بررسی دو مقوله مصرف انرژی و امنیت در شبکه های بیسیم Ad Hoc

عسگرعلی بویر
کارشناس ارشد مهندسی کامپیوتر- گرایش نرم افزار
Msmit2006@yahoo.com

چکیده:

در این مقاله ابتدا نگاهی گذرا به شبکه های بی سیم Adhoc داشته و سپس مقوله امنیت را بعنوان یکی از چالشهای اساسی در شبکه های بی سیم بررسی می کنیم. امنیت برای انواع شبکه که شبکه‌های بدون سیم را نیز در بر می‌گیرد مسئله مهمی است. واضح است که امنیت برای شبکه‌های بدون سیم امنیتی سخت‌تر از دیدن آن در شبکه‌های ثابت است. این امر معلول محدودیت‌های سیستم در تجهیزات متحرک و نیز تغییرات مکرر توپولوژی در شبکه‌های بدون سیم است. این محدودیت شامل، قدرت پایین، سیستم حافظه کوچک‌تر و پهنای باند کمتر و قدرت پایین انرژی(باطری) می باشد. تحرک و پویایی نودهایی بازسازی شده و ظرافت یا تغییر مسیر، معماری شبکه بدون سیم Ad-hoc را تبدیل به معماری پرخطر می‌کند. هیچ موجودیتی متقاعد نمی‌شود که در هر زمان حاضر باشد. پس امکان ندارد که به معماری متمرکزی که بتواند ساختار شبکه یا حتی سندیت آن را تصدیق کند تکیه کند. مقوله دیگری که دراین مقاله به آن پرداخته ایم بحث مصرف انرژی در شبکه های Adhoc میباشد. مصرف انرژی یکی از مهمترین استانداردهای اجرایی برای شبکه بدون سیم Ad-hoc است زیرا دقیقاً به عمر اجرایی و عملی شبکه مربوط است. اجزای متحرک مجبورند به منبع انرژی تکیه کنند و درحالیکه فن‌آوری باطری در ورای زمان بهبود می‌یابد، نیاز به مصرف انرژی تقلیل نمی‌یابد. این نکته تأثیر مضری بر زمان اجرا می‌گذارد همانطور که بر کیفیت و پهنای باند ارتباط می‌گذارد. در شبکه بدون سیم Ad-hoc جایگزینی باطری امکان ندارد. پس تا آنجا که میل مصرف انرژی وجود دارد باید سعی کنیم برای مواقعی که ارتباط بلندپایه‌ای وجود دارد انرژی باقی بگذاریم. در ادامه این مسئله را با مثالهایی بیان خواهیم کرد.

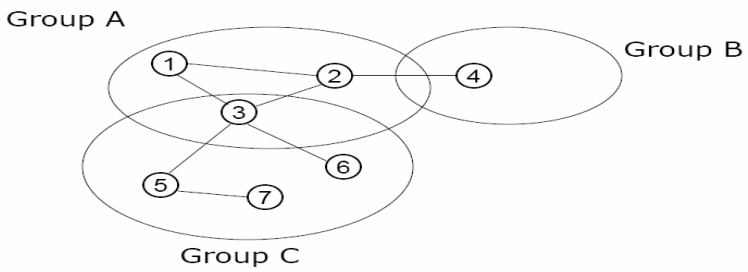
کلمات کلیدی: شبکه های بیسیم Adhoc - نود – شبکه متحرک- توپولوژی

۱- مقدمه:

شبکه‌های متحرک Ad-hoc که در سال ۱۹۹۰ مستقر شدند سالها به طور گسترده مورد مطالعه قرار گرفته اند. شبکه‌های متحرک Ad-hoc مجموعه‌ای از دو یا چند گره یا نود با ارتباطات بدون سیم و قابلیت شبکه‌ای است. این تجهیزات فورا می‌توانند با نودهایی که در درون دامنه رادیویی قراردارند و یا خارج از دامنه رادیویی قرار دارند ارتباط برقرار کنند. شبکه‌های بدون سیم Ad-hoc ورودی ندارند و هر نودی می‌تواند به عنوان ورودی عمل کند.

