Alma Mater Studiorum - Università di Bologna

Facoltà di Scienze MM. FF. NN.

Corso di Laurea Specialistica in Informatica

Una rassegna di algoritmi di routing per le reti wireless opportunistiche

Tesi di Laurea

di

Luciano Maiorino

Relatore

Chiar.mo Prof.

Luciano Bononi

Sessione II

Anno Accademico 2009-2010

Indice

Elenco delle Figure

Capitolo 1

Introduzione

Negli ultimi decenni, si e' assistito ad un cambiamento rivoluzionario nelle comunicazioni wireless. Negli anni novanta, dispositivi mobili (es. laptop, PDA, telefoni cellulari), hanno avuto un grande successo da parte degli utenti che cosi' hanno scoperto, cambiando tra l'altro le loro abitudini nell'uso dei computer, la possibilita' di accedere in modo agevole a tutte le informazioni di loro interesse in qualunque momento e in qualunque luogo. Prima degli anni novanta l'uso dei dispositivi di calcolo era mirato esclusivamente al lavoro e allo studio; i dispositivi erano intesi come desktop potenti localizzati negli uffici o in altri luoghi di lavoro. Oggi, nella cosidetta eta' dei *dispositivi mobili*, gli utenti hanno la possibilita' di sfruttare il dispositivo digitale in modo nuovo per trarne numerosi vantaggi. Ad esempio l'accesso mobile ad Internet e' stato uno dei primi incentivi all'uso di dispositivi portabili; gli utenti mobili hanno cosi' potuto utilizzare i loro cellulari e/o altri dispositivi wireless per controllare e-mail e navigare sulla rete sfruttando le connettivita' internet messe a disposizione in aeroporti, stazioni ferroviarie ed altre ubicazioni pubbliche.
Da allora, anche grazie ai progressi nel mondo hardware e software, sono stati introdotti nel mercato sempre piu' dispositivi mobili potenti tanto che il periodo attuale e' detto eta' dei Sistemi Pervasivi[1]. Attualmente la connettivita' wireless e' fornita da wireless LANs (adattandole, per esempio allo standard IEEE 802.11), o da apparecchiature meno costose e di dimensioni ridotte come il Bluetooth. In ambienti dinamici, dove veicoli e/o persone hanno bisogno di essere temporaneamente

[1]Con il termine "sistema pervasivo" si intende una rete eterogenea formata da vari dispositivi quali sensori, palmari, telefoni cellulari, ecc.

interconnessi in aree senza un'infrastruttura di comunicazione preesistente (es. reti inter-vehicular e disaster-relief), o dove i costi di infrastruttura non sono giustificati (es. specifiche reti di comunita' residenziali, ecc.), le reti non basate su infrastruttura o reti ad hoc forniscono soluzioni sicuramente piu' efficienti. La piu' semplice rete ad hoc e' una rete di peer-to-peer, formato da un set di stazioni, all'interno di un range di comunicazione, che dinamicamente si auto-configurano per realizzare una provvisorio rete ad hoc single-hop.
L'estesa adozione della tecnologia di Bluetooth nei vari dispositvi ha reso quest'ultimo la soluzione piu' attinente per la realizzazione di una rete ad-hoc single-hop.
In una rete ad-hoc single-hop i dispositivi trasmettono pero' solamente quando si trovano all'interno di un range di trasmissione; questa limitazione puo' essere superata sfruttando la teconoligia ad-hoc multi-hop (MANET). A differenza delle WLANs, infatti le reti MANETs[2] sono prive di infrastruttura fissa ed i nodi che vi partecipano si autoconfigurano ed autoorganizzano tra di loro. Le MANETs si mostrano particolarmente adatte ad esigenze temporanee di gruppi di utenti che vogliano condividere dati, scambiarsi messaggi, o altro.
A tutt'oggi uno dei principali interessi di ricerca nell'ambito delle reti MANETs ha riguardato lo studio dei protocolli di routing per l'instradamento delle informazioni fra nodi sorgente e nodi destinatari. In una rete MANET infatti, vista l'assenza di infrastruttura, ogni nodo e' coinvolto nella funzione di instradamento.
In quest'ambito sta attualmente rivelandosi di particolare interesse una nuova tipologia di reti wireless, quella delle reti opportunistiche che non si appoggiano su alcuna infrastruttura fissa e non cercano di autoconfigurarsi in una infrastruttura wireless temporanea costituita da nodi vicini.
Esse sfruttano le opportunita' di contatto che si verificano fra i nodi (dispositivi wireless di piccola taglia) trasportati dagli utenti nelle loro attivita' quotidiane (ad esempio a lavoro, sugli autobus, a scuola o alluniversita', ecc.). L'idea delle reti opportunistiche deriva dalla rivisitazione critica delle ricerche sulle MANET. Purtroppo pero', pur essendo trascorsi piu' di 10 anni di ricerca sulle MANET, questa promettente tecnologia non ha massimamente coinvolto il mercato di massa. Una delle principali ragioni di cio' e' da ritrovarsi nella mancanza di un accesso concreto alla progettazione/concezione di una rete di infrastruttura ad hoc per le reti opportunistiche.

[2]Mobile Ad-hoc NETwork: e' definita come un sistema autonomo di nodi mobili connessi mediante collegamenti wireless.

Convenzionalmente la ricerca sulle MANET privilegia la progettazione di protocolli che nascondono le caratteristiche delle reti mobili via routing, in modo da esporre ai livelli piu' alti l'astrazione delle reti internet. Le peculiarita' delle reti wireless, come la mobilita' degli utenti, la disconnessione dei nodi, le partizioni delle reti, l'instabilita' dei collegamenti, sono considerati eccezioni. Cio' spesso causa che la progettazione delle reti MANET ammassi cio' che e' complesso e incerto nello stesso tempo. Anche le reti opportunistiche mirano a costruire reti fuori dai dispositivi mobili trasportati dalle persone, possibilmente senza contare su una infrastruttura preesistente. Tuttavia, le reti opportunistiche guardano alla mobilita', alla disconnessione, alle partizioni etc come caratteristiche della rete piuttosto che come sue eccezioni. Attualmente, la mobilita' e' utilizzata come modo per collegare "nubi" di nodi disconnessi e permettere la comunicazione, piuttosto che come un inconveniente di cui bisogna occuparsi. Piu' specificamente le reti opportunistiche non assumono l'esistenza di un percorso completo tra 2 nodi che desiderano comunicare. Il nodo sorgente e il nodo destinazione non potrebbero mai essere connessi alla stessa rete nello stesso tempo. Ciononostante la tecnica delle reti opportunistiche permette a tali nodi di scambiarsi messaggi. Attraverso il paradigma *store-carry and forward*, i nodi intermedi (quelli tra sorgente e destinazione) memorizzano i messaggi quando non c'e' l'opportunita' di inoltrarli alla destinazione finale e sfruttano ogni possibilita' di contatto futuro con altri dispositivi mobili per portare il messaggio piu' prossimo e piu' vicino alla destinazione. Questa tecnica di costruzione di una infrastruttura auto-organizzante delle reti wireless risulta essere molto piu' pratica del convenzionale paradigma MANET. In verita', malgrado il fatto che con la ricerca sulle reti opportunistiche si e' ancora ad uno stadio precoce, il concetto di reti opportunistiche e' oggi gia' sfruttato in un buon numero di applicazioni concrete, come si vedra' nel corso di questa trattazione. E' necessario comprendere che i modelli di mobilita' degli utenti siano la chiave in questo ambiente di rete dal momente che e' la mobilita' che permette le comunicazioni end-to-end. Infatti il successo della trasmissione delle reti opportunistiche e' strettamente legato alle dinamiche sociali in cui sono coinvolti gli utenti che trasportano i dispositivi, ed alla storia degli incontri tra individui. Data la mobilita' estremamente elevata che caratterizza questo nuovo scenario di reti e la nota rumorosita' delle comunicazioni wireless, l'affidabilita' delle trasmissioni emerge come uno dei fattori di principale interesse. Non a caso, le comunicazioni possono aver luogo soltanto durante i periodi di contatto tra i nodi e devono essere veloci ed efficaci. Questo porta a dover progettare nuovi pro-

tocolli di comunicazione che si diversifichino da quelli oggi piu' diffusi e basati sulla ritrasmissione dei dati mancanti. Le ritrasmissioni infatti, nella maggior parte dei casi, potrebbero non poter essere eseguite per mancanza di tempo. Una strategia valida per gestire l'affidabilita' delle comunicazioni opportunistiche in simili scenari estremi (caratterizzati cioe' da scarse risorse e scarsa connettivita') prevede l'utilizzo combinato di tecniche di codifica dei dati e strategie di instradamento di tipo epidemico. Questo approccio sfrutta la ridondanza sia delle informazioni, sia dei percorsi. La ridondanza delle informazioni da' robustezza a fronte della perdita dei dati in rete poiche' e' necessario che soltanto un sottoinsieme dei codici generati arrivi a destinazione per consentire la ricostruzione corretta delle informazioni. La ridondanza dei percorsi invece e' necessaria poiche' non e' possibile predire in anticipo la sequenza dei contatti che puo' portare i dati a destinazione e pertanto e' necessario distribuire l'informazione in piu' direzioni. Le reti opportunistiche caratterizzate dalla presenza di dispositivi con limitata autonomia energetica e risorse limitate, offrono attualmente lo scenario che meglio traduce il concetto di sistemi pervasivi.

Capitolo 2

Evoluzione: dalle MANETs alle RETI OPPORTUNISTICHE

Negli ultimi anni abbiamo assistito alla diffusione delle MANETs (Mobile Ad hoc NETworks) in molti ambienti applicativi. Originariamente concepita per applicazioni militari con l'obiettivo di migliorare le comunicazioni e la sopravvivenza nei campi di battaglia, le MANETs stanno recentemente trovando applicazioni in scenari civili. In agricoltura, per esempio, per raccogliere informazioni riguardo le condizioni del suolo, quelle metereologiche. Informazioni utilizzate per mettere a punto la semina, il fertilizzante al fine di migliorare la quantita' e la qualita' del raccolto. Un altro scenario le autostrade intelligenti, sono state diffuse per sfruttare le comunicazioni ad hoc tra veicoli per fornire assistenza guidata, migliorare la sicurezza.
Reti ad hoc possono anche servire piccole comunita' per esempio, per fornire un servizio temporaneo di condivisione dei dati. Infine, *home automation* sta emergendo come un nuovo interessante campo di applicazioni. Recentemente supportato dalla tenologia Zigbee, consente basso data rate e bassi consumi di energia tra applicazione e dispositivo, inoltra consente un sistema di controllo della luce, del condizionamento, delle porte e delle finistre. Oggi le reti ad hoc stanno evolvendo verso le reti opportunistiche dove gli approcci la gestione del routing sono integrati con tecniche che sfruttano le *comunicazioni opportunistiche*.
Molti dei concetti che stanno dietro le reti opportunistiche provengono dai primi studi su *Interplenetary Networks (IPNs)* e, successivamente, su *Delay Tolerant Networks (DTNs)*. Sebbene questi tipi di rete non sono ad hoc (specialmente IPNs) essi originariamente affrontarono il problema della intermittenza della connettivita' e servendosi di tecniche basate sul *store and forward* per il routing.

Questo capitolo propone una panoramica sull' Interplenetary and Dalay Tolerant Networks e succisamente si vedra' in dettaglio la rete opportunistica.

2.1 Da InterPlaNetary networks ai Delay Tolerant Networks

Nel 1998, la DARPA Next Generation Internet finanzia l'iniziativa dell'Interplenetary Internet Project con l'obiettivo di definire un sistema di comunicazione in grado di garantire gli stessi servizi forniti da internet attraverso distanze interplanetarie. Originariamente sviluppato per supportare le esplorazioni nello spazio. Durante la fase realizzativa del progetto, presto si capi' che il sistema di comunicazioni terrestre non si sarebbe adattato nello spazio in quanto si basano su assunzioni che non sono verificati nello spazio, come:

- *End-to-end connectivity*: ci si attende che si conosca un percorso completo tra nodo sorgente e nodo destinazione;
- *High capacity links*: le comunicazioni terrestre permettono di inviare segnali alla velocita' della luce con piccoli ritardi di propagazione (frazioni di secondi per un singolo pacchetto quando si usa il protocollo TCP);
- *Reliable links*: le comunicazioni terrestri presentano un basso livello di errore, sebbene possono soffrire le congestioni della rete dovute;
- *Symmetric links*: i ritardi di propagazione dalla sorgente alla destinazione e dalla destinazione alla sorgente sono generalmente gli stessi.

Grazie alle assunzioni vista, le comunicazioni terrestre possono far uso di protocolli *chatty* per gestire le informazioni scambiate (sia dati e controlli) tra le parti comunicanti. I protocolli chatty garantiscono affidabilita' e alta reattivita' alla perdita dei dati, ma nello stesso tempo fa uso di un modello di comunicazione stile phone-call, in quanto necessita di uno scambio real-time per essere realizzato.
Nello spazio, le comunicazioni sono invece caratterizzate da:

- *High propagation delays and round trip times* [1]*:* le distanze tra pianeti sono enormi e inducono a forti ritardi di propagazione dell'ordine di minuti. Questo

[1]Round Trip Time:Il tempo necessario per un pacchetto per raggiungere la destinazione e tornare indietro.

rende improponibile utilizzare un protocollo di trasporto che si basi su un lungo handshaking tra coppie di nodi (come per esempio TCP) in quanto potrebbe richiedere molto tempo il solo trasferimento di un singolo dato;

- *Low data rate:* i segnali radio si degradano facilmente e si attenuano su lunghe distanze;

- *Intermittent connectivity:* delle volte e' possibile che non esista un percorso completo dovuto al movimento dei pianeti. Inoltre, le distanze tra pianeti variano e questi cambiamenti avranno effetti negativi sui ritardi, capacita' delle trasmissioni, connettivita' e topologia della rete.

- *Asymetric links:* le trasmission da Marte a Terra, per esempio, possono essere ricevuta a 100 Kilobits/secondo mentre viceversa soltanto a 1 kilobits/secondo;

- *Nedd for special equipment:* le trasmissioni nello spazio sono costose in quanto necessitano di speciali strumenti.

Appare chiaro, dalle caratteristiche appena viste, come risulti neccessario adottare protocolli non-chatty, in quanto risultano piu' adattabili per le comunicazioni nello spazio. Inoltre, i protocolli piu' adatti dovrebbero anche impacchettare piu' dati possibili in una singola trasmissione per minimizzare il numero di round-trip necessari. In questo modo la totale trasmissione puo' finire velocemente in una IPN e rendere piu' efficiente l'uso di reti ad alte velocita'. L'architettura che sta emergendo dal progetto Internet InterPlaNetary consiste in una rete di internet; per esempio, un insieme di internet indipendenti, interconnessi da un sistema di *IPN gateway*. Le singole reti di internet sono locate lontane le une dalle altre fino a formare distinte *regioni IPN*. Ognuna di queste regioni si appoggia su differenti protocolli che sono scelti tra quelli che meglio si adattano alla particolare infrastruttura, ai mezzi di comunicazione, alle tecnologie disponibili in quella particolare regione di internet, differendo naturalmente dai protocolli delle altre regioni IPN. In aggiunta ai livelli di trasporto di ogni IPN, abbiamo un protocollo di copertura per gestire le comunicazioni end-to-end tra le stesse regioni. Per identificare un nodo appartenente ad una rete IPN, viene introdotto un indirizzo speciale costituito da due identificatori: il primo e' un region ID che identifica, al livello di copertura, la regione IPN in cui il nodo e' locato; anche il secondo e' un identificatore regionale che identifica il nodo dentro la sua regione IPN, ma al livello di trasporto. Va notato che il sistema di

denominazione deve differire da regione a regione IPN e conseguenzialmente gli identificatori regionali non possono essere risolti ovunque, ma in ogni loro propria regione IPN. Cosi' l'inoltro del messaggio viene realizzato mediante due passaggi. Inizialmente il region ID di destinazione del messaggio viene interpretato e il messaggio e' inoltrato al corretto IPN region di destinazione (ogni nodo e' in grado di interpretare il region ID).Giunto all'IPN region di destinazione, il region ID di destinazione viene interpretato e il messaggio inoltrato allo specifico nodo di destinazione. Da questo momento, il messaggio inoltrato e' guidato al livello di copertura finche' la regione IPN di destinazione non viene raggiunta; poi viene condotto al livello di trasporto dove il region Id e'interpretato e il messaggio viene finalmente mandato al nodo di destinazione. I nodi possono essere distinti in *hosts, routers e gateways*. I nodi hosts possono inviare e ricevere messaggi, ma non possono inoltrarli. I routers inoltrano i messaggi alla stessa IPN region e possono a richiesta agire come hosts. Infine i nodi gateways sono in grado di inoltrare messaggi tra due o piu' regioni IPN e sono percio' i piu' complessi nodi nella complessiva architettura IPN. Quando le comunicazioni avvengono all'interno di una singola regione, essi hanno bisogno di gestione solamente al livello di trasporto che e' fornito dallo specifico protocollo di trasporto implementato in quella regione. Tra l'altro le comunicazioni tra regioni IPN seguono, in sequenza, i protocolli di trasporto di ogni singola regione che attraversano. Quindi le comunicazioni tra le regioni IPN non possono essere gestite ovunque, ma solo al livello di copertura poiche' questo abbraccia tutte le regioni IPN attraversate. Ogni trasporto di connessione termina al margine della corrispondente regione IPN, precisamente all'IPN gateway. Inoltre il gateway provvede alla trasmissione dei dati in arrivo da un'interfaccia ad un'altra dopo aver cambiato il protocollo di trasporto e puo' anche comportarsi da nodo host. Il livello di copertura e' una sorta di protocollo di trasporto a lungo raggio ed e' anche chiamato *bundle layer* ed e' presente in tutte le regioni IPN.*Bundle* e' anche il nome di un messaggio scambiato in una IPN. Infatti esso colleziona molte parti di informazione, includendo gli user data generati dalla applicazione sorgente e qualche informazione di controllo fornita anche dalla sorgente per l'applicazione di destinazione. Ulteriori informazioni concernono il modo di processare, memorizzare e in generale trattare gli user data.Un bundle puo' altresi' contenere informazioni per l'autenticazione all'host di destinazione (es. login , password....)oltre alle specifiche di affidabilita', qualita' del servizio, sicurezza o anche gestione del recupero di errori. La motivazione alla base del bundle e' il bisogno di ridurre il complessivo ritardo di trasmissione anche se le distanze interplanetarie

tendono ad aumentare. Non a caso e' piu' efficace mandare tutti i dati necessari subito piuttosto che seguire la lunga sequenza di handshaking. Oltretutto un bundle include uno special header aggiunto dallo stesso bundle layer. La lunghezza totale di un bundle puo' essere arbitraria, anche se al bundle layer viene gestita qualche forma di frammentazione. Durante la trasmissione bundle lungo il percorso tra il nodo sorgente e il nodo destinazione , puo' accadere che un hop successivo non sia disponibile per l'inoltro, cioe' all'hop successivo non disponibile la connessione (connettivita' intermittente). Questo puo' accadere perche' le risorse da utilizzare per la trasmissione sono temporaneamente impegnate a trasmettere traffico di alta priorita' o perche' l'hop successivo e' raggiungibile solo attraverso una connessione di linea (es. quando un satellite e' visibile). Percio' i bundles hanno necessita' di buffering mentre sono in attesa di inoltro. Inoltre, dato che la connessione puo'essere disponibile in ore, giorni o anche settimane, e' tipicamente richiesto un persistent storage. Questo e' differente da cio' che generalmente succede in internet in cui i messaggi sono memorizzati in routers intermedi per pochissimo tempo, cioe' per frazioni di secondo. Il paradigma di comunicazione store and forward sfruttato anche per consentire la minimizzazione di interattivita' tra endpeers durante un trasferimento bundle. Cosi' il nodo che per primo manda un bundle mantiene una sua copia in una memoria persistente dopo la trasmissione fino al recepimento di un acknowledge dall'hop vicino. Questo e' il primo custode del bundle perche' trattiene la sola copia affidabile del bundle e, se necessario, la usera' per la ritrasmissione. Quando il custode del bundle lo manda al suo nodo successivo, quest'ultimo richiede la *custody bundle* per quel bundle e inizia un time-to-acknowledgement di ritrasmissione. Se il livello bundle dell'hop successivo accetta la custodia del bundle, esso rimanda un acknowledgement al mittente. Se il custode del bundle non riceve alcun acknowledgement prima che il time-to-acknowledgement del mandante spiri, esso trasmette ancora una volta il bundle all'hop vicino. Il custode del bundle memorizza il bundle fino a quando un altro nodo non accetta la custodia del bundle o il tempo-di-vita del bundle non spiri. Poi, o viene ad esistenza un nuovo custode del bundle o il bundle non ha piu' ragione di esistere. Cosi' la copia del bundle viene scartata dall'obsoleto custode. Il tempo-di-vita di un bundle e' ovviamente molto piu' lungo del time-to-acknowledgement di ciascun custode. L'affidabilita' node-to-node viene percepita dalle ritrasmissioni locali gestite al livello di trasporto dentro le singole regioni IPN. Cio' e' differente da quello che succede nel protocollo TCP dove le ritrasmissioni sono trattate in maniera end-to-end e il nodo sorgente ritrasmette i dati nel caso

di un acknowledgement perso dal nodo destinazione. Questo approccio e' impossibile in un ambiente IPN a causa degli elevati ritardi end-to-end coinvolti, mentre le ritrasmissioni dentro le singole regioni IPN sono piu' veloci e piu' efficienti. Per questo, i protocolli affidabili al livello di trasporto e i trasferimenti che riguardano la custodia sono usati dal livello bundle per muovere i punti di ritrasmissione progressivamente verso il nodo destinazione. Nel caso in cui il nodo sorgente desideri una notificazione finale della consegna, il nodo destinazione deve inviare una separata ricevuta di ritorno alla sorgente dopo aver ricevuto il bundle. La ricevuta di ritorno viene trasmessa come un nuovo bundle ed e' soggetta agli stessi trasferimenti in custodia, come la trasmissione originale. La ricevuta e' simile a quella utilizzata nel sistema postale. Nell'Ottobre 2002 un nuovo gruppo di ricerca fu istituito in seno all' Internet Research Task Force per trasformare l'architettura internet IPN in *Delay Tolerant Network (DTN)*.Questa architettura piu' generale e' destinata a diventare sempre piu' importante nel panorama delle comunicazioni terrestri dato che lo scenario globale di internet va rapidamente evolvendosi con l'introduzione di nuove tecnologie per l'accesso e con la diffusione di nuovi ed eterogenei dispositivi aventi differenti portabilita' e capacita' in termini di elaborazione, memoria e fornitura di energia. Internet e' sempre piu' simile ad un'aggregazione di *isole (le regioni) di omogeneita'* dove il percorso dei dati end-to-end da un nodo sorgente ad un nodo destinazione abbraccia un'ampia varieta' di ambienti. Ogni singolo dato hop e' inserito in un'area di omogeneita' ed e' quasi istantaneamente attraversato; solo un po' di ritardo e' accumulato tra le aree consecutive per cambiare tecnologia e protocollo. Date le somiglianze tra l'architettura IPN e l'attuale Internet, i concetti del protocollo DTN devono essere pensati come avebti il potenziale per aumentare in modo significativo la capacita' di Internet di adattare l'estrema eterogeneita' che ne emerge cosi' da favorire eventualmente la consegna end-to-end di informazioni. Esempi di ambienti con applicazioni terrestri per l'architettura DTN sono: Military Tactical Networks, Sensor Network e Intelligent Highways. Nel primo i nodi sono interconnessi dalla strumentazione di elicotteri, satelliti, aerei etc. e a causa della loro elevata mobilita', le connessioni potrebbero essere intermittenti e talvolta asimmetriche. Inoltre, i ritardi entro le parti connesse della rete potrebbero essere estremamente variabili. Il Sensor Network invece potrebbe soffrire di partizionamento dato che qui i nodi hanno vincoli riguardo all'energia e hanno periodicamente bisogno di passare ad una condizione di basso consumo di potenza. Nell'Intelligent Highways i nodi comunicanti sono sui veicoli nelle autostrade e il

dato e' instradato da veicolo a veicolo fino a che non giunge ad un'infrastruttura. Questo tipo di rete e' concepita per evitare il congestionamento del traffico, per poter calcolare dei percorsi alternativi, per localizzare dei punti di interesse, per salvaguardare la sicurezza, etc. Un'altra applicazione interessante del DTN e' stata di recente presa in considerazione nel contesto del progetto *SAAMI NETWORK CONNECTIVITY(SNC)*. Il progetto teso a fornire la connettivita' alle popolazioni di pastori di renne nomadi Saami. Essi vivono nella regione del Sapmi (conosciuta anche come Lapland), situata nella parte piu' settentrionale della Svezia, della Norvegia e della Finlandia. Il Popolo delle Otto Stagioni, cosi'i Saami sono chiamati, si muovono attraverso i loro villaggi durante l'anno seguendo la migrazione delle renne. Sebbene vi sia un grande interesse a tutelare e difendere le abitudini, la cultura e le tradizioni di questa popolazione aborigena, vi e' anche un crescente bisogno di favorire la loro integrazione nella societa' moderna dei loro Paesi. Infatti, dato che il reddito di un pastore di renne non e' sufficiente a fornire i mezzi di sussistenza necessari, sempre piu' persone Saami sono impegnate in lavori diversi dalla pastorizia, come ad esempio nell'insegnamento, nella professione di infermiera e nel giornalismo. La possibilita' di lavorare a distanza e attraverso la rete permetterebbero ai Saami di continuare a vivere secondo le loro tradizioni e, allo stesso tempo, di avere piu' sostentamento economico. I servizi basati sulla rete potrebbero altresi' permettere ai bambini Saami di essere educati senza la necessita' di lasciare i loro genitori per frequentare i collegi e la connettivita' di rete potrebbe contribuire a favorire i diritti dei Saami per essere piu' visibili e cosi' influenzare gli affari politici ed economici dei loro Paesi. Nella sua fase iniziale il progetto SNC si e' solo focalizzato sulla consegna di email, sul trasferimento di file e sulla fornitura di servizi web per il popolo Saami; in prospettiva si vorrebbe fornire un supporto al pastore anche per la sua attivita'.Tutto cio' ci permette di dire che l'IPN e il DTN sono di fatto dei punti di partenza per le reti oppotunistiche. Infatti i concetti di base della rete opportunistica sono tutti inclusi nei paradigmi IPN e DTN, dalla connettivita' intermittente al modello di comunicazione store and forward fino alla tecnica di custodia nel trasferimento.

