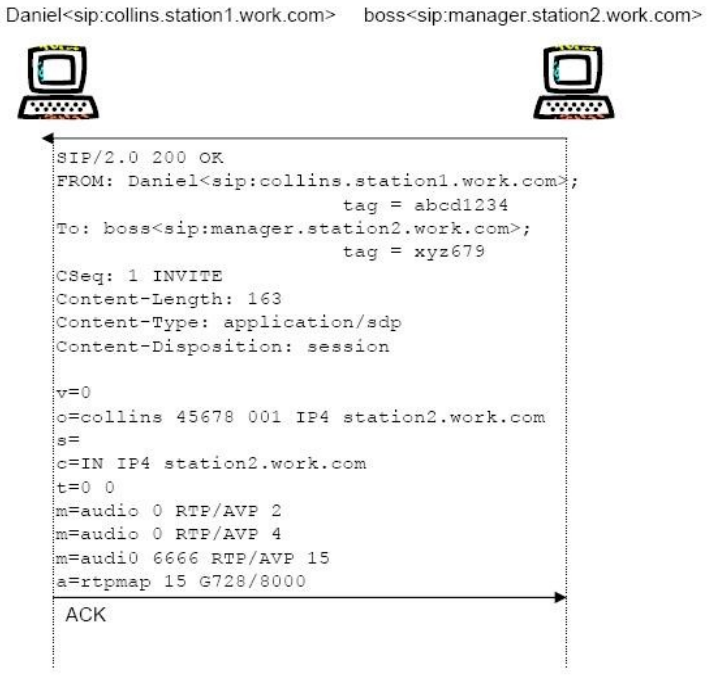


Fig. 3.6: Esempio di chiamata con SDP.

Per capire meglio l'esempio, è necessario chiarire il significato dei vari campi. Si ricorda che l'informazione SDP è una sequenza di righe del tipo: *field* = *value*.
"*field*" è un carattere, e le righe obbligatorie sono:

- v = versione del protocollo; è il segnale che inizia la descrizione di una sessione.
- o = origine ed identificativo di una sessione.
- s = nome della sessione; stringa di caratteri, utile nelle sessioni in conferenza.
- t = start e stop time della sessione, usato solo in casi particolari, quando le parti sanno quando finirà la chiamata. Se non si ha questa informazione si imposta t = 0.
- m = tipo del media, protocollo di trasporto, porta utilizzata, tipo di payload.

Poi ci sono alcune righe opzionali:

- i = informazioni aggiuntive al nome sella sessione.
- u = per specificare una URI, se necessario.
- e = indirizzo email, se necessario.
- p = numero di telefono, se necessario.
- c = dati della connessione a basso livello.
- b = banda in kbit/s.
- r = in sessioni schedulate, specifica ogni quanto ripetere la sessione.
- z = aggiustamenti "timezone", per sincronizzare la notazione dell'orologio.
- k = dati su chiave di crittazione.
- a = attributi tradizionali.

Ogni campo può avere dei sottocampi, che non vengono qui menzionati.
Si ricorda che i messaggi SDP sono inclusi negli INVITE e nelle relative risposte, inclusi nei message body dei relativi messaggi SIP, con il quale SDP interagisce minimamente.
SDP può essere usato, in interazione con SIP, per riservare risorse di canale.

3.3.2 Protocollo di gestione dei Media

Per distribuire i media, IMS impiega il Real time Transport Protocol (RTP) e il Real time Transport Control Protocol (RTCP), che fa parte di RTP.

RTP- Real time Transport Protocol

RTP [27] esegue funzioni di trasporto end - to - end in rete adatte ad applicazioni che prevedono la trasmissione di dati in real-time, come audio e video su servizi di rete multicast o unicast. RTP fornisce la distribuzione end-to-end di servizi per dati con caratteristiche di real-time. Questi servizi includono: identificazione del tipo di payload, numerazione della sequenza, time stamping e controllo della distribuzione. RTP non presuppone che la rete sottostante sia disponibile e consegni i pacchetti in sequenza. I numeri di sequenza inclusi in RTP permettono al ricevente di ricostruire la sequenza di pacchetti inviata dal mittente. RTP consiste di due parti strettamente legate:il Real time Transport Protocol, per trasportare dati con proprietà real-time, e il Real time Transport Control Protocol, per controllare la qualità del servizio e portare le informazioni relative ai partecipanti nella sessione nascente. RTCP è basato sulla trasmissione periodica di pacchetti di controllo a tutti i partecipanti alla sessione, usando lo stesso meccanismo di distribuzione dei pacchetti dati.

In conclusione, si può considerare che nella nuova emergete cultura della comunicazione che ruota attorno alla condivisione della propria vita di tutti i giorni con gli altri, in qualsiasi luogo, momento, su qualsiasi dispositivo, IMS è la scelta naturale verso cui indirizzare la trasformazione. IMS combinaqualità e interoperabilità delle telecomunicazioni con il rapido ed innovativo sviluppo di internet, rendendo i valori unici dell'industria delle telecomunicazioni rapidamente disponibili per la comunità.

Adesso che si ha una visione d'insieme della piattaforma IMS, si può brevemente introdurre il prototipo che è stato usato nel lavoro di tesi, ovvero Open IMS Core.

3.4 Open IMS Core

Open IMS Core [29] è una implementazione open source delle varie entità che costituiscono il core del sistema IMS, ovvero i CSCFs e un HSS (in forma semplificata e alleggerita). Tutti i componenti sono basati su software open source (ad esempio SIP Express Router (SER) o MySQL). Open IMS Core costituisce il centro dell' Open IMS Playground @ FOKUS[29]. L'Open IMS Playground è un ambiente di test per nuove tecnologie IMS basate su implementazioni open source ad aperto ad accogliere idee e proposte[30].

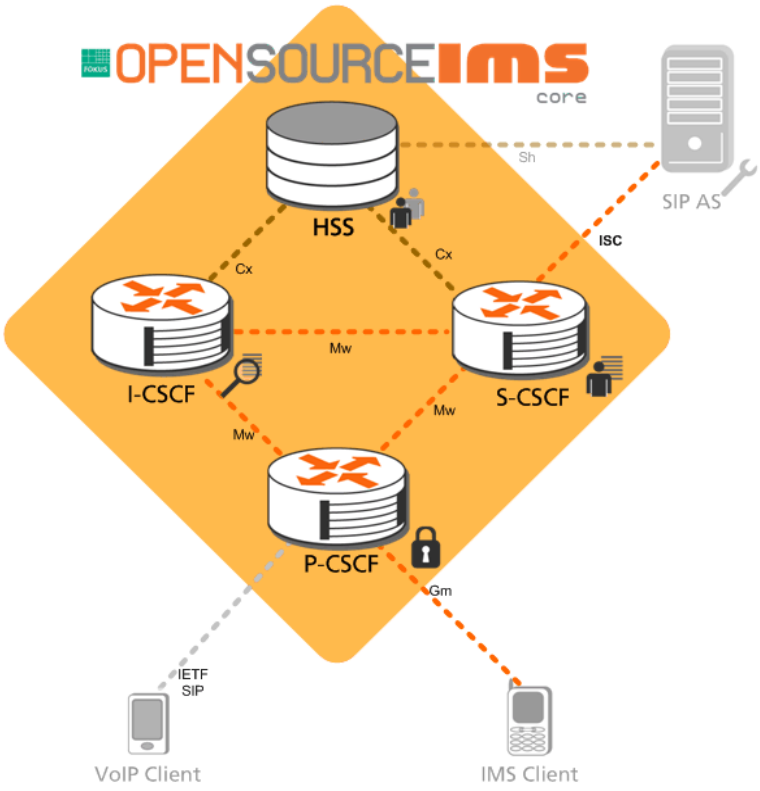


Fig.3.7: Elementi costitutivi della piattaforma Open IMS Core.

29FOKUS sta per "Fraunhofer Institute for Open Communication Systems".E' un centro di ricerca che si occupa della formulazione di soluzioni per partner industriali nell'ambito di tecnologie di telecomunicazione, architetture e protocolli di rete, sistemi di IT, ecc [26].

30 Tutte le informazioni dettagliate relative a Open IMS Playground sono reperibili sul sito ufficiale http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground.

In Fig. 3.7 si vedono tutte le parti che costituiscono il sistema (HSS, I-CSCF, S-CSCSF, P-CSCF) e alcuni esempi di entità con cui è possibile l'interazione.
Per gli scopi della tesi, ovvero gestire le chiamate d'emergenza, serve integrare la piattaforma Open IMS Core con il ramo di gestione delle emergenze. Questo contiene due nuove parti: E-CSCF (Emergency CSCF) e LRF (Location Retrieval Function), le quali sono istanze di SIP Express Router, come gli altri CSCFs dell'architettura. L'implementazione è basata su specifiche tecniche rilasciate da 3GPP (TS 23.167, TS 24.229, TS 29.228). Le implementazioni P/I/S-CSCF sono state estese per rilevare registrazioni di emergenza, nel cui caso I-CSCF aggiunge un flag nella richiesta di autorizzazione Diameter in modo che HSS ignori le restrizioni di roaming. Il P-CSCF è inoltre in grado di identificare le chiamate d'emergenza ed inoltrare quindi la richiesta iniziale di INVITE d'emergenza ad un E-CSCF appartenente allo stesso dominio IMS. L'E-CSCF ha il compito di scoprire il PSAP (Public SafetyAnswering Point) più appropriato (ad esempio la centrale di polizia più vicina), e ad esso inoltrare la chiamata.

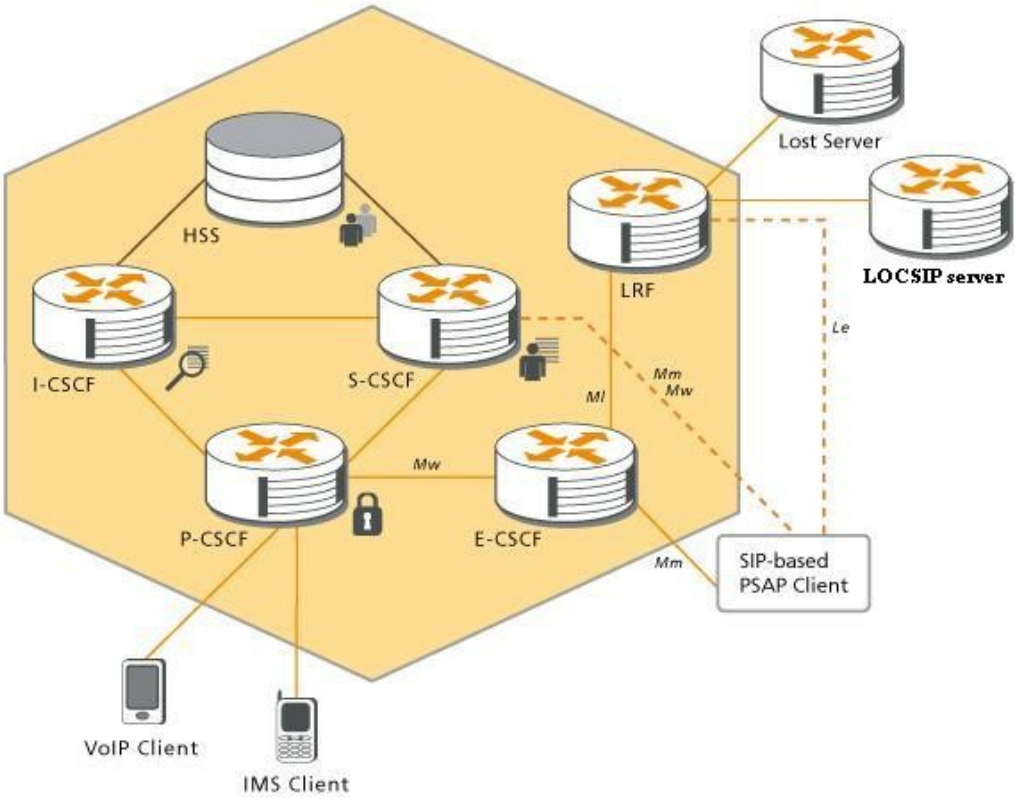


Fig.3.8: Architettura della piattaforma Open IMS Core comprensiva di ramo per la gestione delle emergenze.

L'E-CSCF mantiene inoltre le statistiche relative alle chiamate, ovvero memorizza alcune informazioni, come stato dei dialoghi, durata, chiamata anonima o no, ecc. Attualmente sono supportati solo PSAP basati su SIP. La sessione di callback per utenti registrati usa l'interfaccia da PSAP a S-CSCF nello stesso modo di una chiamata normale verso il chiamante. Per il momento non è implementata l'interrogazione di localizzazione dal PSAP al LRF (interfaccia Le).

In Fig.3.8 si ha una visione d'insieme del sistema Open IMS Core completo del ramo di gestione delle emergenze.

Quando viene generata una chiamata d'emergenza, l'utente può essere in una delle seguenti situazioni:

- L'utente ha già effettuato una registrazione regolare e non è in roaming: può generare direttamente una chiamata d'emergenza.
- L'utente non è registrato: indipendentemente dallo stato di roaming, prima deve effettuare una registrazione d'emergenza e poi può generare la chiamata.
- L'utente è in roaming e nonostante abbia precedentemente effettuato una registra-

zione regolare deve effettuare una registrazione d'emergenza prima di fare la chiamata.

- L'utente non ha abbastanza credenziali per autenticarsi: proverà ad effettuare una cosiddetta "chiamata d'emergenza anonima".