شبکه‌هایAd-hoc در استفاده‌های نظامی نقش مهمی دارند و تلاشهای تحقیق دوباره را گزارش می‌دهند. مثل برنامه سیستمهای اطلاعاتی هسته‌ای متحرک(Glomo) و برنامه رادیویی دیجیتالی(NTDR) و نیز اخیراً سیل جدیدی از استفاده‌های تجاری و صنعتی شبکه‌های بدون سیم Ad-hoc نیزصورت گرفته‌است.

یک نوع از شبکه های بدون سیم، شبکه‌های بدون زیرساختار است که به عنوان شبکه‌های متحرک Ad-hoc(یا MANET) شناخته شده‌اند. این شبکه‌ها مسیریاب ثابتی ندارند و هر نود می‌تواند مسیریاب باشد. همه نودها قادر به حرکت هستند و از لحاظ پویایی به شیوه دلخواه می‌توانند متصل شوند. مسؤلیتهای سازماندهی و کنترل شبکه میان خروجی‌ها توزیع می‌شود. شبکه در کل متحرک می‌باشد و خروجی‌های شخصی اجازه دارند که آزادانه حرکت کنند. برخی خروجی‌ها شاید قادر نباشند مستقیما با یکدیگر ارتباط برقرار کنند و مجبورند که روی خروجیهایی که پیغام‌ها را به مقصدهای مورد نظر می‌رساند، تکیه کنند. چنین شبکه‌هایی اغلب شبکه‌های چند مرحله‌ای هستند بطوریکه پیغام‌ها را ذخیره و بعد ارسال می‌کنند. نودها شاید درون یا روی هواپیماها، کشتی‌ها، کامیون‌ها، ماشین‌ها و حتی شاید روی انسان یا تجهیزات بسیار کوچک نیز پیدا می‌شود. گمان می‌رود که از شبکه‌های متحرک Ad-hoc برای کشف فاجعه ارتباطات جنگی و عملیات امنیتی استفاده کنند زیرا شبکه سیم‌دار در چنین مواردی قابل دسترس نیست.



شکل ۱- این تصویر سه گروه شبکه ad-hoc را نشان می دهد که باهم بصورت ادغام شده کار می کنند.

۲- امنیت:

۱-۲)چالشهای موجود در سیدن به امنیت در شبکه‌های بدون سیم Ad-hoc

از آنجایی که شبکه‌های بدون سیم Ad-hoc در اصل متفاوت از شبکه‌های بیسیم معروف(معمول) هستند بنابراین آن یک معماری کاملاً جدید و منحصر به فرد است. پس برخی چالشها از دو جنبه مهم افزایش پیدا می‌کنند: ۱- دینامیک بودن توپولوژی و متغیر بودن و متحرک بودن ایستگاهها و نود خود سازماندهی[1] ۲- آسیب پذیر بودن پیوندهی بیسیم: مانند استراق سمع، کلاهبرداری، عدم پذیرش سرویسها، تقاب زنی و جعل هویت و .. ۳- گردش آسان در یک محیط خطرناک: مثلاً یک نود بدخواه و یا بدرفتار می تواند تدارک یک حمله را ببیند یا دیگر نودها را از هر نوع سرویسی محروم کند. پیش از هـــر کار دیگر از آنجایی که نودها در یک شبکه بدون سیم Ad-hoc برای حرکت اختیاری در زمان آزاد هستند، بنابراین توپولوژی شبکه‌های MANET احتمالا بصورت تصادفی و به سرعت در زمانهای غیر قابل پیش‌بینی تغییر کنند که این امر مسیریابی را سخت‌تر می‌کند زیرا توپولوژی پیوسته در حال تغییر است و نودها نمی‌توانند وانمود کنند که ذخیره اطلاعات را به طور پایدار دارند. ما نمی‌دانیم که نود تا یک دقیقه دیگر باقی می‌ماند یا نه زیرا نود در هر لحظه شبکه را ترک می‌کند. به علاوه پهنای باند غیر طبیعی خود چالشی بزرگ است. لینکهای بدون سیم اساساً ظرفیت کمتری نسبت به بخشهای سیم کشی شده دارد. همچنین به علت دسترسیهای چندگانه، محوسازی، نویز، شرایط مداخله و غیره، لینکهای بدون سیم توان عملیاتی پایینی دارند. انرژی درعمل فشار وارد می‌کند. برخی یا همه نودها در MANET شاید روی باطریها تکیه دارند. اکثر متخصصین شبکه بر این باورند که، ویژگی مهمی که شبکه بدون سیم Ad-hoc را از شبکه‌های سلولی جدا می‌کند این واقعیت است که آنها بر زیر ساختار ثابتی تکیه ندارند. آنها همچنین معتقدند که شبکه‌های متحرکAd-hoc برای ارتباط تاکتیکی در انجام امور نظامی بسیار جالب هستند. همچنین معتقدند که شبکه بدون سیم Ad-hoc نقش مهمی را نه فقط در کاربرد اورژانسی و نظامی، بلکه در مکانهای شهری نظیر مراکز همایش، کنفرانسها، کلاسهای الکترونیکی و غیره ایفا می کنند.

