Metode de complexitate redusă pentru măsurarea interferenţei în reţelele 802.11

Dragoş Niculescu
Catedra de Telecomunicaţii, ETTI,
Universitatea Politehnica din Bucureşti

Rezumat

Harta interferenţei este o bază de date formată din trei componente disjuncte: rata livrării pachetelor pentru fiecare pereche de noduri din reţea, relaţiile de detecţie a purtătoarei (CS, carrier sense) pentru fiecare pereche, şi rata de livrare pentru fiecare triplet (sursă, destinaţie, factor de interferenţă). Metodele curente de achiziţionare a acestei baze de date au complexitate ridicată $O(n^2)$, unde n este numărul de noduri, ceea ce le face impracticabile pentru populaţii mari de dispozitive. În această articol, propunem metode aproximative de măsurare, care reduc timpul total de achiziţie prin suprapunerea probabilistică a măsurătorilor.

1 Introducere

Reţelele radio locale şi personale sunt mai populare ca oricând. Mediul principal de transmisie sunt frecvenţele fără licenţă in general limitate la 3 pentru 2.4GHz sau 13 pentru 5GHz. Standardele in vigoare (IEEE 802.11, 802.15) nu prevăd metode de gestionare a interferenţei sau de partajare a frecvenţelor de access la mediu. Atât în mediile instituţionale cât şi în cele domestice, dispozitivele folosesc metode ad hoc de gestionare a frecvenţelor. Alternativa este configurarea manuală si reevaluarea periodică – ambele necesitând efort uman si expertiză inaltă în propagarea radio.

Reţelele de telefonie celulară existente (2G si 3G) sunt limitate de interferenţă, şi vor continua această tendinţă în viitor. Reţelele radio pentru date nu au încă aceeaşi popularitate, întindere, şi importanţă socială, dar toţi aceşti indicatori sunt in creştere. Cele mai multe reţele radio pentru date folosesc frecvenţele fără licenţă la 2.4GHz şi 5GHz disponibile in majoritatea ţărilor. Utilizarea frecvenţelor fără licenţă este de obicei asociată cu plasarea ad-hoc, fără planificarea în detaliu a propagarii radio. In cazul instituţiilor, propagarea radio este estimată iniţial, dar procedura de mentenanţă este costisitoare. Funcţionarea fără licenţă a adus cu sine şi o diversitate mare de aplicare – medii domestice, instituţionale, municipale. Pentru aceste reţele de date, problema monitorizării interferenţei este importantă în multiple domenii de comunicaţie:

- reţelele municipale. În Statele Unite şi Europa un numar mare de retele municipale (Metro-Fi) au fost initiate in ultimii ani – Google Wifi, Philadelphia, Londra, New York City, etc. Specifice acestor retele sunt extinderea geografica (sute de km^2), numarul mare dar omogen de dispozitive implicate, varietatea conditiilor radio. Folosirea judicioasa a frecvenţelor si evitarea auto-interferentei necesita reevaluarea periodica a mediului radio pentru a mentine acoperirea si functionarea in conditii schimbatoare. - retele institutionale. Majoritatea institutiilor folosesc WiFi (in viitorul apropiat WiMax) in mod centralizat pentru a furniza acces wireless in interior. Propagarea radio in interior este notorie pentru caracterul impredictibil, depinzand de natura cladirilor si nivelul de activitate umana. Gestionarea acestor retele din punct de vedere radio necesita costuri recurente pentru mentenanta acoperirii si a calitatii. Interactiunea cu dispozitivele personale duce la rezultate impredictibile si la imposibilitatea de a oferi servicii ce necesita QoS (voce, video).

- reţele WiMax. Standardul 802.16 este in lucru, dar se preconizeaza finalizarea sa in 2010. Dispozitivele insa sunt deja disponibile, unele incluse in laptop-uri (Intel) sau asistenti digitali (Nokia). Standardul vizeaza problema QoS insuficient rezolvata in 802.11, atat pentru retelele de date cat si pentru cele de voce. Se preconizeaza ca aceste retele vor avea o popularitate mare in urmatorii ani, cu utilizare atat cu licenta cat si fara.

- reţele domestice. WiFi este proliferat la o densitate crescanda in aparta-

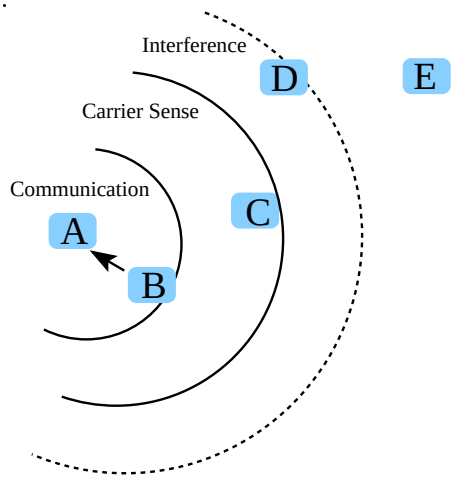
mente prin: telefoane WiFi/VoIP, dispozitive MP3, distribuire media in apartament (media center), calculatoare personale (laptop), asistenti digitali (PDA), camere si imprimante. Fiecare dispozitiv activ este de fapt un agent de interferenta pentru o comunicatie legitima desfasurata de un alt dispozitiv in alt apartament. Din p.d.v administrativ, reţelele domestice sunt independente deci nu pot fi coordonate intr-un mod centralizat.

- reţelele personale. Acestea sunt o subclasa a reţelelor domestice si implica conectarea fara fir a dispozitivelor portabile – casca Bluetooth pentru telefonul celular, player-ul MP3, etc. Frecvenţele folosite sunt deasemenea cele fara licenta in banda de 2.4GHz, in competitie directa cu dispozitivele WiFi.

- reţelele de senzori. Protocolul Zigbee standardizat de 802.15.4 deasemenea foloseste banda fara licenta de 2.4GHz in posibila competitie cu dispozitivele WiFi. reţelele de senzori sunt folosite pt monitorizare in agricultura, mediu, sau in interiorul cladirilor. In cazul topologiilor multihop furnizeaza exemplul clasic de auto-interferenta, cand pachetele aceleiasi conexiuni concureaza pentru accessul la mediu (aer). Aceste reţele sunt caracterizate de conditii stabile, durata lunga de functionare, dificultate de gestionat manual – datorita numarului mare de dispozitive, fiecare cu capabilitati hardware foarte reduse.