Per essere riconosciuta come parte di una registrazione d'emergenza, la richiesta di REGISTERdeve contenere nel Contactheader un parametro SIP URI di "sos", come specificato dal documento "draft-patel-ecrit-sos-parameter" di IETF. Un esempio si questo URI è:

```
Contact:"Alice" <sip:alice@example.com;sos>;q=0.7;expires=3600
```

Il P-CSCF rifiuterà tutte le chiamate che non usino un contatto registrato per scopi d'emergenza, rispondendo con un 403 (Forbidden). Se il P-CSCF non supporta servizi d'emergenza o se non è configurato per ricevere la chiamata nella forma in cui la recepisce (anonima, nel caso specifico) risponderà invece con un 503 (Service Unavailable). Se il P-CSCF riceve una chiamata d'emergenza che non coincide con nessuno dei casi appena menzionati, risponde con 380 (Alternative Service).
Una richiesta di INVITE viene considerata come parte di una chiamata d'emergenza se la URI richiesta è una delle URNs definite da IETF nel documento RFC 5031. La tabelle contenente gli URN definiti viene riportata in Fig. 3.9. La richiesta di INVITE d'emergenza verrà inoltrata all'E-CSCF. Usando una richiesta OPTIONS, l'E-CSCF interrogherà LRF per conoscere l'URI del PSAP adatto al caso, impostando:

- L'URI richiesto all'URI utente. Se la chiamata è anonima, l'E-CSCF imposterà come URI richiesto: `sip:anonymous@domain.org`, in modo che LRF lo possa riconoscere come tale.
- Il nome del servizio nel campo "Service" dell' header.
- L'informazione di localizzazione (se presente) nel corpo del messaggio.

```
Service                      Reference   Description
-------------------------------------------------------------------
```

-counseling	RFC	5031	Counseling services
counseling.children	RFC	5031	Counseling for children
counseling.mental-health	RFC	5031	Mental health counseling
counseling.suicide	RFC	5031	Suicide prevention hotline
sos	RFC	5031	Emergency services
sos.ambulance	RFC	5031	Ambulance service
sos.animal-control	RFC	5031	Animal control
sos.fire	RFC	5031	Fire service
sos.gas	RFC	5031	Gas leaks and gas emergencies
sos.marine	RFC	5031	Maritime search and rescue
sos.mountain	RFC	5031	Mountain rescue
sos.physician	RFC	5031	Physician referral service
sos.poison	RFC	5031	Poison control center
sos.police	RFC	5031	Police, law enforcement

Fig. 3.9 : Tabella degli URN definita nel RFC 5031.

L'informazione di localizzazione inclusa nella richiesta di INVITE iniziale è considerata essere "Location-by-value", come definito nel draftIETF "draft-ietf-sip-location-conveyance" [30]. Sia E-CSCF che LRF esigono un formato geopriv PIDF[31] dell'oggetto di localizzazione (come descritto in RFC 5491) o quello civico (come descritto in RFC 5139). In alternativa E-CSCF invia al chiamante come risposta un 424 (Bad Location Information).

Se LRF riceve un'informazione di localizzazione da E-CSCF, può essere configurato per interrogare il server LoST per conoscere l'URI del PSAP appropriato. LoST (Location to Service Translation Protocol) è stato analizzato nel capitolo precedente. Si ricorda che è un protocollo che può essere usato per mappare informazioni di

31 Geopriv è un formato ad oggetti definito nella RFC 4119 atto al trasporto di informazioni geografiche su Internet che estende il PIDF (Presence Information Data Format), progettato per comunicare informazioni di presenza con proprietà di riservatezza [31].

localizzazione e tipo di servizio su un certo URI (la spiegazione di come avviene nel dettaglio è nella RFC 5222).

Nel caso in cui venga determinato l'URI, viene inviata una risposta 200 OK a LRF contenente:

- L'URI del PSAP nell'nell' "PSAP-URI";
- L'ESQK assegnata (Emergency Service Query Key, specificata in TS 23.167) nel campo "ESQK" dell' header;
- L'informazione di localizzazione.

Altrimenti, E-CSCF riceverà un messaggio d'errore.
LRF ha inoltre il compito di memorizzare, per ogni chiamata non anonima, un certo numero di informazioni: l'URI SIP, l'ultima informazione di localizzazione conosciuta, il nome del servizio richiesto (ad esempio "urn:service:sos"), l'URI SIP del PSAP e l'ESQK allocato.

Quando LRF riceve una risposta del tipo 2XX, l'E-CSCF inoltra l'INVITE d'emergenza al PSAP. In caso di risposta "errore", l'E-CSCF può essere configurato in modo da usare l'opzione Last Routing, ovvero scegliere un PSAP di default.
Prima di inoltrare l'INVITE, l'E-CSCF dovrà:

- Sostituire l'URI richiesto e il campo "To" dell'header con l'URI del PSAP;
- Aggiungere l'header ESQK;
- Aggiungere l'informazione di localizzazione inoltrata da LRF , se presente nella risposta.

Se non è configurato nessun PSAP di default, al chiamante verrà inviata una risposta d'errore.
E-CSCF memorizza tutti gli scambi di informazioni che avvengono all'interno del dialogo d'emergenza (a meno di errori).

Capitolo 4

Algoritmi decisionali e parametri di valutazione

Fino a qui sono state descritti PICO, ECRIT, LoST e IMS (con OpenIMSCore), ovvero tutte le entità e strutture già esistenti da cui si è partiti per svolgere il lavoro di tesi. In questo capitolo si passa all'esposizione di ciò che è stato creato come lavoro di tesi.

Si ricorda che l'obiettivo della tesi è la realizzazione di un sistema efficiente per l'instradamento delle chiamate d'emergenza in ambiente IMS. Tenendo conto delle specifiche fornite dal progetto PICO, sfruttando come punto di partenza il lavoro svolto da ECRIT, in particolare studiando LoST, si è proseguito nel lavoro di tesi con l'obiettivo di produrre un prototipo di sistema funzionante da implementare tramite OpenIMSCore. In figura 4.1 si può vedere una schematizzazione della gestione della chiamata d'emergenza che si vuole ottenere: lo User Agent effettua la chiamata d'emergenza (in SIP, questa consiste in un messaggio di INVITE avente come destinatario un numero o URN d'emergenza) verso la piattaforma IMS, la quale riconoscendo il tipo di richiesta, la inoltra al branch di gestione apposito (in OpenIMSCore questo è il blocco E-CSCF), che sceglie il server adatto a cui

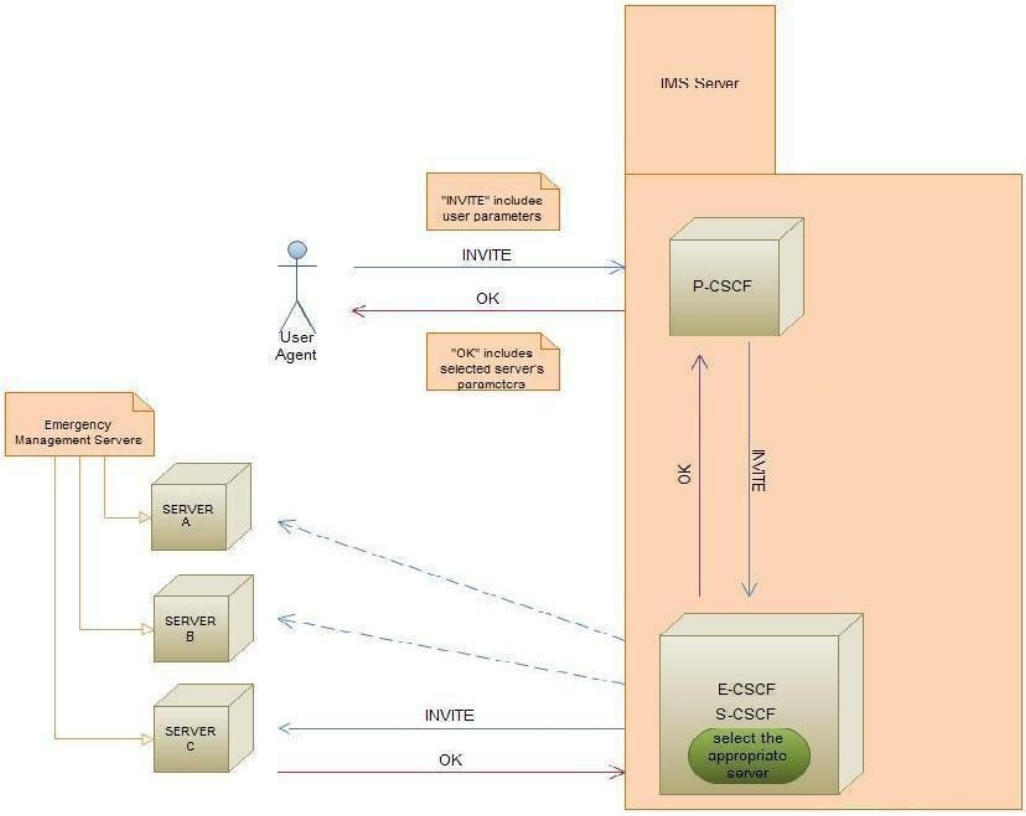


Fig.4.1: Gestione della chiamata d'emergenza.

connettere il chiamante. Nel nostro caso, la decisione verrà presa tramite reindirizzamento alla piattaforma LoST, come spiegato in seguito.

L'efficienza aggiuntiva del sistema qui studiato deriva dalla scelta più ponderata del server a cui connettere il chiamante che richiede l'emergenza; ovvero, non basare l'associazione solamente sulla vicinanza geografica, come avviene attualmente, ma anche sulla considerazione di altri fattori che possono influire sull'efficienza del collegamento.

Con il termine generico "server" si indica la centrale telefonica di una delle strutture adibite alla risposta alle chiamate d'emergenza: ospedali, centri di primo soccorso, caserme di vigili del fuoco, centrali di polizia e altre forze dell'ordine.

La scelta dei fattori influenti è stata fatta considerando il contesto di utilizzo del sistema, analizzando i possibili scenari ed estrapolando le caratteristiche più significative. Nel par.4.1 vengono illustrate le caratteristiche di contesto scelte come determinanti.

Una volta focalizzati i punti da considerare, si definiscono i files XML che il chiamante dovrà inviare alla piattaforma server (P-CSCF, S-CSCF e E-CSCF) per essere associato al server adeguato, dopo che il sistema avrà valutato i campi compilati dall'utente.
Lo step successivo è l'individuazione di algoritmi che permettano di scegliere il server valutando le caratteristiche del client. Questi vengono descritti nel par. 4.2.

4.1 Definizione del contesto

Nello scenario di integrazione operatore-dispositivo a cui si assiste all'interno del progetto PICO è chiaramente molto importante l'aspetto di "context-awareness" , ovvero l' apparecchiatura usata dall'operatore deve essere in grado di fornire dettagli sull'ambiente in cui si sta lavorando per consentire una fornitura di servizio più mirata ed efficace.
Per avere questa contestualizzazione è necessario individuare quali parametri sono decisivi per definire l'ambiente di lavoro.
Nell'ambito del lavoro di tesi sono stati definiti due tipi di identificazione del contesto: uno più essenziale e uno più particolareggiato.
Le macrocategorie (ognuna descritta da diversi parametri) che è necessario valutare per definire il quadro della situazione di appartenenza sono: localizzazione, utente, dispositivo, tempo e tipo di servizio richiesto. A queste si aggiunge quella relativa all'ambiente, nel caso di identificazione più particolareggiata.

Si analizzano ora i campi di cui è composta ogni categoria, sia nel caso essenziale che in quello più esteso:

- Localizzazione: questo parametro ha gli stessi campi in entrambi i casi, definiti in base al protocollo LoST, di cui abbiamo parlato nel capitolo 2.
- Utente: nel caso essenziale, si hanno i campi "nome utente" e "identificativo utente", che sono sufficienti ad identificare univocamente l'operatore che sta usando il dispositivo. Nel caso esteso, si aggiunge il campo "utenti vicini", che può essere utile per stabilire la necessità o meno di inviare ulteriore forza lavoro

sul luogo.

- Dispositivo: per sfruttare appieno le possibili applicazioni implementabili sull'apparecchiatura in dotazione, serve conoscere le sue caratteristiche tecniche, per connetterlo al server più adeguato. Le particolarità da valutare nel caso essenziale sono: tipo di dispositivo, versione di java implementata, sistema operativo, versione del sistema operativo, dimensioni dello schermo (altezza e larghezza, a seconda di queste si stabilisce il grado di definizione delle immagini da adottare), memoria disponibile e tipo di accesso (queste ultime due caratteristiche sono fortemente legate al tipo di applicazioni di cui il dispositivo può usufruire). A queste va aggiunta la localizzazione di altre risorse nelle vicinanze, che avviene nel caso di valutazione estesa del contesto.
- Tempo: l'ora del giorno e la data sono elementi utili per contestualizzare la situazione di soccorso, infatti a seconda delle coordinate temporali fornite si può valutare quale percorso sia preferibile percorrere per raggiungere il luogo interessato o verso quale centro di assistenza indirizzare l'operatore. Questo campo viene integrato con l'informazione relativa al "gmt" (Greenwich Mean Time), e nella contestualizzazione estesa anche con l'informazione di festività del giorno in questione.
- Ambiente: questa parte non è presente nella forma essenziale. Prevede una descrizione sommaria delle condizioni ambientali in cui si trova l'utente, ovvero tipo di area, temperatura, luce, condizioni meteo, livello di rumore.
- Servizio: presente in entrambe le contestualizzazioni, indica il tipo di servizio richiesto dall'utente (soccorso medico, vigili del fuoco, polizia..)

Le categorie appena elencate permettono di fornire una prima descrizione dello scenario, abbastanza essenziale (anche nella forma estesa). Si potrebbero ampliare introducendo altri campi che rendano più dettagliata la descrizione, differenziata a seconda del caso di emergenza di cui si tratta. Ad esempio, se si chiama soccorso in seguito ad un incidente stradale, specificare quante persone sono coinvolte, se ci sono corpi incastrati (e quindi servono i vigili del fuoco),ecc.

In base ai parametri di interesse appena individuati, come lavoro di tesi sono stati stilati due script XML, riportati in seguito, contenenti tutte le informazioni necessarie ad eseguire la corretta associazione PSCD - PSCS; il dispositivo lo invierà al centro direzionale di soccorso al momento della chiamata d'emergenza.

È da precisare che i files qui riportati sono semplificati, anche nella versione "estesa", poiché hanno lo scopo di essere usati nell'implementazione prototipale del sistema, per avere una prima valutazione delle prestazioni. In seguito vedremo quali ulteriori informazioni potrebbero essere richieste (variabili a seconda dei casi).
Entrambi gli XML sono conformi ai principi stabiliti dal protocollo LoST visto in precedenza (cap. 2).
La prima versione (Figura 4.2) riportata è quella più essenziale (vedi par.4.1), mentre la seconda (Figura 4.3) è quella più estesa.
Come si vede, gli elementi essenziali che vengono tenuti in considerazione sono quelli appena spiegati. Ogni elemento è corredato da una breve descrizione.