Capitolo 3

Opportunistic Networks

Le reti opportunistiche sono uno delle piu' interessanti evoluzioni delle classiche Mobile Ad Hoc Network(MANET). L'ipotesi principali in un ambiente MANET e' che il mittente e la destinazione di un messaggio siano collegate contemporaneamente alla rete. In un ambiente pervasivo, i nodi verranno raramente a trovarsi collegati contemporaneamente alla rete. Le reti opportunistiche mirano a rendere gli utenti in grado di scambiare dati in tale ambienti, sfruttando la vicinanza di altri dispositivi per inoltrare messaggi piu' vicini alla destinazione. A tal fine, i protocolli progettati per le MANET dovrebbero essere drasticamente riprogettati. Un primo approccio di routing consiste in una inondazione controllata: i messaggi vengono inoltrati con un tempo di vita limitato (TTL, Time-To-Live) e consegnati ad un destinatario che entri in contatto con un nodo che abbia ricevuto il messaggio durante l'inondazione. Altri approcci cercano di limitare i costi delle inondazioni acquisendo informazioni riguardanti il contesto. Le informazioni di contesto sono informazioni che descrivono la realta' in cui l'utente vive e la storia delle relazioni sociali tra gli utenti. Cosi', il contesto puo' essere definito da informazioni personali sull'utente (ad esempio il nome), sulla sua residenza (ad esempio l'indirizzo), sul suo lavoro (ad esempio istituzioni). Il protocollo di routing potrebbe trasmettere i messaggi attraverso persone che vivono nello steso luogo o in luoghi vicini.

3.1 Applicazioni e casi di studio delle Reti Opportunistiche

Nonostante il fatto che la ricerca sulle reti opportunistiche risalga a pochi anni or sono, le sue applicazioni concrete e gli studi sui casi reali sono gia' disponibili. Molti esperimenti sono stati condotti allo scopo di provare la possibilita'di sfruttare i contatti tra gli utenti mobili nella loro vita quotidiana. Le esperienze sono state fatte prendendo in considerzione comunita' molto differenti tra loro: studenti di una Universita', cittadini di diverse citta', macchine sulle autostrade o sulle strade urbane, specie selvatiche nel loro ecosistema. Tutti questi esperimenti differiscono per molti aspetti:

Modelli di mobilita' degli utenti Gli utenti presi inconsiderazione sono stati dei pedoni, delle auto, delle zebre, delle balene, etc.. Essi si muovono tutti a velocit differenti e seguendo sia percorsi liberi che percorsi obbligati. Le zebre si muovono liberamente nella savana, cosi' come le balene nell'oceano. Gli studenti in un campus lo fanno in maniera piu' sciolta, ma in spazi piu' piccoli. Persone e macchine seguono invece percorsi obbligati cio pavimenti e strade. Tra l'altro la mobilita' influenzata anche dalla particolare situazione che i soggetti stanno vivendo e dalle loro intenzioni e scopi. Cosi' una zebra e' piu' lenta quando pascola che quando scappa da un predatore. Similarmente una macchina in un area a traffico congestionato cammina piu' lentamente di quando viaggia su una strada deserta e uno studente quando passeggia in un cortile va piu' adagio rispetto a quando corre, perche' in ritardo,in direzione della sua classe. Anche il tempo influenza il modello di mobilita', specialmente tra la gente. La densita' demografica e le auto in strada sono diverse dal giorno alla notte, cosi' come nelle varie ore della giornata, ad es. nell'ora di punta rispetto alle altre ore del giorno.

Dispositivi di comunicazione Generalmente le persone portano con loro laptops o PDAs; una strumentazione piu' pesante e maggiormente potente e' invece adatta alla comunicazione tra auto a causa dell'assenza di vincoli di peso; alle balene sono applicate sensori molto luminosi e resistenti all'acqua, mentre le zebre indossano collari con sensori e pannelli solari. Tutti questi dispositivi sono caratterizzati da differenti ranges di trasmissione.

Fenomeni di interferenza e disturbi Mentre le comunicazioni nella savana si verificano praticamente senza fenomeni di disturbo, sulle autostrade come sulle strade urbane e suburbane esse sono frequentemente soggette a interferenze dovute al

rumore o a fenomeni di riflessione causati ad esempio dalle costruzioni. Sott'acqua le comunicazioni di suoni sono molto lente a causa degli stessi mezzi di comunicazione e in posti affollati esse sono rese difficili perche', per esempio, piu' persone desiderano comunicare nello stesso tempo, creando cosi'la congestione della rete.

Modello di connettivita' Il modello di connettivita' dipende dalla densita' della rete, dal range di trasmissione dei dispositivi usati e dalle interferenze presenti nell'ambiente. Una buona connettivita' e' realizzabile in poche reti quando i dispositivi sono molto potenti e hanno un lungo range di trasmissione. D'altra parte le reti dense hanno bisogno di piu' bassi ranges di trasmissione, ma sono piu' inclini ad errori di comunicazione, dovuti a congestione e interferenza. In definitiva, e' piuttosto difficile, o anche impossibile, prevedere il modello di connettivita' di un ambiente reale. Da cio' deriva l'importanza delle esperienze che saranno descritte, dato che esse mostreranno cosa accade attualmente nelle fattispecie prese in considerazione, evidenziando anche gli aspetti-chiave a cui stare attenti mentre si progettano le architetture e i servizi di rete. Sfortunatamente, pero', come e' comprensibile, l'esperimento in ambienti reali richiede enormi sforzi ed e' molto oneroso. Di conseguenza, sono stati utilizzati diversi metodi sperimentali e spesso le esperienze reali sono state mischiate alle simulazioni per ragioni di semplicita' e per evitare costi elevati.

3.1.1 Campus college

Questo esperimento e' stato condotto di recente in una Universita' di Toronto, Canada. L'intenzione e' quella di dimostrare che e' possibile favorire la consegna dei messaggi tra i componenti di una comunita' sfruttando semplicemente i contatti a coppia tra gli stessi partecipanti, in assenza dei tradizionali protocolli ad hoc di routing. I messaggii vengono assunti per essere inoltrati in maniera casuale, cosi' come casuali sono gli incontri tra le persone. Quando la gente si incontra, diffonde dei messaggi intorno a se': si manda il messaggio a colui che si incontra, che pero'non abbia gia' ricevuto lo stesso messaggio (inoltro epidemico). E' stato anche accertato che i soggetti piu' socievoli hanno piu' successo nelle trasmissioni dei messaggi in quanto sono interessati ad un piu' alto numero di contatti a coppia e percio' sono in grado di consegnarli alla stragrande maggioranza della comunita'. Pertanto, mediante i diversi modi di spedizione dei partecipanti, e' possibile concepire piu' efficienti politiche di inoltro, piuttosto che soffermarsi su un'unica politica di inoltro epidemi-

co. Due distinti esperimenti [7] sono stati condotti in differenti periodi. Durante la prima fase di ambedue esperimenti, ad alcuni studenti (a laureati nel primo caso e ad universitari nel secondo) furono dati dei dispositivi palmari, dotati di tecnologia bluetooth, da portare con se'tutto il giorno. I PDA tennero traccia dei contatti pair-wise avuti dagli studenti durante la loro vita quotidiana per alcune settimane. Furono anche nascosti dei PDA fissi in alcuni luoghi abitualmente frequentati dagli studenti, in modo da simulare la presenza di stazioni-base. Essi tuttavia non avevano una speciale caratteristica di implementazione. Durante la seconda fase degli esperimenti, i dati raccolti furono elaborati tramite una simulazione e furono studiate le opportunita' di pacchetti di consegna multi-hop. Furono messe in evidenza molte di queste opportunita', oltre che una serie eccessivamente ridondante di percorsi tra le coppie di nodi. L'esperienza dimostro'che la mobilita' degli utenti puo' essere sfruttata con successo per dare vita a reti ad hoc. Infatti i nodi ebbero contatto e raggiungibilita' significativa tra loro. Inoltre, i modelli di connettivita' non furono particolarmente influenzati dai nodi fissi, il che significa che la mobilita' degli utenti fu la principale responsabile della connettivita' tra i nodi. Tutto cio' porto' a concludere che i potenziali guadagni della rete sarebbero stati possibili se la comunicazione pair-wise fosse stata utilizzata, per esempio, per estendere il campo degli WI-FI hot-spots. La raggiungibilta' multi-hop fu studiata, considerando una politica di inoltro epidemico. Comunque, dall'analisi della percentuale di consegne avvenute con successo, e' stato scoperto che alcuni nodi vicini erano piu' affidabili di altri, evidenziando cosi' la possibilita' di concepire strategie di routing piu' efficienti. I risultati furono abbastanza incoraggianti, anche se ottenuti su un numero relativamente piccolo di utenti (venti per ogni esperimento). Aumentando il numero di utenti coinvolti, la connettivita' di rete sicuramewnte migliorerebbe. Da questo esperimento si e' anche messa in luce l'importanza del meccanismo di *power management* attualmente disponibile nei dispositivi mobili. Durante l'esperimento si e' avuta una drammatica perdita di dati, dovuta all'esaurimento della batteria (i dispositivi furono forniti solo con memorie volatili). Non furono abbastanza sufficienti 8-10 ore di carica, considerando che i PDA per la monitorizzazione dei contatti erano utilizzati anche per terze applicazioni (es. giochi) in modo da motivare gli utenti a portarseli con loro per piu' tempo possibile. Gli esperimenti non trasmisero alcun dato reale, ne' tantomeno rilevarono la qualita' della connessione, non misurarono il bandwidth, ne' tracciarono la locazione dell'utente.

3.1.2 Pocket Switched Networks

I contatti pair-wise possono essere descritti mediante due parametri: durata dei contatti e tempo intercorrente tra i contatti. Il primo e' il tempo totale durante il quale due nodi mobili sono in vista uno dell'altro e dunque hanno la possibilita' di comunicare. Il secondo e' invece il tempo che intercorre tra due opportunita' di contatto. Mentre la durata dei contatti influenza direttamente la capacita' delle reti opportinistiche poiche' limita la quantita'di dati che possono essere trasferiti tra i nodi, il tempo tra contatti influisce sulla fattibilita' delle reti opportunistiche. Infatti esso determina la frequenza con cui i pacchetti possono essere trasferiti tra dispositivi di rete. L'Universita' di Cambridge, insieme con l'Intel Research of Cambridge ha recentemente studiato [11] sia il problema della fattibilita' che quello della capacita' delle Oppnets, analizzando i risultati di esperimenti similari a quello sopradescritto del college campus. Il primo esperimento che deve essere preso in esame fu condotto all'Universita' della California di San Diego (USA) col coinvolgimento di 275 utenti PDA, precisamente studenti della stessa universita' [12]. Il campus aveva una vasta area di copertura wireless di cui gli studenti potevano usufruire con i loro PDAs. La zona di ricezione fu fornita di circa 400 punti di accesso. I PDAs con sistema WiFi periodicamente registravano informazioni di tutti i punti di accesso che essi potevano percepire (il periodo di campionatura era di circa 20s). L'esperimento duro' 11 settimane. Il secondo esperimento [13] fu condotto al Dartmouth College di Hanover, anch'esso in un college campus con una copertura di 802.11b, provvista di 566 punti di accesso. Durante l'esperimento, furono raccolte per oltre 17 settimane le informazioni (indirizzi MAC e IP) relative ai clienti associati con ogni punto di accesso.I dispositivi WiFi monitorati erano PDA, laptop e anche qualche telefono VoIP, mentre gli utenti presi in considerazione furono circa 7000. Sebbene gli esperimenti descritti nel paragrafo precedente non fossero stati condotti su mere reti ad hoc, essi hanno fornito comunque preziose informazioni sulla mobilita' degli utenti in ambienti reali. Per cui, le tracce provenienti da quelle esperienze furone trasformate per ottenere informazioni sui contatti di una potenziale rete ad hoc. I dati furono trasformati come segue. Si suppone che ci fosse una opportunita' di contatto tra due nodi ogni volta che quest'ultimi risultassero essere simultaneamente in vista di uno stesso punto di accesso. Oggi sappiamo che tale ipotesi e' soggetta ad errore dato che, pur essendo in vista di uno stesso punto di accesso, due dispositivi potrebbero non essere uno alla portata dell'altro. D'altra parte due dispositivi potrebbero essere uno nel range dell'altro, ma posizionati in luoghi in cui non e' presente un

punto di accesso strumentato, quindi le loro opportunita' di connessione potrebbero non avere la possibilita' di essere registrate. Nonostante queste imprecisioni, i dati raccolti possono essere considerati una buona approssimazione degli attuali dati e sono una fonte preziosa di risultati poiche' l'esperimento si estese per parecchi mesi e incluse migliaia di nodi. Un altro esperimento fu condotto dalla stessa Universita' di Cambridge e dall'Intel Research; furono usati dei dispositivi dotati di Bluetooth costituiti da molto leggere e portatili piattaforme iMote che le persone potrebbero portare con loro per tutto il giorno. Lo stesso esperimento fu ripetuto per 2 volte; la prima volta all'Intel Research e la seconda all'Universita' di Cambridge. Il primo esperimento coinvolse 17 ricercatori per 3 giorni, mentre il secondo coinvolse 18 persone , sia studenti dottorandi che ricercatori, per 5 giorni. Periodicamente le piattaforme iMote eseguirono delle indagini per tenere traccia delle altre iMotes visibili o anche di dispositivi esterni dotati di bluetooth (il periodo di campionatura era di due minuti). Quindi, con l'inclusione di coloro che usavano un dispositivo dotato di bluetooth, le persone coinvolte furono molto piu' di quelle che erano state individuate inizialmente. Infatti la scelta del bluetooth come tecnologia wireless da usare per l'esperimento fu proncipalmente motivata proprio dalla vasta diffusione dei dispositivi bluetooth (cuffie, PC set, etc...) che garantivano di avere piena contezza dei modelli di mobilita'e dei contatti pair-wise. L'analisi dei risultati porto' ad affermare che sia il tempo tra contatti, sia le durate dei contatti sono delle *funzioni di distribuzione*, simili a leggi di potenza [1]eggi di potenza ricorrono nelle distribuzioni di probabilit di molti fenomeni fisici (ad esempio la magnitudo dei terremoti, il diametro dei crateri dei pianeti, la dimensione dei frammenti degli oggetti che si infrangono per urti, l'intensit delle esplosioni solari), sociali (il numero dei morti nelle guerre, la popolazione delle citt, il numero di collegamenti ai siti web, il numero di citazioni) ed economici (la distribuzione della ricchezza, le vendite di libri e cd, ecc.). Inoltre le funzioni della legge di potenza hanno differenti coefficienti che dipendono dalla diversa tecnologia in uso. Questo ha interessanti implicazioni sul ritardo che ogni pacchetto si presume subisca in tutta la rete. Specificamente e' stato provato con analiticita' che algoritmi stateless di inoltro causano un infinito ritardo previsto cioe' essi non convergono, mentre lo fanno quegli algoritmi che usano trasmissioni multiple.

[1] L

3.1.3 Veicoli che si muovono in autostrada

Possono i veicoli in una autostrada formare una rete ad hoc e scambiare messaggi? Inoltre, possono le auto essere considerate una comunita' dove i contatti occasionali possono aiutare la consegna dei messaggi? Di seguito sono presentati due studi, condotti usando la stessa metodologia, ma aventi obiettivi differenti. Tali studi consistono in simulazioni basate sul simulatore di rete ns-2 [14] con il modello di mobilita' dei nodi generato dal CORSIM (CORridor SIMulator) [15] [2]n simulatore di traffico sviluppato dalla Federal Hightway Administration al dipartimento di trasporto degli US. Mentre il primo caso di studio [16] consiste nell'analizzare le caratteristiche di una Vehicle Ad hoc NETwork (VANET) in termini di cambiamenti della topologia, durata dei collegamenti, e ridondanza dei percorsi; il secondo caso di studio [17] si concentra sulle capacita' opportunistiche di una rete ad hoc in relazione alla mobilita' dei veicoli in autostrada. I risultati [18] del primo studio mostrano che una VANET su un'autostrada e' soggetta a rapidi cambiamenti della topologia della rete e a forti frammentazioni, a causa della velocita' dei veicoli che viaggiano in entrambe direzioni. Inoltre i diametri delle porzioni di rete connesse erano molto brevi. Le simulazioni si sono realizzate su un segmento di autostrada di circa 15km, con 10 uscite, con solo il 20% di nodi con dispositivi radio e assumendo nodi con una portata radio di 150m. La connettivita' ha mostrato miglioramenti con l'aumentare del range di trasmissione. Tuttavia ogni nodo generalmente riuscito a raggiungere non piu' del 37% degli altri nodi presenti nella stessa sezione di autostrada. Infine, si e' notato che la connettivita' ha subito dei rapidi cambiamenti, che spesso hanno causato la disconnessione dei percorsi prima che il trasferimento di un intero dato potesse essere completato. In seguito si e' concluso che l'utilizzo di algoritmi di routing, basati su un preventivo calcolo del percorso, fosse inadatto per tale scenario. L'ambiente di simulazione [17] per il secondo studio e' stata una porzione di autostrada di 10 km. Si e' supposto che ogni nodo avesse un range fisso di trasmissione di 200m e che fosse a conoscenza della propria posizione e di quella degli altri nodi all'interno della rete. L'invio del messagio e' stato eseguito su una base hop-by-hop e ha seguito un'avida strategia. Specificamente, ogni messaggio e' stato spedito all' hop successivo, quello piu' vicino al nodo destinazione. Si sono indagate due varianti della strategia di routing: il *routing ottimistico* e il *routing pessimistico*. In base ad una politica pessimistica, un pacchetto e' stato scartato

[2] u

ogni volta che non c'era alcun nodo successivo che risultava essere piu' vicino alla destinazione rispetto allo stesso nodo designato per la spedizione. In accordo, invece, con un inoltro ottimistico, nel caso in cui non c'era alcun hop successivo disponibile per l'invio, il pacchetto e' stato memorizzato in attesa di una susseguente opportunita' di inoltro. I risultati hanno mostrato che l'inoltro ottimistico ha contribuito ad aumentare l'indice di consegna, anche se al prezzo di un ritardo un po' piu' lungo (entro 200s). E' stato cosi' possibile concludere che una rete che approfitta della mobilita' dei nodi puo' operare con una densita' di nodi inferiore e mantiene la stessa media di ritardo. I risultati hanno anche evidenziato che sia il numero crescente di corsie (meglio se piu' di tre), sia il relativo movimento dei veicoli nelle due opposte direzioni contribuiscono a diminuire il ritardo end-to-end.

3.1.4 FleetNet

Le VANETs possono essere studiate anche nel contesto del FleetNet Project che e' stato realizzato dal 2000 al 2003 col finanziamento parziale dei Ministero dell'Educazione e della Ricerca tedesco. Lo scopo del progetto era quello di sviluppare una piattaforma per la comunicazione in modo tale da permettere le trasmissioni vehicle-to-vehicle (da veicolo a veicolo) e vehicle-to-roadside (da veicolo a margine della strada). La prima forma di comunicazione ha il potenziale per aumentare la sicurezza e il comfort degli autisti, ad esempio dando loro la possibilita' di ricevere degli avvisi di emergenza dai veicoli davanti che circolano nella loro stessa o nella opposta direzione o permettendo la diffusione delle condizioni del traffico, che possono essere usate per scegliere percorsi alternativi. Inoltre le comunicazioni vehicle-to-vehicle consentono ai passeggeri di un veicolo di contattare i passeggeri dei veicoli che circolano nelle vicinanze. Le comunicazioni vehicle-to-roadside possono permettere l'accesso ad internet e cos favorire le applicazioni commerciali per esempio informando i passeggeri dei veicoli dei punti di interesse turistici o anche dei servizi locali. La soluzione FleetNet e' stata testata attraverso la simulazione e anche, cosa interessante, attraverso la conduzione di alcuni esperimenti in ambiente reale con macchine vere. Le sperimentazioni hanno dimostrato che le comunicazioni nelle VANETs sono drammaticamente influenzate dalle costruzioni e da altri tipi di ostacoli che intervengono nel traffico. Peraltro e' stato scoperto che i range di trasmissione wireless realistici sono molto piu' brevi di quelli che generalmente vengono presupposti negli studi con simulazione per dedurre dei percorsi end-to-end.

Questo scoraggia, ancora una volta, l'utilizzo nelle VANETs di strategie di routing che si basano su percorsi predeterminati end-to-end poiche' esse non risultano ne' affidabili, ne' di lunga durata. La piattaforma sviluppata [**?**] [20] nel progetto FleetNet nasconde l'uso che si puo' fare della conoscenza della posizione dei veicoli. Di base si suppone che i veicoli siano dotati di ricevitori GPS per conoscere la loro posizione e scambiare periodicamente con uno degli hop vicini informazioni su di essa attraverso dei messaggi *faro*. Si presuppone cosi' che ogni veicolo conosca anche la posizione dei suoi vicini piu immediati. Il messaggio inoltrato e' trattato con avidita' su una base hop-by-hop. Nelle prime fasi di FleetNet infatti e' stata presa in considerazione una strategia GPSR (Greedy Perimeter Stateless Routing). In base a questa il nodo da scegliere per l'inoltro del messaggio dovrebbe essere quello piu' prossimo (rispetto al nodo mittente), piu' vicino al nodo destinazione e quello la cui direzione sia piu' vicina alla direzione del nodo di destinazione. L'introduzione di un sistema di Reactive Location Service (RLS) puo' poi fornire la posizione geografica del nodo destinazione quando esso non e' disponibile. Tuttavia, ulteriori studi hanno mostrato che l'approccio GPSR non e' adatto ad ambienti cittadini reali ed e' probabilmente destinato a a fallire. Cio' e' principalmente dovuto alle costrizioni fisiche imposte alla mobilita' dei veicoli dalle strade vere. Infatti, le distanze dal nodo destinazione dovrebbero essere misurate sulle direzioni di una strada reale e anche le direzioni di inoltro dovrebbero essere mappate tenendo conto delle direzioni dei percorsi disponibili attualmente. La strategia di inoltro e' stata percio' sostituita dal GRS. Quest'ultimo si basa su mappe della citta' al fine di selezionare la direzione di inoltro migliore, ad esempio la direzione piu'vicina a quella del nodo destinazione tra quelle presenti negli itinerari attuali. Nello specifico, il nodo mittente calcola un percorso verso il nodo destinazione che puo' essere tracciato su una sottostante mappa della citta'. Il percorso e' una sequenza di giunzioni che il pacchetto deve attraversare al fine di raggiungere la destinazione. La sequenza puo' essere collocata nel paccheeto header o calcolata da ogni nodo inoltrante per poter scegliere sempre la giunzione successiva piu' conveniente. L'efficacia di questa soluzione [**?**] [22] [23] e' stata testata su un simulatore ns-2. Per produrre dei risultati realistici, i modelli di mobilita' dei nodi sono stati accuratamente scelti per rispecchiare i movimenti dei veicoli in ambiente cittadino. Pertanto e' stato usato uno strumento molto valido per la simulazione dei comportamenti dei guidatori: il FARSI, usato da DaimlerChrysler AG per determinare il tempo di vita di alcune parti dei veicoli, come gli ammortizzatori o le frecce direzionali. Durante le simulazioni, si e' supposto che i ranges di

trasmissione fossero fissi (500m). Inoltre, nodo sorgente e nodo destinazione sono stati sempre scelti tra quelli che avevano tra loro una connettivita' end-to-end. I risultati hanno mostrato che il protocollo di routing GRS sovraperforma sia il DSR, sia il protocollo AODV (scelti come rappresentativi della tipologia base dei protocolli di routing delle reti ad hoc). Ulteriori studi, fatti mediante simulazioni, sono stati condotti variando il range di trasmissione wireless da 0 a 4000m e considerando differenti moduli di comunicazione tra i nodi osservati. Ponendo che ogni coppia di nodi dista da ogni altra meno di quanto il range possa tramettere, si e' osservato che si verifica nella rete un numero trascurabile di partizioni quando tutte le auto partecipano all'inoltro del messaggio, sia quelle che circolano nella stessa direzione sia quelle che scorrono nella direzione opposta. Il partizionamento della rete e' meno intenso per i ranges di trasmissione maggiori di 500m. Oltre agli studi con simulazione, e' stata condotta qualche esperienza pratica con quattro macchine Smart. Esse sono state fornite di routers FleetNet con incluse delle cards con tecnologia wireless IEEE 802.11b. In primo luogo sono stati esainati i limiti delle comunicazioni dirette (single-hop) tra coppie di nodi statici. I risultati hanni mostrato conformita' con gli studi fatti mediante simulazione. Poi si sono misurati i rendimenti, risultanti dalle comunicazioni multi-hop, dell'UDP e dell TCP. Tuttavia le misurazioni ottenute on road con le auto circolanti in un ambiente cittadino reale hanno evidenziato un elevata sensibilita' agli ostacoli che si sono incontrati come costruzioni e auto poste sul percorso. Sono stati riscontrati rendimenti piu' bassi e un'elevata perdita di pacchetti rispetto ai risultati della simulazione, dimostrando che i fattori ambientali influenzano profondamente le caratteristiche della propagazione radio. I risultati hanno altresi' mostrato che la connettivita' end-to-end tra l'auto sorgente e l'auto destinazione e' quasi sempre disponibile ad una distanza di uno, due o tre salti. In assenza di connettivita' end-to-end, ad esempio quando non puo' essere trovato alcun hop vicino disponibile,i pacchetti sono stati scartati.

La difficolta' della comunicazione vehicle-to-vehicle in ambiente reale [**?**] e' stata ulteriormente confermata da altri risultati ottenuti on-road al di fuori del contesto del progetto FleetNet. Osservando le caratteristiche del collegamento wireless presente tra due veicoli in movimento in scenari diversi, si e' scoperto che un range di connettivita' si puo' realizzare fino a 1000m, ma solo a determinate condizioni di guida. Le misurazioni della qualita' del collegamento, per distanza tra i veicoli fino a 400m, hanno dimostrato che il piu' favorevole alle comunicazioni tra veicoli e' l'ambiente suburbano e che le piu' ostili sono le condizioni di guida in citta'.

Inoltre , variando la misura del pacchetto, cosi' come cambia la distanza media tra i veicoli in certi scenari, si puo' avere un aumento della performance della rete ad hoc. Si e' osservato che la qualita' del collegamento o Signal-to-Noise Radio (SNR) degrada con l'aumentare della distanza. Anche il rendimento ha mostrato un andamento decrescente con l'aumentare della distanza. Sebbene l'approccio con il routing FleetNet non faccia attualmente uso di paradigmi opportunistici, e infatti ricerca percorsi end-to-end tra il nodo sorgente e il nodo destinazione, puo' tuttavia essere considerato opportunistico, almeno in una versione, in quanto i pacchetti sono inoltrati su una base hop-by-hops senza avere a priori una conoscenza dell'intero persorso (insieme di congiunzioni) della sorgente verso la destinazione. In piu', come dimostrano le esperienze del mondo reale, i ranges di trasmissione sono parecchio influenzati dall'ambiente reale e generalmente sono ridotti (circa 150 a 200m vs. 500m della simulazione). Cio' naturalmente conduce ad un incremento di partizioni nella VANET globale. Una condizione simile potrebbe attualmente portare un vantaggio opportunistico.