- reţelele cognitive. Un domeniu nou de cercetare sunt reţelele care permit o "agilitate" limitata in domeniul frecvenţelor (spectrum agility). Desi in faza incipienta de cercetare, aceste reţele promit accesul la un numar mai mare de frecvenţe pentru utilizatorii fara licenta (secundari) – in cazurile in care utilizatorii cu licenta (primari) nu sunt prezenti. Caracterul interferentei generate depinde de frecvenţa puratoare si necesita solutii algoritmice diferite. Exemplu: protocolul 802.11 a fost proiectat pt a functiona la frecvenţe 900MHz-2.4GHz. Adaptarea la 5GHz a adus cu sine necesitatea schimbarii temporizarilor si a parametrilor din protocol. O problema deschisa este legata de posibilitatea folosirii 802.11 la 10GHz (distanta redusa, directionalitate, interferenta redusa, dar necesita ceasuri de inalta precizie) sau la 400MHz (propagare prin cladiri, arie mare de interferenta, numar redus de benzi de frecvenţa). In toate aceste cazuri masurarea interferentei este necesara pentru a garanta utilizatorilor primari (platitori

Fig. 1: Posibilele relaţii de interferenţă între dispozitive aflate în aceeaşi vecinatate radio.



de licenta) un nivel maxim de interferenta din partea celor secundari. Deasemenea, prezenta unui numar mare de canale disponibile duce la cresterea complexitatii pentru coordonarea utilizatorilor secundari (vezi mai jos secţiunea 2.3).

2 Problematica generală a interferenței

Posibilele relatii de interferenta intre doua dispozitive radio de tip CSMA sunt ilustrate in figura 1. In realitate aceste zone nu sunt circulare ci adopta forme neregulate, dictate de propagarea radio, dar relatiile de incluziune intre regiuni raman valide. Cea mai mica regiune, intre dispozitivele A si B este cea in care comunicarea este posibila la nivelul legaturii de date. De obicei, aceasta relatie este bidirectionala, de exemplu in cazul 802.11 fiecare pachet este confirmat de catre recipient. La o distanta mai mare, C poate detecta prezenta lui A, dar semnalul este prea slab pentru a decoda pachetele. Aceasta este zona de “carrier sense”, si implementeaza o caracteristica de baza a protocoalelor de tip CSMA, precum 802.11. Folosind vectorul NAV, C amana folosirea mediului pe perioada cat mediul este perceput ca ocupat de catre A, chiar daca decodarea pachetelor de la A nu este posibila. Dispozitivele aflate la o distanta mai mare (de exemplu D) nu pot detecta prezenta lui A, si pot distruge involuntar pachetele primite de A. Aceasta ultima zona

nu are un caracter fix, ci depinde de pozitia si puterea emitatorului catre A. Din acest motiv, relatia de interferenta este definita pentru triplete ordonate (B,A,D) = (sursa, destinatie, agent de interferenţă) si nu pentru perechi de noduri (D,A).

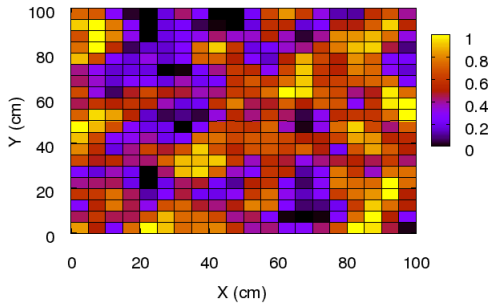
Pentru fiecare dispozitiv A, scopul este de a determina care este relatia cu partenerul de comunicatie B si cu potentialele surse de interferenta (dispozitive de tip C si D). Comunicarea dintre A si B poate fi exprimata ca o probabilitate de livrare (PDR packet delivery ratio), concurenta dintre A si C poate fi exprimata ca o ratie de partajare a mediului, iar influenta lui D asupra comunicarii A-B ca o fractie din PDR. Obtinerea acestor statistici si actualizarea lor in timp real necesita fie colaborarea altor dispozitive, fie rezervarea unui timp doar pentru masurare. Trebuie subliniat ca desi in acest exemplu C si D apar ca factori de interferenta la transmisie respectiv receptie, ei transporta trafic legitim in alta regiune a reţelei pentru care A sau B pot fi factori de interferenta. Nodurile B, C, si D trebuie deasemenea sa-si determine vecinii si relatiile de interferenta cu acestia.

Intr-o retea cu multe dispozitive – de exemplu WLAN in institutie – statiile de acces sunt configurate de obicei manual in functie de acoperirea pe care o furnizeaza. In reţelele de tip mesh sau ad-hoc, nodurile formeaza un graf conectat in care interferenta este mai intensa. reţelele de senzori sunt similare in structura reţelelor mesh, cu diferenta ca resursele nodurilor sunt mult mai reduse, iar regimul de functionare are un caracter mai stabil pe termen lung. In toate aceste cazuri este posibil ca performanta unei matrici de trafic sa fie predictibila in cazul in care toate relatiile de tip (A,B), (A,C), si (B,A,D) sunt cunoscute cu fractiunile asociate.

Relatiile de interferenta au un caracter variabil in timp, si masurarea lor trebuie repetata periodic. In cazurile in care dispozitivele sunt nomade, relatiile de interferenta se pot schimba la scara orelor sau minutelor. Datorita multitudinii cailor de propagare (multipath) in interior, mici schimbari de pozitie a unui dispozitiv pot duce la schimbari masive in propagarea semnalului. Pentru a exemplifica tipicul problemei, prezentam urmatorul experiment. Cu ajutorul unui robot, am masurat distributia spatiala a semnalului WiFi de la infrastructura de access WiFi intr-o camera de birou tipica. Semnalul este caracterizat la nivelul legaturii de date de probabilitatea de livrare (PDR).