۲-۲)ارائه راهکارهای امنیتی:

شبکه‌های متحرک نسبت به شبکه های کابلی معمولا بیشتر در مقابل تهدیدات امنیت فیزیکی قرار دارند. مسائلی که در برقراری امنیت بایستی درنظر داشت شامل موارد زیر است:

---

[1] - *self-organization*

۱- امنیت در سطح پیوند: یکی از چالشهای مهم در Ad-hoc برقراری یک محیط ارتباطی مطمئن است. یکی از روشهایی که می تواند برقراری یک ارتباط ایمن در محیط بدون سیم Ad-hoc را تا حدی تضمین کند استفاده از تکنیکهای بکار رفته در Firewallها و کنترل دسترسی به شبکه میباشد. زیرا در غیر اینصورت هر نود براحتی می تواند هر کار خرابکارانه ای که دوست داشته باشد انجام دهد و یا ارتباط دیگر نودها را با شبکه مختل کند.

۲- مسیریابی مطمئن: این نیز یکی از مسائل مهم می باشد که در زیر بحث خواهد شد.

۳- مدیریت کلید: یکی از روشهای اعمال امنیت استفاده از کلیدهای خصوصی و عمومی در مکانیزمهای رمزنگاری و رمزگشایی و یا امضاء دیجیتالی می باشد. این مکانیزمها توسط مدیریت متمرکزکلید پشتیبانی می شود بطوریکه گواهینامه احراز هویت مطمنی را فراهم می کند.

۴- دسترس اختصاصی(privacy): کلاهبرداری از هویت یا اطلاعات محرمانه بحث خصوصی سازی را مطرح میکند، که با اینکار میتوانیم از حملات مختلفی مثل حملات DoS جلوگیری کنیم.

طبیعتاً امنیت در شبکه‌های بدون سیم امنیتی سخت‌تر از شبکه‌های ثابت است این امر معلول محدودیت‌های سیستم در تجهیزات متحرک و نیز تغییرات مکرر توپولوژی در شبکه‌های بدون سیم است. این محدودیت شامل، قدرت پایین، سیستم حافظه کوچک‌تر و پهنای باند کمتر و قدرت پایین انرژی(باطری) می باشد. متحرک بودن نودهای و ظرافت یا تعیین مسیر در معماری، شبکه بدون سیم Ad-hoc را تبدیل به معماریهای پرخطر می‌کند. هیچ موجودیتی متقاعد نمی‌شود که در هر زمان حاضر باشد پس امکان ندارد که به معماری متمرکزی که بتواند ساختار شبکه یا حتی سندیت آن را تصدیق کند تکیه کند. به خاطر متحرک بودن ایستگاهها یا نودها و نیز استفاده از امواج رادیویی برای ارسال، امنیت به شدت تهدید می شود زیرا یک نفر به راحتی و بصورت غیرمجاز میتواند از طریق یک کامپیوتر کیفی در محدوده شبکه قرار گرفته و براحتی اطلاعات لازم را بردارد. برای رفع این مشکل یک روشی که پیشنهاد می شود استفاده از تکنولوژی بلوتوث به همراه الگوریتمهای جدید رمزنگاری در شبکه های Ad-hoc کوچک می باشد زیرا بلوتوث برد کوتاهتری داشته و به خاطر استفاده از تکنیکهای خاص در لایه های خود امنیت را تا حد ممکن در نظر می گیرد. البته برای شبکه های Ad-hoc در محدوده یک شهر این مورد نمی تواند استفاده شود.