3.1.5 Ad Hoc City

Una Ad Hoc City e' una citta' dove i nodi mobili possono comunicare tra loro in modalita' wireless o anche accedere ad internet da qualsiasi luogo perche' la copertura wireless e' garantita su tutto il territorio. Avendo di mira la realizzazione di citta' ad hoc, recentemente alcuni ricercatori hanno proposto di stabilire nelle citta' dei backbone di rete (dorsali) formati sia da nodi fissi sia da nodi mobili. I nodi fissi dovrebbero agire come stazioni base, scarsamente utilizzati sul territorio cittadino, mentre i nodi mobili dovrebbero essere implementati su flotte, come i bus cittadini, i taxi che coprono le aree della citta'. Un nodo mobile che desidera comunicare con un altro dovrebbe semplicemente attendere o anche cercare un'opportunita' di mandare un messaggio. L'opportunita' e' rappresentata dal fatto che il nodo mobile si trova all'interno del range di comunicazione di un nodo trasmettitore. Per esempio potrebbe trovarvisi per caso un bus o alternativamente il nodo mittante potrebbe intenzionalmente raggiungere la piu' vicina fermata dell'autobus dove presto o tardi arrivera' un bus. Una volta trasmessi al primo nodo trasmettitore, i messaggi sono inoltrati al nodo destinazione secondo le tradizionali tecniche di routing ad hoc in modo da limitare l'intero ritardo di propagazione. Infatti l' architettuta ad hoc nelle citta' e' un'applicazione indipendente e quindi e' adatta

sia per le applicazioni con ritardo tollerante sia per quelle con ritardo sensibile. Le tecniche opportunistiche potrebbero essere sviluppate per questi ambienti, cos da favorire le applicazioni con ritardo tollerante e dunque contribuire alla diminuzione del carico totale della rete e, se e' possibile, evitare la congestione. La citta' Ad Hoc e' un'architettura multi-strato [24] che fornisce la comunicazione wireless all'ambiente urbano. La connettivita' end-to-end tra i nodi e' ottenuta mediante degli apparecchi di un set di stazioni base wired distribuiti nella citta' e tramite un backbone wireless multi-hop formato dai bus cittadini e da veicoli preposti alla consegna dotati di dispositivi wireless. I nodi sono classificati in: *nodi mobili personali* come PDA e laptop, usati dagli utenti che si muovono per la citta', *nodi mobili di rete* come i bus o i veicoli preposti alle consegne, usati come ripetitori per la consegna del messaggio e *stazioni base fisse* aventi la capacita' di accedere ad internet. I primi possono essere nodi sorgente o nodi destinazione dei messaggi, mentre i secondi e i terzi possono essere usati solo per l'inoltro. I nodi mobili personali non sono usati per inoltrare il messaggio allo scopo di risparmiare energia. Un nodo mobile personale puo' accedere ad internet tramite un percorso multi-hop che consiste in una sequenza di nodi mobili di rete e una stazione base finale. Esso puo' anche mandare un messaggio ad un altro nodo mobile personale molto distante attraverso un percorso composto da una sequenza di nodi mobili di rete diretti alla piu vicina stazione base, seguita da un insieme di host fissi, in internet, rivolti alla stazione base piu' prossima al nodo destinazione e infine da una sequenza di nodi mobili di rete che vanno dalla stazione base al nodo destinazione. Due nodi mobili personali, vicini l'un l'altro, possono comunicare anche solo con gli strumenti dei nodi mobili di rete cioe' senza stazioni base intermedie. Questa architettura e' nuova in quanto sfrutta la mobilita' del nodo per garantire la connettivita' end-to-end in tutto un ambiente cittadino. Naturalmente l'efficienza e' data dai nodi mobili di rete che coprono l'intera area urbana nello spazio e nel tempo cosi' da creare un backbone network che puo' facilmente inoltrare i messaggi tra qualsiasi coppia di nodi della citta'. La citta Ad Hoc propone anche un algoritmo di routing, il C-DSR (il DSR aumentato per scalabilita') e uno studio con simulazione. La simulazione e' stata condotta con un simulatore di rete ns-2. E' stato sfruttato un modello realistico di mobilita', costruito precedentemente sulla base delle attuali tracce dei movimenti dei bus a Seattle e a Washington , lasciate durante le loro normali corse per accompagnare i passeggeri nei vari luoghi della citta'. Il numero di nodi mobili di rete e' variato da 750 a 850 ed ha fornito il servizio wireless su un'area di oltre 5000

km^2. Si e' presupposto che i nodi mobili di rete avessero un range radio di 1.5 km. Il rapporto di consegna dei pacchetti, l'overhead del pacchetto, la lunghezza del percorso e la latenza del pacchetto, osservati per le comunicazioni tra i nodi, sono stati scelti a caso tra tutte le coppie connesse di nodi mobili di rete. Il rapporto di consegna spaziava tra 92% e 97%, la latenza media e' stata di circa 42.52 ms e la media dell'overhead e' stata di 222 pacchetti di trasmissione per nodo di rete. Il percorso e' stato quasi sempre inferiore a 6 hops; comunque la maggiorparte delle trasmissioni si e' riscontrata oltre i 2 hops.

3.1.6 ZebraNet

Il progetto ZebraNet e' molto differente dal precedente. In ZebraNet la stazione base non puo' coprire l'intera area di interesse come la wireless backbone fa in Ad Hoc City. Quindi tutti i nodi nel sistema ZebraNet sono in grado di agire come ripetitori e scambiarsi tutti i messaggi ogni volta che si incontrano. Saltando di nodo in nodo, si prevede che i messaggi giungano alla stazione base quando il loro nodo trasportatore e' prossimo alla stessa stazione base. ZebraNet [25] [26] e'un progetto in corso all'Universita' di Princeton e vede impegnati congiuntamente il Dipartimento di Ingegneria Elettronica, quello di Science dei Computers e quello di Ecologia e Biologia Rivoluzionaria. Esso pone l'attenzione sul monitoraggio delle informazioni riguardanti le specie selvatiche con l'obiettivo di indagare a fondo il loro comportamento e capire le loro interazioni e le loro reciproche influenze. Una raccolta dati molto accurata deve anche essere capace di comprendere i modelli migratori degli animali selvatici, comelo sviluppo umano nelle aree selvagge influenza le specie indigene, come gli animali selvatici possono essere condizionati dai cambiamenti climatici, dall'introduzione di specie non indigene, da altri fattori. Lo scenario per il ZebraNet e' una vasta area della savana al centro del Kenya, controllata dal Mpala Research Centre [27]. Finora le uniche specie studiate sono state le zebre. Il sistema ZebraNet consiste di speciali collari, portati dagli animali per raccogliere dati, da una stazione base che si muove periodicamente per la savana per raccogliere le informazioni che provengono dai collari e da una protocollo di rete per filtrare i dati mandati dai collari alla stazione base mobile. I collari contengono le necessarie attrezzature di rilevamento (per esempio un ricevitore GPS per conoscere la posizione degli animali) per i dati periodici di campionamento oltre che una memoria per immagazzinare i dati raccolti. Inoltre includono un'unita' di processo per com-

piere una parziale elaborazione dei dati, un breve range e un lungo range radio per la trasmissione dei dati. I nodi collare formano una rete ad hoc e comunicare tra loro in modalita' peer-to-peer. La stazione base e' un veicolo mobile con dentro dei ricercatori. Dato che sia i nodi collare che la stazione sono mobili e , in piu', quest'ultima e' solo sporadicamente presente nell'area di studio, e' molto impegnativa la raccolta completa di dati provenienti da tutti i nodi zebra. Per al raccolta dei dati sono stati presi in considerazione due protocolli alternativi che sfruttano entrambi le opportunita' di contatto tra le zebre. Il primo e' il *protocollo di inondazione* e propone che ogni collare mandi tutti i dati che ha immagazzinato a ciascuno dei nodi vicini che trova. Il risultato e' che ogni collare immagazzina , insieme con i suoi dati, i dati ricevuti dal suo hop vicino e dal vicino multi-hop. Alla fine, i collari, che possono vedere la stazione base, mandano a questa l'intero pacchetto di dati raccolti. Quindi man mano che riceve i dati dal singolo collare, la stazione base raccoglie le informazioni campionate da tutti i collari. Questa metodologia e' molto utile per studiare la vita animale perche' ci possono essere zebre che non si avvicinano mai alla stazione base poiche' generalmente vivono lontane dalle altre mandrie e quindi e' piu' facile che incontrino le altre zebre piuttosto che la stazione base. Il secondo protocollo che e' stato usato e' quello basato sulla storia e propone che ogni nodo selezioni, come ripetitore per i suoi dati, solo uno dei suoi vicini. Il nodo selezionato e' quello che ha la piu' alta probabilita' di incontrare la stazione base. Ad ogni nodo e' assegnato un livello gerarchico (inizialmente zero) che aumenta ogni qualvolta incontra la stazione base e per converso diminuisce quando per un certo periodo di tempo non vede la stazione base. Durante l'invio dei dati, il nodo piu' vicino da selezionare e' quello che ha il livello gerarchico piu' elevato. Per valutare la performance dei due protocolli, sono state condotte delle simulazioni con un simulatore speciale chiamato ZNetSim. Esso implementa un modello di mobilita' realistico per le zebre che si basa su delle osservazioni e su delle statistiche riguardanti il comportamento delle zebre, effettuate dai biologi al Mpala Research Centre. I risultati delle simulazioni hanno mostrato che entrambi i protocolli consentono il miglior grado di successo rispetto al protocollo diretto che permette le comunicazioni zebra-to-base station e non quelle zebra-to-zebra. In piu' il protocollo basato sulla stopera meglio di quello di inondazione quando si prendono in considerazione la presenza di immagazinamento e le costrizioni di bandwidth, specialmente per ranges radio superiori a 4 km che favoriscono l'incremento del numero di nodi vicini ad ognh zebra. Il protocollo basato sulla storia opera meglio anche quando si tratta di risparmiare energia perche' limita

il numero totale di scambi tra i peers.

3.1.7 Rete sulle balene - SWIM

L'obiettivo di questo progetto e' simile a quello di ZebraNet: raccogliere dati sulle balene e indagare le loro abitudini oltre che i modi in cui reagiscono all'intervento umano nel loro habitat. Questo sistema e' composto da delle speciali etichette che sono applicate alle balene per monitorare i dati e da delle stazioni base che possono essere fisse (su boe) o mobili (su uccelli marini). Le comunicazioni avvengono sia tra balena e balena, sia tra balena e stazione base. Infine i dati sono inoltrati a terra dalle stazioni base. Questo sistema e' totalmente simile a quello di ZebraNet, specialmente la versione che utilizza un protocollo di inondazione per lo scambio dei dati, e mostra un altro possibile scenario applicativo delle Oppnets, laddove il ritardo di propagazione dei dati non risulta essere un problema per il progetto. In piu' e' da notare che generalmente sott'acqua le trasmissioni fanno affidamento su tecniche di acustica, caratterizzate da ritardi di propagazione non trascurabili. Quindi le applicazioni concepite per questi ambienti sono per lo piu' a ritardo tollerante e , di conseguenza, naturalmente adatti per le reti opportunistiche.

Lo Shared Wireless Infostation Model (SWIM) [28] e' concepito per raccogliere dati biologici, associati alle balene nell'oceano. Il dato e' monitorato sulle balene da delle speciali etichette di cui le balene stesse sono equipaggiate. Le etichette possono comunicare con le altre e scambiarsi dati. Cosi' ogni volta che due balene si avvicinano e le loro etichette possono comunicare, si verifica uno scambio di dati. La conseguenza e' che ogni balena immagazzina i propri dati e quelli di ogni altro esemplare che incontra. I dati sono replicati e diffusi attraverso le balene in movimento e infine arrivano alla speciale stazione SWIM posizionata su qualche boa che galleggia sull'oceano. Poi dalle stazioni SWIM i dati sono trasferiti a qualche posto sulla terraferma per essere elaborati ed utilizzati. Le stazioni SWIM hanno il potenziale per comunicazioni ad alta velocita' (per quanto riguarda le comunicazioni da etichetta ad etichetta), ma sono solo sporadicamente connesse alle balene dato che quest'ultime generalmente sono molto lontane. Non sono disponibili risultati sperimentali per dimostrare l'efficacia del sistema SWIM sulle balene. Comunque, delle simulazioni realistiche sono state condotte attraverso la creazione di ambienti e parametri per ottenere risultati sul mondo delle balene. Secondo i risultati delle simulazioni, il ritardo nell'arrivo dei dati alla stazione base per l'elaborazione non

e' trascurabile. Tuttavia, esso decresce con l'aumentare del numero di balene coinvolte o anche con l'aumento delle boe. La performance migliore e' realizzabile anche quando le boe sono ben posizionate, per esempio in posti in cui alle balene piace maggiormente andare. Infatti gli studi sui modelli di mobilita' delle balene hanno mostrato che questi mammiferi sono creature molto abitudinarie e periodicamente visitano gli stessi posti, ad esempio per mangiare. Inoltre esse tendono a formare dei gruppi (un gruppo e' generalmente formato da una femmina e diversi maschi), cosi' si incrementa la possibilta' di diffondere i dati raccolti. Infine, quando le stazioni SWIM sono mobili, l'efficienza del sistema migliora sensibilmente.

3.1.8 Progetto Haggle

Anche Haggle permette di comunicare in assenza di connessione fisica. E' un progetto finanziato dall'Unione Europea e sara' concluso entro il 2010 che sfrutta gli Hot spot Wi-Fi di una citt, cio le aree libere istituzionali di connessione Wi-Fi gratuita, viaggiando quindi via etere o i dispositivi bluetooth e wireless presenti in una zona. Gli Hot spot nelle maggiori metropoli, da Londra a New York e HongKong vanno sempre pi moltiplicandosi, con ancora pochi esempi italiani purtroppo. Un area metropolitana wireless, dunque, che si autorganizza in una rete Haggle in Wi-Fi. Se si deve mandare un messaggio sulla rete Wi-Fi, non si ha bisogno di sapere se si e' vicino ad un Hot spot, ma solo se qualche altro dispositivo mobile vicino a e potr far rimbalzare il messaggio fino a destinazione, fungendo semplicemente da nodo intermittente o piattaforma di comunicazione. Il progetto, finanziato dal 5 programma quadro dell'Ue con sei partner tecnologici di cinque Paesi (Italia, Francia, Svizzera, Regno Unito e Finlandia) realizzato alla Supsi (Scuola Universitaria professionale della Svizzera italiana) da due team coordinati da Silvia Giordano e Christian Marrazzi. Haggle consolida l'esperienza acquisita in Mobile man (Mobile metropolitan ad hoc Networks, cnd.iit.cnr.it/mobileMAN), uno studio del Cnr di protocolli per le reti mobili ad hoc, come i comuni cellulari, nelle quali i nodi partecipanti (ovvero i singoli utenti provvisti di dispositivo mobili) formano la rete facendo sparire l'infrastruttura fissa. Nelle reti mobili ad hoc, due utenti riescono a comunicare tra loro anche in mancanza di collegamento diretto. I nodi intermedi fungono da rete e non c' l'infrastruttura fissa n un antenna centrale come autorit di connessione. Il vantaggio, rispetto a una rete mobile convenzionale, che anche i nodi lontani dall'area di un antenna, possono comunicare, attraverso il dispositivo

mobile pi vicino in una sistema a rimbalzo. E' l'utente stesso, dunque, con il suo dispositivo mobile che parte integrante di questa rete, divenendo nodo e fornitore di servizi per gli altri utenti. Haggle prevede collegamenti anche con Internet e le applicazioni variano dalla trasmissione di testi (alternativi rispetto ad Sms della telefonia mobile ed e-mail di Internet) o immagini multimediali audio-video, in una rete di collegamento Haggle di tutti i dispositivi wireless.

3.2 Un possibile uso della Oppnet in caso di emergenza

Tipicamente in una rete, i nodi sono tutti disposti insieme e la loro locazione e predesignata (o in maniera completamente deterministica o con un certo grado di casualita come nel caso di una rete ad hoc o mobile. Diversamente avviene nella rete opportunistica dove linsieme iniziale dei nodi, chiamati anche seed nodes, pu anche non essere approssimativamente predesignato. Questa e la categoria di reti in cui i diversi dispositivi, non utilizzati originariamente come nodi di una rete, sono inviati ad aderire ai seed nodes per divenire oppnet helpers. Gli helpers svolgono delle operazioni, dunque, a cui sono stati invitati a partecipare. Attraverso lintegrazione degli helpers, una seed oppnet cresce e diventa una expanded oppnet. Per esempio, la seed oppnet diventa la expanded network attraverso l'ammissione dei seguenti helpers: (a) rete di computer di un vicino college-campus, (b)un cellulare (rappresentato dalla torre per telefonia mobile), (c)un satellite, (d) uno smart appliance (esempio un frigorifero) che fornisce l'accesso alla rete domestica, (e)un trasmettitore microonde che fornisce l'accesso alla microwave network, (f)una rete informatica veicolare , connessa con la rete di computer messa sui corpi di coloro che occupano la vettura. In generale, l'insieme dei potenziali helpers per le reti opportunistiche e' molto ampio, includendo la comunicazione, i sistemi di sensori e di calcolo,wired e wireless e l'insieme destinato ad incrementarsi man mano che i dispositivi informatici diventano piu' pervasivi. Naturalmente le aree maggiormente popolate avranno in generale una piu' fitta copertura da parte dei potenziali helpers. Di conseguenza,in tali aree sara' piu' facile influenzare le capacita' di una oppnet. Con piu' potenziali helpers disponibili in un ambiente oppnet, c'e' bisogno solo di integrarli in modo piu' chiaro. Cosi' la rete opportunistica puo' essere usata anche in casi di emergenza, laddove il disastro puo' essere predetto con una certa accu-

ratezza. Prendiamo il caso di un disastro provocato da un uragano. In questo cao le Oppnets possono significativamente migliorare l'efficienza e l'effettivit delle operazioni di soccorso: le seed oppnets possono essere messe in azione prima del disastro quando e' ancora piu' facile localizzare ed invitare altri nodi o clusters nella oppnet. I primi helpers invitati da un nodo seed potrebbero essere i SensorNet disposti per monitorare e valutare il danno strutturale sui palazzi, sulle strade o sui ponti.

3.3 Tecniche di Routing Opportunistico

Le tecniche di routing in Intermittently Connected Networks (ICN) tipicamente mirano a massimizzare la probabilita' di consegna del messaggio. Questa probabilita' e' misurata dal rapporto di consegna, definito come il rapporto tra la quantita' totale di dati che alla fine arrivano alla destinazione e la quantita' totale di data immessi nel sistema. Un altro obiettivo del routing e' quello di minimizzare il ritardo che ogni messaggio sperimenta durante la consegna. Nello specifico esso e' composto dal tempo che intercorre tra l'immissione da parte del nodo sorgente del messaggio e il momento in cui quest'ultimo viene completamente ricevuto dal nodo destinazione. Date le frequenti dinamiche della topologia che caratterizza ICN, sia il routing proattivo che quello reattivo non riescono a trovare gli opportuni percorsi per l'inoltro perche' essi tentano di trovare dei cammini completi tra il nodo sorgente e quello destinazione che e' probabile che non esistano. Il routing di maggior successo in ICN e' invece il *per-hop routing* che cerca di trovare un percorso su base hop-by-hop, ad esempio cerca l'hop prossimo piu' appropriato solo dopo aver attraversato quello precedente. Un nodo next-hop e' scelto per sfruttare l'informazione locale sui contatti disponibili ad ogni salto verso gli altri nodi oltre che sulle code dei messaggi in attesa (che attendono per l'inoltro) verso il nodo deputato all'inoltro sia verso i suoi nodi vicini. Questo approccio ha il vantaggio di utilizzare sempre l'informazione piu' recente. L'informazione puo' anche derivare dal sottostante livello di routing proattivo o reattivo. Per esempio un routing proattivo puo' essere usato per fornire il set di nodi che sono correntemente raggiungibili e tra questi selezionare gli hops vicini preferiti. Un protocollo reattivo invece puo' essere usato per fornire i percorsi all'interno dlle parti connesse di una rete. La prestazione del routing migliora quando e' disponibile ed e' sfruttata una maggiore conoscenza della topologia futura della rete. Sfortunatamente questo tipo di conoscenza non e' facilmente disponibile

e deve essere fatto un compromesso tra la realizzazione della prestazione e l'esigenza di conoscenza. [29] introduce quattro categorie di conoscenza, chiamate ORACLES.

Il **Contacts Summary Oracle** fornisce le caratteristiche sommarie sui contatti. Esso, per ogni coppia di nodi, da' la media del tempo di attesa fino al successivo contatto disponibile. Cosi' fornisce informazioni sul TEMPO-INVARIANTE.

Il **Contact Oracle** da' informazioni sui contatti tra due nodi ad ogni intervallo di tempo. Questo e' l'equivalente di conoscere il multigrafo del TEMPO-VARIANTE dell'ICN.

Il **Queuing Oracle** da' informazioni sulle occupazioni istantanee del buffer (queuing) in ogni nodo e in qualsiasi momento. Esso puo' essere usato per fare il percorso tra i nodi congestionati. A differenza degli altri oracles, il queuing oracle e' influenzato sia daLL'arrivo nel sistema di nuovi messaggi sia dalle scelte degli algoritmi di routing. Probabilmente questo e' il piu' difficile oracle da realizzare in un sistema distribuito.

Il **Traffic Demand Oracle** risponde, alla fine, a ogni questione che riguarda la domanda di traffico presente e futuro. Esso e' in grado di dare informazioni sulla quantita' di messaggi immessi nel sistema in qualunque momento.

Gli algorirtmi di routing possono essere concepiti proprio per sfruttare uno o piu' dei suddetti oracles. Essi stabiliscono i costi ai margini del grafico di rete e calcolano una forma di percorso che abbia il minimo costo (il piu' breve). Il costo di un margine e' determinato attraverso la consultazione degli oracles disponibili e tramite l'elaborazione del ritardo che un messaggio sperimenta nell'arrivare a quel margine. Le componenti del ritardo sono prese in considerazione di seguito.

- Queuing delay (ritardo di accodamento): e' la somma del tempo occorrente perche' un margine (es. un contatto) diventi disponibile per la trasmissione e del tempo per drenare i messaggi gia' pronti per la partenza verso il margine.
- Transmission delay (ritardo di trasmissione): e' il tempo occorrente per immettere completamente un messaggio in un margine (contatto)
- Propagation delay (ritardo di propagazione): e' il tempo che occorre per attraversare il margine (contatto)

Piu' gli oracles sono disponibili, piu' real accetto che tu nn ci faccia male durantistici sono i ritardi che vengono elaborati, piu' accurate sono le decisioni che riguardano il routing. Una volta che e' stato stabilito un costo per ogni margine, puo' essere

calcolato il percorso piu' breve usando l'algoritmo Dijkstra Shortest Path. Quando non e' stabilita alcuna conoscenza dagli oracle, un messaggio che bisogna inoltrare e' semplicemente consegnato al primo contatto che e' disponibile allo spedizioniere o al contatto scelto a caso tra quelli disponibili. Esso e' ovviamente il protocollo piu' facile da implementare, ma generalmente ha scarsi risultati rispetto ai protocolli piu' intelligenti. Possono essere convenienti in molti casi le soluzioni basate su *message splitting* (la scissione del messaggio). I messaggi sono suddivisi in frammenti multipli in modo che il singolo frammento possa adeguarsi di volta in volta ai singoli contatti disponibili tra due nodi. I differenti frammenti possono anche essere instradati attraverso percorsi diversi per ridurre il ritardo o migliorare il bilanciamento del carico tra collegamenti multipli. Ovviamente per trovare percorsi multipli e appropriate dimensioni dei frammenti occorre un elevato sforzo. Dovrebbero essere presi in considerazione differenti algoritmi di routing [29], ognuno dei quali facente uso di un diverso set di oracles per dimostrare che le soluzioni migliori sono quelle che utilizzano la conoscenza piu' completa della topologia futura della rete e del traffico in arrivo. Sfortunatamente l'assunzione di disponibilita' degli oracles attualmente non e' realistica. Gli algoritmi di routing che saranno descritti non fanno affidamento sugli oracles, ma trovano soluzioni alternative.
Essi possono essere descritti come segue:

- Dissemination-based Routing;
  a) Replication-based Routing
  b) Coding-based Routing

- Utility-based Routing;
  a) History-based Routing
  b) Shortest path-based Routing
  c) Context-based Routing
  d) Location-based Routing

- Infrastructure-based Routing;

- Carrier-based Routing;

3.3.1 Dissemination-based Routing

Questa tecnica di routing, basata sulla diffusione dei dati, opera la consegna alla destinazione con la semplice diffusione del messaggio a tutta la rete. Dietro a questa politica c'e' un'euristica ben precisa: dato che non c'e' conoscenza ne' di un possibile percorso che porti al nodo destinazione di un messaggio,ne' di un appropriato nodo next-hop, il messaggio puo' solo essere mandato dappertutto. Esso alla fine giungera' al nodo destinazione passando di nodo in nodo. La tecnica della diffusione ovviamente lavora bene solo nelle reti molto dense e con un elevato grado di mobilita'dove le opportunita' di contatto, necessarie per la diffusione dei dati, sono molto comuni. Le opportunita' di contatto garantiscono che ci sia il piu' breve ritardo possibile nella consegna, ma sono anche risorse molto avide sia in termini di occupazione di memoria e di bandwith usato cosicche' si verifica un elevato consumo di energia e una bassa scalabilita'. Dal momento che non e' possibile ottenere una ottimizzazione globale delle risorse, il loro consumo e' generalmente scambiato per ritardo. La memoria dei nodi e' tipicamente gestita da tecniche che includono:

- *Tecniche di sostituzione del Buffer* per fare spazio nel buffer di ingresso di un nodo quando lo stesso buffer e' pieno e arriva un nuovo messaggio. Queste tecniche evitano di sovrascrivere i messaggi che non sono stati ancora inoltrati o che non sono presenti nella rete in molte copie perche' la loro cancellazione potrebbe impedire la consegna finale alla destinazione.

- *Tecniche di Rilevamento del Messaggio Duplicato* per permettere al nodo destinazione di riconoscere l'arrivo di copie multiple dello stesso messaggio in modo che esso possa mandarle tutte.

- *Tecniche di Garbage Collection (Raccolta di rifiuti)* per consentire alla memoria la deallocazione ai nodi intermedi, dopo l'arrivo della prima copia di un messaggio alla destinazione.

A causa del notevole numero di trasmissioni coin

$$P_o^k(i)$$

volte, le tecniche basate sulla diffusione soffrono di elevato conflitto e potenzialmente possono portare congestione alla rete. Per incrementare la capacita' della rete, generalmente si limita il raggio di diffusione di un messaggio introducendo un numero

massimo di hops ripetitori permessi per ogni messaggio o anche limitando il numero totale di copie del messaggio presenti nella rete nello stesso momento. Quando non e' piu' permessa alcuna ripetizione, ogni nodo puo' essere direttamente mandato alla destinazione quando o nel caso in cui la incontrasse. I protocolli di routing basati sulla diffusione possono essere divisi in due categorie: quelli basati sulla replicazione e quelli basati sulla codifica. Nei primi le copie multiple dello stesso messaggio sono diffuse in giro per la rete; mentre nei secondi, prima della consegna vengono eseguite delle elaborazioni sul messaggio originale. I blocchi che scorrono lungo la rete contengono generalmente un' informazione codificata parziale. I messaggi originali possono solo essere ricostruiti quando giungono al nodo destinazione, dopo avere ricevuto un dato numero di blocchi codificati.