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceserviceBoundary="value" recursive="true"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:/Users/Franchi/work/Essenz.xsd">

<location id="6020688f1ce1896d" profile="geodetic-2d">
<p2:Point id="point1" srsName="urn:ogc:def:crs:EPSG::4326">
<p2:pos>37.775 -122.422</p2:pos>
</p2:Point>
</location>

<user>
<name>....</name>
<userid>.....</userid>
</user>

<device>
<typeofdevice>...</typeofdevice>
<javaversion>....</javaversion>
<ostype>...</ostype>
<osversion>....</osversion>
<screenheight>....</screenheight>
<screenwidth>....</screenwidth>
<availablememory>....</availablememory>
<accesstype>...</accesstype>
</device>

<time>
<hour>...</hour>
<day>...</day>
      <gmt>...</gmt>
</time>

<service>urn:service:sos.police</service>

</findService>
```

Fig.4.2: XML “essenziale” per la descrizione del contesto.

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceserviceBoundary="value" recursive="true"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:/Users/Franchi/work/xsEsteso.xsd">

<location id="6020688f1ce1896d" profile="geodetic-2d">
<p2:Point id="point1" srsName="urn:ogc:def:crs:EPSG::4326">
<p2:pos>37.775 -122.422</p2:pos>
</p2:Point>
</location>

<user>
<name>....</name>
<userid>.....</userid>
<nearbyusers>.....</nearbyusers>
</user>

<device>
<typeofdevice>...</typeofdevice>
<javaversion>....</javaversion>
<ostype>...</ostype>
<osversion>....</osversion>
<screenheight>....</screenheight>
<screenwidth>....</screenwidth>
<availablememory>....</availablememory>
<accesstype>...</accesstype>
<nearbyresources>....</nearbyresources>
</device>

<time>
<hour>...</hour>
<day>...</day>
      <gmt>...</gmt>
<festivity>....</festivity>
</time>

<environment>
<typeofarea>.....</typeofarea>
<temperature>...</temperature>
<lighting>....</lighting>
```

```
<weatherconditions>.....</weatherconditions>
<noiselevel>.....</noiselevel>
</environment>


<service>urn:service:sos.police</service>

</findService>
```

Fig.4.3: file XML "esteso" per la descrizione del contesto.

Come si accennava in precedenza, queste versioni di file descrittivi del contesto sono solo approssimazioni semplificate. In realtà, le informazioni potrebbero essere molto più dettagliate, per permettere un'automazione totale del servizio di soccorso. Ad esempio, se un civile si trovasse in presenza di un incidente stradale,chiamando i soccorsi potrebbe istantaneamente specificare quante persone sono coinvolte, se qualche corpo è incastrato (e perciò rendere necessario l'intervento dei vigili del fuoco), e via dicendo.
Se invece la chiamata è effettuata da un medico o paramedico, egli potrebbe indicare se sia necessario l'intervento di unità speciali (cardiologiche, neurologiche, ortopediche, ecc..).
Stessa cosa per una chiamata destinata ai vigili del fuoco: l'indicazione di fiamme o allagamento porterebbe all'immediata sospensione di gas o energia elettrica in zona.
Questi sono solo alcuni esempi, ma le informazioni possono essere aumentate a piacimento per lasciare meno indeterminazione possibile e fornire un servizio sempre più efficiente.

4.2. Algoritmi di selezione

Quando E-CSCF riceve la richiesta di inizio di chiamata d'emergenza, ovvero l'INVITE, deve estrapolare le informazioni interessanti in essa contenute ed usarle per effettuare la scelta di associazione migliore possibile.
Sono stati esaminati precedentemente gli aspetti del contesto che vanno tenuti in considerazione per ottenere risultati soddisfacenti. Il problema è come tenerne conto, ovvero trovare l'algoritmo decisionale.
Gli algoritmi formulati in questo lavoro di tesi sono elencati in seguito.

4.2.1 Algoritmo ad eliminazioni successive

Una volta valutato il tipo di servizio richiesto (polizia, vigili del fuoco, soccorso medico), si avrà un sottoinsieme di PSAP possibili a cui associare il chiamante.
Da questo gruppo dovrà essere scelto un solo PSAP. Nell'algoritmo ad eliminazioni successive, si procede eliminando progressivamente le entità meno idonee.
Più dettagliatamente: una volta stabilita la macrocategoria di tipo di servizio richiesto, si valutano localizzazione, tipo di dispositivo in uso ed ora del giorno.
Per ognuna di queste caratteristiche il server ha a disposizione dei database da consultare. In quello riguardante la localizzazione, si avrà per ogni zona l'elenco dei PSAP presenti.
Quindi, scelta la macrocategoria, in base alle informazioni di localizzazione fornite dal chiamante, il server consulterà il database di localizzazione ed eliminerà tutti i PSAP non presenti né nella zona in cui si trova il chiamante né nelle (ad esempio) quattro più vicine.
Si valuta poi il database relativo al dispositivo in uso: tutti i PSAP non compatibili con quello utilizzato dal chiamante vengono eliminati dalla lista.
Nel caso di implementazione di sistema di base (ovvero usando il modello di XML di Figura 4.1) resta da valutare solo il database relativo al tempo. A seconda dell'ora del giorno in cui viene effettuata la richiesta di soccorso, si individua il PSAP più

velocemente raggiungibile tra quelli rimasti.

Se venisse implementata la forma estesa, prima della scelta finale in base al tempo, si toglierebbero dall'elenco anche i PSAP non raggiungibili in modo sicuro a seconda delle condizioni meteo. Inoltre, se l'utente chiamante fosse un medico e disponesse di altri medici o paramedici nelle vicinanze (il tutto definito dal campo "user") si potrebbero considerare più centri anche se meno vicini, dato che probabilmente il requisito di velocità di intervento sarebbe attenuato.

In Fig.4.4 si può vedere il diagramma di flusso riassuntivo dell'algoritmo ad

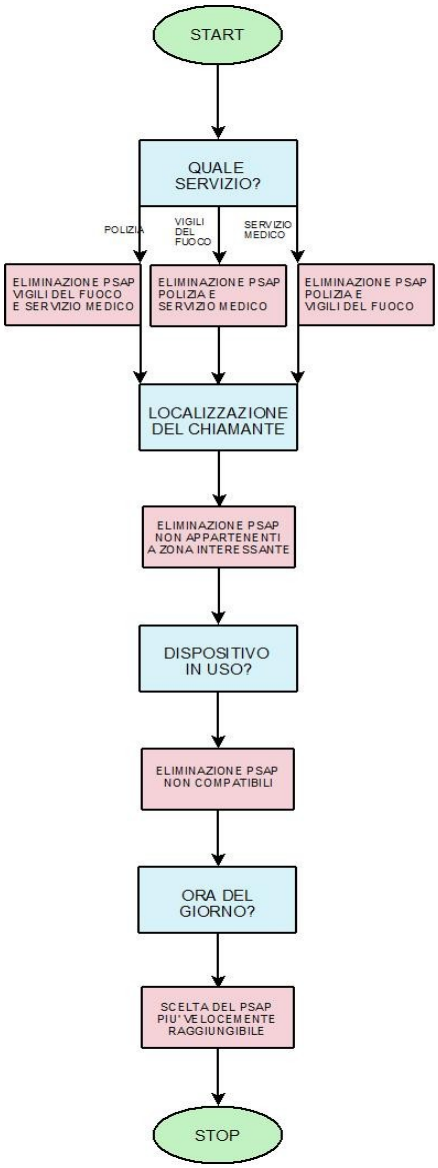


Fig.4.4: Diagramma di flusso relativo all'algoritmo ad eliminazione (caso "essenziale").

eliminazione nel caso di contestualizzazione “essenziale”. Eventuali blocchi di domande e azioni supplementari andrebbero poste prima del blocco “ORA DEL GIORNO?”, che è la domanda discriminatoria tra le parti rimaste.

4.2.2 Algoritmo a maggioranza

I criteri da valutare sono gli stessi dell’algoritmo precedente, ma stavolta anziché procedere eliminando man mano i meno idonei, si elegge il migliore a maggioranza. Ovvero, per ogni categoria valutata vengono selezionati (e contrassegnati, riportandoli in un nuovo database) i quattro (ad esempio, ma potrebbero essere di più o di meno) candidati migliori. Il PSAP che sarà risultato idoneo per più aspetti verrà selezionato. In caso di parità, si può usare come discriminante la valutazione del tempo di percorrenza.

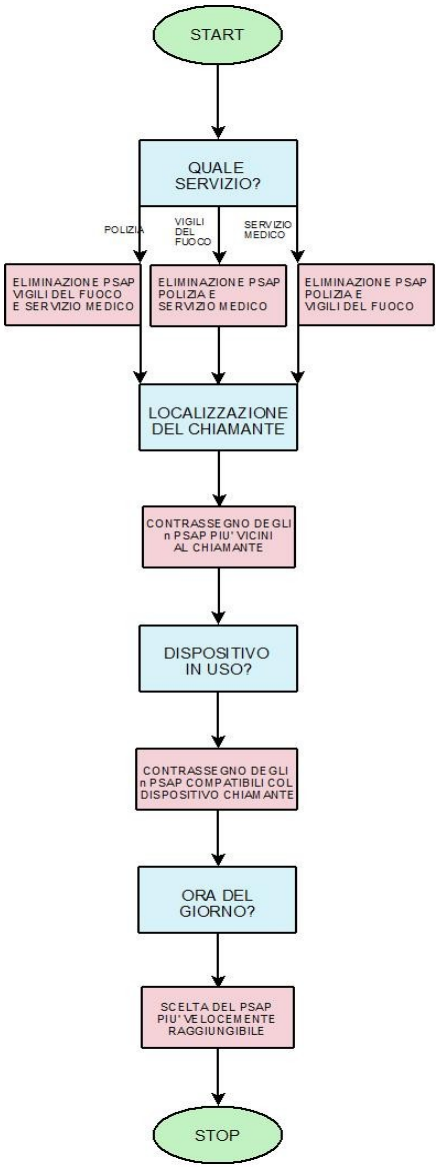


Fig.4.5:Diagramma di flusso relativo all'algoritmo a maggioranza (caso "essenziale")

Anche in questo caso, a seconda della quantità di informazioni inviate dal chiamante si avrà una scelta più o meno articolata.

In Fig.4.5 si ha una rappresentazione tramite diagramma di flusso dell'algoritmo appena descritto.

4.2.3 Algoritmo a pesi

In questo algoritmo si suppone di assegnare del "pesi" ai diversi PSAP a seconda delle caratteristiche possedute.
Dopo la ovvia selezione della macrocategoria di servizio in base alla richiesta dell'utente, si inizia valutando la localizzazione.
Se il PSAP appartiene alla stessa zona dell'utente, gli si assegna peso "0", se si trova in una zona direttamente confinante avrà peso "1", se è ancora più lontano "2", e via così, crescendo i pesi a seconda delle distanze.
Si valuta poi il tipo di dispositivo in uso: se il PSAP è perfettamente compatibile si assegna peso "0", se è compatibile ma non si riescono a sfruttare tutte le caratteristiche dell'uno o dell'altro (sistema operativo precedente rispetto all'altro, risoluzione dell'immagine penalizzante per una delle due parti, e così via..) allora il peso assegnato sarà "1", e via via crescente con l'aumento delle diversità.
A questo punto si valuta la tabella del tempo di percorrenza in base all'ora del giorno: il PSAP più velocemente raggiungibile avrà peso "0", il secondo "1", e così via.
Alla fine, il PSAP che ha totalizzato il peso inferiore viene scelto come servente della chiamata in corso.
In Fig.4.6 si vede una rappresentazione tramite diagramma di flusso dell'algoritmo appena descritto.

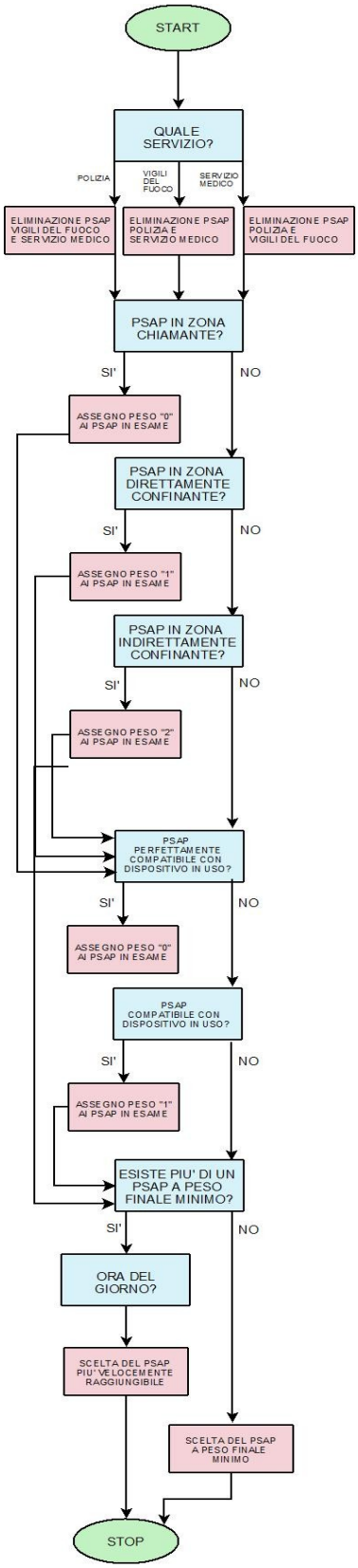


Fig.4.6:Diagramma di flusso relativo all'algoritmo a maggioranza (caso "essenziale")

4.3 Valutazione della validità degli algoritmi

Per verificare che gli algoritmi formulati siano validi, è necessario individuare i parametri di valutazione fondamentali del sistema. È necessario cioè trovare alcune funzioni che permettano l'analisi delle prestazioni di servizio erogato dal sistema. Si devono raccogliere e osservare i dati statistici al fine di misurare la qualità del servizio percepita dall'utente.
In generale, lo studio e l'analisi delle performance di una rete di telecomunicazioni si basano sulla definizione di indicatori che permettono di confrontare diversi sistemi di comunicazione. Nel nostro caso, si confronteranno i diversi algoritmi implementati.
Si era pensato inizialmente di sfruttare alcune classificazioni fatte dallo standard ITU-T M-3400, che divide tutte le funzioni svolte da un'infrastruttura di rete in macrocategorie di gestione.
Come si capirà meglio nel seguito, questo tipo di valutazione non si adattava del tutto alle esigenze di questo lavoro di tesi, poiché l'interesse non è incentrato sulle performance della piattaforma IMS nella gestione delle registrazioni, chiamate, e così via: quello che serve valutare è il funzionamento dei metodi proposti per la gestione innovativa delle chiamate d'emergenza.

Verrà effettuata in primo luogo una valutazione sui tempi di risposta del server LoST modificato, in tutti i casi possibili, ma questo non è sufficiente per avere un quadro completo della situazione. Pertanto si è dovuta introdurre una valutazione logica del funzionamento del sistema, osservando caratteristiche non direttamente misurabile ma determinanti per gli scopi prefissati.
In particolare, sono state individuate come valutazioni di interesse quelle relative a tre aspetti principali: la varietà di scelta offerta da ogni algoritmo (intesa come quantità di opzioni considerate da ogni metodo), la difficoltà di gestione del database relativo all'algoritmo in questione (come si vedrà nel prossimo capitolo, a seconda dei metodi implementati si usano versioni differenti di database), e la probabilità di risposte equivalenti (che diminuisce con la complessità della valutazione effettuata dal metodo).