آنهایی که شبکه های متحرک Ad-hoc را بررسی کردند معتقدند معماری ناقصی نیست در حالیکه ما نمی‌توانیم در عمل استفاده آن را ببینیم به خاطر اینکه بیشترین کاربردهای آن در امور نظامی است که به کل اشتباه است. هرکس می‌داند که نیاز اصلی برای کاربردهای نظامی رجوع به اعتماد و امنیت است. بهتر است بگوییم که امنیت مساله مهمی برای شبکه‌های Ad-hoc است به ویژه برای کاربردهای حساس امنیتی. بعد از بررسی و پژوهش ما دریافتیم که دو نوع مسئله مربوط به امنیت در شبکه‌های Ad-hoc وجود دارد. یکی حملاتی است که پایه آن شبکه های دیگری مثل اینترنت است و دیگری تشخیص خطاست.

الگوریتم تشخیص خطا یا نقص برای یافتن نودهای نقص دار و حذف همزمان آن نود از کل شبکه‌ها استفاده می‌شود. این مراحل باید بی‌درنگ باشند تا کارایی کل شبکه‌ها را تضمین کند. برای حل مسئله تشخیص نقص بیشتر الگوریتم‌های تشخیص نقص جدیداً پدید آمدند. بعد از بررسی دقیق الگوریتمهای موجود، ما دریافتیم که آنها نمی‌توانند به خاطر تغییر توپولوژی شبکه، نود نقص‌دار را تشخیص دهند و اینکه این الگوریتم ها با تشخیص‌های مکرر برای همه میزبان‌های متحرک تحلیل می‌شوند و باعث می‌شوند سربار یک سیستم بزرگ به سبب ارسال پیام های تشخیص با سیلی از آنها در سرتاسر شبکه‌ها حادث شود در حالی که توپولوژی شبکه‌های متحرک Ad-hoc هر لحظه تغییر می‌کند ما نمی‌توانیم از این الگوریتم برای حل حل مسائل استفاده کنیم پس می‌توانیم بگوییم که الگوریتم‌های جاری تشخیص نقص نمی‌تواند مشکل تشخیص نقص را حل کند. به دلیل حملات شبکه‌ها چندین عامل امنیتی وجود دارند که باید مورد توجه قرار گیرند.

۱: دسترس‌پذیری که قابلیت خدمات شبکه را علیرغم انکار حملات سرویس مطمئن می‌سازد.

۲: اطمینان‌سازی که اطمینان دهد اطلاعات محرمانه برای هویت‌های غیرمجاز باز نمی‌شوند.

۳: ضمانت بی‌نقصی که پیام را هرگز گسسته نمی‌کند.

۴: سندیت که قادر است نود را برای شناسایی نود همتا که در ارتباط با همدیگرند مطمئن سازد.

شبکه‌های متحرک Ad-hoc به طور ذاتی در مقابل حملات امنیتی آسیب‌پذیرند. از آنجاکه MANET نمی‌تواند نیاز امنیتی کاربردهای مختلف را رفع کند پس معماری ناقصی دارد.

۳-۲) امنیت در سطح مسیریابها در شبکه‌های Ad-hoc

شبکه‌های بدون سیم Ad-hoc بدون زیرساختار ثابتی عمل می‌کنند. چندمرحله‌ای بودن[1]، تحرک پذیری، اندازه بزرگ شبکه به همراه عدم تجانس تجهیزات و پهنای باند، محدودیت‌های توان باطری و غیره، که همه اینها عواملی هستند که طراحی پروتکل‌های مسیریابی را با چالش بزرگی روبرو کرده اند. بسیاری از محققان روی پروتکل‌های مسیریابی شبکه‌های بدون سیم Ad-hoc بسیار کار کرده‌اند. MANETها شبکه‌های میانی هستند که بوسیلهٔ مسیریابهای بدون سیم متحرک شکـــل می‌گیرند که هر روتر یا مسیریاب یک یا چند میزبان مربوط به خود دارد. هر مسیریاب MANET پروتوکلهای مسیریابی را که بی‌شباهت با تکنیکهای متداول مسیریابی است اجرا می‌کند.