Replication-based Routing

Epidemic Routing

In base al protocollo di routing **Epidemic** [30], i messaggi si diffondono nella rete in modo simile alle malattie o ai virus, cioe' attraverso i contatti a coppia tra singoli nodi. Un nodo e' infettato da un messaggio quando questo genera quel messaggio o quando lo riceve da un altro nodo per l'inoltro. Il nodo infettato memorizza il messaggio in un buffer locale. Un nodo e' suscettibile di infezione quando non ha ancora ricevuto il messaggio, ma puo' potenzialmente riceverlo in caso esso venga a contatto con un nodo infetto (es. un nodo che memorizza quel messaggio). Quest'ultimo diventa recuperato (cioe' guarito dalla malattia) una volta che ha consegnato il messaggio al nodo destinazione; di conseguenza e' diventato immune alla stessa malattia e non provvede piu' a trasmettere lo stesso messaggio. Piu' tecnicamente, Epidemic Routing lavora nel modo seguente. Ogni nodo possiede un buffer per memorizzare i messaggi che esso genera e quelli in arrivo da altri nodi che hanno bisogno di inviarli. I messaggi sono ordinati in una lista che e' accessibile attraverso una hash table e che solitamente viene gestita in base ad una politica FIFO. Un vettore di sintesi descrive quali voci dell'hash table corrispondono agli attuali messaggi e inoltre contiene una loro compatta rappresentazione. Ogni nodo ha un suo IDentifier (ID). Ogni volta che due nodi entrano nel range di comunicazione l'uno dell'altro (es. si verifica un contatto pair-wise), quello con il piu' piccolo ID , detto ID_1 ,consegna il suo vettore di sintesi all'altro nodo con il piu' grande ID, detto ID_2 . Il nodo ID_2 confronta il vettore di sintesi ricevuto con il suo vettore di sintesi e

costruisce una lista con quei messaggi, memorizzati dal nodo ID_1 ,che non ha ancora ricevuto. Quindi il nodo ID_2 fa richiesta dei messaggi che gli mancano al nodo ID_1 e successivamente attende che il nodo ID_1 glieli mandi. Dopo che i messaggi sono giunti dal nodo ID_1 al nodo ID_2 , il nodo ID_2 manda il suo vettore di sintesi al nodo ID_1 che ripete la stessa procedura in qualita' di nodo ID_1 , come mostrato in **??**. La scelta dei messaggi da chiedere all'altro nodo e' basata su considerazioni fatte sulla misura totale di buffer disponibile. Una scelta piu' intelligente puo' anche tenere in considerazione il nodo destinazione dei messaggi resi noti. Cosi' un nodo richiedera' preferibilmente al nodo incorantrato quei messaggi che hanno come destinazione un nodo che e' il piu' frequentemente incontrato. La procedura di scambio dei messaggi e' chiamata *sessione di antientropia* (anti-entropy session) ed ha inizio ogni qualvolta due nodi si incontrano. Comunque, per evitare di ripetere questa procedura inutilmente, ai nodi e' raccomandato di conservare una lista dei nodi incontrati piu' recentemente e di iniziare gli scambi solo con i nodi che non appartengono a questa lista. La diffusione per tutta la rete garantisce che alla fine i messaggi arrivano alle loro effettive destinazioni. Il processo di diffusione e' in qualche modo delimitato perche' ad ogni messaggio, quando e' generato, viene assegnato un *hop count limit* che da' il massimo numero di hop che quel messaggio e' in grado di attraversare prima di giungere alla destinazione. Quando l'hop count limit e' impostato su un uno, il messaggio puo' solo essere mandato direttamente al nodo destinazione. Piu' grande e' l'hop count limit del messaggio, piu' ampiamente quest'ultimo e' sparso nella rete e, di conseguenza, ha piu' chances di arrivare alla fine alla destinazione. Inoltre e' piu' probabile che sia bassa la latenza della consegna. Quando si impone che l'hop count limit sia basso, un messaggio non puo' frequentemente essere inoltrato e soprattutto si muove da punto a punto grazie alla mobilita' dei nodi che lo memorizzano (la consegna sfrutta la mobilita' piu' che le trasmissioni wireless). Studi fatti mediante simulazioni hanno mostrato che epidemic routing permette la consegna dei messaggi nelle reti ad hoc disconnesse dove i tradizionali algoritmi di routing generalmente falliscono. Offrendo una vasta e rapida diffusione dei messaggi in tutta la rete, epidemic routing massimizza il tasso di successo di consegna dei messaggi e minimizza le latenza sperimentata da ogni messaggio. Tuttavia questo protocollo tende a consumare una grande quantita' di risorse, in particolare la capacita' di memoria, il bandwith di rete per le trasmissioni e l'energia per il messaggio memorizzato e per quello mandato. Un'alta capacita' di memoria e hop count limits

comportano un elevato tasso di successo nella consegna e bassa latenza.[3]. In piu' cresce anche il fabbisogno totale di risorse. Un grado di successo nella consegna del 100% sarebbe concesso se ogni nodo potesse memorizzare tutti i messaggi che circolano nella rete in un momento. Comunque e' stato dimostrato che sono possibili un buon tasso di successo nella consegna e una latenza ragionevole solo se ogni nodo riesce a memorizzare tra il 5% e il 25% di tutti i messaggi generati in un momento nella rete. In alternativa sarebbe altrettanto positivo se alcuni nodi avessero una considerevole capacita' di memoria per fungere da backbone di nodi, mentre gli altri nodi avessero solo una minima capacita' di buffer. Chiaramente l'efficacia di epidemic routing, come originariamente concepito, e' limitata dalla scarsita' della capacita' di memoria disponibile nei nodi. Dopo la creazione di un messaggio, molte sue copie vengono diffuse per tutta la rete e continuano ad essere memorizzate anche dopo l'arrivo di una delle copie alla destinazione. Questo ovviamente porta ad uno spreco di memoria. Un messaggio e' cancellato solo quando un nuovo messaggio arriva ad nodo che necessita di memoria e il buffer e' pieno. Percio'per fare spazio per il nuovo messaggio, viene selezionato dal buffer un vecchio messaggio per essere scartato e finalmente sostituito dal nuovo. Nello specifico sono prese in considerazione quattro tecniche particolari di sostituzione [31].

Drop-Random (DRA): il pacchetto viene eliminato a caso. Questa politica da' la priorita' di consegna ai messaggi che sono generati dalle sorgenti piu' silenziose (le sorgenti che hanno un basso tasso di generazione di pacchetti). Infatti, piu' sono i pacchetti generati dalla stessa sorgente, piu' sono i pacchetti, provenienti da quella stessa sorgente, che potrebbero essere memorizzati nello stesso buffer ed e' piu' probabile per ognuno di loro che vengano eliminati.
Drop-Least-Recently-received (DLR): i messaggi che sono scartati per primi sono quelli che hanno trascorso piu' tempo nel buffer. Infatti quei messaggi hanno una probabilita' maggiore di essere gia' giunti a destinazione.
Drop-Oldest (DOA): i messaggi che sono scartati per primi sono quelli che hanno trascorso piu' tempo nella rete. Quei messaggi hanno una probabilita' piu' alta di essere gia' stati consegnati alla destinazione.
Drop-Least-Encountered(DLE): il messaggio da scartare dal buffer e' quello con la peggiore probabilita' di consegna stimata. Quest'ultima corrisponde alla probabilita' del nodo che contiene quel messaggio di essere a portata di mano del nodo

[3]Cio' avviene perche' molti nodi possono contemporaneamente memorizzare il messaggio, cosi' da incrementare le possibilita' che uno di loro incontri presto la destinazione finale

destinazione di quel messaggio o in alternativa di essere in prossimita' di un altro nodo che probabilmente incontrera' la destinazione. Si suppone che ogni nodo conservi una lista delle probabilita' di consegna, una per ogni nodo conosciuto nella rete. La lista e' aggiornata dopo ogni contatto pair-wise. Poniamo che $M_t(A, B)$ sia la probabilita' del nodo A di essere a portata di mano del nodo B al tempo t. Se il nodo A incontra il nodo B, esso incrementa la probabilita' di consegna al nodo B che ha appena incontrato, oltre che la probabilita' di consegna ad altri nodi a cui B probabilmente viene incontro (es.se il nodo B viene incontro probabilmente al nodo C e il nodo A viene incontro al nodo B allora il nodo A portera' a termine con successo la consegna al nodo C attraverso il nodo B). Ovviamente il nodo B aggiorna opportunamente anche la sua lista di probabilita' di consegna. Alla fine , le probabilita' di consegna sono periodicamente diminuite in assenza di contatti pair-wise. La formula seguente esprime analiticamente l'euristica nel caso in cui A incontra il nodo B, con $\alpha = 0.1$ e $\lambda = 0.95$.

Figura 3.1:

$$M_{t+1}(A,\ C) = \begin{cases} \lambda M_t(A,\ C) + 1 & if\ C = B \\ \lambda M_t(A,\ C) + \alpha M_t(B,\ C) & for\ all\ C \neq B \\ \lambda M_t(A,\ C) & if\ none\ met \end{cases}$$

I risultati della simulazione mostrano che le strategia DOA e DLE sono quelle che si comportano meglio rispetto alle altre strategie. Inoltre tenendo fisso il buffer e aumentando il carico di rete, l'algoritmo DLE sovraperforma l'algoritmo DOA. L

MV

Il protocollo di routing **MV** [32] e' un ulteriore passo in avanti rispetto ad epidemic routing. I messaggi sono scambiati durante i contatti pair-wise attraverso la stessa sessione di antropia del protocollo precedente. Tuttavia questo protocollo introduce un metodo piu' sofisticato di selezione dei messaggi da richiedere al nodo che si incontra. Fondamentalmente la scelta dipende da quanto un nodo sia fiducioso di riuscire a consegnare quei messaggi alle loro rispettive destinazioni. Quindi ogni nodo calcola la probabilita' di consegna ad ogni altro nodo della rete (ogni nodo infatti e' un potenziale nodo destinazione). La probabilita' di consegna si basa su osservazioni che riguardano gli *incontri (meetings)* tra nodi e le *visite (visits)* dei nodi a luoghi geografici che si sono verificate nel recente passato. Lo stesso nome

MV protocol viene da *Meetings* e *Visits*. Le probabilita' di consegna sono elaborate come segue.
Poniamo che $P_o^k(i)$ sia la probabilita' che il nodo k visiti la regione i. Cio' corrisponde anche alla probabilita' di consegnare con successo un messaggio e trasmettere ad ogni nodo, senza alcun intermediario, quello che si trova nella stessa regione i. Essa puo' essere calcolata in base alla seguente formula

$$P_o^k(i) = \frac{t_i^k}{t}$$

dove t_i^k e' il numero delle unita' di tempo in cui il nodo k ha visitato la regione i durante l'ultima unita' di tempo t (un'unita' di tempo e' un periodo di tempo arbitrario cioe' un periodo di tempo di riferimento). Poniamo che $P_1^k(i)$ sia la probabilita' del nodo k di consegnare un messaggio al nodo posto nella regione i proprio attraverso un nodo intermedio. Questa probabilita' corrisponde alla possibilita' per il nodo k di incontrare un nodo intermedio, ad esempio un nodo j, che successivamente visita la regione i. Essa puo' essere ottenuta come segue:

$$P_1^k(i) = 1 - \prod_{j=1}^{N}(1 - m_{jk}P_0^j(i))$$

dove N e' il numero totale di nodi e m_{jk} e' la probabilita' di incontro che i nodi j e k visitino simultaneamente la stessa regione e cosi' abbiano un'opportunita' di contatto. m_{jk} e' calcolata nel modo seguente.

$$m_{jk} = \frac{t_k^j}{t}$$

dove $t_{j,k}$ e' il numero delle unita' di tempo in cui i nodi j e k hanno visitato simultanemente la stessa regione, durante l'ultima unita' di tempo t. La probabilita' che un messaggio dal nodo k al nodo j attraversi esattamente n ripetitori e' data anche da:

$$P_k^n(i) = 1 - \prod_{j=1}^{N}(1 - m_{jk}P_{n-1}^j(i))$$

Oltre all'osservazione del modello di mobilita' dei nodi nella rete, il protocollo MV prende in considerazione anche la possibilita' di cambiare questo modello per facilitare le operazioni di inoltro e incrementare la capacita' della rete. Percui sono aggiunti alla rete speciali nodi chiamati *Agenti Autonomi*. Essi sono dei robot mobili, posti a terra e in aria, che si muovono per la rete seguendo dei percorsi precalcolati,

progettati proprio per meglio contribuire alla raccolta e all'inoltro dei dati e in generale al miglioramento delle prestazioni della rete. Sfortunatamente il calcolo di percorsi ottimali e' notoriamente un problema NP-completo. Nel routing MV, i modelli di mobilita' sub-ottimali sono trovati attraverso gli strumenti di un *multi-objective controller system*, preso dalla teoria del controllo robotico. Un *controller* e' l'algoritmo usato per generare il moto di un agente. Nel *multi-objective controller system*, i differenti controllers sono definiti a seconda degli scopi:

- *Total Bandwith Controller*: esso mira a raggiungere il primo di quei nodi che memorizzano il numero piu' elevato di messaggi non recapitati;
- *Unique Bandwith Controller*: esso mira a visitare il primo di quei nodi che fungono da vettore;
- *Delivery Latency Controller*: esso cerca di visitare il primo dei nodi che sono caratterizzati dalla piu' alta latenza di consegna;
- *Peer Latency Controller*: esso inizia a visitare i nodi visitati meno di recente;

Gli obiettivi di tali controllers non possono essere raggiunti tutti insieme e tutti nello stesso momento, per cui e' necessario trovare una combinazione che sia ragionevolmente appropriata. Sono state ricercate allora due possibili combinazioni:*Nullspace Composition* e *Subsumption*, derivate entrambe dalla teoria del multi-objective control. Il protocollo MV e' stato testato attraverso le simulazioni ns-2 presupponendo che le trasmissioni si verificavano da nodi mobili a nodi stazionari. In base al modello di mobilita' usato nelle simulazioni, generalmente i nodi si muovono verso tre punti di attrazione: una home location e due remote locations. I nodi sono attratti per il 50% del tempo dalla home location e per il 25% dalle altre locations. I risultati delle simulazioni mostrano che il protocollo MV sovraperforma FIFO queuing-based protocols e che la somma degli agenti autonomi incrementa significativamente il tasso di consegna della rete. Inoltre il routing MV permette di attenuare la latenza del messaggio. Con riguardo alla strategia di controllo, la Nullspace Composition sovraperforma l'approccio Subsumpition. Il protocollo reagisce bene all'incremento di carico offerto.

Spray and Wait

Il protocollo **Spray and Wait** [33] e' ispirato agli schemi di consegna per inondazione in cui non si fa uso delle informazioni sulla topologia della rete o della

conoscenza dei passati incontri dei nodi. Tuttavia il protocollo riduce in modo significativo la trasmissione overhead, limitando il numero totale di copie che possono essere trasmesse per ogni singolo messaggio. Cosi' Spray and Wait e' in merito all'energia piu' efficiente rispetto ai protocolli basati sull'inondazione. Inoltre l'esperienza del ritardo del messaggio e' abbastanza simile al caso ottimale di epidemic routing. Infine il protocollo Spray and Wait e' molto robusto e scalabile. Esso lavora come segue. La consegna del messaggio e' divisa in due fasi: la fase *spray* e la fase *wait*. Durante la prima fase copie multiple dello stesso messaggio sono diffuse nella rete dal nodo sorgente e da quei nodi che hanno ricevuto per primi dalla stessa sorgente il messaggio. Questa fase termina quando un dato numero di copie, detto L, e' stato diffuso nella rete. Poi, nella fase wait, ogni nodo che possiede una copia del messaggio (es.ogni nodo ripetitore) memorizza la sua copia e alla fine la consegna alla destinazione quando o nel caso in cui questa fosse a portata di mano. La fase spray puo' essere eseguita in vari modi. In base all'euristica *Source Spray and Wait*, il nodo sorgente inoltra tutte le L copie al primo nodo L definito che incontra. Invece secondo l'euristica *Binary Spray and Wait*, il nodo sorgente del messaggio consegna le prime $\frac{L}{2}$ copie del messaggio al primo nodo che incontra e mantiene le $\frac{L}{2}$ copie rimanenti. Quindi ogni nodo A, che memorizza $n > 1$copie del messaggio (o la fonte o il ripetitore successivo) e che e' a portata di mano di un altro nodo B che non possiede alcuna copia del messaggio, consegna $\frac{n}{2}$ copie a B e trattiene le rimanenti $\frac{n}{2}$ copie per se stesso. Quando un nodo e' lasciato con una sola copia del messaggio, passa alla *trasmissione diretta* e trasmette solo il messaggio alla destinazione finale quando o nel caso in cui la incontrasse. Sotto l'assunto che i nodi si muovono in base ad una distribuzione i.i.d, il routing Binary Spray and Wait e' quello che piu' propriamente puo' essere in accordo con tutti gli altri algoritmi di routing spray and wait e che permette il minimo ritardo. Un'interessante caratteristica di questo routing e' quella che esso puo' essere opportunamente sintonizzato per raggiungere la performance desiderata in uno scenario specifico. Nello specifico il numero di copie di un messaggio, L, puo' essere fissato per conseguire un dato ritardo atteso. Spray and Wait e' estremamente scalabile; infatti, quando cresce il numero di nodi nella rete, la percentuale di nodi che hanno bisogno di diventare ripetitori per realizzare la stessa performance diminuisce, mentre la maggiorparte degli altri schemi multicopia realizza rapidamente un incremento del numero di trasmissioni e cresce anche la densita' dei nodi. La performance di spray and wait e' stata testata teoricamente e per via simulativa. Le simulazioni sono state condotte su un simulatore even-driven

con i nodi che si muovono in base ad un modello di mobilita' random way-point; esse mostrano che spray and wait sovraperforma chiaramente altri protocolli di routing multi-copy, come epidemic routing o single-copy come quelli basati sulla utilita' in termini di numero di trasmissioni e di ritardo sperimentato dai messaggi.

3.3.2 Coding-based routing

Erasure-Coding Routing

In **Erasure-Coding Routing** [34] i messaggi sono codificati in prossimita' del loro nodo sorgente e per ogni messaggio sono generati dei *code blocks* molto piu' piccoli. Nello specifico, se M e' la lunghezza in bytes del messaggio, il numero dei code blocks che e' generato e' uguale a $\frac{Mr}{b}$, dove b e' la lunghezza di un singolo code block $b < M$ e r e' la costante *replication factor*. Dopo la generazione, i code blocks sono equamente distribuiti a kr ripetitori, essendo k un valore costante. Dunque l'algoritmo ha bisogno di $\frac{(1+\epsilon)M}{b}$ code blocks per arrivare a ricostruire il messaggio originale: $\frac{(1+\epsilon)M}{b}$ sul totale di blocks $\frac{Mr}{b}$. ϵ e' una costante che dipende dal particolare algoritmo di codifica che viene usato; tuttavia esso puo' essere considerato sufficientemente piccolo da essere trascurato e si puo' affermare che solo $\frac{1}{r}$ del totale dei code blocks e' necessario per arrivare a decodificare il messaggio originale. Cio' aiuta a ridurre il ritardo di propagazione dal momento in cui i blocks del messaggio sono codificati e mandati dal nodo sorgente fino al momento in cui la destinazione decodifica lo stesso messaggio. Infatti, dato l'alto numero di ripetitori coinvolti, c'e' una elevata possibilita' che almeno $\frac{1}{r}$ di questi siano affidabili e veloci. Per la stessa ragione Erasure-Coding e' abbastanza robusto contro la perdita di pacchetti dovuti alla cattiva qualita' del canale o alla congestione. Inoltre esso non subisce l'incremento del ritardo di propagazione dovuto a cattive scelte riguardo ai ripetitori per l'inoltro o ai percorsi. Esso introduce un protocollo overhead controllato in termini di bytes trasmessi ed e' molto efficiente rispetto al consumo di energia. Il routing Erasure-Coding e' stato testato analiticamente e anche attraverso simulazioni con dtnsim, che e' un discreto simulatore di eventi per ambienti DTN. Sono stati testati due modelli di mobilita': quello del sistema ZebraNet e poi quello basato su heavy-tailed inter-contact time. I risultati mostrano che questo routing si confa' bene con la densita' dei nodi e con la misura della rete. Esso ha il miglior caso peggiore di ritardo rispetto alle tecniche basate sull'inondazione e sulla storia.

Network Coding Routing

Nel **Network Coding Routing** [35], i pacchetti che viaggiano per la rete sono ottenuti dalla combinazione dei pacchetti che sono effettivamente generati al nodo sorgente. Inizialmente i nodi sorgente trasmettono i pacchetti che generano. I nodi intermedi ricevono i pacchetti dai nodi sorgente e da altri nodi intermedi, quindi eseguono una combinazione di tutte le informazioni ricevute e infine inviano i pacchetti risultanti dalla combinazione. I pacchetti vengono diffusi per tutta la rete e alla fine giungono alla destinazione in cui i pacchetti originali sono ricostruiti attraverso un processo di decodifica. Poniamo che A,B e C siano i soli tre nodi di una piccola rete e che il nodo A generi l'informazione a e il nodo C generi l'informazione c. Supponiamo poi che l'informazione prodotta debba essere nota a tutti gli altri nodi. Quindi il nodo A e il nodo C mandano la loro informazione al nodo B; quest'ultimo poi, piuttosto che mandare due differenti pacchetti rispettivamente per a e c, trasmette un singolo pacchetto contenente $a \oplus c$($\oplus$ sta per XOR). Una volta ricevuto$a \oplus c$, sia A che C possono finalmente dedurre l'informazione mancante, per esempio il nodo A puo' inferire c e il nodo C puo' inferire a.

In base al protocollo Network Coding Routing, dato ogni nodo $v \in V$ nella rete (V da' il set completo di nodi nella rete) e N(v) il set dei suoi vicini raggiungibili attraverso il livello fisico di trasmissione, ogni volta che un set di *vettori di informazioni* $x_i \in 0,1^k$ (per k,i=1,...,m) e' pervenuto al nodo v, viene elaborata una combinazione lineare come quella che segue e mandata ai vicini.

$$\sum_{i=1}^{m} g_i x_i$$

Dove g_i e' il *vettore di codifica* per x_i . I vettori di informazioni sono sempre mandati insieme con il corrispondente vettore di codifica. Ogni nodo che riceve memorizza le tuple in arrivo $< g_i x_i >$ insieme con le tuple corrispondenti ai pacchetti generati su di esso costituiti nella forma $< e_i x_i >$, dove e_i e' l'unita' vettoriale *i-th*. Tutte le tuple sono raccolte in una matrice di decodifica G_v , il cui ordine da' il numero di pacchetti che possono essere decodificati momentaneamente. Se m e' il numero totale di pacchetti generati nella rete, ogni nodo puo' decodificarli tutti quando la sua matrice di decodifica avra' ordine m. Quando arriva un nuovo pacchetto ad un nodo, si dice che e' *innovativo* se incrementa l'ordine della matrice di decodifica, altrimenti esso viene semplicemente ignorato. Dato il fattore di inoltro $d > 0$, con un pacchetto innovativo ricevuto, il vettore d sara' generato dalla corrispondente

matrice e trasmesso a tutti i nodi vicini. Un successivo vettore sara' generato e inviato con una probabilita' $d - \lceil d \rceil$. In caso di un nodo sorgente, $max\{1, \lceil d \rceil\}$ vettori saranno generati e trasmessi. Un nuovo pacchetto e' inviato dalla sorgente almeno una volta. Per evitare una gestione di matrici troppo estese, quando molte sorgenti sono presenti nella rete, ognuna producente differenti pacchetti, i vettori sono raggruppati in *generazioni*. Esiste una matrice per ogni *generazione* e solo vettori di alcune generazioni possono essere combinati. Il lavoro in [9] propone una funziona hash usata per distinguere i membri delle generazioni. $\Gamma_\gamma = \{x_i \mid f(x_{i,j}) = \gamma\}$ e' l'insieme di tutti i vettori sorgente della generazione γ. Dove $x_{i,j}$ e' la $j-$esima vettore della $i-$esima sorgente. $f(x_{i,j})$ determina a quale generazione appartiene il pacchetto. Ognivolta che una matrice diventa troppo grande, viene generata una nuova funzione hash. Una volta che un nodo ha decodificato l'intera generazione, la matrice non e' piu' utile al nodo; inoltre, la propria informazione potrebbe essere necessaria ai nodi vicini per poter effettuare la codifica. Un nodo dovrebbe mantenere le informazioni di una matrice, fino a quando e' ammissibile che generi pacchetti. Per salvaguardare la memoria, in qualsiasi momento, i nodi sono capaci di cambiare il grado della memoria. Il Network coding routing gode di buone performance in termini di consegna dei pacchetti sia in dense reti mobili, sia in reti scarse con un alto coefficente di perdita dei pacchetti e con nodi che dormono per lunghi periodi. IL routing, rispetto ad altri protocolli stateless, trae vantaggio dalla mobilita' dei nodi.

Utility-based Routing

I protocolli di routing basati sulla disseminazione offrono un ottimo livello di consegna dei messaggi, minimizzando i ritardi di consegna. Purtroppo,c'e' pero' un alto consumo di bandwith e di memoria e quindi un elevato spreco di risorse. I protocolli presentati in questa sezione sono caratterizzati dalla consegna dei messaggi in reti ad hoc a connessione intermittente al fine di ottimizzare l'uso delle risorse utilizzate dai nodi. La strategia di base consiste nel limitare il numero di copie del messaggio che sono inoltrate nella rete tramite una selezione dei nodi. Ogni messaggio e' inoltrato soltanto a quel nodo o a quei nodi che hanno la piu' alta probabilita' di consegnare il messaggio con successo al nodo destinazione, evitando inutili scambi, repliche e ritrasmissioni di messaggi. L'utilita' di un nodo, per l'inoltro di un messaggio, si basa sull'*utility* del nodo. Anche se ottimizzano l'uso di bandwidth e il consumo di energia della rete, le tecniche di questa categoria portano ad un incremento nei ritar-

di di consegna dei messaggi rispetto ai protocolli basati sull'inondazione. Questo e' dovuto alle inesattezze ed agli errori nella scelta dei nodi. Inoltre, tali tecniche hanno un elevato costo computazionale rispetto alle tecniche basate sulle replicazioni, in quanto i nodi hanno bisogno di mantenere uno stato che tenga traccia dei valori di *utility* associati a tutti gli altri nodi presenti nella rete (es., tutti i possibili nodi destinazione); di conseguenza e' necessaria una memoria maggiore per mantenere gli stati e i messaggi. Inoltre occorre considerare anche i costi relativi al mantenimento e all'aggiornamento degli stati.
I protocolli di routing basati sull'utility possono essere suddivisi come segue:

1. *protocolli di routing basati sulla storia*: questi protocolli elaborano programmi di utilit, sulla base della storia degli incontri tra i nodi o anche sulla base della storia delle visite nei vari luoghi. Come rappresentanti di questa categoria verranno presentati i seguenti protocolli: a) Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET) e b) MobySpace.

2. *protocolli di routing basati sul percorso breve*: questi protocolli mirano a a minimizzare i costi di consegna dei messaggi selezionando i percorsi meno costosi. Corrispondono a percorsi che possono essere attraversati con minimi ritardi. I protocolli che rappresentano questa categoria sono: a) protocollo di Routing Extremely Opportunistic (EX-OR), b)protocollo di routing Shortest Expected Path (SEPR).