Nel seguente capitolo verranno illustrati il lavoro di implementazione e i risultati ottenuti corredati dalle valutazioni appena menzionate, sia quantitative che qualitative, relativamente ad ogni metodo.

Capitolo 5

Implementazione e Risultati

Finora sono stati analizzati l'ambiente di sviluppo definito per il progetto, i protocolli usati e gli algoritmi formulati per risolvere il problema oggetto di tesi, ovvero l'assegnazione ottima di server di sicurezza pubblica al singolo utente che richiede l'intervento d'emergenza.

Il lavoro di tesi ha ovviamente compreso anche l'implementazione di tale sistema, per verificarne la validità dei risultati. Per raggiungere tale scopo sono state utilizzate diverse entità, creando una piattaforma di lavoro unificata che gestisce la chiamata dall'inizio, compresa la registrazione dell'utente.

Nello specifico, il sistema è composta da: uno User Agent creato ad hoc per soddisfare le esigenze di progetto, la piattaforma OpenIMSCore (descritta nel Cap.2) e il blocco LoST Server, del quale faremo una breve analisi qui di seguito.

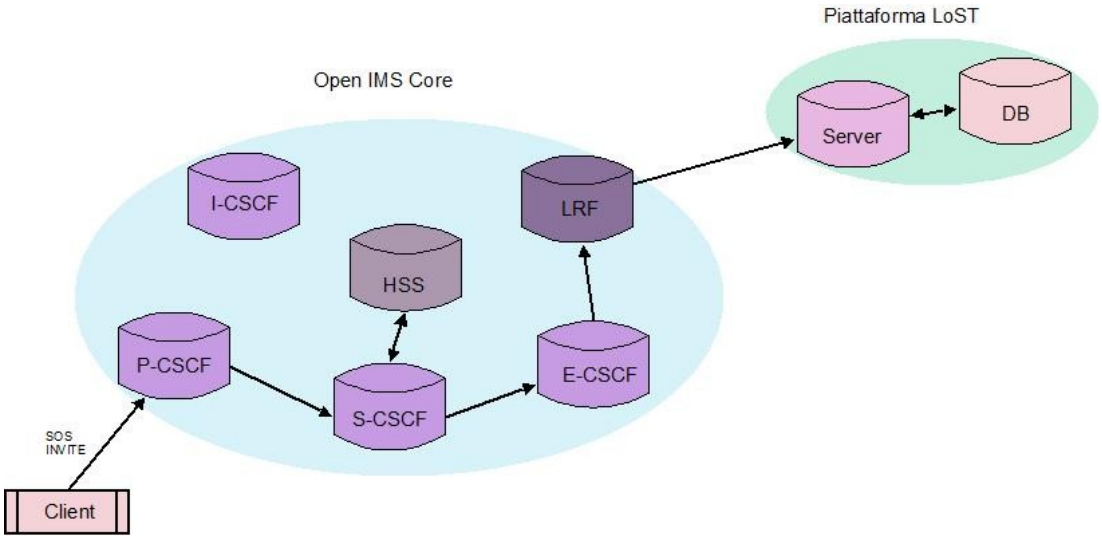


Fig. 5.1: Schema generale del sistema implementato.

In Figura 5.1 si ha uno schema generale del sistema implementato: lo user agent invia la richiesta di chiamata d'emergenza (SOS INVITE) alla piattaforma Open IMS Core; in particolare, come spiegato nel capitolo 3, la richiesta viene ricevuta dal Proxy-CSCF e inoltrata al Serving CSCF, che si occupa della consultazione del database degli utenti (HSS), riconoscendo la chiamata come chiamata d'emergenza. A questo puntoil S-CSCF la inoltra all'Emergency-CSCF, che consulta LRF per avere una risposta sul servente da associare al chiamante. LRF a sua volta va a consultare la piattaforma LoST, che gestisce la chiamate secondo gli algoritmi presentati nel capitolo precedente, restituendo l'URN di servizio adeguato, con cui viene instaurata la comunicazione.

Il lavoro di implementazione non è stato banale, ha richiesto l'approfondimento della conoscenza del linguaggio Java e del funzionamento di PostgreSQL[32], oltre all'analisi dettagliata del funzionamento della piattaforma OpenIMSCore con emergency branch (non del tutto spiegato nella documentazione) e del LoST server (la cui struttura è stata ricavata dalla lettura dei file sorgenti).

Si vanno ora ad analizzare più precisamente le varie parti che compongono il sistema.

32PostgreSQL è un completo database relazionale ad oggetti rilasciato a licenza libera, sviluppato dal PostgreSQL Global Development Group [32].

5.1 User Agent

Inizialmente si sono valutati gli User Agent esistenti che potevano essere usati (adattandoli) all'interno del progetto. Gli UA considerati sono stati: IMS Communicator[33] , UCT IMS Client[34], Mercuro[35]e alcune versioni di Android[36].
Per essere impiegati avrebbero dovuto essere open source, per poterli adattare agli scopi del progetto, e, ovviamente, già predisposti all'interoperabilità con la piattaforma IMS.
IMS Communicator non funzionava, dando continui problemi di autenticazione e non effettuando quindi la registrazione alla piattaforma in modo corretto; UCT IMS Client non supportava per niente le funzionalità di chiamata d'emergenza, rendendo difficoltosa la modifica dei sorgenti.
Mercuro non è open source, mentre per quanto riguarda Android, il client IMS compatibile è attualmente in sviluppo e non ancora disponibile per il download [37].
Di conseguenza, è stato necessario creare uno user agent ad hoc per il progetto di tesi. Per gli scopi di test era sufficiente sviluppare la parte client, perciò per semplicità implementativa ci si è limitati a quella, sviluppando un client attraverso Microsoft Windows Form [38]. In Fig.5.2 è riportata l'interfaccia grafica del client, quella che l'utente deve gestire, inserendo i dati relativi alla propria situazione.
Prima di spiegare il significato dei campi da compilare, è necessario fare una precisazione: la struttura dell'indirizzo per la localizzazione segue il modello degli

33 L'IMS Communicator è un client sviluppato da PT Inovação per supportare lo sviluppo ed il test di componenti IMS/NGN. È un progetto open source, licenziato secondo la Apache Software License e la GNU Lesser General Public License (LGPL) [33].

34 Client sviluppato dal CommunicationResearch Group dell'Università di Cape Town, Sud Africa [34].

35Mercuro IMS Client è uno dei client IMS più completi in circolazione, ma non è open source [35].

36Android è una piattaforma open source per dispositivi mobili, basata su sistema operativo Linux e sviluppata dall'Open HandsetAlliance [36].

37Pagina del progetto:http://code.google.com/p/android-ims/[37].

38 Microsoft Windows Form è il nome dato alla parte GUI (*GraphicalUser Interface*) del framework Microsoft ".NET" (una piattaforma di sviluppo software basata sulla tecnologia di programmazione ad oggetti) [38].

Stati Uniti, per seguire l'impostazione del LoST Server usato all'interno del progetto, il quale contiene un database, che è stato modificato, ma di cui si è scelto, per semplicità, di conservare la struttura.

Possono essere fatti dei database compatibili ad hoc, ovviamente, ma essendo questo un progetto sperimentale atto a valutare la funzionalità degli algoritmi di scelta formulati, ci si è limitati a modificare il materiale esistente, per limitare il lavoro di implementazione focalizzandosi sulla funzionalità logica del sistema.

In particolare, la struttura dell'indirizzo, ovvero il significato dei campi contrassegnati da codici (A1, A2, ecc …) segue il modello definito nel documento RFC 4119 - "A Presence-Based GEOPRIV Location Object Format" [31].

Nel dettaglio, i campi da compilare sono:

- Target: deve contenere nella prima finestra (a sinistra) l'indirizzo IP del server, e nella seconda la porta a cui il client deve connettersi. Nel caso in esame, l'indirizzo IP della macchina virtuale su cui è installata la piattaforma IMS (ricordiamo che è stata installata su macchina virtuale poiché richiede sistema operativo Linux, che non è il sistema operativo del computer su cui si lavora).
- Local: nelle due finestre, nell'ordine, deve contenere l'indirizzo IP e la porta della macchina su cui si trova il client.
- User address: va compilato con l'indirizzo dell'utente. La struttura dell'indirizzo è "nome_utente@open-ims.test". Al momento sono previsti come utenti solo "alice" e "bob", altri utenti possono essere creati tramite l'interfaccia web http://localhost:8080 (una volta installata la piattaforma OpneIMSCore).
- Password: contiene la password dell'utente in questione. È da notare che se si sta effettuando una chiamata d'emergenza , anche immettendo una password sbagliata (o nessuna password), l'utente viene comunque abilitato alla chiamata
- Country: nel nostro caso, "US", in generale potrebbe contenere il Paese in cui si trova il chiamante.

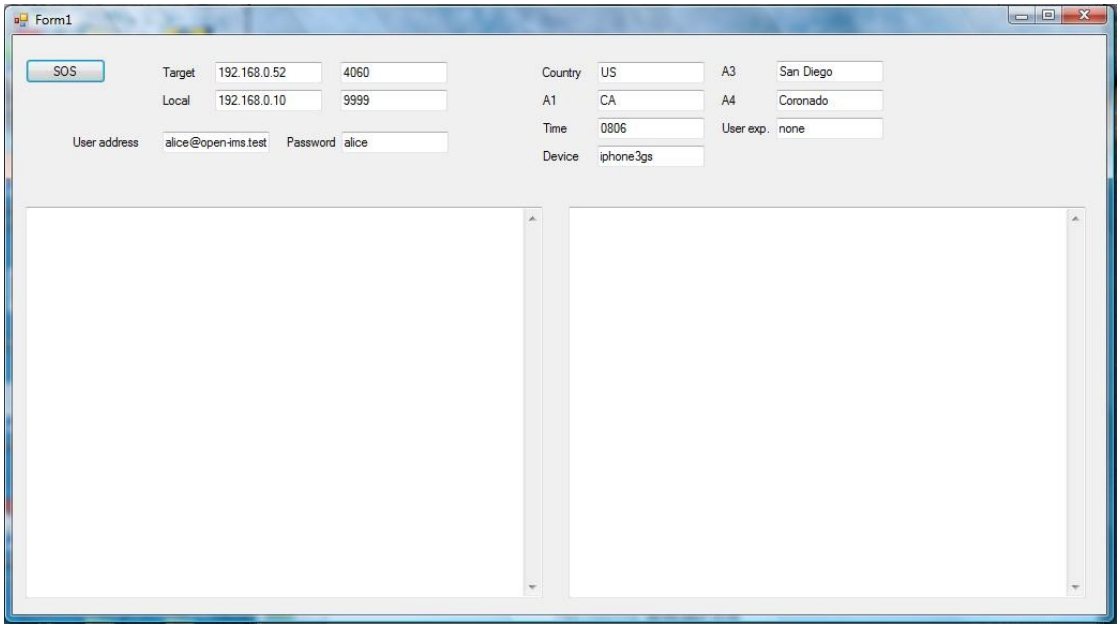


Fig.5.2: Interfaccia grafica del client usato.

- A1: contiene lo stato di appartenenza.
- A3: contiene la città in cui ci si trova.
- A4: definisce il quartiere.
- Time: va compilato con l'ora del giorno (in formato 24 ore). In un dispositivo reale questa informazione verrebbe rilevata in automatico, ma volendo fare simulazioni distinte a diverse ore del giorno è stato impostato per il cambio manuale.
- Device: deve contenere il tipo di dispositivo in uso. Per semplicità di implementazione è stato predisposto, lato database, un numero abbastanza ristretto di dispositivi utilizzabili. Anche questa informazione, comunque, in un dispositivo reale potrebbe essere inviata automaticamente dallo strumento.
- User exp.: (User Experience) contiene la qualifica dell'utente che sta effettuando la chiamata.

Le due finestre nello spazio sottostante sono state fatte per visualizzare a sinistra i dati inviati dal client e a destra quelli ricevuti. Si ha un esempio di finestre "compilate" in Figura 5.3.

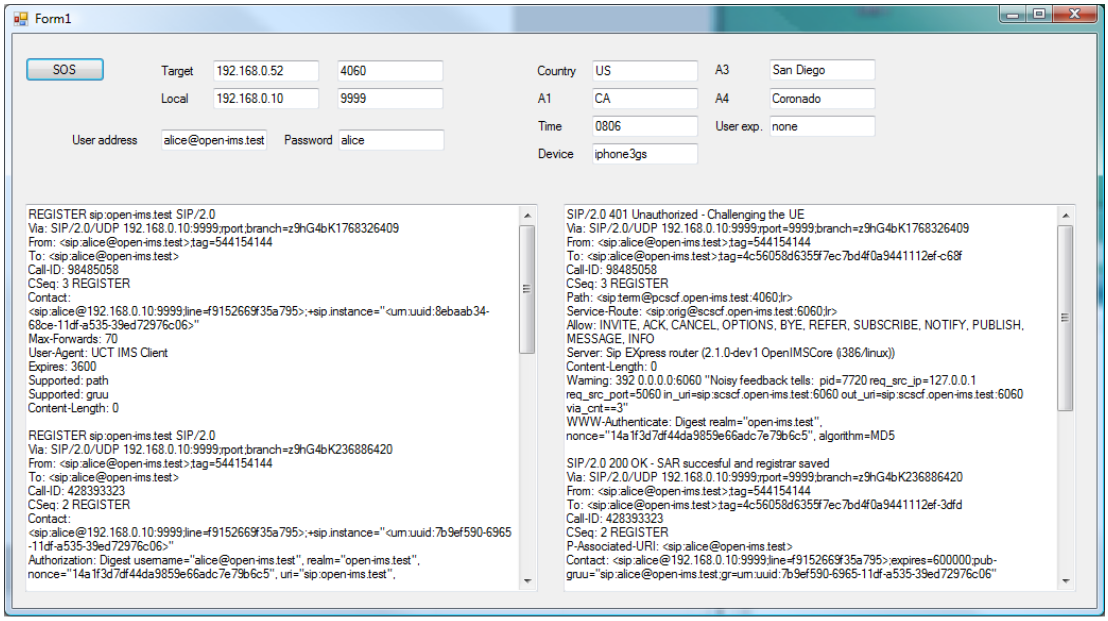


Fig. 5.3: Esempio di interfaccia del client dopo una chiamata d'emergenza.