مسائل اصلی درمورد پروتکل‌های مسیریابی بصورت زیر هستند:

- اول از همه یک الگوی عبوردهی سریع را در نظر می گیریم. الگوی عبور سریع میتواند یک نود باشد که توسط آن عبوردهی به سرعت و در کل شبکه صورت خواهد گرفت. بطوریکه نود گذردهی سریع، در کل شبکه آثاری بر جای می‌گذارد. این آثار می تواند بصورت زیر باشد:

اولاً تغییر سریع توپولوژی شبکه به احتمال زیاد باعث از دست رفتن بسته‌ها می‌شود. ثانیاً ما مجبوریم که جدول مسیریابی را برای هر نود که با نود گذردهی سریع در فاصله دورتری رابطه برقرار می‌کند، تعریف کرده و یا تغییر دهیم که در حد زیادی مصرف پهنای باند و سربار[2] شبکه‌ها را بهبود می‌دهد. ثالثاً واضح است که تأخیر زیادی در فرستادن اطلاعات به نود گذردهی سریع به وجود می‌آید. و یا بعنوان مثال فرستادن جداول مسیریابی پهنای باند شبکه و توان باطری را هدر می‌دهد.

۳- مصرف انرژی شبکه‌های بدون سیم

مصرف انرژی یکی از مهمترین استانداردهای اجرایی برای شبکه بدون سیم Ad-hoc و مستقیما به عمر عملی شبکه‌ها(مدت زمان استفاده موثر از شبکه) مربوط است. اجزای متحرک مجبورند به منبع انرژی تکیه کنند. درحالیکه فن‌آوری باطری با گذشت زمان بهبود می‌یابد ولی نیاز به مصرف انرژی تقلیل نمی‌یابد. این نکته تأثیر مضری بر زمان اجرا می‌گذارد همانطورکه بر کیفیت و پهنای باند ارتباط تاثیر می‌گذارد. در شبکه بدون سیم Ad-hoc جایگزینی باطری

---

[1] - Multi-hop
[2] - Overhead

امکان ندارد. هر نود به باطری‌هایی با ظرفیت پایین بعنوان منابع انرژی وابسته است و طبیعتاً نمی‌توانیم انتظار داشته باشیم که وقتی عملیات در نواحی دور و مثلاً متعلق به دشمن در حال انجام است، جایگزینی باطری یا همان انرژی صورت بگیرد. برای شبکه بدون سیم Ad-hoc کاهش و نقصان انرژی، فاکتور اصلی و مهم در پایین آمدن اتصالها(برقرای اتصال با شبکه) و طول عمر اجرایی(استفاده موثر) می باشد.

تلاش‌های تحقیقی بیشتر بر رقابتهای اجرایی و سبک و سنگین کردن مطالعات بین انواع مسیریابیهای مختلف با انرژی کم و نیز پروتوکلهای خودسازماندهی متمرکز است. درحالیکه پارامترهای دیگر سیستم ثابت نگه داشته شده اند. نتیجتاً اینکه ویژگیهایی مانند رابطهٔ بین تراکم مصرف انرژی و پارامترهای بدون قرارداد نظیر چگالی نود و پوشش سطحی شبکه و ویژگی‌های پاور فرستنده و گیرنده کمتر به چشم می آیند. ما بر مصرف انرژی تأکید می‌کنیم نه فقط به این دلیل که مشکل اصلی در تحقیق شبکه بدون سیم Ad-hoc بلکه بخاطر اینکه ما می‌دانیم که مشکل مصرف انرژی بر قراردادهای تبدیل و QOS کل شبکه‌ها اثر می‌گذارد. فرض کنیم که هر منبع بطور تصادفی یکی از مسیریابیهای ممکن را انتخاب می‌کند و از نودهای میانی درباره ترافیک مربوط به مسیریابی سؤال میشود. از آنجائیکه انرژی منبع باارزشی است، نودهای میانی ممکن است تمایل نداشته باشند که مصرف انرژیشان را برای حمل ترافیک مبداء مصرف کنند. این به نام (جاذبه) SelFish نود معروف است. ولی اگر هر نود خودخواهانه رفتار کند و از همکاری با دیگر نودها پرهیز کند در اینصورت توان عملیاتی شبکه احتمالا به شدت کاهش می‌یابد. متأسفانه اطلاعات اجرایی کمی درمورد رفتـار مصـرف انرژی شبکه بدون سیم Ad-hoc موجود است. اینترفیس‌ها و تجهیزات خاص اطلاعات را به شکلی که برای پروتکلهای توسعه دهنده مفید باشد، فراهم نمی‌کند. این امر ثابت می‌کند که شبکه‌های بدون سیم نمی‌توانند در عمل بکار گرفته شوند،