3. *protocolli di routing basati sul contesto*: sono protocolli che fanno considerazioni piu' generali per inoltrare i messaggi. Essi prendono in considerazione la mobilita' degli utenti e il livello di batteria residua. I protocolli che rappresentano questa categoria sono: a)HIBOP, b)Interrogation-Based Relay Routing (IBRR) , c) Context-Aware Routing protocol (CAR).

4. *protocolli di routing basati sulla locazione*: di norma, si sforzano di individuare il nodo di destinazione di un messaggio con un sottostante protocollo di routing classico, sia proattivo o reattivo. Nel caso in cui un nodo di destinazione non venga trovato, sono attuate diverse strategie: invio di un pacchetto locale in modo broadcast, ricerca di un percorso connesso alla destinazione attraverso i nodi vicini raggiunti, avvicinamento all'ultima locazione conosciuta della destinazione e diffusione del messaggio nella vicinanze. I protocolli che rapp-

resentano questa categoria sono: a) Spraying protocol e b)Mobile Relay-based Protocol (MRP).

3.3.3 History-based Routing

Probabilistic Routing Protocol using History of Encounters and Transitivity

Il PROPHET [36] e' l'evoluzione dell'Epidemic che introduce il concetto di prevedibilita' di consegna. La prevedibilita' e' la probabilita' per un nodo di incontrare la destinazione. Ogni nodo detiene una tabella con tutte le probabilita' di consegna per ogni nodo presente nella rete. Ovviamente, la probabilita' di consegna aumenta quando viene incontrato il nodo destinazione e diminuisce ogni volta che non lo si incontra. La $Probabilita'diconsegna$ di ogni nodo a, verso un nodo destinazione b e' indicata come $P_{(a,b)} \in [0,1]$. Ogni volta che i nodi a e b si incontrano, la loro probabilita' di consegna aumenta come segue.

$$P_{(a,b)} = P_{(a,b)old} + (1 - P_{(a,b)old}) \times P_{init}$$

$P_{(a,b)old}$ e' l'ultimo valore conosciuto della probabilita' di consegna, mentre $P_{init} \in [o,1]$ e' una costante di inizializzazione. La probabilita'di consegna decresce , come mostrato sotto, ogni qualvolta i nodi non si incontrano.

$$P_{(a,b)} = P_{(a,b)old} \times \gamma^k$$

$\gamma \in [0,1)$ rappresenta la costante di invecchiamento e k e' il numero di unita' di tempo trascorso dall'ultima volta che la prevedibilita' di consegna e' stata invecchiata. Le probabilita' di consegna vengono aggiornate anche mediante l'utilizzo di proprieta' transitive. Se un nodo a,incontra un nodo b e quest'ultimo incontra un nodo c, si puo' dedurre che il nodo a e' un buon inoltro per il nodo c e viceversa.

$$P_{(a,c)} = P_{(a,b)old} + (1 - P_{(a,c)old}) \times P_{(a,b)} \times P_{(b,c)\times\beta}$$

$\gamma \in [0,1]$ e' un fattore di scala e da' l'impatto della transitivita' sulla probabilita' di consegna. Ogni volta che due nodi entrano in contatto si scambiano i vettori di sintesi dei messaggi che essi immagazzinano. Essi aggiungono a ciascun messaggio la probabilita' di consegna relativa al nodo di destinazione del messaggi; entrambi i nodi decidono quali messaggi chiedere all'altro, sulla base di queste probabilita'. In

dettaglio, il nodo a richiede un messaggio al nodo, b destinato al nodo c ,solo se la propria probabilita' di consegna, dal nodo a al nodo c, e' maggiore della probabilita' dal nodo b al nodo c. L'algoritmo PROPHET e' stato testato con un simulatore per reti con, inizialmente, un modello di mobilita' casuale e successivamente un modello di mobilita' piu' realistico. Le simulazioni mostrano, rispetto all'epidemic routing, miglioramenti in termini di consegna e di ritardo; inoltre il routing introduce meno overhead di traffico.

MobySpace routing

Il protocollo MobySpace [37] sfrutta le conoscenze del modello di mobilita' dei nodi per costruire un alto spazio dimensionale Euclideo, chiamato *MobySpace*, dove ciascuna dimensione rappresenta una locazione nello spazio fisico e le coordinate (chiamate *MobyPoint*) corrispondono alla probabilita' di trovare il nodo in corrisponza della locazione. Due nodi che hanno una serie di frequenze di contatti simili, sono vicini al *MobySpace*. Il nodo migliore per la trasmissione e' il nodo che e' piu' vicino possibile al nodo di destinazione in questo spazio. Cio' in effetti aumenta la probabilita' del messaggio di giungere a destinazione. Ovviamente, nello spazio virtuale di contatto appena descritto, la conoscenza di tutti gli assi dello spazio richiederebbe inoltre la conoscenza di tutti i nodi che sono in circolazione nello spazio, ma questa conoscenza non e' necessaria per un routing di successo.

Uno spazio virtuale alternativo puo' essere definito con dimensioni minori, con la condizione che le visite dei nodi a particolari locazioni siano tracciate e che i nodi abbiano una certa regolarita' nel visitare un certo insieme di locazioni. Quindi, ogni asse e' scelta per rappresentare una particolare locazione e la distanza dagli assi e' la probabilita' di un nodi di visitare quella locazione. Nodi che hanno la stesse probabilita' di visitare una certa locazione, vuol dire che i nodi avranno maggiore probabilita' di incontrarsi rispetto a nodi che presentano differenti valori di probabilita'. Efficacia di questo spazio virtuale come strumento decisionale per l'inoltro dei messaggi puo' essere limitata se i nodi cambiano le loro abitudini troppo rapidamente. Per permettere ad ogni nodi di costruire il proprio MobySpace di riferimento con le informazioni di tutti gli altri nodi, i modelli di mobilita' dei nodi devono essere trasmessi nella rete (tramite uno forma di inondazione epidemica) ma questo comporta ad un elevato overhead. Secondo la strategia di trasmissione del MobySpace, messaggi sono inoltrati verso i nodi che hanno il modello di mobilita' piu' vicino al modello di mobilita' della destinazione, cio' comporta l'introduzione

di una funzione di somiglianza per confrontare i modelli di mobilita'. Diverse alternative sono state studiate sulla base di diversi parametri di distanza: *distanza euclideana* [4], *distanza Canberra*[5]. Il routing MobySpace e' stato testato su differenti modelli di mobilit derivanti da sperimentazioni reali in ambienti WiFi. Le locazioni MobySpace sono state fissate presso dedgli Access Point che forniscono connettivita' wireless ad Internet in un campus universitario. Una coppia di nodi sono in grado di comunicare solo si strovano nello stesso Access Point (MobyPoint). Il movimento dei nodi erano basati su leggi di potenza e ogni nodo ha un modello di mobilita' definito dalla distribuzione di P. $P(i)$ e' la probabilita' per i nodi di trovarsi nella locazione i.

$$P(i) = k(\frac{1}{d})^{n_i}$$

n_i e' l'indice di preferenza della locazione i; d e' l'esponente della legge di potenza, k e' una costante. Il protocollo MobySpace e' stato confrontato con altri protocolli come:epidemic routing, wait-for-destination, random routing (il salto successivo e' scelto in modo causale), ottenendo risultati contrastanti in termini di ritardi dei messaggi e lunghezza dei percorsi. I risultati delle simulazioni mostrano che con lo scambio di pieni modelli di mobilita', il MobySpace supera gli altri algoritmi sia con la metrica euclideana sia con la Cosin Angle. Invece la metrica canberra offre migliori prestazioni anche con la diffusione di modelli di mobilita' parziali.

3.3.4 Shortest path-based Routing

Extremely Opportunistic Routing (Ex-OR)

Questo protocollo [38] differisce da quelli visti nella sezione precedente perche' non ricerca subito il nodo successivo migliore per inoltrare il messaggio prima di trasmetterlo. Infatti, rinvia ogni decisione che riguarda il miglior inoltratore per un messaggio al periodo successivo a quello in cui questo e' stato inviato. Il migliore inoltratore e' scelto fra i nodi che hanno ricevuto il messaggio ed e' quello che puo' offrire, in quel particolare momento, la migliore opportunita' di consegna del messaggio rispetto a tutti gli altri nodi che lo hanno ricevuto. ExOR assume che ogni nodo sia a

[4]La distanza euclidea la distanza fra due punti, ossia la misura del segmento avente per estremi i due punti.

[5]La distanza di Canberra esamina la somma di serie di una frazioni tra le coordinate di un paio di oggetti. Ogni termine della frazione ha un valore compreso tra 0 e 1. Se una delle coordinate e' zero, l'unit di termine assume l'altro valore

conoscenza del tasso di perdita della trasmissione tra qualsiasi coppia di nodi nella rete e che percio' puo'stimare, dato un particolare messaggio, il costo di consegna previsto (Expected Delivery Cost) da ogni nodo della rete al nodo destinazione del messaggio stesso. L' Expected Delivery Cost misura la distanza di un nodo al nodo destinazione e corrisponde al minimo costo di consegna da quel nodo al nodo destinazione (in caso di percorsi alternativi). Il costo di consegna di un percorso e' la somma di tutti i costi di ogni singolo link (diverso dalla probabilita' di consegna) che compongono l'intero percorso. Per supportare il calcolo dei costi di consegna prevista da qualsiasi nodo per ogni destinazione possibile, ogni nodo deve monitorare la debolezza dei suoi legami locali e nel tempo compiere inondazioni periodiche delle misure effettuate. Dopo aver fatto il calcolo, ogni nodo e' capace di creare una lista contenente tutti i migliori inoltratori per ogni possibile destinazione; la lista elenca dai migliori ai peggiori inoltratori. Per esempio, un nodo A puo' avere la sua lista di inoltratori per un messaggio destinato al nodo D; usando i migliori inoltratori, il messaggio viene spedito al nodo E, successivamente al nodi F, al nodi G e cosi' via. Quando i nodi, con priorita' maggiore, sono temporaneamente non utilizzabili, per l'inoltro del messaggio, verranno scelti i nodi con priorita' inferiore.
Il protocollo ExOR lavora come segue.

Ogni nodo sorgente, che desidera consegnare un numero di pacchetti ad un nodo destinazione, organizza gruppi di pacchetti e li trasmette uno alla volta (il protocollo lavora su piu' pacchetti, piuttosto che su singoli pacchetti, per alleggerire l'overhead per ogni singolo pacchetto). Ad ogni pacchetto viene aggiunta una lista di nodi inoltratori (inizialmente lo stesso per tutti i nodi del gruppo); questa lista contiene i nodi che presentano i minori costi di consegna verso i nodi destinazione. La lista elaborata dalla sorgente stessa viene chiamata batch map; tutti i nodi inclusi, dal migliore al peggiore, aiuteranno l'inoltro dei pacchetti verso la destinazione. La lista include anche i nodi sorgente e destinazione e specifica il nodo con la priorita' maggiore che ha appena mandato quel pacchetto. Una volta avvenuta la trasmissione dalla sorgente, il protocollo selezionera' il successivo nodo dalla *batchmap* dei nodi che hanno ricevuto i pacchetti; selezionato il nodo, i pacchetti verranno ritrasmessi. Specificatemente, ogni nodo che ha ricevuto alcuni pacchetti e il cui ID e' incluso nel *batchmap*, i) attende di ricevere l'intero gruppo di pacchetti; ii) attende che il nodo con priorita' maggiore abbia terminato l'inoltro dei pacchetti ricevuti; iii) inizia la trasmissione dei pacchetti ricevuti e che non sono stati ancora trasmessi da un nodo a priorita' maggiore (ogni volta che un nodo sente che un gruppo di pacchetti ven-

gono trasmessi da un nodo con priorita' maggiore, il batch map viene aggiornato a livello locale con la priorita' dell'inoltratore dei pacchetti). Il protocollo regola gli istanti di tempo in cui ogni nodo puo' trasmettere evitando collisioni. Questo tipo di gestione permette a differenti pacchetti di seguire contemporaneamente diversi percorsi verso la destinazione. Attraverso i mezzi a segnali radio a lungo raggio,che sono ad alta perdita di dati, alcuni pacchetti possono raggiungere nodi molto vicini alla destinazione, richiedendo percorsi brevi. Una volta giunti alla destinazione, quest'ultima inviera' solamente il batch name dei pacchetti senza dati. Un approccio fondamentale per il protocollo e' chiaramente quello di costruire una lista per ogni gruppo di pacchetti. Il protocollo e' stato testato in un ambiente reale con 38 nodi fissi, dotati di tecnologia 802.11b, sparsi su di un'area di $6km^2$. I risultati mostrano che EXOR impedisce ritrasmissioni inutili rispetto ai tradizionali protocolli di routing ad hoc ed inoltre aumenta il throughput end-to-end. Il guadagno di throughput varia a seconda del numero di nodi trasmessi dall'origine alla destinazione: e' quasi del 35% quando l'origine e la destinazione sono vicini, e di un fattore 2 a 4, quando sono piu' lontani. Rispetto ai routing tradizionali, ExOR, limitando la trasmissione dei pacchetti, causa meno interferenze tra i nodi della rete. Data la necessita' dell'inondazione dello stato dei link, ExOR fornisce migliori prestazioni quando la rete e' quasi completamente collegata, con scarse occasioni di disconnessioni e di partizioni della rete.

Shortest Expected Path Routing protocol (SEPR)

Il protocollo Shortest Expected Path Routing [39] si focalizza su due aspetti chiave per la strategia di inoltro. Specificatamente, si concentra sul nodo a cui inoltrare il messaggio e su quale politica di sostituzione del buffer adottare. La politica di sostituzione buffer decide il miglior candidato per la sovrascrittura, tra tutte le voci della cache di un nodo, quando arriva un nuovo messaggio, bisognoso di storage, e non c'e' piu' spazio disponibile. SEPR si basa sulla stima della lunghezza del percorso previsto (*Expected Path Lenght*), una metrica simile al costo di consegna prevista (*Expected Delivery Cost*), utilizzato in Exor per prendere decisioni di forwarding. Per ogni nodo della rete e' prevista una *link probability table* che contiene la probabilita' di un link verso i nodi. La probabilita' dei collegamenti tra due nodi, detti nodo i e nodo j, e' calcolata come segue.

$$P_{i,j} = \frac{Time_{connection}}{TimeWindow}$$

$Time_{connection}$ e' il numero totale di unita' di tempo di collegamento tra i due nodi e $TimeWindow$ e' il tempo di campionamento totale. La probabilita' e' aggiornata ogni volta che due nodi entrano in contatto. Inoltre, i link probability table vengono scambiati interamente tra i nodi durante i contatti. Infine, durante i contatti, i nuovi link probability table verranno propagati nella rete. Assumendo che T sia la variabile casuale che modella il tempo totale necessario ad un messaggio m per raggiungere il nodo di destinazione D dalla sorgente S, *Expected Path Lenght* tra nodo S e nodo D e' il valore atteso di T, esempio, E(T). Infatti,possiamo dire che il tempo trascorso per andare dal nodo S al nodo D e' una buon metro per misurare la distanza tra questi due nodi. Dato $\prod(t)$ la funzione di distribuzione di probabilita' per T, l'*Expected Path Lenght* e' calcolata come segue.

$$E(T) = E_{path} = \sum_{t=1}^{\infty} t \times \cdot(t)$$

In caso di percorsi multi-hop dove il tempo trascorso per attraversare ogni link e' rappresentato da variabili casuali indipendenti, dette T_i, l'*Expected Path Lenght* e' calcolato come segue.

$$E_P(T) = \sum_{i=1}^{k-1} E(T_i) \simeq \sum_{i=1}^{k-1} \frac{1}{p_{i,i+1}}$$

Il tempo necessario per percorrere un singolo link pu ragionevolmente essere assunto inversamente proporzionale alla probabilit per quel link. Quando sono possibili multipli percorsi, il migliore ovviamente quello che pi veloce da attraversare, per esempio lo shortest path, come assunto qui. Esso puo' essere calcolato con l'algoritmo Dijkstra. Un messaggio m destinato al nodo D e' inoltrato dal nodo A al nodo B durante un contatto nel caso in cui l'expected path lenght dal nodo B al nodo D sia minore che dal nodo A al nodo D. L'aggiornametno della memoria e' necessario ogni qual volta arriva un nuovo messaggio e la memoria risulta piena. Per gestire questi aggiornamenti, puo' essere introdotta piu' di una metrica chiamata effective path length. Essa e' associata ad ogni messaggio memorizzato in un nodo e da' un'idea del tempo residuo di destinazione per quel messaggio. Cosi, quando un nuovo messaggio arriva, il messaggio da sovrascrivere sara' quello con la minore lunghezza di percorso, in quanto e' piu' probabile che quel messaggio abbia gia' raggiuntola destinazione. Durante i contatti, i nodi confrontano le liste dei corrispondenti messaggi. Se un nodo A memorizza un messagio m destinato al nodo D e comprende che l'expected

path lenght del nodo B incontrato e' piu' breve del proprio expected path lenght, allora il messaggio e' inoltrato al nodo B e viene aggiornata l'effective path lenght, EPL_m per il messaggio m in memoria come segue.

$$EPL_m = min(EPL_m, E_{path}(B, D))$$

Il protocollo SEPR e' stato testato tramite una simulazione usando un modello di mobilita' cittadino, la simulazione mostra che SEPR registra un incremento del 35% sulla consegna dei messaggi rispetto ad epidemic e un decremento di costo delle risorse del 50%.

3.3.5 Context-based Routing

HiBop

HiBop [40] e' un protocollo a conoscenza completa di contesto, include meccanismi per gestire qualsiasi tipo di informazione di contesto. Il contesto e' definito come insieme di informazioni che descrivono la comunita' nel quale l'utente vive e la storia delle relazioni sociali che lo riguardano. Per ogni nodo, le informazioni di contesto possono riguardare informazioni personali dell'utente (ad esempio il nome), la sua residenza (ad esempio l'indirizzo), il suo lavoro (ad esempio istituzione), etc.
In HiBop, i nodi condividono i loro dati proprio durante i contatti e quindi imparano il contesto in cui sono immersi. I messaggi sono inoltrati tramite nodi che condividono sempre piu' dati di contesto con la destinazione del messaggio. Poiche' gli utenti di HiBop hanno possibilita' di condividere informazioni personali, bisogna considerare i problemi relativi alla privacy. La gestione della privacy in reti opportunistiche e' un argomento in gran parte non ancora affrontato. Uno dei principali campi di lavoro futuro sara' proprio la ricerca di soluzioni per la tutela della privacy in HiBop. Infatti, HiBop assume che ogni nodo memorizza localmente una tabella di identita' (IT), che contiene informazioni personali dell'utente, come mostrato in 3.2 .

Figura 3.2: Identity Table [2]

Personal Information		*Residence*	
Name	John Doe	**City**	Pisa
Email	j.doe@iit.cnr.it	**Street**	Via Garibaldi, 2
	...		...

I nodi si scambiano ad ogni contatto la propria IT e l'insieme delle IT dei nodi vicini, che rappresentano il contesto corrente, fornendo una panoramica del contesto del nodo. Il contesto corrente e' utile al fine di valutare l'idoneita' instantanea di un nodo per essere un buon inoltratore. Ma anche se un nodo non e' un buon inoltratore a causa della sua locazione o dei sui vicini, potrebbe essere un supporto valido per via delle sue abitudini e delle sue esperienze passate. Infatti, e' importante recuperare informazioni sui dati di contesto, raccolti da ogni nodo in passato e studiare il ripetersi di questi dati nel contesto attuale del nodo. A tal fine, ogni informazione di contesto vista nel contesto attuale viene registrata in una *History Table*, insieme con un indice di probabilita' di continuita', che rappresenta la probabilita'di incontrare tale informazione in futuro. L'idea principale di trasmissione HiBop e' ricercare nodi che mostrano la maggiore corrispondenza con le informazioni di contesto note alla destinazione. Alta corrispondenza significa alta somiglianza del contesto del nodo con il contesto della destinazione, quindi, un'alta probabilita' per il nodo di portare il messaggio nella comunita' della destinazione (eventualmente, alla destinazione stessa). Percio', un nodo che desidera inviare un messaggio tramite HiBop specifica l'IT del destinatario nell'header del messaggio. Ogni nodo nel percorso tra mittente e destinazione richiede gli attributi del destinatario per calcolare il loro grado di corrispondenza e trasmette il messaggio se il nodo incontrato mostra una corrispondenza maggiore della propria. Va ricordato che i livelli di corrispondenza vengono valutati come probabilita' di consegna e distinte probabilita' sono valutate sulla base del contesto corrente (pcc) e della History (ph).
La probabilita' finale viene valutata come: $p = \alpha * ph + (1 - \alpha) * pcc$, con
α tra $0 < \alpha < 1$.
Il parametro α permette di regolare la relativa importanza del contesto corrente (cc) e della History (ph). In HiBop, solo il nodo di origine e' autorizzato a replicare il messaggio, al fine di ben controllare il trade-off tra affidabilita' e diffusione del messaggio.

Il nodo sorgente replica il messaggio fino a quando la probabilita' di perdita dei nodi utilizzati per le replicazioni sia al di sotto di una soglia ben definita (pl^{max}). In particolare, se p(i) e' la probabilita' di consegna dei ith-nodo utilizzato per replicare il messaggio e k e' il numero di nodi utilizzati per la replica, vale la seguente equazione:

$$k = min\{j | \prod_{J=0}^{j}(1 - p_{(i)}) <= pl^{max}\}$$

Interrogation-Based Relay Routing (IBRR)

Il protocollo IBRR [41] e' stato concepito per una rete ad hoc satellitare e specificatamente per una *ad hoc Scientific Earth Observing(SEO) satellite networks*, composto sia da satelliti che da stazioni terrestre. I satelliti in questa rete non hanno una tipologia predefinita e possono avere differenti altitudini, orbite, capacita' di collegamento. Dato che i collegamenti intersatellitari possono solo garantire connessioni intermittenti, ogni volta che un satellite decide di inoltrare un messaggio ad un altro satellite, esso ricerca il migliore satellite vicino per inoltrare il messaggio. Questo e' realizzato per valutare le informazioni di contesto raccolte durante i contatti tra i satelliti. Le informazioni di contesto includono: i) informazioni sulla locazione spaziale, ii) bandwidth dei collegamenti intersatellitari tra i vari vicini, iii) relativa velocita'/mobilita' iv) vicinanza di altri satelliti e stazioni terrestri. Durante un contatto tra satelliti, vengono scambiate le relative informazioni di contesto del nodo incontrato, le informazioni di contesto dei loro vicini, quindi viene eseguita una cosiddetta one-hop look-ahead. L'one-hop look-ahead fa conoscere al nodo la topologia della rete. Quando un nodo deve inviare un messaggio, seleziona il miglior nodo in base alle informazioni raccolte durante i vari contatti, altrimenti il protocollo IBRR eseguira' un inoltro opportunistico e memorizzera' il messaggio localmente, in attesa di una opportunita' di inoltro.

Context-Aware Routing protocol (CAR)

Il protocollo CAR [42] utilizza un classico protocollo di routing per fornire l'inoltro dei messaggi dentro nubi connesse di un partitioned ad hoc network. Specificatamente, si avvale di un approccio proattivo; cosi' ogni nodo della rete tiene la propria tabella di routing che lo collega ad ogni (potenziale) nodo di destinazione conosciuto, individuato nella propria partizione. Il protocollo di routing proattivo e' in grado di trovare percorsi tra il nodo sorgente e un nodo di destinazione che sia situato all'interno di una nuvola collegata ad hoc. I nodi che risiedono in altre partizioni della stessa rete, non sono rintracciabili tramite un classico protocollo di routing. Tuttavia, possono esistere nodi appartanenti al nodo sorgente o nodi di inoltro che sono in grado di rintracciare la destinazione o altri nodi che possono farlo. CAR si concentra sull'espansione delle tabelle di routing per supportare l'inoltro tra nuvole disconnesse aggiungendo una coppia di colonne. Esse danno il miglior inoltratore verso un nodo destinazione e la corrispondente probabilita' di consegna che misura

le probabilita' delle consegne fatte con successo alla destinazione tramite quel inoltratore. Ogni nodo della rete e' incaricato di produrre le proprie probabilita' verso gli host di destinazione noti; le probabilita' sono scambiate periodicamente cosi' che ogni nodo puo' valutare il miglior nodo inoltratore per ogni destinazione (es., il nodo con la migliore probabilita' di consegna verso ogni nodo destinazione). Quando si invia un messaggio verso una certa destinazione, un nodo inoltra il messaggio sia al corrispondente salto successivo, nel caso in cui la destinazione e' all'interno della stessa nube della sorgente/inoltratore, o al miglior successivo salto nel caso in cui non esiste un percorso completo verso la destinazione. Tra gli attributi di contesto per l'elezione del migliore inoltratore si trova, ad esempio, il livello di batteria residuo, il tasso di variazione di connettivita', la probabilita' di trovarsi nella stessa nube della destinazione e il grado di mobilita'. Quando il nodo trasportatore riceve un messaggio per inoltrarlo, lo memorizza in un buffer locale e lo inoltrera' alla destinazione quando la incontrera', oppure ad un altro nodo con probabilita' di consegna maggiore. Dara la differenza di attributi di contesto definibili, occorre un modo per poterli combinare in una sola probabilita' di consegna. CAR lo realizza utilizzando *multi-attribute utility theory* per produrre la *utility function* di un insieme di attributi $(X_1, X_2...., X_n)$ con valori $(x_1, x_2...., x_n)$. La *utility function* puo' essere derivata sia da una semplice aggiunta di una funzione o da una funzione ponderata che dipende dagli attributi che sono mutualmente indipendenti(*mutually preferentially indipendent*). Segue la formula per calcolare la utility function in entrambi i casi.

$$U(x_1, x_2...., x_n) = \sum_{i=1}^{n} U_i(x_i)$$

$$f(U(x_1, x_2...., x_n)) = \sum_{i=1}^{n} a_i(x_i) \cdot w_i \cdot U_i(x_i)$$

w_i,$i = 1, ..., n$ sono i *pesi significativi* e riflettono le relative importanze di ogni attributo, mentre $a_i(x_i)$,$i = 1, ..., n$, sono coefficenti variabili che incrementano o decrementano nel tempo a seconda del valore assunto da un attributo, dalla sua prevedibilita' (correlazione forte o debole), e dalla sua disponibilita' (quanto sia recente l'arrivo, o l'ultimo update). Come detto sopra, le probabilita' di consegna sono scambiate periodicamente tra i nodi per garantire che le decisioni sugli inoltri siano sempre prese con informazioni recenti. Inoltre, per limitare il consumo di banda, le prevedibilita' di consegna sono aggiornate per mezzo di previsioni, queste

techniche di previsioni fanno uso di filtri Kalman [6]. CAR e' stato testato tramite simulazione su OMNET++ e confrontato con il routing epidemico e di inondazione. Sono stati assunti un gruppo di modelli di mobilita' tra i nodi della rete, prendendo in considerazione i) idiversi livelli di connettivita' e ii)le probabilita' che il nodo si trovi nella stessa nube in cui vi e' la destinazione. Le simulazioni mostrano che l'epidemic routing offre prestazioni migliori rispetto a CAR in termini di consegna e ritardi dei messaggi, mentre CAR risulta sempre migliore del protocollo di inondazione. Comunque CAR mostra una maggiore scalabilita' rispetto ad epidemic routing e un overhead costante per ogni dimensione del buffer.