Una volta compilati i campi in modo corretto, premendo il tasto "SOS", si effettua la registrazione e, in sequenza, la chiamata d'emergenza. Tradotto in comandi SIP, si invia prima una REGISTER e poi una INVITE.

È stato predisposto il client in modo che chiami direttamente il centro di emergenza medica, ma questo aspetto può essere modificato (introducendo la possibilità di chiamare altre entità di soccorso) semplicemente creando un altro campo da compilare all'interno dell'interfaccia. Per ora non si è fatto perché per creare una certa varietà di opzioni di scelta da parte del server è stato necessario ampliare il database LoST (che analizzeremo in seguito) manualmente, il che consiste in un lavoro piuttosto lungo e minuzioso. Per questo ci si è limitati al caso di richiesta di emergenza medica. I principi seguiti sono comunque validi per tutti i casi considerabili.

5.2 Blocco LoST

Il blocco LoST è composto da tre parti distinte (server, client e database) che interagiscono tra loro. Tutte le partipossono essere scaricate dal sito "http://honamsun.cs.columbia.edu/ " , e verranno analizzate qui di seguito.

5.2.1 Server

Il server LoST funziona come Java Servlet[39] su Apache Tomcat[40] 6.0.10. Accetta richieste in HTTP POST che contengano richieste LoST XML-based nel body HTTP, e risponde con un messaggio LoST in HTTP.
Il server LoST è predisposto per accettare richieste formate secondo il protocollo LoST (spiegato nel capitolo 2), dalle quali estrapola le informazioni interessanti ai fini dell'assegnamento ottimo del server. Possedendo le informazioni può poi consultare il database e decidere qual è il servente migliore da assegnare al chiamante.
In Figura 5.4 si ha una panoramica delle principali classi usate dal programma.
Come si può vedere, Tomcat interroga il server, in particolare la sua richiesta viene gestita dalla classe LostSerevletImplementation, la quale, una volta controllato che il messaggio ricevuto rispetti i requisiti di idoneità, si rivolge a LostServiceFactory, che stabilisce se la richiesta ricevuta è in formato "geo" (vengono fornite le coordinate spaziali del chiamante) o "civic" (si è in possesso dell'indirizzo del chiamante). Quest'ultima classe chiama LostHandlerImpl, una classe astratta che decide se istanziare la classe che gestisce le richieste in forma geografica (LostGeoHandler)
Per modificare l'algoritmo di scelta seguendo gli algoritmi definiti nel lavoro di tesi è stato necessario modificare parti del codice sorgente del server. In particolare, sono

39 Le servlet sono oggetti (in campo informatico)che operano all'interno di un server per applicazioni, potenziandone le funzionalità [39].

40 Apache Tomcat è un web container open source sviluppato dalla Apache Software Foundation. Fornisce una piattaforma per l'esecuzione di applicazioni web sviluppate in linguaggio Java [40].

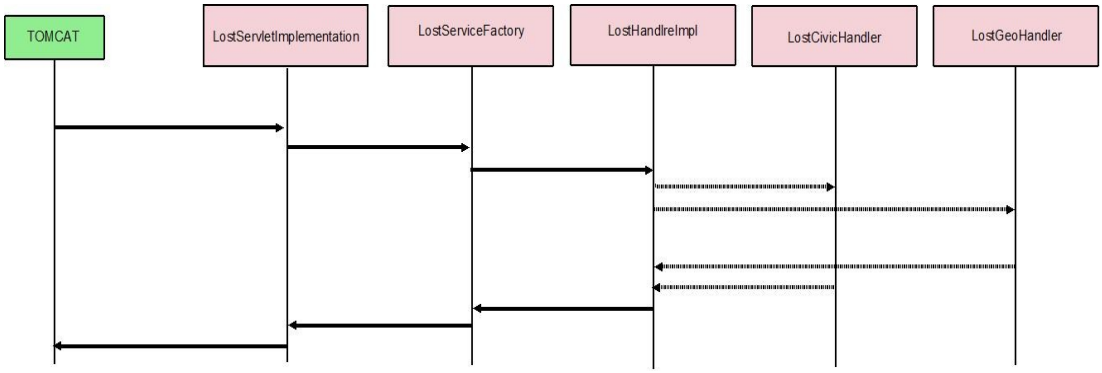


Fig. 5.4: SequenceDiagram del LoST Server.

state preparate tre versioni diverse del file "LostCivicHandler.java", il file che effettua la vera e propria "query" al database, e a seconda del metodo che si vuole usare si sceglie quello relativo. Per fare la query viene usata JDBC[41], l'API[42] che in Java definisce come un client deve effettuare l'accesso ad un database. Sono state create le versioni: "LostCivicHandler1.java", per il metodo ad eliminazioni successive, "LostCivicHandler2.java", per il metodo a maggioranza, e "LostCivicHandler3.java", per il metodo a pesi.

Senza entrare nel dettaglio dell'implementazione, è stato necessario fare in modo che il server ricevesse le informazioni aggiuntive previste dal progetto e le usasse per interrogare il database seguendo l'algoritmo desiderato, tramite l'uso di opportuni costrutti di istruzioni, cicli e chiamate a metodi.

41 JDBC sta per Java DataBase Connectivity [41].

42 Un API (Application Programming Interface) è un'interfaccia implementata da software che abilita l'interazione con altro software [42].

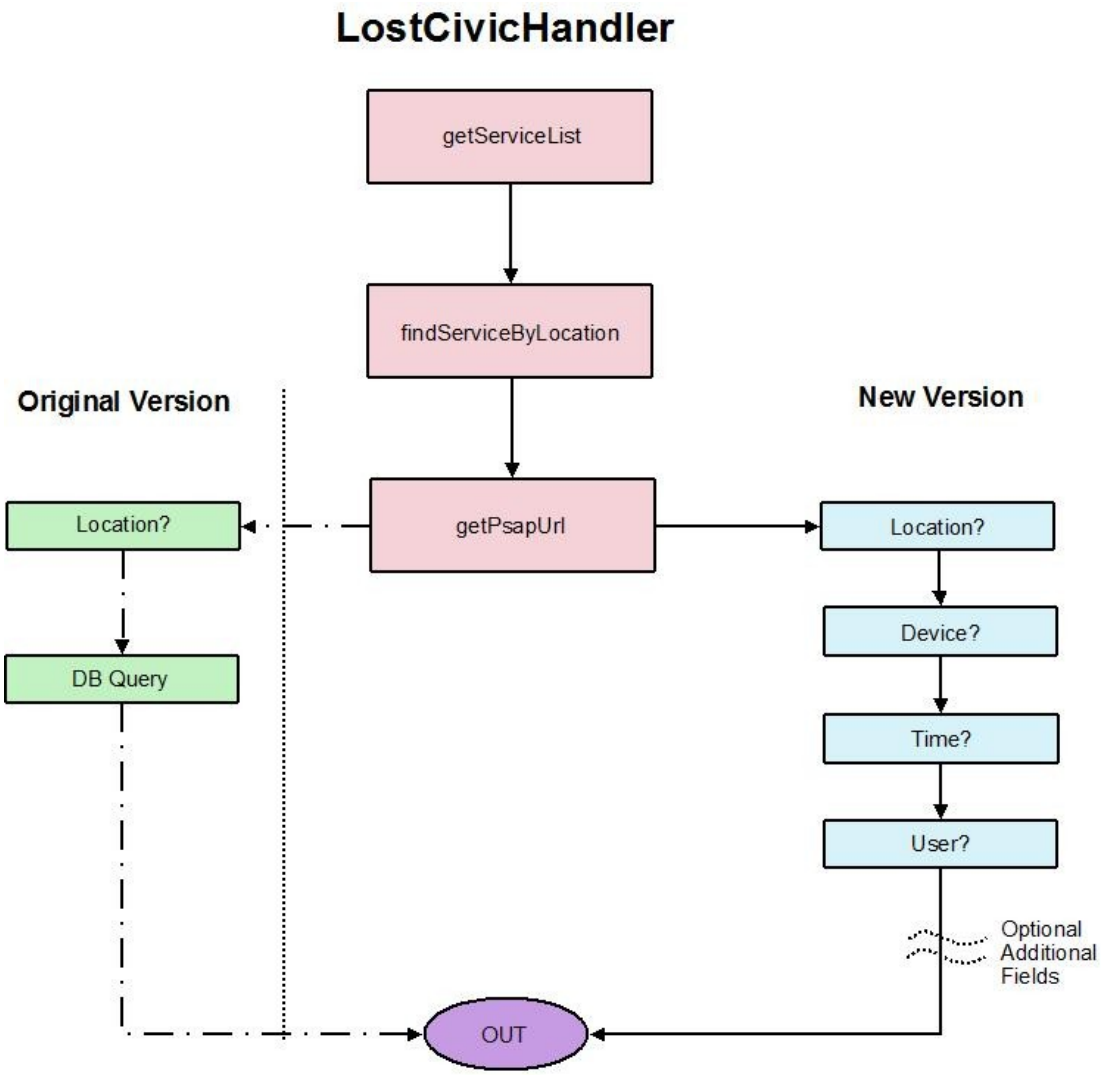


Fig. 5.5: Modifiche apportate alla classe LostCivicHandler.

In Figura 5.5 si ha una rappresentazione delle modifiche apportate alla classe LostCivicHandler, usata per implementare gli algoritmi. In particolare, è riportato il confronto tra il funzionamento originale, sulla sinistra, mentre sulla destra si ha una schematizzazione generale della nuova implementazione. Una volta ricevuto il messaggio, la classe fa un controllo sull'URN di servizio selezionato (getServiceList), poi passa le informazioni ricavate alla funzione findServiceByLocation, la quale tramite Relaxer[43] le porta in forma standard, pronte ad essere passate a getPsapUri, che apre la connessione al database e pone la query in modo da ritornare l'URN del centro di servizio più adeguato.

43 Relaxer è uno schema language per XML, le cui specifiche sono state sviluppate dalla RELAX NG Technical Committee. È anche uno standard internazionale (ISO/IEC 19757-2) [43].

5.2.2. Database

Il database LoST usa PostgreSQL 8.2.4 con l'estensione PostGIS[44] per memorizzare gli indirizzi civici. Nel dataset esemplificativo in esame c'era un PSAP per ogni tipo di soccorso per ogni stato degli Stati Uniti. Per testare gli algoritmi è stato necessario espandere il database, creando più PSAP dello stesso tipo per ogni stato, in modo da fornire la possibilità di scelte molteplici.
Le varie parti che compongono il database non sono collegate da relazioni logiche, ovvero non interagiscono tra loro: è il server che le interroga separatamente.
I modelli delle tabelle i dati che lo compongono viene comunque riportato in Fig.5.6.
Inizialmente il database non prevedeva l'esistenza delle tabelle "Neighbours" e "Device",che sono state create appositamente per l'implementazione del progetto di tesi, mentre la "civic_us_data" è stata ampliata.
Nella tabelle "Civic_us_data" ogni voce doveva originariamente contenere solo tutti i campi per la compilazione dell'indirizzo (secondo il formato definito nella RFC 4119, come spiegato in precedenza), ma è stata modificata in modo da contenere anche i campi "hour min", "hour max" e "device". L'apparente ridondanza del campo "device", data l'esistenza della tabella apposita, verrà spiegato qui di seguito.
I campi "hour min" e "hour max" indicano l'intervallo di tempo all'interno del quale è opportuno contattare la struttura considerata. Si è usato questo metodo per sfruttare il campo "time" previsto nel progetto di ampliamento del messaggio di INVITE della chiamata (spiegato nel capitolo 3) senza andare ad incidere eccessivamente sulla difficoltà di programmazione. Idealmente, la scelta della struttura deve tenere in considerazione il fatto che a seconda della fascia oraria alcuni centri di soccorso saranno più velocemente raggiungibili di altri. Per questo motivo, si è scelto di assegnare simbolicamente ad ognuno fasce orarie di reperibilità. Ovviamente in un sistema reale questo campo andrebbe aggiornato dinamicamente, tenendo conto costantemente delle condizioni del traffico, che in certi frangenti può assumere comportamenti anomali rispetto alle statistiche (si pensi a casi di manifestazioni che chiudono parti di città, congestionando le vie circostanti, o casi di allagamento di

44PostGIS è un'estensione spaziale per il Database Management System PostgreSQL distribuito con licenza GPL (Gnu General Public License) [22].

parti di carreggiata, incidenti, e così via..) .

Per quanto riguarda il campo “device”, era stato inserito inizialmente per implementare il primo algoritmo, ovvero quello ad eliminazioni successive, poiché era sufficiente avere l’informazione generica relativa al dispositivo in uso per decidere se scartare il centro in esame sia compatibile o meno con il chiamante.