٤- نتیجه

شبکه‌های متحرک Ad-hoc فن‌آوری ایده‌آلی برای ساخت یک ارتباط بدون زیر ساختار است که برای کاربرد نظـامی بیشتر مطرح است که معماری ناقصشان تا حدی در این مقـاله مورد بحث قرار گرفت. همچنین ثابت کردیم که در استفاده از سه تکنیک مهم شبکه‌های بدون سیم Ad-hoc مواردی را می بینیم که در آن Ad-hoc بنا به دلایل تکنیکی زیر معماری معیوب و ناقصی دارد:

- مهمترین چیز در شبکه امنیت است حتی برای شبکه بدون سیم Ad-hoc، زیرا کاربردهای نظامی دارد. و MANET نمی‌تواند به طور تخصصی مشکل امنیت را حل کند.
- مسیریابی مشکل بزرگی است. همه قراردادهای مسیریابی برای شبکه بدون سیم Ad-hoc نیاز به معبر دارند، هیچ پروتکل مسیریابی پایدار و مناسبی تا کنون شناخته نشده است.
- مشکل مصرف انرژی هنوز نمی‌تواند حل شود، روی این موضوع بسیار تلاش شده‌است.

بعلاوه انتظار می‌رود همهٔ شبکه بدون سیم Ad-hoc خود پیکرسازی می‌کنند. خودپیکرسازی دو جنبه دارد: یکی در طی ساخت اولین بار شبکه. و جنبهٔ دیگر وقتی است که میزبان وارد شبکه یا از آن خارج می‌شود، شبکه باید توانایی پیکربندی توپولوژی تمام شبکه را داشته باشد.

به هر حال با پیشرفت مداوم فن‌آوری‌ها، باید امیدوار باشیم که روزی بتوانیم با تکیه بر برخی از انواع شبکه بدون سیم Ad-hoc، خودمان برای کاربرهای خود، شبکه های بیسیم متحرک بسازیم.

منابع:

[1] Yibin Liang, “Multipath “Fresnel Zone” Routing For Wireless Ad Hoc Networks” March 4, 2004
[2] David Malan†, Thaddeus FulfordJones†, " An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care" 2004
[3] IEEE Std 802.11 – 1999: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, Inst. Elec. Electron. Eng., New York, USA, 1999.ISBN 0-7381-1658-0
[4] IPN Progress Report, August 15, 2002, Analysis of Energy Consumption for Ad Hoc Wireless Sensor Networks Using a Bit-Meter-Per-Joule Metric, J.L.Gao
[5] A Distributed Light-Weight Authentication Model for Ad-hoc Networks
[6] S.Chessa, P.Santi, “Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks”, *Proc. IEEE 20th Symp. on Reliable Distributed Systems (SRDS)*, New Orleans, pp. 257-266, October 2001
[7] Erik Skow, Jiejun Kong, Thomas Phan, Fred Cheng, Richard Guy, Rajive Bagrodia, Mario Gerla, and
Songwu Lu, “A Security Architecture for Application Session Handoff”
[8] Lidong Zhou, Zygmunt J. Haas, “Securing Ad Hoc Networks”
[9] David B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts”, Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, December 1994.
[10] Ljubica Blazevic, Levente Buttyan, Srdan Capkun, Silvia Giordano, Jean-Pierre, Hubaux and Jean-Yves Le Boudec, “Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes”
[11] J. A. Freebersyser and B. Leinerr, “A DoD perspective on mobile ad hoc networks,” in *Ad*
Hoc Networking, C. E. Perkin, Ed. Addison-Wesley, 2001, pp. 29–51.
[12] B. Leiner, R. Ruth, and A. R. Sastry, “Goals and challenges of the DARPA GloMo program,”
IEEE Personal Communications, vol. 3, no. 6, pp. 34–43, December 1996.
[14] R. Ruppe, S. Griswald, P. Walsh, and R. Martin, “Near term digital radio (NTDR) system,”
in *Proceedings of IEEE MILCOM*, vol. 3, November 1997, pp. 1282–1287.
[15] M. Satyanarayanan. Fundamental challenges in mobile computing. *submitted paper*.
[16] M. Haardt W. Mohr R. Becher, M. Dillinger. Broadband wireless access and futurecommunication
networks. *Proceedings of the IEEE*, 89(1), 2001.