In functie de unda purtatoare folosita (5GHz in acest experiment cu dispozitive 802.11a) variatiile chiar la scara centimetrilor pot fi majore (figura 2). Prezenta unui laptop sau a altui dispozitiv activ in aceasta harta ar

Fig. 2: Probabilitatea de livrare pachete variază la scară mică.



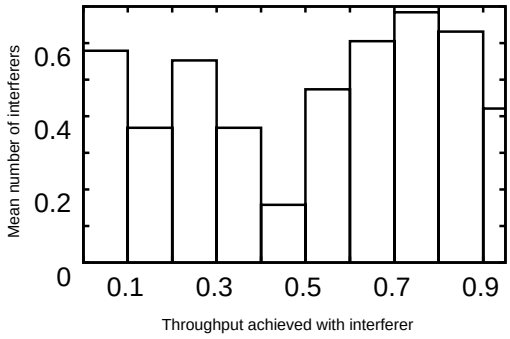
schimba complet peisajul semnalului WiFi – dispozitive de tipul C sau D (folosind notatiile din figura 1). Aceasta imagine este obtinuta in urma unui proces de masurare care dureaza aproximativ 30 de minute si implica libertatea robotului de a explora in detaliu spatiul de interes. O solutie de acest tip, desi ideala din punctul de vedere al estimarii interferentei, este dificil de implementat la scara larga.

2.1 Cât de raspândită este interferența intr-o rețea 802.11 instituționala tipică?

Intr-o cladire de 40x60m am plasat 20 de puncte de acces in banda de 802.11a 5GHz cu o acoperire de tip B, C (notatiile din Figura 1) de aproximativ 18m si o acoperire de tip D de aproximativ 35m. Graful de comunicare obtinut are 5 componente deci reteaua nu este potrivita pentru accesul de tip mesh, ci doar WLAN. Pentru fiecare dispozitiv in medie 1.9 noduri se afla in zona B, 2.6 in zona C, si 5 in zona D. Zonele B si C insa nu sunt cele mai periculoase, fiind tratate prin metoda de access standard CSMA. O parte din cele din zona D pot fi contracarate cu mecanisme de tip RTS/CTS, dar acestea sunt cunoscute pentru reducerea drastica a capacitatii, in speciual pentru pachetele mici (VoIP). Terminalele ascunse (de tip D) sunt cele care au un efect destructiv la destinatie si duc la cresterea numarului de retransmisii.

In figura 3, prezentam histograma dispozitivelor de tip D clasate dupa efectul destructiv pe care il au. Pe orizontala avem rata de livrare (PDR) B \rightarrow A obtinuta in prezenta unui dispozitiv D. Cumuland primele 4

Fig. 3: Histograma dispozitivelor de tip D (agenţi de interferenţă) şi efectul destructive pe care îl au asupra comunicaţiei $A \rightarrow B$.



intervale, se obtine un numar de 2 dispozitive de tip D care reduc capacitatea la 40% sau mai putin. Cumuland primele 2 intervale, obtinem aproximativ un terminal ascuns care reduce capacitatea la 20%. Aceasta estimare arata ca datorita neregularitatilor zonelor de propagare interferenta generata de terminale ascunse determina o scadere dramatica a capacitatii. Intr-o retea mesh, densitatea necesara este mai mare decat in scenariul WLAN, iar ponderea terminalelor ascunse va fi mai mare decat in acest experiment.

2.2 Stadiul actual al cercetării

In sistemele celulare, interferenta este tratata ca zgomot de catre cele mai multe transceivere din telefoanele folosite in prezent. Cercetarea academica si industriala insa a dezvoltat mai multe metode de detectare a utilizatorilor multipli [1], cuplate cu metode de anulare a interferentei. La nivelul fizic, cateva din metodele propuse pentru a anula interferenta sunt ISI (interferenta intre simboluri), MIMO (foloseste mai multe antene pe aceeasi purtatoare atat la transmitator cat si la receptor), si MUD (detectia utilizatorilor multipli). Aceste metode insa folosesc intensiv algoritmi de procesare a semnalelor cu complexitate mare, ceea ce a dus la evitarea lor de catre fabricantii de cipuri radio.

La nivelele superioare, metodele mentionate mai sus nu sunt accesibile, iar un pachet afectat de interferenta este de obicei pierdut. O lucrare recenta [2] propune combinarea copiilor primite la puncte de access diferite pentru a reduce BER (bit error rate). Aceasta insa necesita acceptarea copiilor pachetelor considerate corupte de catre nivelul fizic, si procesarea lor la o lo-

catie centralizata. In cazul particular 802.11 (standard 1997), exista cateva mecanisme care sa diminueze partial interferenta. Mecanismul RTS/CTS functioneaza in modul urmator: transmitatorul cere printr-un mesaj RTS broadcast permisiunea de transmisie, iar nodul destinatie raspunde cu CTS, deasemenea broadcast. Toate dispozitivele care primesc pachetul CTS se abtin de la accesul la mediu pe perioada ceruta. Acest mecanism reduce frecvenţa fenomenului 'terminal ascuns', dar nu rezolva problema unui dispozitiv care nu aude nici RTS nici CTS, dar este suficient de aproape pentru a distruge pachetele la receptor. In plus, mecanismul RTS/CTS are un overhead care este vizibil mai ales in cazul pachetelor mici (voce) pentru care reducerea in capacitate este de 50% - 80%. Un alt mecanism specific 802.11 este cel de carrier sense (care da numele metodei de acces CSMA) a fost deasemenea prevazut ca o metoda de reducere a interferentei. Desi contracareaza un mare numar de coliziuni la receptie, CS sufera de conflicte la transmisie, cunoscute sub numele de 'terminal expus': doua terminale aflate in CS unul de altul nu pot transmite in acelasi timp, desi receptorii lor respectivi sunt in afara zonei de interferenta la receptie. Exista studii [3] care chestioneaza eficienta CS pentru anumite conditii de trafic. CS aduce cu sine un overhead in timpul de arbitrare, care creste cu numarul de coliziuni, iar la incarcari ridicate in reţele de mare densitate se constata ca operarea fara CS are performante mai bune.