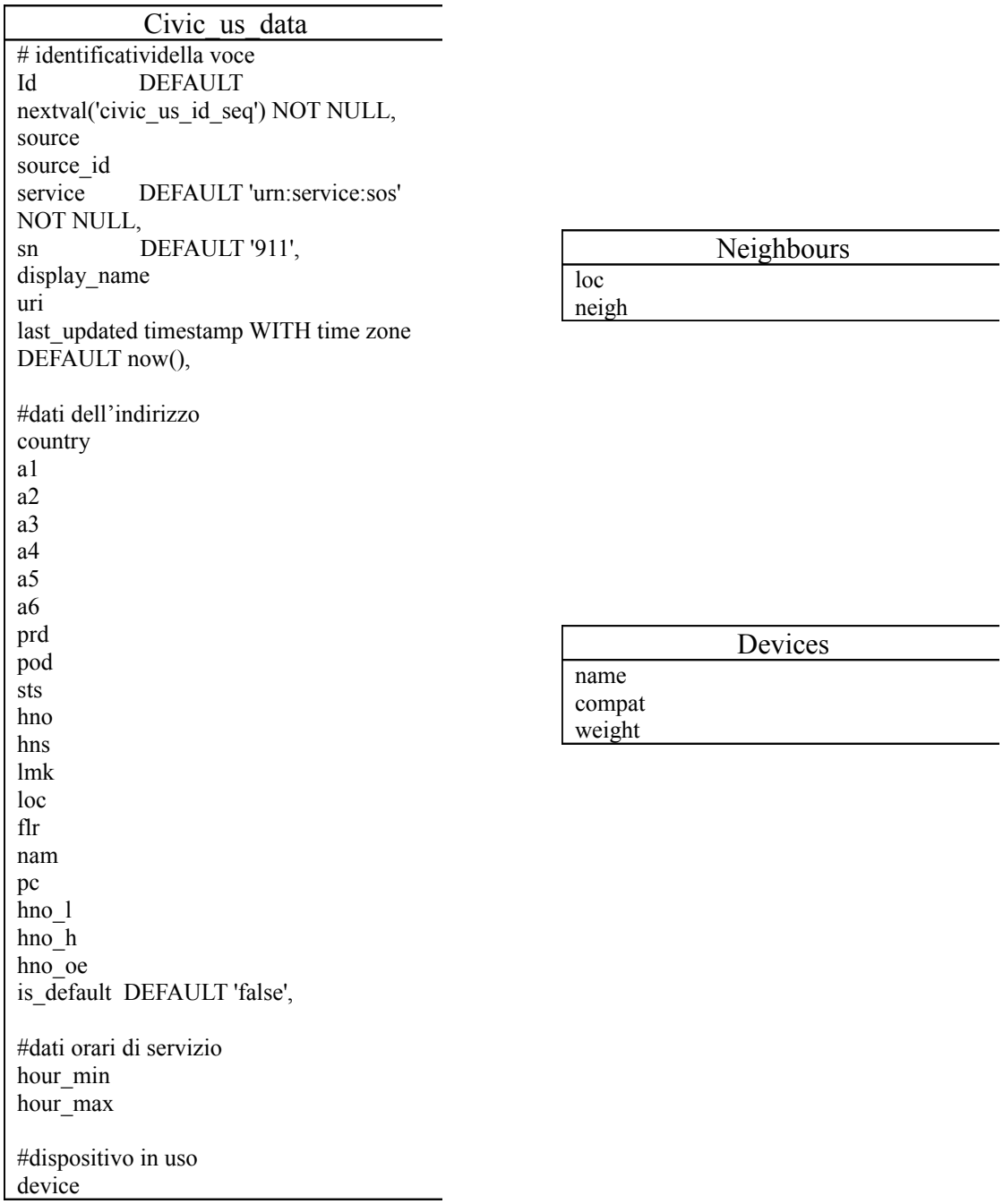


Fig.5.6: Tabelle che compongono il database LoST, non collegate tra loro da relazioni logiche.

Successivamente, per implementare l'algoritmo a pesi è stato necessario costruire una tabella a parte, le cui voci sono:

- Name: nome del dispositivo in uso (quello inserito tramite l'interfaccia del client, come fatto in questo lavoro, che in futuro può essere inviata in automatico dal dispositivo, senza l'intervento dell'utente);
- Compat: contiene il nome di un altro dispositivo, con il quale viene confrontato (il server valuterà il dispositivo del centro di soccorso, e selezionerà così la riga esatta che combacia con i dispositivi da confrontare)
- Weight: è il "peso" della compatibilità tra i dispositivi accostati nella riga in questione, informazione usata per applicare l'algoritmo dei pesi.

La tabella "Neighbours" è stata introdotta invece per l'implementazione dell'algoritmo "a maggioranza", all'interno del quale serviva una valutazione dei "vicini" rispetto alla zona di localizzazione del chiamante. Per semplicità implementativa è stata considerata la vicinanza macroscopica tra stati, ma ovviamente il principio seguito è applicabile in scala ridotta, ovvero ad esempio vicinanza tra quartieri della stessa città o tra province (in caso si intervenga con mezzi veloci, come ad esempio elicotteri). Ogni riga ha solo due voci: ad ogni stato vengono associati gli stati vicini, formando delle copie che coprano tutte le combinazioni possibili.
Si era valutata l'ipotesi di costruire relazioni tra i database, per poter usufruire dei vantaggi che queste offrono, ma alla fine si è optato per una soluzione più semplice, poiché sarebbe stato puro esercizio implementativo, senza benefici agli scopi della tesi.

5.2.3 Client LoST

Il client LoST fornito dal sito http://honamsun.cs.columbia.edu/, da cui è stato preso tutto l'apparato LoST, è un client di test implementato come singola classe Java. Legge le richieste LoST da file e invia/riceve messaggi HTTP verso/da ilLoST server, stampando poi a video il messaggio di risposta. Sul sito è disponibile anche un client Web, che permette di fare simulazioni del funzionamento del sistema LoST senza aver installato tutto l'apparato sulla propria macchina.
Questo client è stato usato soprattutto nella fasi iniziali di implementazione del progetto, per testare il corretto funzionamento della piattaforma LoST.
In Figura 5.7 si ha un'immagine del client mentre si effettua una chiamata.

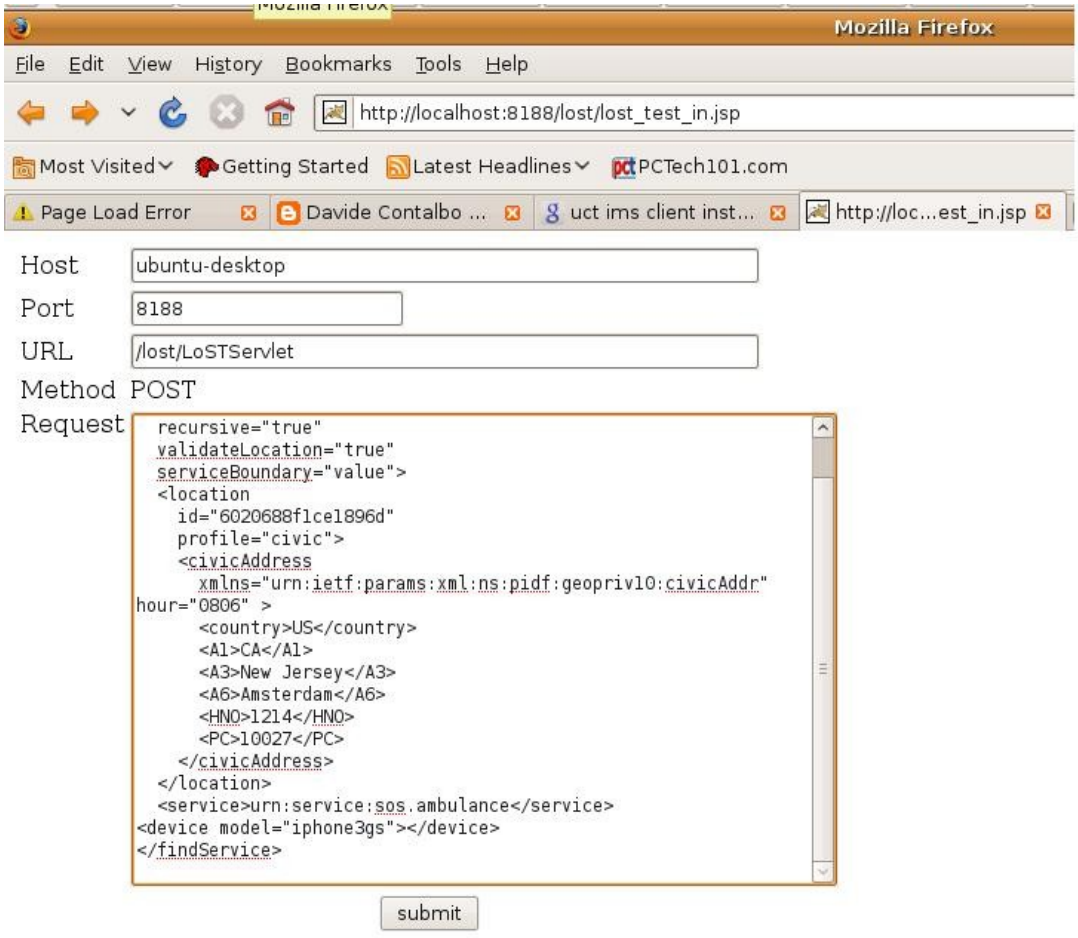


Figura 5.7: Client LoST compilato per effettuare una richiesta di soccorso.

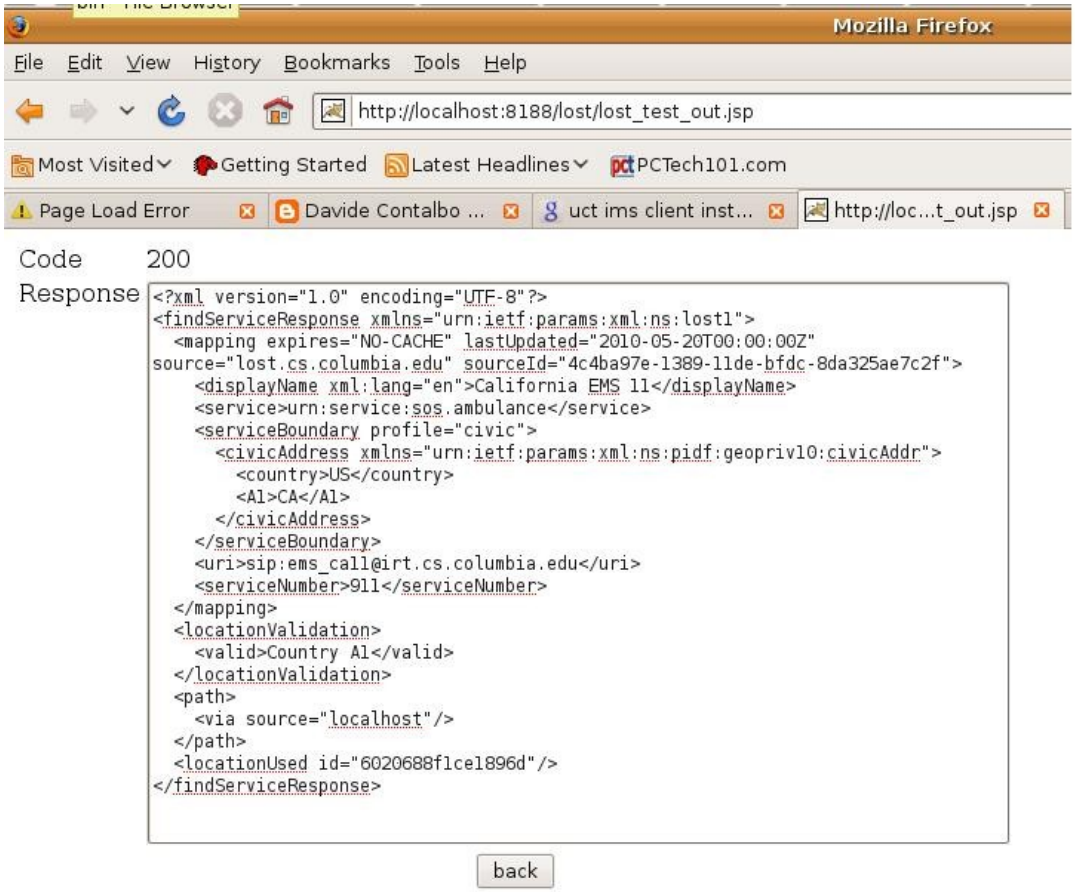


Figura 5.8: Stampata a video della risposta ricevuta dal client LoST dopo una chiamata.

In Figura 5.8 si vede invece la risposta pervenuta attraverso il client LoST.

A questo punto si è delineato un quadro piuttosto completo del sistema che è stato realizzato per testare gli algoritmi di selezione formulati.

È doveroso fare alcune precisazioni.

È stato più volte detto, spiegando i passi dell'implementazione, che sono state effettuate delle scelte progettuali atte a semplificare il lavoro di programmazione. Poiché lo scopo della tesi è verificare la funzionalità degli algoritmi, si è preferito non perdere troppo tempo nei dettagli di sviluppo, favorendo l'aspetto concettuale del progetto.

Inoltre, si ricorda che si è scelto di partire dalla piattaforma LoST già esistente, per essere conformi a ciò che già esisteva in tecnologia, senza creare doppioni inutili dello stesso sistema. In questo modo, però, si è avuta meno libertà di progettazione, dovendo trovare metodi di modifica al database e al codice sorgente del server che dovessero restare in linea con la struttura preesistente.

5.3 Risultati ottenuti

Sono state effettuate alcune simulazioni di chiamate d'emergenza, variando i parametri di volta in volta, per avere un quadro generale della situazione.
Si è ottenuto il risultato atteso, ovvero risposte nell'ordine delle centinaia di millisecondi. Prima di commentarle, si riportano nell'ordine i risultati delle simulazioni fatte impiegando i tre diversi algoritmi: in Figura 5.9 i dati relativi all'algoritmo ad eliminazioni successive, in Figura 5.10 quelli dell'algoritmo a maggioranza, in Figura 5.11 quelli dell'algoritmo a pesi ed infine, in figura 5.12, il confronto dei tre.

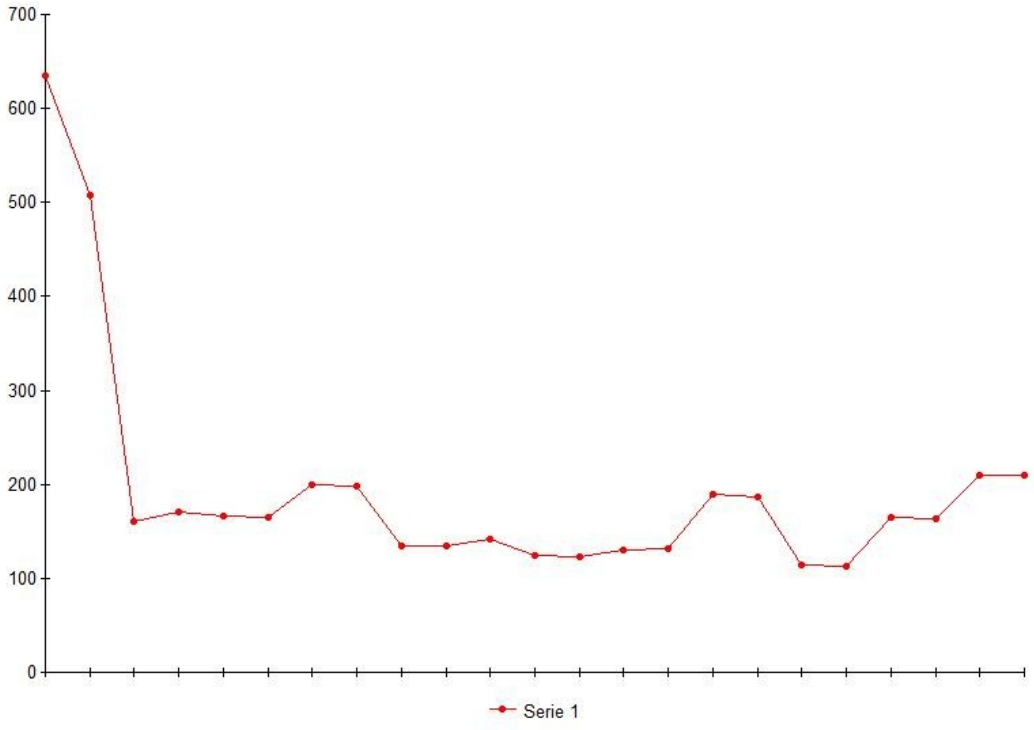


Figura 5.9: Risultato (in ms) delle simulazioni di chiamata gestita con algoritmo ad eliminazioni successive.