3.3.6 Location-based Routing

Spraying Protocol

Il protocollo [43] gestisce la consegna dei messaggi verso nodi altamente mobili, assumendo che i nodi che si allontanano dalla loro posizione attuale possono essere raggiunti, per qualche istante di tempo, nelle vicinanze di questa posizione. Quindi, il miglior modo per trovare la destinazione di un messaggio, che si sposta dalla sua precedente posizione, e' quello di consegnare il messaggio ai nodi presenti nelle vicinanze dell'ultima locazione conusciuta della destinazione. Secondo il modello di rete assunto nel protocollo Spray, esistono due tipi di nodi:*switchs* e *endpoints*. Gli switchs hanno funzioni di instradamento, mentre gli endpoints possono essere nodi sorgente e nodi destinazion. Per ogni locazione , ad ogni endpoints viene associato uno switch che sara' il router di default per il recapito dei messaggi. Un gestore di locazioni (Location Manager LM) si ritiene che sia presente nella rete e che raccolga le informazioni di locazione di ogni nodo della reta in un database. Specificatamente, ogni LM memorizza per ogni endpoint il corrispondente switch (endpoins e swicht sono detti *affiliati*). Cosi, ogni volta che un nodo si sposta dalla sua attuale locazione, esso invia in *Location Update* alla LM l'informazione della sua nuova affiliazione. Mentre, ogni volta che un nodo desidera inviare un messaggio, prima invia una *Location Subscribe* al LM per chiedergli l'ultima affiliazione del nodo destinazione. La LM risponde con una *Location Information* informando il nodo dell'ultima affiliazione conosciuta della destinazione e da' una coppia di parametri:

[6] il Filtro di Kalman un algoritmo utilizzato per il filtraggio dei dati costruiti sulla base di una media ragionata tra il prossimo valore predetto e il prossimo valore stimato

depth e *width*. Il nodo sorgente inoltra in modalita' unicast[7] il messaggio nell'ultima affiliazione conosciuta della destinazione (il percorso e' trovato tramite un protocollo reattivo)e il ricevente inoltra in modo broadcast[8] il messaggio a tutti i suoi vicini e ai vicini dei vicini. *Width* restituisce il numero dei vicini verso il quale il messaggio sara' mandato in multicast [9] L'ultimo gruppo di vicini che ricevono il messaggio sono *depth* hop, a partire dal primo nodo che realizza il broadcast (lo switch). Il calcolo dei parametri width e depth e' realizzato dal LM prendendo in considerazione la storia dei cambiamenti delle affiliazioni per ogni endpoint. Se un nodo cambia frequentemente la propria affiliazione, esso e' altamente mobile, cosi' la dimensione e la profondita' del broadcast saranno incrementati. L'efficacia del protocollo e' stato testato via simulazione, lo strumento di simulazione e' stato scritto in linguaggio C++. L'unico modello di mobilita' considerato per i nodi e' stato Extended Random Walk. Il protocollo supera i protocolli reattivi quando la mobilita' dei nodi aumenta.

Mobile Relay Protocol (MRP)

L' MRP [44] e' stato concepito per integrare i protocolli di routing ad hoc preesistenti e gestisce l'inoltro dei messaggi quando non viene trovato nessun percorso per raggiungere la destinazione e le applicazioni che hanno generato il messaggio possono tollerare dei ritardi. Ai messaggi inoltrati in modo opportunistico vengono assegnati due parametri: h e $d.h$ rappresenta il limite superiore per il numero di volte che un messaggio puo' essere trasmesso. Ogni volta che un messaggio raggiunge un nuovo nodo, h viene decrementato di un'unita. d rappresenta il limite superiore per la durata di un percorso multi-hop verso la destinazione secondo un protocollo di routing tradizionale. Quindi un messaggio puo' attraversare h hop su un percorso non connesso e d hops su un percorso connesso. Il protocollo MRP lavora come segue. Si supponga che uno strato MRP e' aggiunto nel livello di rete (dove uno protocollo di routing classico viene implementato) in modo da poter essere coinvolto nella trasmissione dei messaggi che vengono generati dalle applicazioni tolleranti ai ritardi, quando il protocollo di routing traditionale fallisce la consegna. Supponiamo inoltre che i messaggi sono contrassegnati quando vengono trattati con MRP in

[7] un messaggio destinato ad un solo sistema

[8] Per broadcasting si intende la trasmissione di informazioni da trasmittente a tutti i riceventiche non sono definiti a priori in grado di ricevere.

[9] Con il termine Multicast si indica la distribuzione simultanea di informazione verso un gruppo di destinatari.

modo che possano essere trattati diversamente dagli altri. Quando un nodo gestisce la consegna di un messaggio che non e' stato trattato precedentemente da MRP, esso cerca un percorso mediante una tabella di ricerca (approccio proattivo) o di una scoperta di un percorso (approccio reattivo). Se viene trovato un percorso verso la destinazione che e' minore di d salti, il nodo consegna il messaggio tramite quel percorso. In caso contrario, esso tenta una trasmissione locale del messaggio ai suoi immediati vicini nella speranza che alcuni dei suoi vicini siano in grado di trovare la destinazione. Esso memorizza il messaggio localmente ed entra in uno cosiddetto *stato di trasmissione (relaying state)*; nello stato di trasmissione il nodo controlla periodicamente se il percorso esistente verso la destinazione sia minore di d salti. Se e' cosi', il messaggio e' consegnato direttamente. Quando un nodo riceve un messaggio da un altro nodo e questo messaggio e' stato trattato da MRP (es., il messaggio e' stato broadcastato una sola volta), esso cerca uno standard di percorso multi-hop connesso verso la destinazione e consegna il messaggio se il percorso viene trovato. In caso contrario, il nodo entra nello storing state e memorizza il messaggio; se il messaggio e' gia' presente nel buffer di nodo il nuovo messaggio viene eliminato, altrimenti se il buffer e' pieno il vecchio messaggio viene sostituito dal nuovo. Il messaggio che e' stato scartato viene inviato agli immediati vicini dopo aver decrementato il parametro h, solo nel caso in cui il risultato non e' 0. Se h e' uguale a 0 il messaggio viene scartato. L'immediato vicino per l'inoltro e' scelto a caso. Una volta memorizzato il messaggio, il nodo entra nello stato di trasmissione e periodicamente controlla la disponibilita' di un percorso verso la destinazione di tutti i messagi trasmessi. Questo protocollo trasmette sulla presunzione che, anche se un nodo non ha un percorso verso una particolare destinazione, e' probabile che uno dei suoi immediati vicini sia in grado di farlo. Limitando la diffusione del messaggio, il protocollo MRP limita l'utilizzo della larghezza di banda; inoltre, gestisce una limitata capacita' di memoria. L'efficacia del protocollo e' stata testata via ns-2 simultaneamente sotto una varieta' di modelli di mobilita' (giocatori di calcio, movimento dei piccioni). Il protocollo e' stato testato in combinazione col protocollo di routing DSDV.

3.3.7 Infrastructure-based routing

Nel protocollo basato su infrastrutture, la rete include alcune infrastrutture per realizzare la consegna dei messaggi. L'infrastruttura e' costituita da nodi fissi che sono

delle stazioni base distribuite nella rete e che fungono da raccoglitori di messeggi. Le stazioni base offrono alta capacita' e robustezza di scambio tra i nodi; inoltre hanno un'alta capacita' di memorizzazione di dati raccolti dai vari nodi. Un nodo che desidera spedire un messaggio, lo memorizza nella propria memoria, fino a quando non entra in contatto con una stazione base. La stazione base, conserva il messaggio fino a quando non entra in contatto con la destinazione. Esistono due variazioni di questo protocollo. Il primo lavora esattamente come descritto sopra. Solo le comunicazioni nodo-stazione sono permesse. Come risultato si ha che i messaggi subiscono alti ritardi. Tuttavia, questa soluzione porta ad una alta efficienza energetica in quanto i nodi sono esenti dal carico di lavoro per la spedizione del messaggio. La seconda versione permette comunicazioni nodo-stazione base e comunicazioni nodo-nodo. Un nodo inoltrera' il messaggio o direttamente alla stazione base, se si trova nel proprio range di trasmissione, oppure ad un altro che provvedera' ad inoltrarlo alla stazione base. Questo protocollo rispetto al primo ha una minore efficienza energetica, ma garantisce minori ritardi. Nonostante il risparmio energetico previsto da questo protocollo, risulta una soluzione altamente costosa a causa dei costi di infrastruttura.

Infostation [45] sono stazioni base che offrono una copertura wireless limitata, le infostation supportano connessioni wireless ad alto bit-rate per nodi mobili che si trovano dentro il proprio range di comunicazione. Secondo il paradigma di comunicazione, lo scambio dei dati puo' avvenire solo in prossimita' delle infostation. Servizi basati sul web possono essere accessibili solo in presenza di un'infostation: esempio, centri commerciali o lungo i marciapiedi, lungo le autostrade ecc. Considerando che l'obiettivo delle industrie cellulari e' la copertura in qualsiasi momento e in qualsiasi posto, le infostation offrono una sorta di modello che permette servizi locali ai nodi mobili. La soddisfazione dell'utente e' resa possibile dalla grande capacita' di comunicazione che le infostations possono sostenere e che rende possibili grandi quantitativi di scambio di dati in pochissimo tempo (corrispondente alla durata complessiva dell' utente mobile di trovarsi nel raggio di copertura della stessa infostation). Il problema principale con i servizi offerto dalle infostation e' l'intermittenza di connessioni che possono portare alla diminuzione della soddisfazione degli utenti. Cosi', infostations diversi possono organizzarsi in gruppi, che sono controllati da un controller. Ogni volta che e' in corso un download da parte di un utente mobile tramite una particolare infostation, a seconda della velocita' e direzione dell'utente

mobile, il responsabile del cluster puo' decidere di attivare l'inoltro dei dati da una infostation ad un altra, che molto probabilmente sara' la successiva infostation visitata dall'utente mobile. Questo puo' aiutare a garantire con una certa misura la continuita'.

3.3.8 Carrier-based routing

In questo protocollo, speciali nodi assumono il ruolo di portatori di messaggi. Essi si muovono lungo la rete seguendo un percorso predeterminato o arbitrario e raccolgono i messaggi dai nodi che essi incontrano. Questi nodi speciali possono essere chiamati *trasportatori, muli, inoltratori*: sono le sole entita' responsabili della consegna dei messaggi quando sono concesse solo comunicazioni nodo-trasportatore oppure possono semplicemente aiutare ad incrementare la connettivita' in una rete e garantire la connettivita' per nodi isolati. In questo caso, la consegna dei messaggi e' gestita sia dai nodi speciali e sia dai semplici nodi, in quanto sono cencesse comunicazioni nodo-inoltratore e nodo-nodo. Introdurre uno speciale nodo per la consegna dei messaggi risulta vantaggioso in termini di efficienza energetica. In caso di sole comunicazioni nodo-inoltratore, i nodi non prevedono carichi di lavoro per l'inoltro dei messaggi. Inoltre, le comunicazioni nodo-inoltratore sono generalmente comunicazioni a breve raggio, di conseguenza economiche. Tuttavia, questo sistema di comunicazione ha lo svantaggio di creare un alto ritardo di consegna dei messaggi. I sistemi che adottano i protocolli basati su inoltratori devono essere altamente tolleranti ai ritardi,si pensi ai sistemi di monitoraggio dalla fauna selvatica. Per ridurre i ritardi di consegna dei messaggi, occorre che anche le comunicazioni nodo-nodo sia concesse, ovviamente a discapito dell'efficienza energetica. I trasportatori mobili aggiungono scalabilita' alla rete in modo che il recapito dei messaggi viene concesso anche quando il numero totale dei nodi aumenta, e senza aumentare l'overhead di routing. Tuttavia, all'aumento dei nodi corrisponde un aumento dei ritardi di consegna. Per limitare i ritardi occorre aggiungere alla rete nuovi nodi inoltratori. L'uso di multipli trasportatori e' raccomandato per garantire robustezza nella consegna dei messaggi: un singolo nodo trasportatore sara' responsabile della consegna e necessariamente rappresentera' l' unico punto di guasto per la rete.

Capitolo 4

Prestazioni di strategie di routing opportunistici sotto modelli di mobilita' sociale

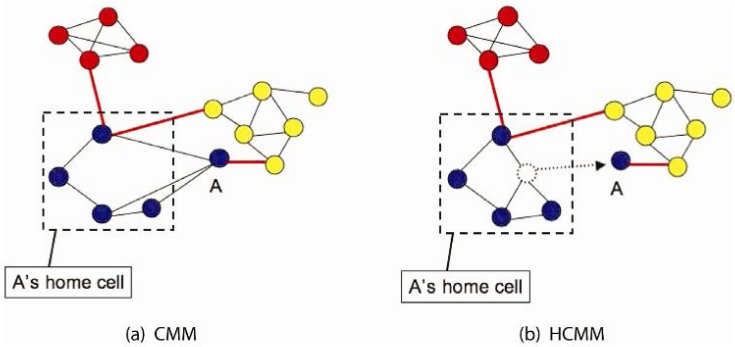
L'obiettivo di questo capitolo e' quello di confrontare i diversi approcci di routing opportunistici in realistici scenari della mobilita' umana. In particolare, si vedra' il comportamento dei protocolli per quanto riguarda un certo numero di parametri che descrivono schemi di movimento degli utenti. Si confronta un protocollo basato sulla dissusione (Epidemic Routing) con un protocollo a conoscenza di contesto (HiBop)

4.1 Mobilita' realistica: Home-cell Community-based Mobility

HCMM e' una evoluzione della *Community-based Mobility Model (CMM)*. I modelli di mobilita' del CMM sono interessanti per le ricerche nell'opportunistic network, poiche' sono adatti ai modelli realistici riguardanti le relazioni sociali tra le persone a le loro mobilita'. Come in CMM, in HCMM ogni nodo appartiene ad una comunita' sociale (social community); i nodi presenti nella stessa community sono chiamati *friends*, diversamente *non-firends*. Le relazioni tra i nodi sono modellate tramite social link (ogni social link ha un peso associato). All'inizio del sistema tutti i *friends* hanno un link verso ogni altro; anche due nodi, che non siano *friends*, possono avere un link secondo il parametro di *rewired probability* (p_r). I social link sono usati per guidare i movimenti dei nodi. I nodi si muovono in una griglia, e ogni community

inizialmente e' collocata in modo casuale in un quadrato della griglia, come si vede in 4.1.

Figura 4.1: Community-based Mobility Model vs. Home-cell Community-based Mobility Model [2]



Dopodicche' un nodo deve selezionare la cella verso la quale si dirige. I nodi selezionano la cella secondo le attrazioni sociali esercitate da ogni cella su un nodo. L'attrazione e' misurata come somma dei pesi dei link tra i nodi e dei nodi che attualmente si muovono nella o verso la cella. Infine, la cella obiettivo viene selezionata in base alla probabilita' definita dall'attrazione delle celle (per esempio se a_j e' l'attrazione della *j-esima* cella, la probabilita' di selezionare la cella e' data da $a_j / \sum_j a_j$). Dopo aver selezionato la cella di destinazione, il nodo seleziona l'obiettivo all'interno di una cella (il punto preciso verso cui il nodo si dirigera') in base ad una distribuzione uniforme. CCM (e HCMM) permette inoltre un movimento collettivo. Dopo ogni periodo di riconfigurazione i nodi di ogni gruppo selezionano una (differente) cella e si muovono verso di essa. Le riconfigurazioni sono sincrone tra i gruppi, vale a dire tutti i gruppi iniziano a muoversi nella nuova cella allo stesso tempo. Pertanto, nel corso delle riconfigurazioni i nodi appartenenti a diversi gruppi possono entrare in contatto. La differenza tra HCMM e CMM e' il modo di considerare le relazioni sociali con i nodi che sono fuori dalla loro cella iniziale (chiamata *home-cell* in HCMM). Come in 4.1, in CMM, quando un nodo A esce fuori dalla sua home-cell, porta con se' tutte le relazioni sociali, ad esempio i nodi che hanno una relazione sociale con A sono attratti verso una qualche cella dove A e' diretta. E' dimostrato che questo ha un effetto valanga in modo tale che tutti i nodi

nella home-cell di A seguono A. Questo comportamento non permette al CMM di rilevare i modelli di mobilita', poiche' i nodi non sono attratti dalle locazioni fisiche, ma solo dalle relazioni sociali dei nodi. In HCMM, quando A muove fuori dalla sua *home-cell*, non trasporta fuori i social link; i nodi che hanno una relazione sociale con A sono ancora attratti dalla *home-cell* di A. Per di piu', una volta che A e' fuori dalla sua *home-cell*, A seleziona l'obiettivo del prossimo movimento fuori dalla cella con una probabilita' p_e, e l' obiettivo di tornare a casa con una probabilita' $1-p_e$. La logica alla base di queste modifiche e' il fatto che ci sono diversi scenari in cui anche i luoghi fisici (oltre alle relazioni sociali) svolgono un ruolo nella determinazione dei movimenti degli utenti. In HCMM, le persone che desiderano incontrare A (vale a dire che c'e' attrazione sociale nei confronti di A) sono attratti verso la *home-cell* di A perche' e' il luogo fisico piu' probabile dove A puo' trovarsi o perche' la loro relazione sociale con A e' condizionata dal fatto che A e' nella sua *home-cell* (ad esempio, se qualcuno vuole incontrare un agente di assicurazione, andra' in ufficio piuttosto che nella sua abitazione).

4.2 Strategia di valutazione delle prestazioni

Nel seguito, si evidenzia come i diversi approcci di routing sono in grado automaticamente di reagire e adattarsi dinamicamente alle condizioni in evoluzione. A tal fine, si sfruttano le manopole di controllo fornite da HCMM per evidenziare le diverse proprieta' di Epidemic e HiBop. In particolare, si identificano tre casi di riferimenti principali per il nostro studio:

- Nel primo scenario, si analizzera' la reattivita' dei protocolli di routing per i contatti occasionali tra i gruppi. In particolare ci si concentrera' sui gruppi chiusi ($p_r = 0$), e poi i gruppi verranno forzati a muoversi collettivamente con diverse frequenze. I messaggi indirizzati ai nodi fuori dal gruppo possono essere consegnati solo tramite contatti tra i diversi membri del gruppo durante i movimenti. Quest'analisi ci permette di capire se i protocolli di routing sono in grado di sfruttare anche poche occasioni per trovare percorsi buoni;

- Nel secondo scenario, vogliamo capire come i protocolli di routing reagiscono a differenti livelli di socialita' degli utenti, misurata come la probabilita' degli utenti di avere rapporti al di fuori del loro gruppo di appartenenza. E' chiaro che per raggiungere questo occorre variare il parametro di p_r. Maggiore sara'

p_r, maggiore sara' la socialita' dei nodi; se minore sara' p_r, allora i gruppi saranno piu' chiusi;

- Nel terzo scenario, vedremo come lavorano i protocolli in gruppi completamente chiusi. In questo caso nessun ricablaggio e nessuna riconfigurazione sono consentiti, e sono posti differenti gruppi in ogni cella della griglia. Pertanto l'unica possibilita' di recapitare i messaggi tra diversi gruppi e' quello di sfruttare i contatti tra i nodi lungo i margini delle celle. Le performance dei protocolli vengono studiate in funzione dei range di trasmissione. Fondamentalmente, questo scenario ci permette di capire come i protocolli siano in grado di sfruttare i rapporti che non siano relativi ai rapporti sociali, ma solo ad incontri causali a causa della co-ubificazione fisica (ad esempio, i contatti tra persone che lavorano per diverse aziende nello stesso piano di un edificio).

Le performance dei routing vengono valutate in termini di *QoS*[1] *percepita dagli utenti*, e *consumo di risorse*. La *QoS percepita dagli utenti* e' valutata in termini di ritardo sulla consegna dei messaggi e in termini della loro perdita. I ritardi di consegna vengono stimati sulla base della replica del messaggio prima di raggiungere la destinazione; mentre la perdita dei messaggi e' valutata sulla base dell'eventuale perdita di tutte le repliche. Per evidenziare alcuni comportamenti specifici che differenziano *Epidemic* e *HiBop*, in alcuni casi, si prende in considerazione anche il numero di salti richiesti dai messaggi per raggiungere la destinazione, e si separano i ritardi dei messaggi indirizzati ai nodi *friends* e i ritardi dei messaggi mandati ai *non-friends*. Il *consumo di risorse* e' valutato in termini di buffer occupato e overhead di bandwidth (di banda). In particolare, l'overhead della banda e' calcolato come il rapporto tra il numero di byte generati in tutta la rete nel corso di una intera simulazione, e il numero di byte generati dal mittente. Sono da considerare, nel consume delle risorse, le spese relative al routing e alla trasmissione, come ad esempio gli scambi di IT, le richieste di probabilita', ecc.. Per evidenziare ulteriori differenze specifiche, tra i due protocolli in certi casi si mostra il numero di copie diffuse in rete, e separatamente si evidenzia l'overhead di bandwidth relativo ai messaggi data e ai messaggi non-data.
Per evidenziare solo l'effetto dei modelli di mobilita' umana, assumiamo:

- buffer infinito;

[1] QoS: Qualita' dei Servizi

- un livello MAC ideale che evita completamente la congestione della rete;
- un canale fisico ideale in cui i nodi presentano 0% pacchetti persi all'interno di un range di trasmissione, e un 100% al di fuori;
- bandwidth infinito (nel senso che i messaggi possono essere scambiati sempre quando i nodi entrano in contatto).

Come ampiamente discusso in Boldrini, Conti e Passarella(2007a), questa impostazione tende a favorire uno schema di diffusione come l'*Epidemic*. Piu' specificatamente, in questo tipo di configurazione, il miglior risultato per *HiBop* sarebbe quello di avere un ritardo ed una perdita di pacchetti realizzato da Epidemic, riducendo in modo significativo il consumo di risorse. Infine, lo scenario di simulazione, si compone di 30 nodi equamente suddivisi in tre gruppi, una superficie quadrata di dimensione $1.250mx1250m$ divisa in una griglia di 5x5. Il raggio di trasmissione di default e' di $125m$, se non diversamente indicato, ogni nodo genera messaggi, con un inter-tempo di generazione distribuita in modo esponenziale (con media di 300sec). Ogni messaggio e' rivolto ad un *friends* e ad un *non-friends* con il 50% di probabilita'. I messaggi scadono dopo 18.000 sec. Ogni simulazione dira 90.000 sec (tempo simulato). Per assicurarsi che i messaggi non ancora consegnati al termine di una corsa, non saranno mai consegnati (in modo da ottenere una misura corretta dell'indice di perdita di pacchetti), nel corso degli ultimi 18.000 sec, i mittenti non generano alcun nuovo messaggio.

4.3 Fase di configurazione: impatto dei movimenti collettivi dei gruppi

Vale la pena ricordare che in questo scenario la probabilita' di ricablaggio e' uguale a 0, e quindi, fatta eccezioni per riconfigurazioni, i nodi non hanno possibilita' di incontrarsi. L'intervallo di riconfigurazione varia tra i 2.250sec, 9000sec e 36.000sec. La 4.2 mostra le prestazioni QoS in funzione dell'intervallo di riconfigurazione. Come previsto, sia la perdita di pacchetti e sia i ritardi aumentano con questo parametro, perche' i messaggi indirizzati al di fuori del gruppo del mittente sono costretti ad aspettare una riconfigurazione. Le prestazioni in termini di ritardo possono essere meglio evidenziati concentrandosi sui ritardi nei confronti dei nodi friends, piuttosto che dei non-friends. In particolare le figure 4.3, 4.4 e 4.5 mostrano la distribuzione di

ritardo verso i nodi friends (valori a sx) e nodi non-friends (valori sulla dx) per i tre periodi di riconfigurazione. Prima di tutto, i ritardi verso i nodi friends in fondo non dipendono dall'intervallo di riconfigurazione, in quanto i nodi friends sono sempre co-localizzati nello stesso gruppo. Mentre solo una piccola quantita' di messaggi destinati ai nodi friends presenta un ritardo superiore ai 10sec. La maggior parte (tra i 60% e il 70% a seconda dell'intervallo di riconfigurazione) dei messaggi indirizzati ai nodi non-friends presenta un ritardo superiore ai 10^3 secondi. Inoltre, si noti che

Figura 4.2: User Quality of Service [2]

	Reconf (s)	*HiBOp*	*Epidemic*
P loss (%)	2,250	0 ± 0	0 ± 0
	9,000	8.16 ± 1.68	5.52 ± 1.46
	36,000	25.64 ± 1.30	24.12 ± 1.31
Delay (s)	2,250	1202.52 ± 91.09	907.10 ± 67.08
	9,000	3651.68 ± 295.05	3204.58 ± 278.70
	36,000	5615.43 ± 225.93	5445.11 ± 161.53

a seconda della frequenza delle riconfigurazioni, le code di distribuzioni sono piu' o meno *pesanti*. Il caso peggiore e' chiaramente per un intervallo di riconfigurazione pari a 36000 sec, dove circa il 50% dei messaggi destinati ai nodi friends non scade. Si noti inoltre che, anche se HiBop prevede la perdita di pacchetti e ritardi superiori, la differenza con Epidemic e' molto sottile. Si sottolinea anche che, dato che buffer e il bandwidth non sono limitati, Epidemic da' un limite superiore di riferimento in materia di rendimento ottenibile da qualsiasi protocollo di routing. Questi risultati mostrano chiaramente che HiBop e' in grado di identificare buoni inoltri anche con contatti sporadici durante la riconfigurazione tra i nodi appartenenti a gruppi diversi. Le buone prestazioni in termini di QoS dimostrate da HiBop coincidono con una drastica riduzione nell'uso delle risorse. La 4.6 mostra l'occupazione del buffer nel corso del tempo indicato come percentuale di durata di una intera simulazione (i punti sono i valori medi delle repliche). HiBop e' molto meno avido nel diffondere messaggi, e quindi l'occupazione del buffer e' drasticamente ridotta. Questa e' una differenza generale tra Epidemic e HiBop, confermato in tutti gli scenari che sono stati testati.