Noul standard IEEE 802.11n a fost finalizat in octombrie 2009 şi incorporează modificari care confirma problema interferentei. Doua metode de cresterea a capacitatii folosite in 802.11 sunt MIMO (pentru cresterea fiabilitatii si implicit a distantei de operare), si unirea canalelor (channel bonding). In principal, politica de unire a canalelor si de utilizare a unei benzi de 40MHz poate duce la degradare severa pentru dispozitivele existente folosing 802.11 b sau g. Solutia de buna vecinatate (good-neighbor policy) este ca 802.11n sa se limiteze la canale de 20MHz in prezenta dispozitivelor mai vechi (b sau g). Aceasta este o solutie conservativa si simpla din punct de vedere tehnic, dar poate conduce la o subutilizare masiva a capacitatii 802.11n.

La nivelele superioare, interferenta intre rute a fost studiata pentru reţelele prin cablu [4]. Problema se pune in a gasi rute pentru o matrice de trafic, astfel incat circuitele stabilite sa interfereze cat mai putin in interiorul ruterelor din retea. In cazul reţelelor wireless considerate in acest proiect, situatia este exacerbata de interferenta in aer, descrisa in paragrafele de mai sus. De obicei, interferenta cea mai destructiva se produce intre dispozitivele care nu au contact la nivelul legaturii de date.

Un caz oarecum simplificat pentru reţelele wireless este acela al auto-interferentei. Intr-o retea multihop nodurile folosesc mediul radio cu dispozitive semi-duplex, utilizate atat pentru transmisie cat si pentru receptie. Folosirea aceleiasi frecvenţe de catre toate nodurile conduce la fenomenul de autointerferenta in care pachetele aceleiasi conexiuni concureaza pentru obtinerea accesului la mediu. Problema auto-interferentei in reţelele multihop a fost identificata mai intai in 2000 [5] in mod teoretic, si o limita de $O(\frac{1}{\sqrt{n}})$ biţi-metri/secundă a fost stabilita pentru limita capacitatii. Pentru cazuri mai simple (simplu sir de noduri) capacitatea a fost determinata experimental in 2001 [6] la $\frac{1}{4}..\frac{1}{7}$ pentru UDP si $O(\frac{1}{n})$ pentru TCP. Aceste rezultate pesimiste sunt valabile pentru cazul in care fiecare nod foloseste un singur card. Prezenta unui singur card face problema tractabila din punct de vedere teoretic - [7] arata ca este posibil de a prezice capacitatea unei reţele date daca relatiile de interferenta sunt cunoscute, dar nu si cum se obtin aceste relatii. Trecand la arhitecturile cu carduri multiple, in 2004, Raniwala [8] a aratat ca problemele interferentei, alocarii frecvenţelor, si rutarii sunt interdependente. Orice modificare in unul din aspecte duce la schimbari in celelalte doua probleme. Alte contributii [9, 10] incearca obtinerea de rezultate predictibile atunci cand graful de dependinte a interferentei este cunoscut. Acesta insa este dificil de obtinut in realitate [11], complexitatea fiind de $O(n^2)$ unde n este numarul de noduri. Desi de obicei considerate simetrice de majoritatea algoritmilor, frecvenţele au in realitate performante diferite, deasemenea si cardurile - ceea ce duce la o crestere a complexitatii odata cu cresterea numarului de frecvenţe sau a numarului de carduri disponibile [12]. Cele mai recente metode de contracarare a interferentei [13, 14] folosesc atat modele (inexacte) cat si masuratori (necesita mult timp) pentru estimarea relatiilor de interferente dintre dispozitive. Pentru cazul distribuit, fiecare dispozitiv ia decizii locale pentru a evita interferenta. Pentru schimbarea frecvenţei, solutiile propuse fie nu respecta standardele in vigoare [15], fie sacrifica performanta/echitatea pe termen scurt [16].

Pentru studiul acoperirii radio si a calitatii semnalului, exista programe precum Radioscape [17], care folosesc algoritmi de ray-tracing si ray-launching pentru modela propagarea semnalului si efectele de fading si multipath. Acestea insa necesita un efort semnificativ in descrierea in detaliu a cladirii, materialelor, chiar a mobilei de interior. Cerintele de calcul pentru aceste modele sunt de obicei mari (Radioscape ruleaza pe un cluster de servere de mare putere).

2.3 Probleme rămase nerezolvate

Dificultatea masurarii sistematice a interferentei consta in doua aspecte: primul administrativ, si al doilea de complexitate algoritmica. Aspectul administrativ se refera la coordonarea dispozitivelor care pot apartine unor entitati diferite (institutii, persoane fizice), dar trebuie sa pastreze compatibilitatea de protocol. Deasemenea, deconectarea utilizatorilor pentru efectuarea masuratorilor de interferenta nu este acceptabila in multe cazuri. Complexitatea se refera la necesitatea coordonarii intre un numar mare (zeci - sute) de dispozitive pentru care relatiile de interferenta se schimba des (interval de zile, ore sau chiar minute).

2.3.1 Complexitatea algoritmică

Continuand exemplul anterior, pentru a identifica interferenta asupra comunicatiei B→A este necesar sa consideram toate dispozitivele de tip C si D prezente in retea. Deoarece nivelul de trafic nu poate fi cunoscut in avans, in principiu orice combinatie de dispozitive C si D trebuie considerata separat. Pentru o retea de intindere mica si cu aria de interferenta mare este posibil ca toate dispozitivele sa intre in zona D. In consecinta toate partile acestei multimi, (adica toate dispozitivele in afara de A si B) duc la o complexitate exponentiala chiar si pentru o singura pereche de comunicare A - B. Asa cum am aratat in [12], interferenta pentru o populatie mare de dispozitive are un numar de proprietati:

1. rata de livrare A→B depinde in mod linear atat de rata oferita pentru A→B cât şi de rata la care agentul de interferenta de tip D opereaza. Acest fapt este important in reducerea numarului de masuratori.