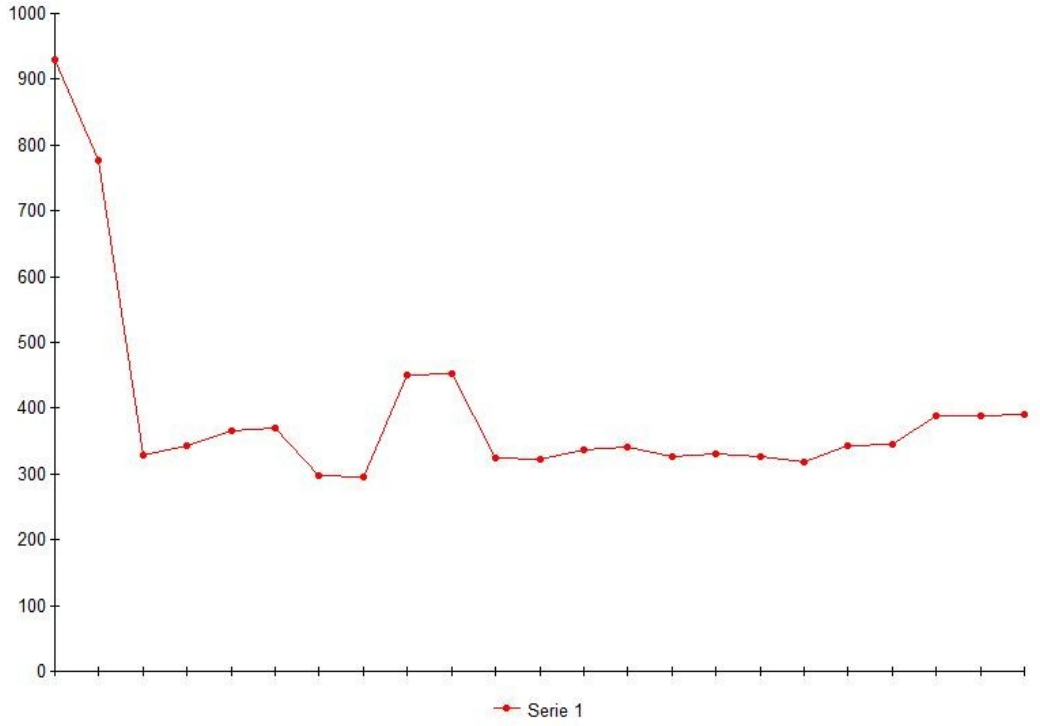


Figura 5.10: Risultato (in ms) delle simulazioni di chiamata gestita con algoritmo a maggioranza.

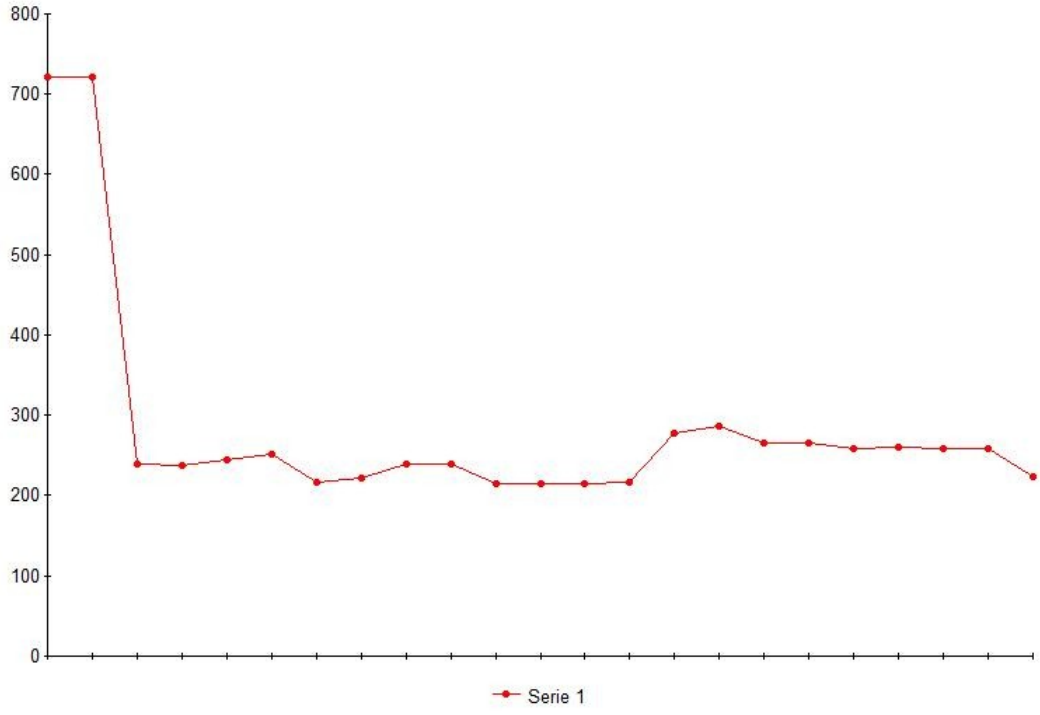


Figura 5.11: Risultato (in ms) delle simulazioni di chiamata gestita con algoritmoa pesi.

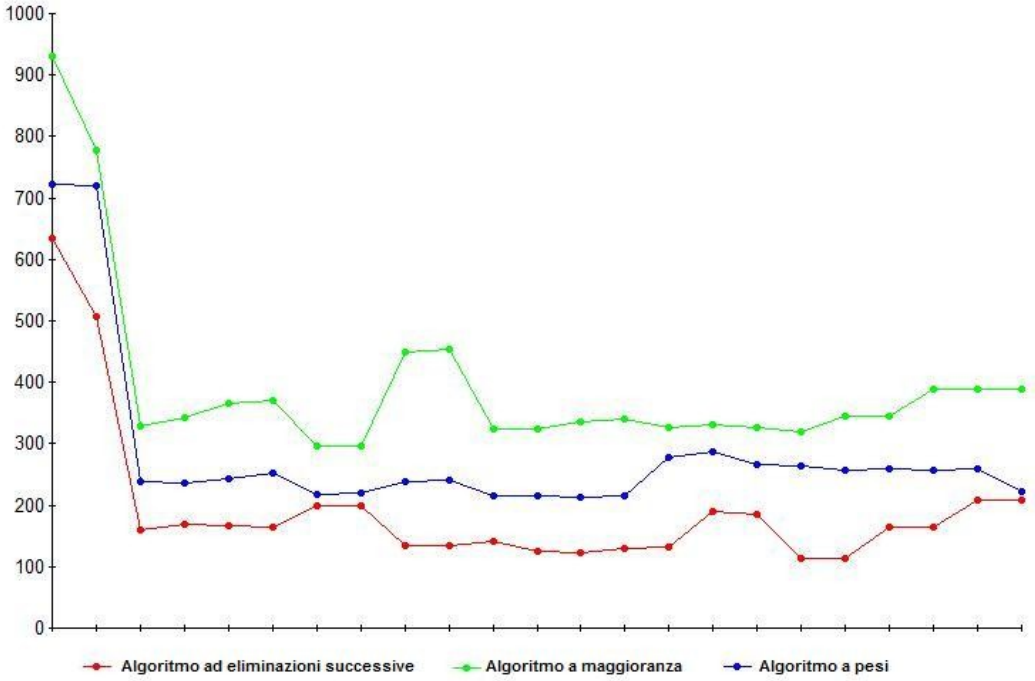


Figura 5.12: Risultati (in ms) delle simulazioni dei tre algoritmi a confronto.

Come si può notare, l'andamento dei tempi di risposta è abbastanza uniforme in tutti e tre i casi, con un picco nella prima simulazione (il server deve assestarsi sull'uso di un "nuovo" algoritmo).
Si cerca di fare ora un'analisi da diversi punti di vista.

Valutazione quantitativa – Tempo di risposta

Dai grafici sopra riportati è evidente che l'algoritmo ad eliminazioni successive sia il più veloce. Questo era prevedibile dato che è il più semplice, basandosi sulla cancellazione in sequenza.
Gli altri due sono più complessi, e pertanto richiedono più tempo, anche se la risposta del sistema differisce di qualche centinaio di millisecondi. L'aumento di tempo di risposta dipende ovviamente dalla complessità dell'algoritmo, in particolare dal tempo necessario a consultare il database che varia a seconda della quantità di alternative considerate nei diversi algoritmi. In quello ad eliminazioni successive vengono presi in considerazione meno centri di servizio, eliminando sistematicamente tutti quelli non compatibili. Negli altri, invece, la scelta è più

ponderata, tenendo in gioco anche serventi apparentemente non perfettamente compatibili con la richiesta.
Ad un'analisi superficiale dei risultati ottenuti sembrerebbe non esistere la possibilità di determinare quale algoritmo sia migliore, ma l'analisi del lavoro non può essere ridotta ad un'analisi dei tempi di risposta.
Anzi, il fatto che uno dei metodi proposti non sia nettamente migliore degli altri può essere un vantaggio nella libertà di scelta del più adatto alle proprie esigenze.

Valutazione qualitativa – Varietà di scelta

Un importante fattore da considerare nelle considerazioni di valutazione è senza dubbio la varietà di scelta offerta dai diversi metodi. Nello specifico, gli algoritmi a pesi e a maggioranza sono impostati per valutare un numero maggiore di opzioni, e la loro risposta è quasi sempre allineata, diversamente da quella fornita dall'algoritmo ad eliminazioni successive, che automaticamente ignora tutti i centri che non sono conformi alle richieste del chiamante. Questo rende l'algoritmo più veloce, il database più semplice da gestire, ma impedisce la considerazione di connessioni potenzialmente vantaggiose. Ad esempio, se l'utente che effettua la chiamata è identificato come operatore del settore (medico, poliziotto o vigile del fuoco) può essere vantaggiosa la connessione ad un centro che permetta di sfruttare al massimo le potenzialità del dispositivo in uso, in modo da comunicare in tempo reale gli aggiornamenti sulla situazione, per far portare sul luogo le unità più specifiche richieste.

Valutazione qualitativa – Difficoltà di gestione del database

Un'altra doverosa considerazione è che i tempi misurati sono da considerarsi ridotti rispetto ad un'implementazione reale del sistema poiché il database gestito ha una dimensione piuttosto ridotta. Questo riporta alla considerazione che un algoritmo può essere preferito rispetto ad un altro in base alla gestione degli aggiornamenti dei database, che è più o meno complessa a seconda dell'algoritmo usato: l'algoritmo a maggioranza è il più oneroso in termini di amministrazione, poiché, come si è

accennato in precedenza, richiede l'aggiornamento delle tabelle considerando un vasto numero (almeno "n", con "n" definito dall'algoritmo, nel nostro caso 4, ma è una quantità che risulterebbe insufficiente in un uso reale del sistema) di opzioni in ogni caso, per ogni voce da consultare (localizzazione, device, utente, orario, ecc…). Viceversa, se si usa l'algoritmo ad eliminazioni successive è sufficiente mantenere l'aggiornamento della tabella "Civic_us_data".
Per questo motivo, nella valutazione del sistema implementato è da tenere in considerazione soprattutto l'aspetto concettuale del progetto, poiché ciò che si voleva fare era migliorare la scelta effettuata dal server senza intaccare in modo significativo il tempo di risposta, e questo scopo è stato raggiunto, riuscendo a considerare come fattori di scelta anche i parametri di contesto individuati come rilevanti ai fini della scelta ottima.

Valutazione qualitativa – Probabilità di risposte equivalenti

Un problema che si potrebbe presentare, e che è stato considerato, è quello dell'equivalenza di due centri di servizio rispetto alla medesima richiesta di soccorso. Per ora, il sistema prende semplicemente il primo nell'ordine del database. È da considerare però un fattore fondamentale: il sistema implementato per questo lavoro di tesi è abbastanza semplificato, mentre in un apparato reale le caratteristiche delle diverse entità sarebbero più marcate.
Inoltre, è da considerare il fatto che aumentando il dettaglio delle richieste fornite dal chiamante (informazioni supplementari sul dispositivo, ad esempio, o integrazione con lo stato della rete in termini di quantità di banda disponibile) la probabilità di avere due serventi perfettamente equivalenti tende a diminuire drasticamente.
Quindi, se si vuole evitare il più possibile che si manifesti questa equivalenza di serventi, con conseguente scelta solo in base all'ordine nel database, conviene usare l'algoritmo a maggioranza, che essendo il più minuzioso riduce le probabilità di risposta multipla.

Si fa ora un ultimo quadro riassuntivo del funzionamento dei diversi algoritmi:

- L'algoritmo ad eliminazioni successive, più elementare, offre meno varietà di scelta, eliminando sistematicamente i serventi non compatibili con le caratteristiche del chiamante. Richiede anche un database più semplice e più facilmente gestibile, ma ha una maggiore probabilità di risposte equivalenti.
- L'algoritmo a maggioranza, il più elaborato, ed il più oneroso in termini di tempi di risposta, valuta un maggior numero di opzioni rispetto agli altri due, ma richiede una gestione più complessa del database, riducendo al minimo la possibilità di risposte equivalenti.
- L'algoritmo a pesi si colloca nel mezzo: ha tempi di risposta intermedi, valuta un buon numero di opzioni, e richiede una gestione piuttosto complessa del database, riducendo rispetto all'algoritmo ad eliminazioni successive la possibilità di risposte equivalenti.