La 4.7 confronta Epidemic e HiBop per quanto riguarda il numero di copie generate (si ricordi che il numero dei nodi della rete e' di 30, quindi il numero mas-

Figura 4.3: Distribuzione dei ritardi con la configurazione a 2250sec. [2]

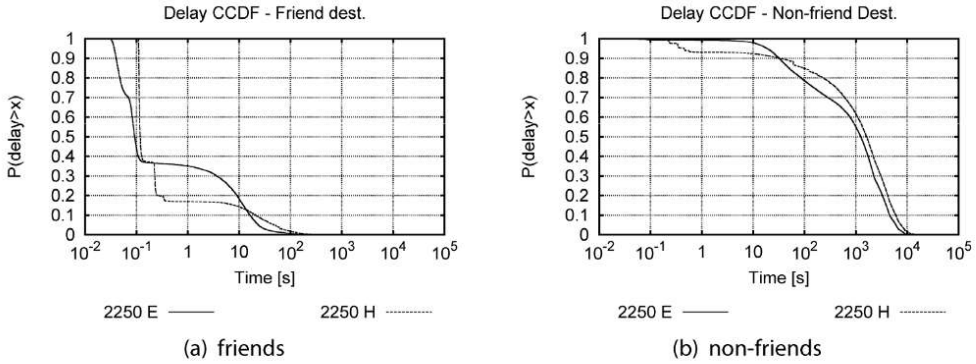
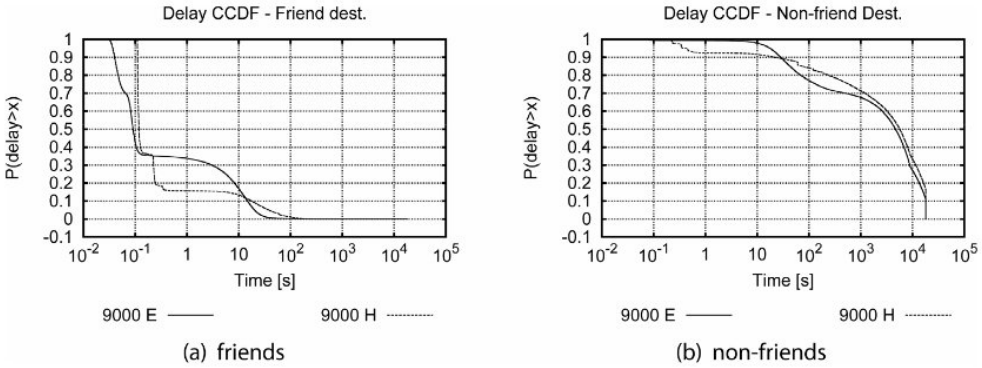
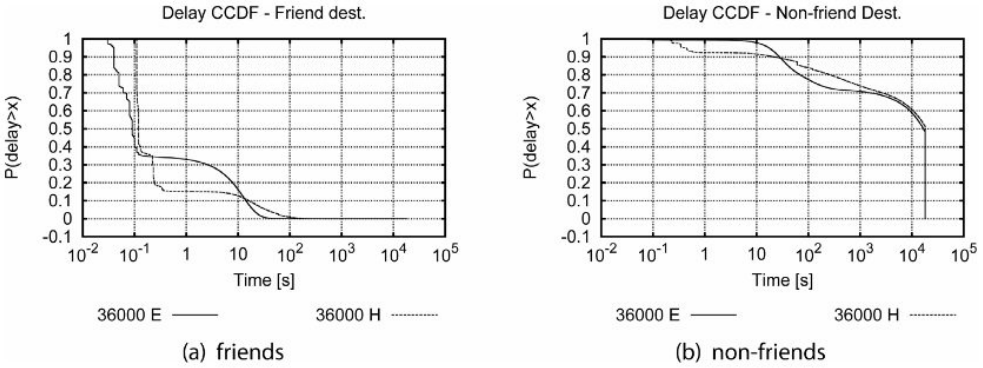


Figura 4.4: Distribuzione dei ritardi con la configurazione a 9000sec.[2]



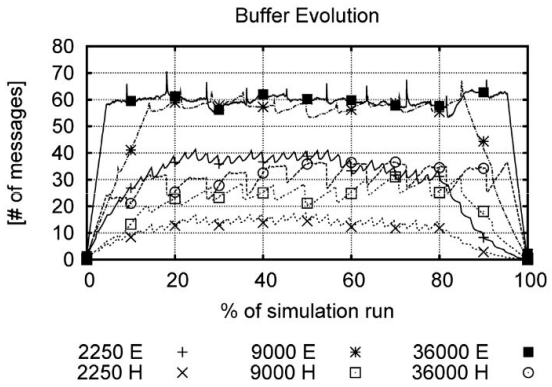
simo di copie e' 29). L' alto consumo di risorse per Epidemic e' dovuto al fatto che ogni nodo copia il proprio messaggio in tutti gli altri nodi che incontra; pertanto, piu' sono i contatti tra i nodi, piu' e' la diffusione di messaggi. La 4.7 mostra che circa il 50% dei messaggi (corrispondenti ai messaggi con una destinazione non-friends) e' diffuso in modo epidemico in tutta la rete, quando l'intervallo di riconfigurazione e' uguale a 2250sec e 9000sec. Le prestazioni in termini di ritardo e perdita di pacchetti, dimostrano che questo scenario di inondazione non produce significativi vantaggi. I contatti durante le riconfigurazioni coinvolgono interi gruppi. Una replica all'interno di ogni gruppo non e' piu' comoda del replicare il messaggio su un singolo nodo di ciascun gruppo. HiBop tende a replicare il messaggio all'interno del gruppo

Figura 4.5: Distribuzione dei ritardi con la configurazione a 36000sec.[2]



del mittente, ma non inonda gli altri gruppi sulle riconfigurazioni, con conseguente minor numero di copie. Infine, 4.8 mostra il sovraccarico di banda dei due protocolli. Esso ci permette di evidenziare una differenza principale tra HiBop ed Epidemic, relativa al modo in cui reagiscono ai schemi di movimento. Ridurre l'intervallo di riconfigurazione (da 36000sec fino a 2250sec) significa aumentare le possibilita' di trasmissione, perche' i nodi entrano in contatto con maggiore frequenza. Epidemic non utilizza questi contatti aggiuntivi in modo saggio, in quanto si basa sulle inondazioni, pertanto, il sovraccarico di banda aumenta. HiBop si comporta in modo differente: quando i gruppi non si mescolano (intervalli di riconfigurazioni pari a 36000sec), i percorsi per i messaggi da inoltrare al di fuori del gruppo sono raramente disponibili. HiBop realizza questo perche', essendo l'informazione di contesto sui nodi al di fuori del gruppo raramente disponibile, evita di consumare inutilmente risorse. Quando i vari nodi si mescolano sempre piu' (gli intervalli di riconfigurazione pari a 9000sec e 2250sec), anche HiBop (come Epidemic) genera piu' overhead, in quanto con maggiori contatti vi saranno piu' percorsi per una destinazione. Tuttavia, il tasso di incremento dell'overhead in HiBop e' significativamente inferiore a quello dell'Epidemic, cosi' da mostrare un uso piu' razionale delle risorse di rete disponibili. Questi risultati indicano che le informazioni sul contesto, sfruttando HiBop, risultano molto piu' efficienti di quelle basate su inondazioni, nonostante le risorse supplementari necessarie ai fini della gestione di contesto.

Figura 4.6: Occupazione Buffer.[2]

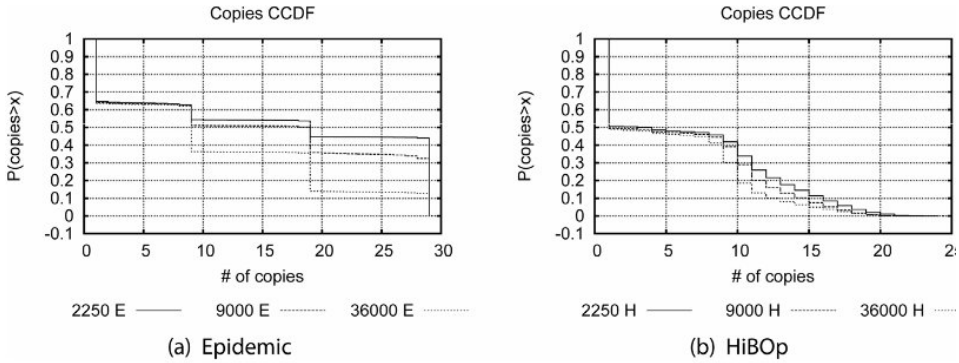


4.4 Impatto della socialita' degli utenti

Per capire l'impatto della socialita' degli utenti sulle prestazioni viene cambiato il parametro di ricablaggio (P_r). Quando un nodo va in una cella diversa dalla sua *home-cell*, mostra le sue informazioni di contesto legati alla propria *home-cell*, diventando cosi' un buon nodo per l'inoltro di messaggi destinati ai suoi nodi *friends*. D'altra parte, un nodo si muove per un certo numero di volte in ogni cella e colleziona informazioni sul contesto sui nodi incontrati. Quando il nodo rientra nella propria *home-cell*, le conoscenze raccolte possono essere efficacemente utilizzate per inoltrare messaggi verso nodi *non-firends*. Infatti, il nodo e' come se fosse tornato indietro per via dei suoi contatti esterni ancora attivi. Chiaramente, le prestazioni di routing sono sensibili alla socialita' degli utenti perche' le relazioni sociali degli utenti sono l'unico modo possibile per ottenere messaggi fuori dal gruppo originario. La 4.9 mostra l'utilizzo delle risorse di HiBop e di Epidemic.

Simili osservazioni verranno fatte per quanto riguarda gli intervalli di riconfigurazione. Maggiore e' la socialita' degli utenti (alto P_r), piu' elevato e' il movimento tra i nodi e le possibilita' di trasmissione. Mentre Epidemic utilizza tutte le risorse per la diffusione dei messaggi, HiBop sfrutta il movimento dei nodi (e la conseguente diffusione di informazioni di contesto) per individuare i migliori percorsi. La 4.10 mostra come il traffico di dati e non-dati contribuisce al sovraccarico della banda. Come gia' detto, Epidemic sfrutta tutte le possibilita' di raggiungere la destinazione copiando i messaggi sui nodi per quanto possibile. Cio' comporta un overhead elevato, che e' inutile, soprattutto per gli scenari altamente connessi dove ci sono molte

Figura 4.7: Distribuzione copie.[2]



opportunita' di inoltro. Si noti che l'overhead elevato in Epidemic e' essenzialmente costituito dalla replica aggressiva dei messaggi (cioe' a partire dai dati di traffico). Infatti, 4.10(b) mostra che il traffico relativo alla trasmissione (vale a dire il traffico per lo scambio dei vettori di sintesi), diminuisce quando le possibilita' di connettivita' sono disponibili. Per un maggiore ricablaggio, i buffer sotto Epidemic sono meno completi, in quanto i messaggi possono essere forniti piu' rapidamente alle destinazioni. Pertanto, la dimensione dei vettori di sintesi diminuisce, e questo spiega la tendenza della 4.10(b). Tuttavia, alla riduzione in termini di inoltro corrisponde un aumento del traffico, per la diffusione aggressiva del messaggio, che si traduce in un aumento delle spese generali relative al traffico dati (4.10(a)) e , infine, in un aumento dell'overhead globale 4.9. A differenza di Epidemic, HiBop impara il grado di connettivita' della rete e usa questa conoscenza per la regolazione del carico. Piu' specificatamente, HiBop impara lo stato attuale della rete attraverso lo scambio di messaggi di contesto. Quando le informazioni di contesto si sviluppano in maniera sempre piu' ampia (ricablaggio pari a 0.1 e 0.5) i percorsi diventano sempre piu' conosciuti, e HiBop produce gli scambi di dati e i messaggi non dati. Con Epidemic, vi e' un alto consumo di risorse, infatti, tra il 50% e il 70% dei messaggi sono diffusi in tutta la rete. Epidemic tende a sfruttare tutte le opportunita', a prescindere dalla socialita' degli utenti. Pertanto, quando i nodi sono eterogenei (ricablaggio superiore), Epidemic inonda la rete in modo piu' aggressivo. Come abbiamo mostrato al momento di presentare i dati di performance QoS, questo e' praticamente inutile, e

Figura 4.8: Bandwidth overhead [2]

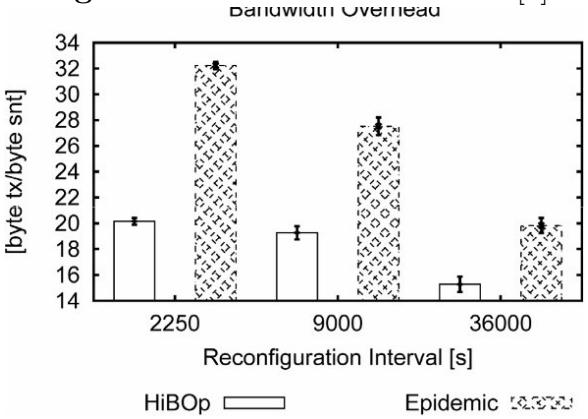
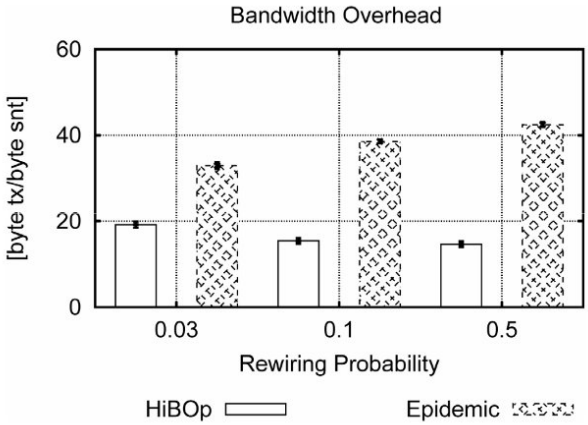


Figura 4.9: Bandwidth overhead - parametro di ricablaggio [2]



quindi ne risulta uno spreco di memoria e di larghezza di banda. HiBop, invece, e' consapevole dello stato attuale della rete e regola il numero di repliche di ciascun pacchetto basato sulla socialita' della rete. Si noti che, anche con la socialita' piu' bassa (ricablaggio = 0.03), solo il 30% dei messaggi viene copiato al piu' su 10 nodi. Si noti inoltre che, a differenza di Epidemic, questa percentuale si riduce a zero, con livelli di socialita' piu' elevati. Per quanto riguarda i dati delle prestazioni QoS, vedi 4.11, ancora una volta la perdita di pacchetti e' trascurabile, mentre - come previsto - la diminuzione media dei ritardi diminuisce con l'aumentare delle socialita' degli utenti.

Le prestazioni di HiBop non sono molto lontani da quelli di Epidemic. E' anche interessante notare che il ritardo dei messaggi verso i nodi friends tende ad aumentare leggermente quando gli utenti diventano piu' sociali, perche' spendono (in media)

Figura 4.10: Bandwidth overhead - parametro di ricablaggio [2]

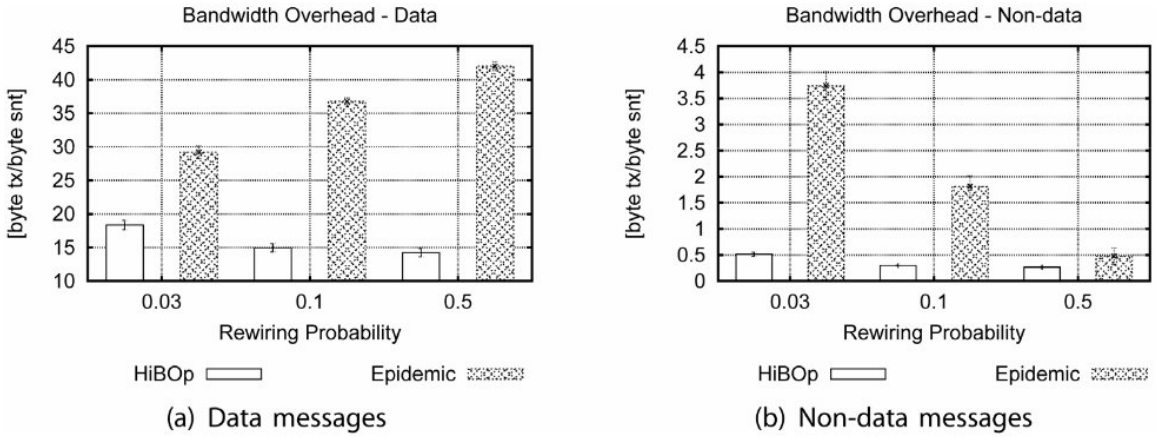


Figura 4.11: Media dei ritardi [2]

	p_r	HiBOp	Epidemic
delay (s)	0.03	170.86 ± 25.86	130.28 ± 20.59
	0.1	129.42 ± 12.51	83.20 ± 8.57
	0.5	104.91 ± 8.87	73.69 ± 7.16

piu' tempo al di fuori del loro gruppo di casa. Tuttavia, il vantaggio di collegare in modo piu' efficente gli utenti e l'aumentare della socialita' comporta una riduzione delle prestazioni con l'esperienza dei nodi fiends. La mobilita' influisce sul numero dei salti che un messaggio deve effettuare prima di raggiungere la destinazione. Data una rete sociale simulata, ci si aspetta che i nodi appartenenti ad una stessa comunita' si incontrino piu' spesso e piu' a lungo. Questo si traduce in migliori prestazioni QoS per i messaggi destinati agli amici. Quando la rete diventa piu' mista, i nodi tendono a passare piu' tempo fuori dalla loro comunita', diventando cosi' un buon nodo di inoltro per i messaggi destinati al di fuori. La vicinanza tra i nodi friends si riduce con l'aumento del ricablaggio e aumentano i salti necessari per raggiungere la destinazione, 4.12. D'altra parte, la vicinanza tra i nodi non-friends aumenta e di conseguenza il numero di salti diminuisce, 4.13.

Figura 4.12: Average delay - Friend Dest. [2]

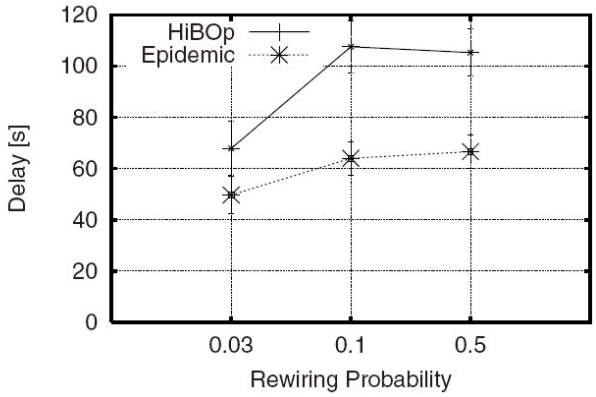
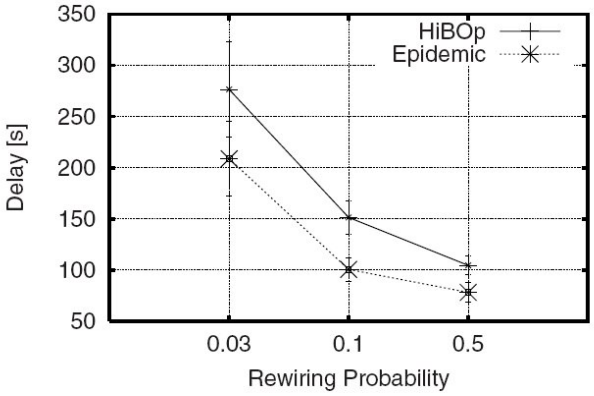


Figura 4.13: Average delay - Non-Friend Dest. [2]



4.5 Rotture dei gruppi chiusi

Nelle simulazioni descritte di seguito, si usa una griglia 3 x 3 con nove gruppi di cinque nodi ciascuna. Solo un nodo, che si trova nella cella in alto a sinistra manda i messaggi ad un nodo posizionato in basso a destra. Ricordiamo che l'unico modo per un messaggio per raggiungere la sua destinazione finale e' attraverso i contatti nei bordi con nodi tra i quali non esiste una relazione sociale. Dati i diversi range di trasmissione dei nodi possiamo analizzare come i contatti sui bordi influenzeranno gli inoltri. Si usano tre valori per i range di trasmissione, vale a dire 62,5 125 e 250m. Pertanto, la copertura dei nodi - in media - e' rispettivamente meno della meta' della cella, un po' meno della cella, e una cella e mezza. La linea di fondo dei risultati e' che HiBop non e' adatto per le reti senza socialita', a distanze di trasmissione molto piccole (62.5m), HiBop non e' in grado di fornire accettabili QoS, 4.14.

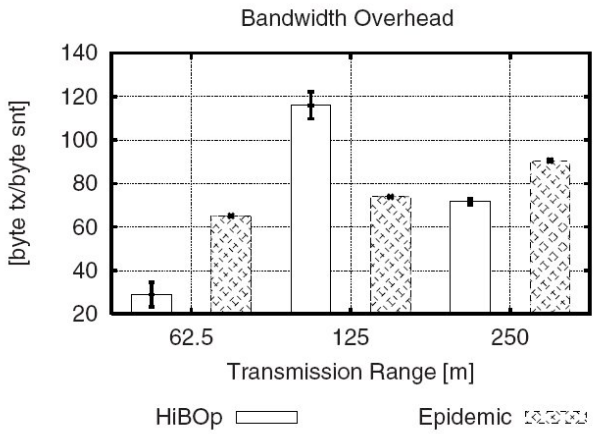
Figura 4.14: User Qos (closed groups) [2]

	range (m)	HiBOp	Epidemic
ploss (%)	62.5	61.41 ± 10.16	0 ± 0
	125	0 ± 0	0 ± 0
	250	0 ± 0	0 ± 0
delay (s)	62.5	14732.57 ± 1242.74	535.50 ± 14.05
	125	576.40 ± 177.56	102.83 ± 1.82
	250	1.77 ± 0.55	23.58 ± 0.80

HiBop ha bisogno di un numero minimo di contatti tra gli utenti per raccogliere informazioni sul contesto. Infatti, a 125m HiBop fornisce dei valori di QoS accettabili in termini di perdita di pacchetti, ed e' pienamente efficace a 250m. Anche in questo caso, Epidemic e HiBop si comportano in modo diverso in termini di overhead di banda, 4.15.

A 62.5m, HiBop raramente inoltra i messaggi. Poiche' i dati di contesto non sono in circolazione (non sono disponibili informazioni di contesto), i nodi del gruppo del mittente sono quasi tutti ugualmente idonei a trasportare i messaggi il piu' vicino possibile alla destinazione. Ad un alto range di trasmissione i dati di contesto circolano in modo efficace, e quindi si possono individuare in breve tempo ottimi percorsi. Nei casi intermedi (ad esempio con range di trasmissione pari a 125m), HiBop non e' (ancora) in grado di apprendere correttamente lo stato della rete, e questo si traduce in un overhead piu' elevato rispetto a Epidemic. Tuttavia, si nota

Figura 4.15: Bandwidth Overhead [2]



che questi risultati confermano che Epidemic non e' in grado di sfruttare scenari ricchi di connettivita' senza inondare la rete, in quanto aumenta l'overhead con l'aumentare del range di trasmissione. Fig 4.16 mostra il numero medio di salti.

Possiamo vedere che Epidemic genera 44 copie di ogni messaggio,4.17, cioe' replica messaggi su tutti i nodi, in quanto non e' a conoscenza dell'attuale stato della rete. In HiBop, il numero di copie aumenta in quanto le informazioni di contesto si diffondono, vale a dire per gli intervalli di trasmissioni in aumento.

Quando il range di trasmissione e' basso non vi e' alcun motivo di replicare i messaggi dal momento che non sono presenti informazioni di contesto per individuare buoni percorsi di inoltro, perche' le informazioni di contesto non si possono diffondere. Appena le informazioni di contesto possono essere diffuse, i percorsi possono essere trovati e HiBop inizia a replicare i messaggi. Infine, la 4.18 mostra il numero medio di salti. In entrambi i casi, i valori diminuiscono con l'aumentare del range di trasmissione, le possibilita' di contatto sono disponibili e un salto unico e' in grado di portare i messaggi piu' vicini alla destinazione.

Figura 4.16: Average number of copies (closed groups) [2]

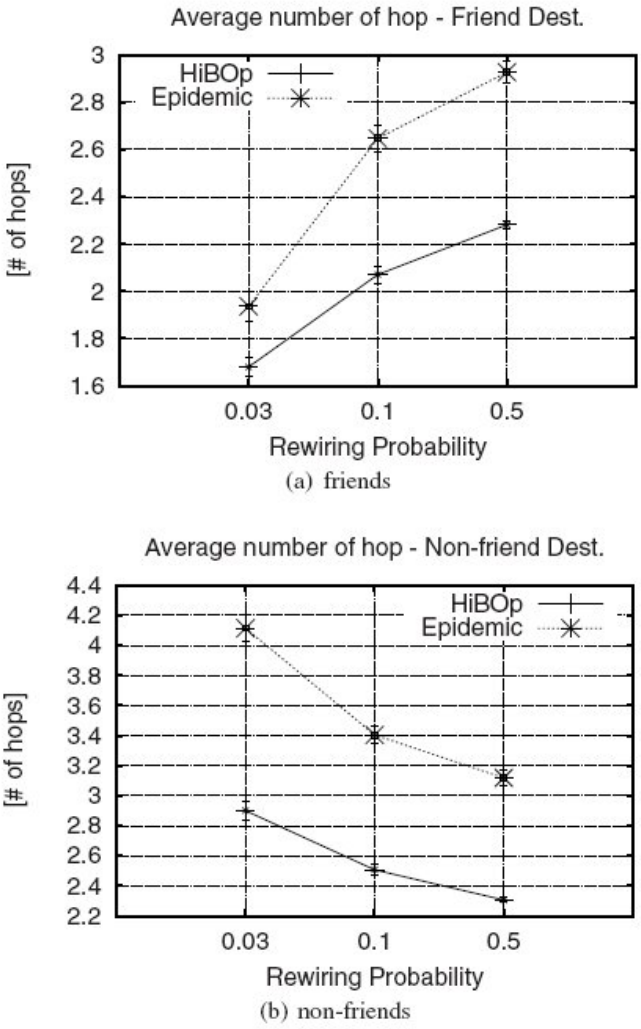


Figura 4.17: Average number of copies (closed groups) [2]

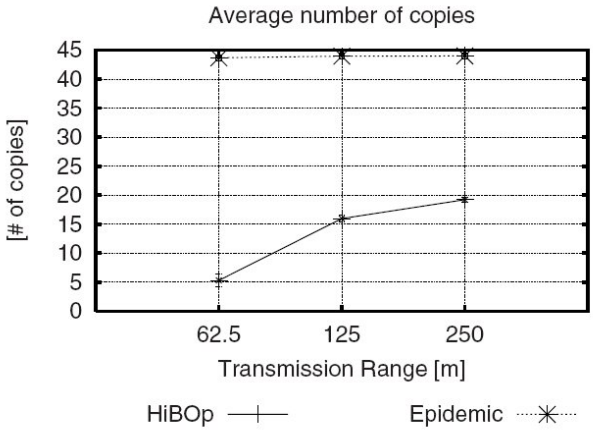
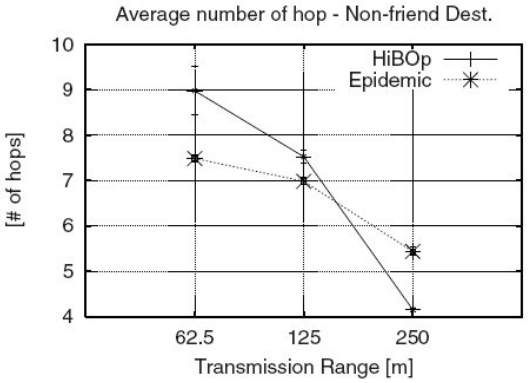


Figura 4.18: Average number of hop [2]



Capitolo 5

Conclusioni

Dal passaggio da uno scenario basato su infrastruttura ad una senza, e in particolare alle *Multi-hop Ad hoc NETwork*, uno dei principali problemi da affrontare ha riguardato l'assenza di un distrubuzione reale. Anche se una grande quantita' di lavoro e' stata condotta sulle MANET per mezzo di studi analitici e di simulazione, molto lavoro rimane ancora da fare su banchi di prova reale. Risultati di prove reali su piccole MANET, composte da 8 a 12 nodi, evidenziano la necessita' di migliorare i servizi utenti nelle MANET. Infatti quando, portate le principali applicazioni su internet, es.,applicazioni p2p in ambienti MANET, sorgono le inefficienze, non solo la qualita' dei servizi percepita risulta essere nettamente inferiore da quella percepita nell'utilizzo di applicazioni basate su internet cablata o wireless, ma il sistema a volte non risulta essere capace di fornire quei servizi. Proseguendo, le *reti opportunistiche* offrono un concetto completamente nuovo riguardo le reti wireless. Essi non si basano su qualsiasi infrastruttura fissa, ne' tentano di auto-configurare una infrastruttura temporanea. Le reti opportunistiche, invece, fanno affidamento sui contatti occasionali che possono avvenire tra i nodi coinvolti nelle loro attivita' quotidiane (es., lavoro, scuola, universita', ecc.). I messaggi vengono scambiati quando e dove possibile e il successo della consegna risulta profondamente legato alle dinamiche sociali e alla storia degli incontri delle persone. Considerata l'elevata mobilita' che caretterizza simili scenari sono nate nuove esigenze, per esempio far fronte all'assenza di contatti. Infatti, le comunicazioni possono avvenire solo nei periodi di contatto e devono essere estremamente veloci ed efficaci. Una strategia utile al fine di affrontare le problematiche delle trasmissioni in questi ambienti estremi, e' combinare le azioni delle tecniche di codica e di disseminazione per l'inoltro dei messaggi. Queste tecniche si affidano alla ridondanza dei dati e dei percorsi.