2. independenta agentilor de interferenta de tip D. Daca acestia sunt independenti din punct de vedere carrier sense, atunci efectul global al agentilor de tip D poate fi compus din efectele individuale. Asadar efectele mai multor dispozitive de tip D pot fi combinate pentru a prezice efectele oricarei multimi arbitrare de dispozitive. Aceasta implica ignorarea dispozitivelor cu nivel foarte redus de interferenta (de tip E) care individual nu pot produce vreun efect asupra comunicatiei A→B, dar luate impreuna pot produce zgomot care afecteaza comunicatia A→B. Ponderea statistica a acestei situatii a fost masurata ca fiind foarte redusa.

3. inconsistenta de la o interfata la alta.
   Am masurat capacitatea de livrare (0-100%) intre doua dispozitive intr-un interval de 17 ore. Dispozitivele sunt dotate fiecare cu doua interfete ath0 si ath1 ale caror antene se afla la o distanta de 40cm. Pentru o frecvenţa purtatoare de 5GHz aceasta diferenta de distanta este suficienta pentru a produce o legatura diferita. Experimentul a fost confirmat pentru un numar mare de perechi de dispozitive pe durata mai multor luni de masuratori. Concluzia este că pentru masurarea interferentei, fiecare interfata trebuie masurata separat.

4. inconsistenta de la un canal la altul.
   In maniera similara cu exeplul precedent, un numar de canale din banda de 5GHz este explorat pe o periada de 28 de ore, si se constata caracterul foarte divers al canalelor considerate. Atat din punct de vedere cantitativ - al capacitatii masurate, dar si din punct de vedere calitativ - in consistenta in timp a legaturii obtinute. Pentru masurarea interferentei, fiecare canal trebuie masurat separat.

Primele doua proprietati identificate au un caracter benefic prin aceea ca reduc numarul de masuratori la triplete ordonate de tipul (A, B, D). Deasemenea, masuratorile pot fi efectuate la o scara nominala atat pentru transmitator cat si pentru agentul de interferenta, si apoi scalate corespunzator. Aceste masuratori pot fi apoi combinate pentru a prezice efectul cumulativ al unui grup arbitrar de agenti de interferenta fiecare cu rate de transmisie arbitrare.

Proprietatile 3 si 4 au un caracter negativ prin aceea ca duc la cresterea numarului de masuratori. Considerand toate proprietatile identificarte masurarea interferentei se poate face cu o complexitate de $O(fn^2c^2)$ pentru intreaga retea unde f este numarul de interfete, n numarul de dispozitive, iar c numarul de canale ortogonale disponibile. Aceasta complexitate este prohibitiva chiar si pentru reţelele de dimensiune redusa. De exemplu pentru o retea de 20 de noduri, un singur canal, o singura interfata, si masuratori de 15 secunde timpul total de masura este de peste 2 ore. In acest interval functionarea reţelei este intrerupta pentru a asigura acuratetea masuratorilor. Considerand punctele de access moderne cu 2 sau mai multe interfete, si cele 13 canale disponibile pentru 802.11a, timpul de masurare a interferentei devine complet inacceptabil.

Pentru reţelele cognitive, in absenta standardelor, cercetarea actuala are mai mult un caracter speculativ. Formulele propuse pentru algoritmii de

acces la mediu precum C-MAC [18] introduc protocoale noi, de obicei in afara standardelor existente. O problema neexplorata inca, dar de interes pentru utilizatorii individuali, este functionarea standardelor existente (802.11) in medii cognitive. Oricare ar fi natura tehnica a acestei adaptari, estimarea continua a interferentei generata de utilizatorii secundari este inca o problema deschisa.

3 Harta interferenţei

Aşa cum am arătat în secţiunea 2, pentru fiecare dispozitiv A, scopul este de a determina care este relatia cu partenerul de comunicatie B si cu potentialele surse de interferenta (dispozitive de tip C si D). Comunicarea dintre A si B poate fi exprimata ca o probabilitate de livrare (PDR packet delivery ratio), concurenta dintre A si C poate fi exprimata ca o ratie de partajare a mediului, iar influenta lui D asupra comunicarii A-B ca o fractie din PDR. Ratele de livrare pot fi vizualizate într-o matrice d_{AB}unde A este emiţătorul iar B receptorul. Concurenţa CS dintre A şi C se exprimă ca un graf CS, în care avem un arc orientat $A \rightarrow C$ atunci când A cedeaza mediul lui C (sau o matrice cs_{AC}). Influenţa lui D asupra comunicarii $A \rightarrow B$ se exprimă ca d^D_{AB}si este o fracţiune din d_{AB}.

Aceste trei structuri de date sunt numite în mod colectiv "harta interferenţei". În această secţiune vom examina metode de măsurare si colectare a hârţii de interferenţă.

3.1 Proceduri de măsurare

Procesul de măsurare se desfăşoară în mai multe etape (această procedura a fost mai întâi propusă în [11]) şi este decris de algoritmul 1. De fapt, sunt incluse doua proceduri distincte: paşii 1.1 şi 1.2 colectează ratele de livrare pentru toate perechile de noduri din reţea. Deşi există n^2 astfel de perechi, n sunt executaţi concurent, prin folosirea difuzăriiiar complexitatea acestei porţiuni este deci liniară. Se poate deasemenea obţine din traficul utilizatorilor (live) dacă sunt îndeplinite condiţii de lipsă a interferenţei. Pentru paşii 1.3 and 1.4, se produc două măsurători: interferenţa la emisie (carrier sense), şi interferenţa la recepţie. A şi B pot trimite pachete la viteza maximă, iar din volumul de conflict pe care îl percep, pot determina cs_{AB} şi cs_{BA} folosindu-se de datele colectate in pasul 1.3b. Complexitatea acestei

Algorithm 1 Procedura de bază

1. un nod A din reţea difuzează pachete la viteza maximă; fiecare alt nod B din reţea măsoară rata de livrare $A \rightarrow B$.

2. toate nodurile rulează pe rând pasul 1.

3. o pereche (A, B) difuzează pachete la viteza maximă.

   (a) fiecare nod C măsoară rata livrării: $d^C_{A,B}$ fiind rata livrării $A \rightarrow C$ cu B pe post de agent de interferenţă; $d^C_{B,A}$ fiind rata livrării $B \rightarrow C$ cu A pe post de agent de interferenţă.

   (b) tot în acest pas, B şi A măsoară rata pachetelor pe care fiecare o poate trimite în mediu.