La scelta di quale implementare dovrà quindi essere basata sulla considerazione di tutti questi fattori.
Gli algoritmi si sono dimostrati tutti funzionanti, fornendo i risultati previsti in fase di progetto. Non è possibile stabilire una classifica di funzionamento che porti a privilegiare la scelta di uno piuttosto di un altro, ma a seconda delle necessità dell'utente si può scegliere il più adatto.
Ad esempio, se le informazioni fornite dal chiamante sono ridotte al minimo, a causa del dispositivo in uso, o della disinformazione dell'utente, è consigliabile usare l'algoritmo ad eliminazioni successive, che sceglie in modo più immediato senza scendere in un livello di dettaglio eccessivo rispetto all'attendibilità delle informazioni fornite dall'utente.
Se invece il chiamante riesce a fornire un quadro molto dettagliato della situazione, soprattutto se è un operatore del settore e quindi riesce a fornire dettagli utili ai fini della scelta di un centro di soccorso rispetto ad un altro, è consigliabile usare l'algoritmo a maggioranza. Ad esempio, se un medico si trova sul luogo di un incidente, è meglio privilegiare un centro che possa sfruttare al massimo la compatibilità di dispositivo in uso, per permettere lo scambio di informazioni preziose per le operazioni di soccorso, anche se non è nella regione del chiamante

(caratteristica che nell'algoritmo ad eliminazioni successive non ne avrebbe permesso la candidatura a centro servente per quel chiamante).
Se l'utente riesce a fornire un buon grado di dettaglio della situazione in cui si trova è consigliabile l'uso dell'algoritmo a pesi, che costituisce una valida via di mezzo tra gli altri due.
Un altro fattore da considerare nella scelta dell'algoritmo da implementare è la quantità di centri di servizio nella regione di interesse: se sono molto distanti tra loro, cosa che rende la vicinanza geografica determinante, è conveniente usare l'algoritmo ad eliminazioni successive, mentre ad esempio in uno scenario cittadino la posizione geografica è meno rilevante. È da considerare comunque che la distanza è da valutare in modo diverso a seconda del mezzo di soccorso che si intende usare (su strada, elicottero, motocicletta, o quant'altro).
Concludendo, la scelta di quale algoritmo impiegare non è determinabile in modo assoluto, varia da caso a caso. Si può dire però che esiste un algoritmo adatto ad ogni possibile scenario.

Capitolo 6

Conclusioni

Il problema della pubblica sicurezza è una tematica interessante a livello globale, di interesse costante e in continua evoluzione. Si usano tecnologie all'avanguardia all'interno di ogni intervento d'emergenza, ed è naturale pensare che anche le nuove tecnologie di telecomunicazione possano essere sfruttate per fornire un servizio più efficiente di quello attuale.

Il presente lavoro di tesi trae origine dal quadro delineato dal progetto PICO, che mira alla creazione di una piattaforma di servizio unificata per il controllo e la distribuzione di servizi in uno scenario di reti di nuova generazione, fornendo servizi di comunicazione innovativi per utenti differenziati in situazioni d'emergenza, relativamente sia alla prevenzione che all'intervento in caso di necessità.

Nello specifico, si ha l'obiettivo di creare un sistema in grado di gestire le chiamate d'emergenza in modo da ottimizzare le informazioni che l'utente può fornire attraverso la chiamata. Allo stato attuale, l'instradamento delle chiamate d'emergenza viene fatto solo tramite la valutazione della localizzazione geografica reciproca tra chiamante e centro operativo. Sfruttando le Internet Technologies si possono usare altri parametri di decisione ugualmente determinanti.

Partendo dall'analisi di ciò che già esisteva, ovvero il gruppo ECRIT, interno all'IETF, che si occupa dello studio delle chiamate d'emergenza in SIP, e del protocollo da esso rilasciato (LoST), si è stilata una serie di elementi interessanti per la definizione del contesto in cui si inserisce il chiamante, e si sono creati degli algoritmi in grado di sfruttare tali elementi per associare all'utente il servente che più si addice alle caratteristiche fornite.

In particolare, sono stati formulati tre algoritmi: un più semplice e due più complessi, e si è costruita una piattaforma per il loro test, con l'obiettivo di raccogliere dati sulle diverse efficienze. I tre algoritmi sono: ad eliminazioni successive (confrontando i dati ricevuti, il sistema elimina tutti i serventi non compatibili), a maggioranza (per ogni caratteristiche rilevata si tengono in considerazione gli "n" centri che maggiormente si avvicinano alla richiesta e si sceglie alla fine quello menzionato più volte), e a pesi (ad ogni centro viene associato un peso a seconda della compatibilità secondo i vari aspetti considerati, scegliendo alla fine quello a peso maggiore).

La piattaforma ha compreso l'implementazione di OpenIMSCore, di cui si è parlato nel capitolo 3, che costituisce l'architettura di rete a cui il client si connette per effettuare la chiamata, uno user agent ad hoc che invii le informazioni di contesto desiderate, e la modifica del funzionamento del server LoST (basato sull'omonimo protocollo prima citato) in modo da usare di volta in volta l'algoritmo desiderato.

Una volta costruito il sistema, sono stati rilevati i tempi di risposta nei tre diversi casi di utilizzo. Ciò che si è ottenuto è stata una lieve differenza di tempi rilevata, il che indica che non esiste un algoritmo nettamente superiore rispetto agli altri. In particolare, l'algoritmo ad eliminazioni successive è risultato il più veloce, e questo era prevedibile dato che tra i tre metodi proposti questo è il più semplice. Il più lento, invece, è stato quello a maggioranza (anche questo risultato era atteso, sempre in base alla difficoltà dell'algoritmo, che valuta molte opzioni prima di prendere una decisione).

Nell'ottica di valutare il sistema implementato, non è sufficiente valutare l'aspetto della risposta temporale, ma vanno considerati alcuni aspetti qualitativi, per avere un quadro più completo della situazione.

In particolare, si è posta l'attenzione sulla varietà di scelta offerta dai diversi metodi, sulla difficoltà di gestione del database e sulla probabilità di risposte equivalenti.

L'algoritmo ad eliminazioni successive, il più immediato, offre meno varietà di scelta, richiede un database più elementare e più facilmente gestibile, ma ha una

maggiore probabilità di risposte equivalenti.
L'algoritmo a maggioranza, il più elaborato, è anche il più oneroso in termini di tempi di risposta, considera il maggior numero di opzioni, richiede una gestione più complessa del database, ma riduce al minimo la possibilità di risposte equivalenti.
L'algoritmo a pesi ha prestazioni intermedie rispetto agli altri due: tempi di risposta intermedi, valutazione di un buon numero di opzioni, e gestione piuttosto complessa del database, con ridotta possibilità di risposte equivalenti rispetto all'algoritmo ad eliminazioni successive.
Non è possibile stabilire l'assoluta preferenza di scelta di un algoritmo rispetto ad un altro, ma valutando attentamente le caratteristiche di ognuno appena esaminate, l'operatore può scegliere quello più adatto a soddisfare le proprie esigenze.

In futuro, si può pensare di sviluppare il sistema in modo di ampliare lo spettro delle informazioni fornite dal client al server, per avere una ricerca sempre più raffinata del centro di servizio idoneo.
Inoltre, si potrebbe pensare alla creazione di uno user agent che mandi alcune informazioni (ad esempio parametri del dispositivo in uso, localizzazione e ora del giorno) in modo automatico con la chiamata, senza la necessità di inserirle manualmente. Si ricorda che per il presente lavoro di tesi è stato necessario poter variare manualmente i parametri per poter fare simulazioni più diversificate.
Si potrebbe introdurre anche, come discriminante ulteriore, un indicatore dello stato della rete, per stabilire la quantità di banda utilizzabile ed ottimizzare il collegamento.

Bibliografia

[1] Pagina di riferimento:: “http://www.itu.int/ITU-T/ngn/” .

[2] Pagina di riferimento:“http://www.cefriel.it/index.php/it/ricerca/ricerca-nazionale/872-pico-firb” e“http://softeng.polito.it/pico/index.html”.

[3] Pagina di riferimento:“http://tools.ietf.org/html/rfc3261” ; ulteriori informazioni ricavate da “http://www.en.voipforo.com/SIP/SIP_architecture.php” .

[4] Pagina di riferimento:“http://www.linfo.org/pstn.html”.

[5] Pagina di riferimento:“http://www.ietf.org”.

[6] Pagina di riferimento:“http://www.ietf.org/dyn/wg/charter/ecrit-charter.html”.

[7] Pagina di riferimento:“http://tools.ietf.org/search/rfc5222” e “http://ecrit.sourceforge.net/”.

[8] Testo di riferimento: “The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds” di Gonzalo Camarillo, Miguel-Angel García-Martín (John Wiley&Sons, 2006);pagine utili: “http://www.3gpp.org/ftp/Specs/html-info/23228.html” e “http://www.ericsson.com/technology” .

[9] Pagina di riferimento: “http://tools.ietf.org/html/draft-ietf-ecrit-lost-sync-09” .

[10] Pagina di riferimento: “http://www.3gpp.org/” .

[11] Pagina di riferimento: “http://www.freewebs.com/telecomm/3g.html” .

[12] Pagina di riferimento: “http://wlan.interfree.it/index.htm” .

[13] Pagina di riferimento: “http://www.etsi.org/tispan/” .

[14] Documento di riferimento: “http://people.brunel.ac.uk/~eesrwwy/handout/4-QoS%20in %20Telecommunications.pdf” .

[15] Testo di riferimento: “Encyclopedia of Networking and Telecommunication”, di Tom Sheldon, ed.McGraw-Hill.

[16] Pagina di riferimento: “http://www.businessdictionary.com/definition/mass-market.html” .

[17] Pagina di riferimento: “http://www.maxim-ic.com/glossary/definitions.mvp/term/adm/gpk/8” .

[18] Pagina di riferimento: “http://www.differencebetween.net/technology/”

[19] Testo di riferimento:"Paul BaranInvents Packet Switching" diStewart, Bill (2000-01-07).

[20] Pagina di riferimento:“http://www.encyclopedia.com/doc/1O11-circuitswitching.html” .

[21] Pagina di riferimento:“http://www.ietf.org/rfc/rfc3588.txt”.

[22] Pagina di riferimento:“http://ww.dhcp.org” .

[23] Pagina di riferimento: “http://www.webopedia.com/welcomead/” .

[24] Pagina di riferimento:“http://www.e164.org/” .

[25] Pagina di riferimento:“http://www.protocols.com/pbook/ss7.html” .

[26] Pagina di riferimento: “http://www.fokus.fraunhofer.de/en/fokus/index.html” .

[27] Pagina di riferimento:“http://networking.ittoolbox.com/topics/proto/rtp” .

[28] Pagina di riferimento:“http://tools.ietf.org/html/rfc3108” .

[29] Pagina di riferimento:“http://www.openimscore.org/” .

[30] Pagina di riferimento:“https://datatracker.ietf.org/doc/draft-ietf-sipcore-location-conveyance/” .

[31] Pagina di riferimento:“http://www.rfc-

editor.org/rfc/rfc4119.txt” , “http://tools.ietf.org/html/rfc3863” .

[32] Pagina di riferimento:“http://www.postgresql.org” .

[33] Pagina di riferimento:“http://imscommunicator.berlios.de/”

[34] Pagina di riferimento:“http://uctimsclient.berlios.de/” .

[35] Pagina di riferimento:“http://www.mercuro.net/” .

[36] Pagina di riferimento:“http//ww.android.com”.

[37] Pagina di riferimento:“http://code.google.com/p/android-ims/” .

[38] Pagina di riferimento:“http://windowsclient.net/” .

[39] Pagina di riferimento:“http://java.sun.com/products/servlet/” .

[40] Pagina di riferimento:“http://tomcat.apache.org/” .

[41] Pagina di riferimento:“http://java.sun.com/javase/technologies/database/” .

[42] Pagina di riferimento:“http://java.sun.com/javase/technologies/database/” .

[43] Pagina di riferimento:“http://www.relaxng.org/” .

Glossario

AAA: Authentication, Authorization and Accounting

AS: Application Server

AUC: Authentication Centre

B2BUA: back-to-back user agent

CAMEL: Customized Applications for Mobile network Enhanced Logic

CCF: Charging Collection Function

CS: Circuit Switching

CSCF : Call Session Control Function

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Server

DSL: Digital Subscriber Line

EAN: Extended Area Network

ECRIT: Emergency Context Resolution with Internet Technologies

EM: Emergency Manager

EMS: Emergency Medical Service

EOC: Emergency Operation Centre

ESQK: Emergency Service Query Key

FF: Fire Fighters

GPRS: General Packet Radio Service

GSM: Global System for Mobile communications

HLR: Home Location Register

HSS: Home Subscriber Server

IAN: Incident Area Network

IC: Incident Command

ID: Identification Data

IETF: Internet Engineering Task Force

IM-SSF: IP Multimedia Service Switching Function

IMS: IP Multimedia Subsystem

IP: Internet Protocol

ISDN: Integrated Services Digital Network

ISUP: ISDN User Part

IT: Internet Technologies

ITU-T:International Telecommunication Union - Telecommunication Standardization Bureau

JAN: Jurisdictional Area Network

LE: Law enforcement

LoST: Location-to-Service Translation Protocol

LRF: Location Retrivial Function

MAP: Mobile Application Part

MMS: Multimedia Messaging Service

MRF: Media Resource Function

NGN: Next Generation Network

OSA – SCS: Open Service Access – Service Capability Server

PAN: Personal Area Network

PDA: Personal Digital Assistant

PDP:Packet Data Protocol

PIDF: Presence Information Data Format

POC: Push to talk Over Cellular

PS: Packet Switching

PSAP: Public Safety Answering Point

PSCD: Public Safety Communication Device

PSCDU: PSCD User

PSTN: Public Switched Telephone Network

QoS: Quality of Service

RAC: Resource Admission Control

RAM: Random Access Memory

RF ID: Radio Frequency Identification Data

RTP: Real Time Protocol

RTSP: Real Time Streaming Protocol

SCTP: Stream Control Transmission Protocol

SDP: Session Description Protocol

SIP: Session Initiation Protocol

SLF: Subscriber Location Function

TCP: Transmission Control Protocol

TISPAN: Telecommunications and Internet converged Services and Protocols for Advanced Networking

TTS: Text-To-Speech

U-NAPTR/DDDS: URI-Enabled NAPTR/Dynamic Delegation Discovery Service

UA: User Agent

URI: Uniform Resource Identifier

URN: Uniform Resource Name

VoIP: Voice over IP

WiMAX: Worldwide Interoperability for Microwave Access

WLAN: Wireless Local Area Network

XML: eXtensible Markup Language

3G: 3rd Generation

3G.IP: 3rd Generation IP

3GPP: 3rd Generation Partnership Project

Ringraziamenti

Una tesi è sempre frutto di un intenso lavoro, durante il quale è necessario trovare la determinazione per superare le difficoltà e portare a termine il proprio progetto. Durante il cammino che si compie per portare a termine questo impegno assumono un ruolo importante le persone che contribuiscono alla realizzazione dell'opera.

Per quanto mi riguarda devo ringraziare in particolare Sara, per le grandi doti di professionalità, disponibilità e pazienza che ha dimostrato di possedere in questi mesi.

Ringrazio anche il Cefriel, che mi ha dato la possibilità di svolgere questo interessante lavoro, fornendo il supporto per lo sviluppo del progetto.

Un grazie particolare anche al Professor Capone, sempre molto disponibile.