La ridondanza dei dati fornisce robustezza contro la perdita dei dati. Cosi' e' richiesto che solo un sottoinsieme dei dati generati arrivi alla destinazione per consentire la corretta ricostruzione dell'informazione originale. La ridondanza dei percorsi invece, e' necessaria poiche'non e' possibile predire la sequenza dei contatti che possano portate i dati alla destinazione, e quindi, basarsi su un unico percorso risulterebbe pericoloso. Le reti opportunistiche sono caratterizzate da dispositivi a bassa potenza e aventi risorse limitate e offrono attualmente il contesto che meglio si adatta al concetto di sistemi pervasivi. In questa tesi, sono stati evidenziati alcune applicazioni concrete sulle reti opportunistiche ed un insieme di tecniche di routing. Successivamente sono stati evidenziati come i diversi approcci al routing in rete sono in grado automaticamente di adattarsi agli scenari dinamici derivanti da modelli di mobilita degli esseri umani. Si sono confrontati i dati sulle prestazioni di due protocolli agli estremi opposti dello spettro per quanto riguarda l'uso delle informazioni di contesto, vale a dire Epidemic e HiBOp. Context-based routing in realta' fornisce un efficace meccanismo di controllo della congestione, e, per quanto riguarda la diffusione, fornisce QoS accettabile con overhead ridotto, drasticamente, se non in grandi scenari negativi. Infatti, HiBOp e' in grado di apprendere automaticamente le possibilita' di connettivita' determinate dagli schemi di movimento degli utenti, e di sfruttarle in modo efficiente. Quando i gruppi sono molto isolati, le informazioni di contesto, non possono circolare, e non possono essere utilizzate per prendere decisioni efficaci per gli inoltri. In tali casi, lo schema basato sulla diffusione sembra l'unico modo per consentire la comunicazione tra i gruppi. Non appena gli utenti diventano piu' sociali, le informazioni di contesto si diffondono nella rete, e il routing basato sulle informazioni di contesto diventa una soluzione preferibile. Un interessante seguito di questo lavoro riguarda come sfruttare le informazioni di contesto per distinguere questi diversi scenari e selezionare lo schema di routing del caso. Da un punto di vista complementare, i risultati mostrano che nelle reti opportunistiche, la socialita' degli utenti aiuta il routing: i contatti tra nodi appartenenti a diversi gruppi consentono la diffusione nella rete delle informazioni di contesto, rendendo l'inoltro sempre piu' efficente. Questi risultati aprono nuove direzioni di ricerca interessanti, la fornitura di privacy e sicurezza. Inoltre, un'altra direzione di ricerca impegnativa e' come interagire con reti meno opportunistiche, con access point per le infrastrutture internet. Infine la progettazione di sistemi di elaborazione dati (costruiti sulla sommita' dei sistemi di routing opportunistiche) per migliorare la disponibilita' dei dati in reti opportunistiche e' un'altra direzione

di ricerca trovata estremamente importante.

Appendice A

La sfida della Privacy nelle OppNets

La tecnologia proposta, Reti Opportunistiche, e' uno dei possibili approcci per proseguire verso i sistemi pervasivi, ai quali sono associati enormi rischi. Tra questi merita un approfondimento quella sulla privacy[3]. In una soluzione semplice, un dispositivo potra' conservare i propri dati privati in modo sicuro (ad esempio, cifrati nella propria memoria) prima di far parte di una oppnets. In caso di involontaria partecipazione (casi di emergenza) , le oppnet comunque permettono al dispositivo di salvare prima i propri dati e successivamente partecipare alla oppnets. Un'altra possibile soluzione si potra' basare su una rigorosa separazione tra aree pubbliche e private all'interno del dispositivo stesso o della rete. Questa metodologia garentira' che una oppnets, (anche in caso di malfunzionamenti) possa acquisire dati sensibili. Essa fornira' anche protezione contro oppnets maligne che potrebbero attaccare la privacy di altri dispositivi o di altre reti, fingendone di averne bisogno.
Altre possibili tecniche includono:

- Protezione della privacy dei soggetti garantendo l'anonimato o tramite l'utilizzo di pseudonimi;

- Fornire algoritmi per la rilevazione di oppnets maligne al fine di evitare attacchi futuri;

- Sviluppo di metodi per proteggere oppnets contro tutti i tipi di attacchi alla propria privacy.

A.1 Sicurezza e Privacy

Una fonte di minaccia per la privacy e per la sicurezza e' la mancanza di autenticazione dei dispositivi presenti nella rete. Non e' possibile garantire che i dispositivi maligni non vi partecipino. Inoltre non e' possibile classificare un dispositivo come pericoloso, fino a quando il suo comportamento non diviene noto. Avere in modo sicuro la chiave segreta per tutti i dispositivi, e' veramente difficile in un simile ambiente. Anche solo basarsi su meccanismi di autenticazione cifrati non aiuta in tutte le situazioni. Infatti minacce come MITM, ID Spoofing, DoS e altri attacchi risultano ancora piu' minacciose nelle oppnets. In A.1 viene mostrato uno schema generale di sicurezza per le oppnets. Data l'assenza di autenticazione, le frecce uscite dal sommatore sono da ritenere passi obbligatori. Le sfide riguardo la sicurezza e privacy possono essere elencate nel seguente ordine:

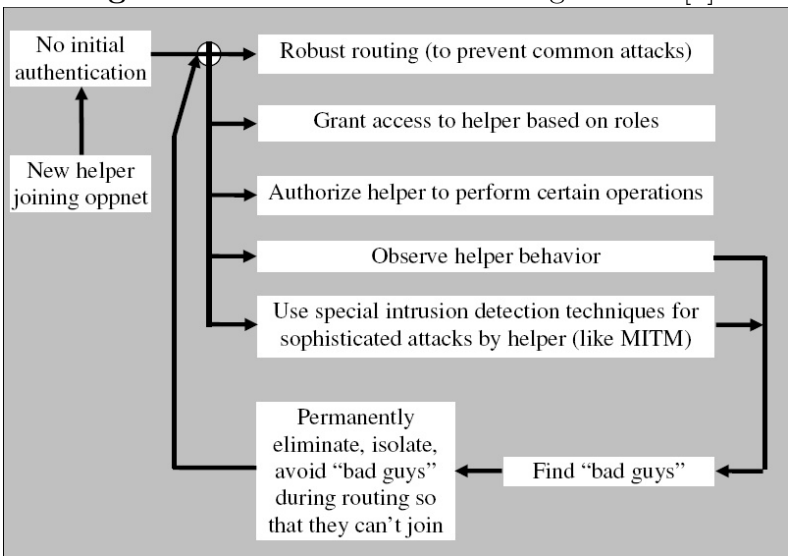
1. Aumento della sicurezza nel routing;
2. Privacy dei dispositivi e delle oppnets;
3. Protezione dei dati privati;
4. Garanzia dell'integrita' dei dati;
5. Individuazione degli attacchi e individuazione delle possibili contromisure;
6. Individuazione delle intrusioni.

E' possibile mantenere una lista di dispositivi sicuri, di proprieta' di alcune istituzioni: stazione di polizia, uffici governativi, ospedali, biblioteche, universita' o societa' di buona reputazione.

1. Incremento della sicurezza nel routing

Una volta realizzata la lista dei dispositivi "sicuri" (che e' gia' una sfida); questi verranno utilizzati per le attivita' piu' critiche, preferendoli a dispositivi sconosciuti o diffidati (a riguardo potrebbe essere mantenuta una lista nera). Per un routing sicuro potrebbero ad esempio essere utilizzate entrambe le liste. Un protocollo sicuro per le oppnets e' Ariadne. Si tratta di un protocollo on-demand che funziona in presenza di nodi compromessi. Ariadne [8] usa una crittografia simmetrica, autentica messaggi utilizzando uno dei tre sistemi:

Figura A.1: Schema di sicurezza generale. [3]



- Condivisione del segreto tra ogni coppia di nodi;
- Combinazione della condivisione del segreto con l'autenticazione broadcast;
- Firma digitale.

Le soluzioni proposte per i protocolli di routing sicuri per le reti wireless, reti ad hoc o per internet, non possono essere usati direttamente per le oppnets, in quanto le oppnets sono tipologie di reti altamente eterogenee. I nodi delle oppnets, presentano differenti processi, differenti fonti di alimentazione, differenti modalita' di trasmissione (wired o wireless), ecc... Gli approcci proposti, ad esempio IPSec, WEP e SSH, utilizzano soluzioni crittografiche per la riduzione delle probabilita' e degli effetti di possibili attacchi.

2. Privacy dei dispositivi e delle oppnets

In questa sezione per "tutela della privacy del sistema" si vuole intendere nessuna intrusione nel sistema, nessun accesso non autorizzato ai dati, alle risorse e ai software di sistemi. Le oppnets sono realizzabili solo se la privacy e' garantita. La privacy e' garantita dal controllo sugli accessi (autenticazione e autorizzazzione) e dalla prevenzione dalle intrusioni (utilizzando la protezioni primitive, basandosi sulla fiducia, sulla sicurezza del routing, ecc..). Le rilevazioni delle intrusioni dovrebbero essere usate come seconde linee di difesa della privacy. L'eliminazione o l'isolamento dei

soggetti, considerati pericolosi per le oppnets, tramite la rilevazione delle intrusioni, e' importante per la preservazione dei nodi.
Il problema di garantire il controllo degli accessi e il rilevamento delle intrusioni in tempo reale per le oppnets e' piu' difficile da realizzare rispetto che per Internet, wireless e reti ad hoc a causa della natura eterogenea dei dispositivi partecipanti e della spontaneita' della formazione delle oppnets. Tuttavia la privacy delle oppnets e' importante, dato che dispositivi "maligni" possono partecipare alle oppnets con il solo scopo di violare la privacy dei membri appartenenti alle oppnets. La paura della violazione della propria privacy puo' portare al rifiuto a partecipare ad una oppnets.

3. Protezione dei dati privati

Nella sotto categoria delle oppnets che dispongono di un controller centrale, i seguenti tipi di messaggi sono piu' importanti.
A) Messaggi broadcast dal controller: La maggior parte degli annunci puo' essere effettuata dal controller (per esempio messaggi di emergenza da inviare a tutti i dispositivi della rete) per cui la privacy non puo' essere auspicata. Ma ci sono messaggi provenienti dal controller che possono richiedere la privacy in quanto destinati a pochi nodi. La mancanza di un segreto o una chiave condivisa tra il controller e i destinatari rendono difficile il problema di fornire dati privati in modo sicuro.

B) Messaggi dai nodi al controller: Quando dispositivo invia messaggi al controller. E' possibile che si desideri inviare i propri dati in modo sicuro. La cifratura e' un modo per dare riservatezza ai propri dati. La crittografia a chiave pubblica puo' essere usata per garantire la trasmissione dei propri dati in modo sicuro verso il controller. Il controller puo' trasmettere in modo broadcast la propria chiave pubblica a tutti i dispositivi della oppnets. I dispositivi possono cifrare i propri messaggi tramite la chiave pubblica, e il controller sara' in grado di decifrarli tramite la propria chiave privata (posseduta da lui soltanto). In questo modo i messaggi viaggeranno in modo cifrato e non piu' in chiaro. Comunque occorre un meccanismo sicuro per la trasmissione della chiave pubblica del controller, per evitare che dispositivi maligni si spaccino per controller e immettano nella rete la propria chiave pubblica.

4. Garanzia dell'integrita' dei dati

L'integrita' dei dati e' parte della sicurezza dei dati che li riguarda nel caso comunicazione sicura. Un modo per garantire l'integrita' dei dati puo' essere la firma digitale. Ma risulta essere molto costoso per i dispositivi che hanno (come cellulari, PDA, ecc..) una limitata capacita' di batteria. Quindi le alternative devono essere concepite per garantire l'integrita' dei pacchetti dati. Inoltre la dimensione dei dati puo' variare quando si viaggia attraverso una oppnets. Supponiamo che un pacchetto venga inviato da un cellulare tramite una stazione base ad un pc collegato ad internet. In questo caso, la dimensione del pacchetto, quando viaggera' dal cellulare al pc avra' una diversa dimensione del pacchetto che viaggera' dal pc alla stazione base. Se la frammentazione e l'aggregazione dei pacchetti non puo' essere eseguita in modo sicuro, il meccanismo end-to-end potrebbe fallire.

5. Individuazione degli attacchi e individuazione delle possibili contromisure

Di seguito verranno presentati alcuni dettagli riguardo i principali attacchi alla privacy, i loro effetti e le soluzioni per evitarli:

- MITM: l'attacco dell'uomo in mezzo, meglio conosciuto come man in the middle attack, MITM o MIM e' un attacco nel quale l'attaccante e' in grado di leggere, inserire o modificare a piacere messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento sia stato compromesso. L'attaccante deve essere in grado di osservare e intercettare il transito dei messaggi tra le due vittime.
  soluzioni: Nel caso in cui un dispositivo debba inviare un messaggio al controller, una possibile soluzione sarebbe quella di inviargli un messaggio ridondante, sfruttando piu' possibili dispositivi vicini (in pratica inviare il messaggio su vari percorsi). Questo aumentera' la possibilita' che almeno uno dei messaggi inviati raggiunga la destinazione. Cosi', la ridondanza dei percorsi puo' essere sfruttata per evitare gli attacchi.

- Packet Dropping: Tale attacco consiste, nel fatto che l'attaccante, elimina alcuni o tutti i messaggi, oppure li sotituisce con altri.
  soluzioni: Anche in questo caso, una possibile soluzione potrebbe essere quella di sfruttare la ridondanza dei percorsi.

- DoS attack (denial of service, letteralmente negazione del servizio): In questo tipo di attacco si cerca di portare il funzionamento di un sistema al limite

delle prestazioni. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, saturando le risorse del sistema e tanto da renderlo - instabile.
soluzioni: Possibile soluzione sarebbe quella di ridurre il limite dei pacchetti al numero di richieste di un qualsiasi dispositivo, in modo tale da limitare possibili attacchi, ed infine di accettare la richiesta solo dopo aver ricevuto una conferma di essa stessa.

- DoS attack on weak link: Questi attacchi hanno come obiettivo dispositivi "deboli", come cellulari, che sono fondamentali per le oppnets (ad esempio, potrebbero essere gli unici dispositivi che permettono di collegare due parti di una citta'). Altri obiettivi sono le batterie dei cellulari, che devono essere usate con parsimonia fino al ritrovamento di un collegamento alternativo.
soluzioni: Una possibile soluzione potrebbe essere rappresentata dalla individuazione dei dispositivi deboli, dal loro rafforzamento (per esempio fornendoli di un backups), o dalla minimizzazione del carico di lavoro, compito importante per mantenere la connettivita' in una oppnets.

6. Individuazione delle intrusioni

Infine possibili attaccanti potrebbero essere in grado di far parte di una oppnets per la mancanza di un primo meccanismo di autenticazione. Pertanto e' necessario individuare e allontanare. A riguardo occorre dire pero' che e' gia' una sfida trovare informazioni sui possibili attaccanti, ma e' altrettanto difficile diffondere tale informazioni in modo sicuro a tutti i partecipanti di una oppnets perche' possano proteggersi. Occorre molto ricordare, che la natura altamente eterogenea delle oppnets rende particolarmente difficoltoso il rilevamento delle intrusioni in tempo reale. Ad oggi dunque l'approccio di rilevamento delle intrusioni piu' rilevante utilizzato nelle oppnets deriva dal progetto AAFID[1], (un sistema distribuito di rilevazione di intrusione, ids). In questa architettura, i nodi del ids sono disposti in una struttura gerarchica ad albero dove agenti autonomi eseguono il rilevamento delle intrusioni mediante sensori incorporati. Un sensore incorporato e' un sensore con l'aggiunta di una logica per rilevare le condizioni che indicano un tipo specifico di attacco o intrusione. Tali rilevatori sono piu' resistenti alle manomissioni o alla disabilitazione, essendo parte del programma di monitorizzazzione e non essendo continuamente in esecuzione, impongono un carico di CPU molto basso.

[1] AAFID (Autonomous Agent for Intrusion Detection)

Bibliografia

[1] J. Widmer and J. Y. Le Boudec, "*The Not So Short Introduction to LaTeX 2ε*", Version 3.15 (2000), http://www.ctan.org/tex-archive/info/lshort/english/lshort.pdf

[2] Chiara Boldrini, Marco Conti and Andrea Passarella "*Autonomic behaviour of opportunistic network routing Int. J. Autonomous and Adaptive Communications Systems, Vol. 1, No. 1, 2008, pp. 130-144*

[3] Lesezek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta "*Opportunistic Networks: the concept and research challenges in privacy and security*

[4] Sanjit Biswas and Robert Morris "*ExOR: Opportunistic Multi-Hop Routing for Wireless Networks*

[5] Peter P. Pham and Sylvie Perreau "*Performance Analysis of Reactive Shortest Path and Multi-path Routing Mechanism With Load Balance*

[6] C. Shen, G. Borkar, S. Rajagopalan, and C. Jaikaeo. "*Interrogation Based Relay routing for Ad hoc Satellite networks. In Proceedings of IEEE Globecom 02, Taipei, Taiwan, November 2002. 125*

[7] J. Su, A. Chin, A. Popivanova, A. Goel, and E. de Lara. "*User Mobility for Opportunistic Ad-Hoc Networking. In Proceedings of the 6th IEEE Workshop on Mobile Computing System and Applications (WMCSA), UK, December 2004. 84*

[8] Y.-C.Hu, A.Perrig,and D.B.Johnson, "*Ariadne: A source On-Demand Routing Protocol for Ad Hoc Network, Proc.8th Ann.Int' Conf.Mobile Computing and Networking (MobiCom 2002, Atlanta,Georgia,September 2002,pp. 12-23*

[9] Tobias Oetiker, Hubert Partl, Irene Hyna and Elisabeth Schlegl, "*In Proceedings of the ACM SIGCOMM 2005 Workshop on delay tolerant networks*

[10] J. Leguay, T. Friedman, and V. Conan, "*Evaluating Mobility Pattern Space Routing for DTNs, Proceedings of the IEEE Infocom 2006, Barcelona, Spain, April 2006*

[11] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. "*Pocket Switched Networks: Real-world mobility and its conse- quences for opportunistic forwarding. Technical Report UCAM-CL- TR-617, Computer Laboratory, University of Cambridge, February 2005. 85, 109, 204*

[12] M. McNett and G. M. Voelker. Access and mobility of wireless PDA users. "*Technical report, Computer Science and Engineering, UC San Diego, 2004. 85*

[13] T. Henderson, D. Kotz, and I. Abyzov. The changing usage of a mature campus-wide wireless network. "*In Proceedings of ACM Mobicom,2004. 85, 125*

[14] The ns-2 network simulator. http://www.isi.edu/nsnam/ns/. 87

[15] L. E. Owen, Y. Zhang, L. Rao, and G. McHale. "*Traffic Flow Simulation Using CORSIM. In Proceedings of the 2000 Winter Simulation Conference, 2000. 87*

[16] J. Blum, A. Eskandarian, and L. J. Hoffman. "*Performance Characteristics of Inter-Vehicle Ad Hoc Networks. In Proceedings of the 6th IEEE International Conference on Intelligent Transportation Systems, Shanghay, China, 2003. 87*

[17] Z. D. Chen, HT Kung, and D. Vlah. "*Ad hoc Relay Wireless Networks over Moving Vehicles on Highways. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking Computing (MobiHoc 2001), October 2001. 87, 88, 126*

[18] J. Blum, A. Eskandarian, and L. J. Hoffman. "*Performance Characteristics of Inter-Vehicle Ad Hoc Networks. In Proceedings of the 6th IEEE International Conference on Intelligent Transportation Systems, Shanghay, China, 2003. 87*

[19] The FleetNet Project web-site. http://www.et2.tuharburg.de/fleetnet/index.html. 89

[20] W. Enkelmann. FleetNet "*Applications for Inter-Vehicle Communication. In Proceedings of the IEEE Intelligent Vehicles Symposium (IV 2003), June 2003. 89*

[21] A. Festag, H. Fler, H. Hartenstein, A. Sarma, and R. Schmitz. "*FleetNet: Bridging car-to-car communication into the real world. In Proceedings of the 11th World Congress on ITS, Nagoya, Japan, October 2004. 90*

[22] Lochert, H. Hartenstein, J. Tian, H. Fler, D. Herrmann, and M. Mauve. "*A Routing Strategy for Vehicular Ad Hoc Networks in City Environments. In Proceedings of the IEEE Intelligent Vehicles Symposium (IV2003), Columbus, OH, USA, June 2003. 90*

[23] H. Fler, M. Mauve, H. Hartenstein, M. Ksemann, and D. Vollmer. "*Location-Based Routing for Vehicular Ad-Hoc Networks. In Proceed- ings of the ACM MobiCom 2002, Atlanta, Giorgia, USA, September 2002. 90*

SBSC02 J. P. Singh, N. Bambos, B. Srinivasan, and D. Clawin. "*Wireless LAN Performance under Varied Stress Conditions in Vehicular Traffic Scenarios. In Proceedings of the IEEE Vehicular Technology Conference, Vancouver, Canada, Fall 2002. 91*

[24] J. G. Jetcheva, Y. C. Hu, S. PalChaudhuri, A. K. Saha, and D. B. Johnson. "*Design and Evaluation of a Metropolitan Area Multitier Wireless Ad Hoc Network Architecture. In Proceedings of the 5th IEEE International Workshop on Mobile Computing Systems Applications, Monterey, CA, October 2003. 92*

[25] S. Schultz. " *Engineers and biologists design wireless devices to unlock secrets of animal kingdom, November 2002. http://www.princeton.edu/pr/pwb/02/1111/. 94, 109*

[26] The ZebraNet Wildlife Tracker, January 2004. http://www.princeton.edu/mrm/zebranet.html. 94, 109

[27] MPALA Wildlife Foundation. http://www.mpala.org/researchctr/index.html.94, 109

[28] T. Small and Z. J. Haas. "*The Shared Wireless Infostation Model - A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way).*

In Proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), Annapolis, MD, USA, June 2003. 96, 133

[29] J. Sushant, K. Fall, and R. Patra. "*Routing in a delay tolerant network.In Proceedings of SIGCOMM04, August 2004.*

[30] A. Vahdat and D. Becker. "*Epidemic routing for partially connected ad hoc networks. Technical Report CS-2000-06, Department of Computer Science, Duke University, Durham, NC, 2000. 9, 101, 105, 203*

[31] J. A. Davis, A. H. Fagg, and B. N. Levine. "*Wearable Computers as Packet Transport Mechanisms in Highly-Partitioned Ad-Hoc Networks. In Proceedings of the Inter-Symposium on Wearable Comput- ing, Zurich, October 2001. 103, 105, 124, 203*

[32] B. Burns, O. Brock, and B. N. Levine. "*MV Routing and capacity build ng in disruption tolerant networks. In Proceedings of the IEEE INFOCOM 2005, Miami, FL, March 2005. 9, 105, 106, 203*

[33] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. "*Spray and Wait:An Efficient Routing Scheme for Intermittently Connected Mobile Networks. In Proceedings of the ACM SIGCOMM 2005 Workshop on delay tolerant networks, Philadelphia, PA, USA, August 2005. 107,108*

[34] Y. Wang, S. Jain, M. Martonosi, and K. Fall. "*Erasure Coding Based Routing for Opportunistic Networks. In in Proceedings of the ACM SIGCOMM 2005 Workshop on delay tolerant networks, Philadelphia, PA, August 2005. 108*

[35] J. Widmer and J. Y. Le Boudec. "*Network Coding for Efficient Communication in Extreme Networks. In Proceedings of the ACM SICOMM 2005 Workshop on delay tolerant networks, Philadelphia, PA,USA, August 2005. 109, 111, 150, 192*

[36] A. Lindgren, A. Doria, and O. Scheln. "*Probabilistic routing in intermittently connected networks. Mobile Computing and Communications Review, 7(3), July 2003. 9, 117, 203*

[37] J. Leguay, T. Friedman, and V. Conan. "*DTN Routing in a Mobility Pattern Space. In Proceedings of the ACM SIGCOMM 2005 Workshop on delay tolerant networks, Philadelphia, PA, USA, August 2005. 118,119*

[38] S. Biswas and R. Morris. "*Opportunistic Routing in Multihop Wireless Networks. In HotNets workshop, 2003. 120*

[39] K. Tan, Q. Zhang, and W. Zhu. "*Shortest path routing in partially connected ad hoc networks. In IEEE Globecom, 2003. 122*

[40] Chiara Boldrini, Marco Conti, Iacopo Iacopini, Andrea Passarella "*HiBOp: a History Based Routing Protocol for Opportunistic Networks*

[41] C. Shen, G. Borkar, S. Rajagopalan, and C. Jaikaeo. "*InterrogationBased Relay routing for Ad hoc Satellite networks. In Proceedings of IEEE Globecom 02, Taipei, Taiwan, November 2002. 125*

[42] M. Musolesi, S. Hailes, and C. Mascolo. "*Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks. In Proceedings of the 6th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2005), Taormina-Giardini Naxos, Italy, June 2005. 9, 126, 203*

[43] F. Tchakountio and R. Ramanathan. "*Tracking highly mobile end points. In ACM Workshop on Wireless Mobile Multimedia (WoWMoM), Rome, Italy, July 2001. 129*

[44] D. Nain, N. Petigara, and H. Balakrishnan. "*Integrated Routing and Storage for Messaging Applications in Mobile Ad Hoc Networks. In Proceedings of WiOpt, Autiplis, France, March 2003. 130*

[45] D. Goodman, J. Borras, N. Mandayam, and R. Yates. "*INFOSTATIONS: A new system model for data and messaging services. In Proceedings of the IEEE VTC97, May 1997. 132*