4. toate perechile (neordonate) de noduri din reţea execută pe rând paşii 3.

proceduri simple este $O(n)$ pentru ratele de livrare, şi $O(n^2)$ pentru grafurile de CS şi de interferenţă. Problema scalabilităţii acestor măsurători provine din faptul că se cere absenţa oricărui trafic în reţea pe durata măsurătorilor. De exemplu, pentru o reţea cu 20 de noduri, măsurători de 10 secunde, 3.5 ore au fost necesare penntru colectarea întregii baze de date.

Interferenţa la recepţie în pasul 1.3 este menţinută atunci când agentul de interferenţă este în afara zonei CS a emiţătorului. Când agentul de interferenţă este în zona CS cu emiţătorul, avem de a face cu interferenţa la emisie, capturată de graful CS.

Solutia pe care o propunem implica măsurători concurente care reduc complexitatea procesului cedand partial din acuratetea masurarii. Prin exploatarea distributiei spatiale a nodurilor, o mare parte din masuratori se pot efectua concurent in cazul in care probabilitatea de coliziune este neglijabila. Teste preliminare au demonstrat fezabilitatea metodei la scara mica de cateva dispozitive. Metoda pe care o investigam se bazeaza pe masuratori la nivelul legaturii de date (livrarea pachetelor), si pe algoritmi de decizie care pot fi plasati la unul din nivelele superioare:

- pentru o retea domestica, masurarea interferentei si deciderea unei politici de alocare a frecvenţelor se poate face doar independent, fara co-

ordonare. Eventual un grup de dispozitive pot fi coordonate sa urmeze o politica comuna si sa partajeze o baza de date de masuratori. Algoritmul de decizie este plasat sub nivelul retea, pentru a proteja utilizatorul de dificultatea (re)configurarii.

- pentru o retea institutionala, o solutie centralizata este acceptabila, o unitate centrala fiind capabila de a analiza masuratorile de interferenta de la o colectie mare de dispozitive WiFi aflate sub administratie comuna. Centralizarea da posibilitatea optimizarii folosind informatii multiple despre starea reţelei: cantitatea de trafic, regimul (date, voce), rutele existente. Algoritmul de alocare a frecvenţelor se afla complet in afara ierarhiei OSI, desi face uz de informatii de la nivelele 2,3, si 4.

- pentru o retea multihop (municipala, senzori) auto-interferenta este inamicul principal in cazul folosirii unui singur card wireless. In cazul folosirii de mai multe carduri, problema interferentei se compune cu problemele de rutare si de alocare a frecvenţelor, rezultand in probleme cu complexitate prohibitiva (NP-complete). Aici se impune folosirea unor euristici pentru rezolvarea aproximativa a colorarii grafurilor (frecvenţa fiind asociata cu o culoare).

4 Algoritmi randomizati de masurare

Complexitatea O(n^2) a metodelor existente provine din doua surse: masurarea interferentei la transmisie si masurarea interferentei la receptie. Pentru transmisie, fiecare pereche de dispozitive aflate in CS trebuie sa emita la flux maxim, pentru a decide in ce proportie au fiecare acces la mediu. O proportie de 100% (cs()=1)denota faptul ca dispozitivul nu sesizeaza nici o alta purtatoare in vecinatate. O proportie de 50% (cs=0.5) semnifica partajarea cu un alt dispozitiv intr-o relatie simetrica de CS. O proportie de 0% (foarte improbabil) semifica cedarea fiecarei arbitrari de acces la mediu in favoarea unui altor noduri.

In Figura 4, un factor de interferenta permanent J este indicat impreuna cu aria legaturii de date, iar nodul A impreuna cu aria CS. Pentru simplificare consideram ca A, B, C si D au arii CS similare. CS(J) nu este indicat in figura, dar poate fi mai mare sau mai mic decat CS(A) in functie de puterea folosita de J. Problema de rezolvat este de a afla daca A se afla in CS(J). In loc de a masura toate perechile de noduri din retea, ceea ce duce la complexitate patratica, propunem suprapunerea randomizata a masuratorilor CS(J,A),

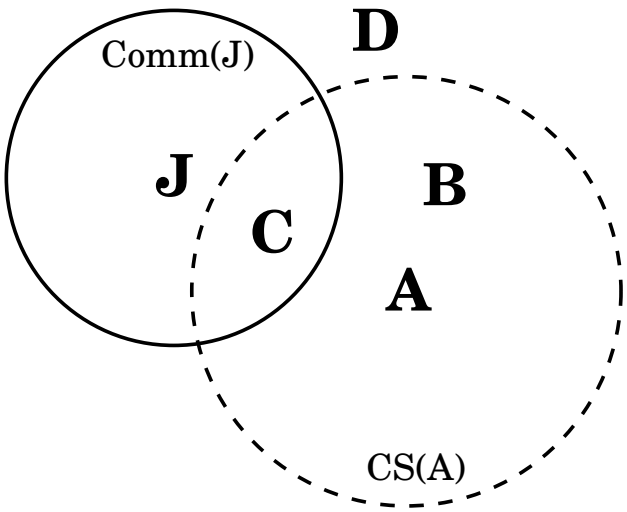


Fig. 4: Detecţia relaţiei de CS între A şi J.

CS(J,B), CS(J,C), etc. Intr-o sesiune, J transmite la capacitatea maxima, iar celelate noduri din retea incearca sa evalueze in ce mod pot capata accesul la mediu in timpul sesiunii. Daca accesul se face in timp scurt, nodul nu are concurenta. Daca timpul este prelungit, se datoreaza pierderii arbitrarii CS. Este esential ca dispozitivele A, B, C, si D sa nu intre in conflict CS unul cu altul, ci doar cu nodul J. Aceasta abordare masoara o discretizare binara a functiei cs(A,J) care poate avea orice valoare intre 0 si 1. Deoarece J foloseste mediul fara a respecta CS, nodurile in CS(J) nu sunt capabile sa trimita nici un pachet, in timp ce nodurile mai departate vor castiga o parte dintre arbitrari.

Pentru interferenta la receptie, metoda curenta cere ca o pereche de noduri, de exemplu J si A in Figura 4 sa emita la flux maxim in acelasi timp, in timp ce nodul C masoara rata de livrare A->C. In principiu toate aceste triplete din retea trebuiesc masurate, ceea ce necesita o complexitate cubica. De fapt, nodul C este doar receptor, deci toate nodurile din retea pot rula in aceeasi sesiune in care A si J sunt transmitatori, ceea ce duce la complexitatea patratica a numarului de sesiuni necesare. Ceea ce propunem in cadrul prezentului proiect este de a reduce si aceasta complexitate la nivel linear. O sesiune consta din J emitand la nivel maxim, iar nodul A emite probabilistic la intervale randomizate. Toate celelalte noduri monitorizeaza receptia de la A in prezenta factorului de interferenta J. Scopul transmisiu-

Algorithm 2 Măsurarea probabilistică a interferenţei la emisie

1. Nodul J difuzează la capacitate maximă cu funcţia CS dezactivată.
2. fiecare nod A (excluzând J) în reţea difuzează cu rata f.
   (a) fiecare nod A (excluzând J) decide dacă $A \in CS(J)$.
3. Fiecare nod din reţea rulează pe rând pasul 2, toate celelalte rulează 2.

nilor randomizate de catre A este de a permite nodurilor din vecinatate - B, C, D, etc de a rula aceeasi procedura cu o probabilitate de coliziune scazuta.

Ambele metode propuse promit masurarea interferentei in intreaga retea intr-un timp linear de sesiuni - 2n (n fiind numarul de noduri). Fiind insa metode randomizate, vor avea o fractiune de detectii fals pozitive sau fals negative pentru CS, respectiv valori imprecise pentru interferenta la receptie (terminal ascuns). Aceasta pierdere de precizie depinde de urmatorii parametrii de functionare: densitatea dispozitivelor 802.11, capacitatea de masurare real-time a sistemului de operare, durata unei sesiuni, corespondenta dintre modelul teoretic si implementarea hardware/software.

Complexitatea masuraorilor poate fi redusă daca paşii 4 în algoritmul 1 pot fi rulaţi simultan. O metoda de a simula aceasta concurenţa este de a avea măsurari scurte distribuite aleator în timp, astfel încât suprapunerea lor să fie neglijabilă.

4.1 Măsurarea probabilistică a interferenţei la emisie (Carrier Sense)

În figura 4, avem un agent de interferenţă J indicat cu zona de comunicaţie, şi un nod A, indicat cu zona CS asociată. Pentru o reprezentare simplificată, presupunem zone CS de dimensiuni similare pentru A, B, C, D. $CS(J)$ nu este indicată in figura şi poate fi mai mica sau mai mare decât a lui A, în funcţie de puterea folosită la J.Sarcina este de a determina dacă $A \in CS(J)$. În funcţie de primitivele hardware disponibile, propunem doi algoritmi:

Algoritmul 2 rulează simultan toţi paşii din algoritmul 1.3b. Un agent de interferenţă emite la capacitate maximă, iar toate celelalte noduri, ca şi emiţători încearca să decida dacă de fapt cedează mediul sau nu. În particu-

Algorithm 3 Măsurarea probabilistică a interferenţei la emisie

1. Nodul J la capacitate maximă.
2. fiecare nod A (excluzând J) în reţea trimite unicast perechi de pachete cu rata f către o adresă MAC inexistentă
   (a) fiecare nod A (excluzân J) decide dacă $A \in CS(J)$.
3. Fiecare nod din reţea rulează pe rând pasul 1.

lar, se măsoară $A \in CS(J)$, ceea ce este o discretizare binară a cs_{AJ}. Această implementare necesită acces la firmware sau la funcţiile card-ului pentru a creşte limita de putere pentru CS la nodul J, cum se foloseşte în [3]. Deoarece J foloseşte mediul indiferent de ce fac alţi emiţători, nodurile în $CS(J)$ nu reuşesc să transmită deoarece mediul le apare ca ocupat. Nodurile care sunt departe de J au acces normal la mediu.

Deoarece A ia o decizie binară dacă se află în $CS(J)$ se poate discuta despre pozitivele false şi despre negativele false ale acestui proces de decizie. Negativele false nu sunt posibile deoarece J difuzează tot timpul. Pozitivele false se pot petrece atunci când accesul lui A este împiedicat de o altă staţie care foloseşte aceeaşi politică de măsurători aleatoare. Probabilitatea acestei coliziuni de măsurători este mică dacă densitatea nodurilor este mică, iar probabilitatea f este deasemenea mică. Această soluţie este simplă, dar depinde de acces la firmware pentru a dezactiva funcţia CS. De exemplu, soluţia menţionată în [3] funcţionează doar pentru chip-urile Atheros 5210, şi nu poate fi reprodusă pe 5212. O altă opţiune ar fi să se folosească extensiile 802.11e care sunt activate pe drivere-le de generaţie mai noua, cum ar fi madwifi. Fereastra de conflict poate fi redusă la 1 (cwmin=cwmax=1) astfel încât J câştigă mereu în perioada de conflict, atunci când staţia A foloseşte un cwmin mare.

Aceast algoritm foloseşte un agent de interferenţă J care are funcţia CSobişnuită, si deci poate ceda mediul unor nodui din preajmă. Nodul A trimite pachete cu un maxim retry de 2 către o adresă inexistentă. Deoarece ACK nu va fi primit, o a doua încercare este transmisă. Diferenţa între recepţiile acestor pachete îi permite lui A să decidă dacă i-a cedat mediul lui J. Dacă diferenţa e scurtă, înseamnă ca pachetele sunt transmise unul după

Algorithm 4 Măsurarea probabilistică a interferenţei la recepţie

1. Nodul J difuzează la capacitate maximă
2. fiecare nod A (excluzând J) în reţea difuzează rafale cu rata f, separte în timp în mod aleator.
   (a) fiecare nod B (excluznd J şi A) măsoară $d^B_{A,J}$.
3. Fiecare nod din reţea ruleaza pe rând pasul 1, în timp ce restul nodurilor rulează pasul 2a.

altul. Dacă diferenţa e lungă, J a acaparat canalul, iar A a trebuit să cedeze înainte de retransmisie. Pentru această măsurătoare, A ncesită un al doilea card, sau un alt receptor cu recepţie bună.

Negativelefale sunt posibile deoarece J nu blochează accesul 100% din timp, si poate chiar ceda altor noduri, iar A poate decide ca $A \notin CS(J)$ doar pentru ca J a cedat mediul unui nod îndepărtat. Pozitivele false sunt deasemenea posibile ca şi la algoritmul precedent - coliziune între măsuratori. Noduri recum C, ce se află în zona de comunicaţie a lui J (Figura 4) nu creează probleme deoarece nu participă la măsurarea CS. Noduri precum D nu pot produce pozitive false deoarece nu-l pot forţa pe A să cedeze mediul. Cazul cel mai defavorabil este atunci când toate nodurile în $CS(A)$ pot produce coliziuni la măsurare.

4.2 Masurarea probabilistică a interferenţei la recepţie

Pentru interferenţa la recpţie, propunem algoritmul 4 care rulează în mod simultan toţi paşii 4a ai algoritmului 1 de mai sus. Un agent de interferenţă trimite la capcitate maximă în timp ce perechile sursă-destinaţie estimează concurent probabilităţile de livrare.

Este important ca emiţătorii de rafale să nu se suprapună în mod sistematic pentru ca aceste măsurători să se desfăşoare cu succes. În orice caz, conlictele potenţiale pentru un emiţător de rafale apar doar în propria zonă de interferenţă, şi nu în întreaga reţea. Rata coliziunilor acestor măsurători este desigur dependentă de rata f si de densitatea nodurilor în zona de interferenţă a emiţătorului.

Ambii algoritmi rulează în timp liniar, fiecare nod din reţea jucând pe rând rolul unui agent de interferenţă, în timp ce toate celelalte noduri estimează în mod concurent fie ratele de livrare, fie relaţia de CS.

5 Sumar

Harta interferenţei este o colecţie de structuri de date ce caracterizează efectul pe care fiecare nod îl are asupra reţelei. Ea este compusa din trei părţi: matricea ratelor de livrare, graful CS, şi graful de interferenţă. Metoda simplă de colectare a ultimelor două structuri foloseşte un timp patratic $O(n^2)$, unde n este numarul de noduri din reţea. Folosind măsuratori probilistice, am arătat ca acestea pot fi culese în timp liniar, ceea ce le face accesibile reţelelor de dimensiune şi densitate mare.

În continuare, se lucrează la implementarea algoritmilor şi la evaluarea acurateţii lor. Rata clasificărilor pozitive false creşte odată cu creşterea densităţii, şi cu rata de pachete folosite de fiecare măsurătoare. Evaluarea cantitativă a acestor pozitive false ajută la dimensionarea reţelei cu privire la noile proceduri propuse, în termeni de densitate, număr de canale, număr de carduri.

Bibliografie

[1] Jeffrey G. Andrews. Interference cancellation for cellular systems: A contemporary overview. *IEEE Wireless Networks*, April 2005.

[2] Grace R. Woo, Pouya Kheradpour, Dawei Shen, and Dina Katabi. Beyond the bits: Cooperative packet recovery using physical layer information. In *ACM MobiCom*, 2007.

[3] K. Jamieson, B. Hull, A. Miu, and H. Balakrishnan. Understanding the real-world performance of carrier sense. In *ACM SIGCOMM E-WIND Workshop*, 2005.

[4] Murali S. Kodialam and T.V. Lakshman. Minimum interference routing with applications to mpls traffic engineering. In *IEEE INFOCOM*, volume 2, pages 884–893, 2000.

[5] P. Gupta and P.R. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2):388–404, 2000.

[6] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris. Capacity of ad hoc wireless networks. In *ACM MobiCom*, pages 61–69, Rome, Italy, July 2001.

[7] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu. Impact of interference on multi-hop wireless network performance. In *ACM MobiCom*, San Diego, CA, September 2003.

[8] Ashish Raniwala, Kartik Gopalan, and Tzi-cker Chiueh. Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks. In *ACM Mobile Computing and Communications Review(MC2R)*, volume 8, April 2004.

[9] Murali Kodialam and Thyaga Nandagopal. Characterizing achievable rates in multi-hop wireless networks: the joint routing and scheduling problem. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 42–54, New York, NY, USA, 2003. ACM Press.

[10] Murali Kodialam and Thyaga Nandagopal. Characterizing the capacity region in multi-radio multi-channel wireless mesh networks. In *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 73–87, New York, NY, USA, 2005. ACM Press.

[11] Jitendra Padhye, Sharad Agarwal, Venkata N. Padmanabhan, and Lili Qiu. Estimation of link interference in static multi-hop wireless networks. In *Internet Measurement Conference*, 2005.

[12] Dragoş Niculescu. Interference map for 802.11 networks. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 339–350, New York, NY, USA, 2007. ACM.

[13] Anand Kashyap, Samrat Ganguly, and Samir Das. A measurement-based approach to modeling link capacity in 802.11-based wireless networks. In *ACM MOBICOM*, 2007.

[14] Charles Reis, Ratul Mahajan, Maya Rodrig, David Wetherall, and John Zahorjan. Measurement-based models of delivery and interference in static wireless networks. In *ACM SIGCOMM*, Pisa, Italy, September 2006.

[15] Arunesh Mishra, Vivek Shrivastava, Dheeraj Agrawal, Suman Banerjee, and Samrat Ganguly. Distributed channel management in uncoordinated wireless environments. In *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*, pages 170–181, New York, NY, USA, 2006. ACM.

[16] D.J. Leith and P. Clifford. A self-managed distributed channel selection algorithm for wlans. In *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on*, pages 1–9, April 2006.

[17] T. Ono, Y. Watanabe, H. Sugahara, K. Okanoue, and S. Yamazaki. Radioscape - a radio propagtion analyzing service for effective coverage area design. In *NEC Journal of Advanced Technology*, volume 1, pages 353–356, 2004.

[18] C. Cordeiro and K. Challapali. C-mac: A cognitive mac protocol for multi-channel wireless networks. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 147–157, April 2007.