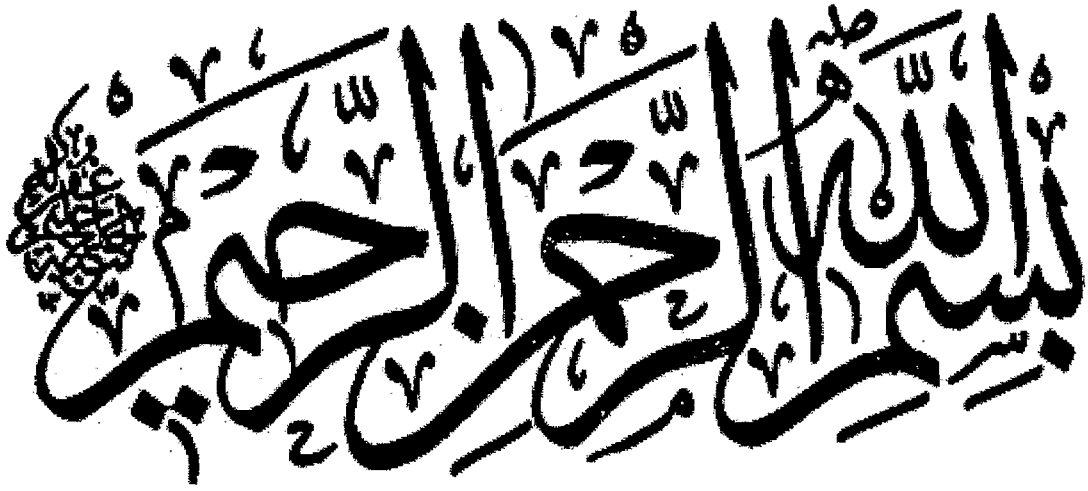


دانشگاه تربیت مدرس

دانشکده‌ی فنی و مهندسی

تعیین اعتبار گواهی‌های کلید عمومی با استفاده از ارزشیابی اعتماد در شبکه‌های اقتضایی

پایان نامه کارشناسی ارشد- مهندسی فناوری اطلاعات

محسن موذن

استاد راهنما

دکتر علی یزدیان

زمستان ۱۳۸۶

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان

آقای محسن موذن پایان نامه ٦ واحدی خود را **با عنوان تعیین صحت اعتبار گواهی های دیجیتال از طریق ارزیابی اعتماد در شبکه های Ad-Hoc** در تاریخ ۱۳۸٦/۱۲/٤ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی صنایع - فناوری اطلاعات پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر علی یزدیان ورجانی	استادیار	
استاد ناظر	دکتر نصراله مقدم چرکری	استادیار	
استاد ناظر	دکتر احمدرضا شرافت	استاد	
استاد ناظر	دکتر حسین پدرام	دانشیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر نصراله مقدم چرکری	استادیار	

۹۹۰۴۹

این نسخه به عنوان نسخه نهایی پایان نامه/رساله مورد تایید است.

امضای استاد راهنما:

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد نگارنده در رشته مهندسی فناوری اطلاعات است که در سال۱۳۸۶ در دانشکده فنی و مهندسی دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر علی یزدیان از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده رابه عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواندخسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده‌نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب محسن موذن دانشجوی رشته مهندسی فناوری اطلاعات مقطع کارشناسی ارشد تعهد فوق و ضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: محسن موذن

تاریخ و امضا:

دستورالعمل حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیات علمی، دانشجویان، دانش آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی که با هماهنگی دانشگاه انجام شده است، موارد ذیل را رعایت نمایند:

ماده ۱- حقوق مادی و معنوی پایان نامه‌ها / رساله‌های مصوب دانشگاه متعلق به دانشگاه است و هرگونه بهره‌برداری از آن باید با ذکر نام دانشگاه و رعایت آیین‌نامه‌ها و دستورالعمل‌های مصوب دانشگاه باشد.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و استاد راهنما مسئول مکاتبات مقاله باشد.

تبصره: در مقالاتی که پس از دانش آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب حاصل از نتایج پایان نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آئین نامه های مصوب انجام می‌شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم الاجرا است و هرگونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری می شود.

نام و نام خانوادگی: محسن موذن

امضاء

تقدیر و تشکر

شایسته است از صمیم قلب مراتب تقدیر و تشکر خود را از استاد ارجمند **جناب آقای دکتر علی یزدیان** که در طول تدوین این پایان نامه اینجانب را با راهنمایی‌های ارزشمند خویش یاری فرموده و پیوسته مشوق من در پیش‌برد آن بودند ابراز نمایم.

ضمنا از استادان محترم آقایان **دکتر حسین پدرام**، **دکتر احمدرضا شرافت** و **دکتر نصرالله مقدم چرکری** به‌جهت شرکت در جلسه دفاعیه کمال سپاسگزاری را دارم.

برای تمامی این عزیزان سعادت و سلامت آرزومندم.

محسن موذن

چکیده:

پیشرفت‌های چشمگیر تکنولوژی ارتباطات به همراه جذابیت‌های گسترده سیستم‌های بی‌سیم به‌واسطه حضور همه‌جایی آنها، کاربرد رو به گسترش شبکه‌های بی‌سیم را به ارمغان آورده است. شبکه‌های اقتضایی بی‌سیم با خصوصیت توانایی تحرک خود و عدم اتکا به زیرساختی از پیش موجود توجه زیادی را به عنوان نسل آتی شبکه‌های بی‌سیم به خود جلب نموده‌اند. شبکه اقتضایی طبق تعریف بر هیچ زیر ساخت ثابتی نباید تکیه داشته باشد و تمامی وظایف شبکه‌ای مانند مسیریابی، مدیریت تحرک و غیره در قالبی خودسازمانده توسط خود گره‌ها ویا با همکاری گره‌ها با یکدیگر انجام می‌شود. این ویژگیهای خاص، چالشهای امنیتی متعددی را برای شبکه‌های اقتضایی به همراه آورده است. از این رو تحقیقات زیادی برای برطرف کردن مشکلات و چالشهای امنیتی به این سمت سوق داده شده است. یکی از اصلی‌ترین چالشهای امنیتی در شبکه‌های اقتضایی عدم وجود یک سرور مرکزی یا مرجعی قابل اعتماد برای ارائه سرویسهای مدیریت کلید عمومی می‌باشد. حتی در صورت وجود، تضمینی برای فرآهم آوری دسترسی دائمی برخط به‌دلیل قسمت شدن شبکه ناشی از شکنندگی لینک‌های بی‌سیم و تحرک گره‌ها وجود ندارد. از این‌رو رویکردهایی توزیع شده برای مدیریت کلید مورد توجه می‌باشند. در این پایان نامه به مهمترین کارکرد سیستم مدیریت کلید پرداخته شده و سعی شده است با استفاده از روشی غیرمتمرکز برای ارزشیابی اعتماد به گره‌های صادرکننده گواهی، طرحی ارائه شود که بتوان مقادیر اعتمادی را به عنوان معیاری برای رد یا قبول گواهی‌های کلید عمومی بکاربرد. در نهایت نتایج شبیه‌سازی نشان می‌دهد که استفاده از این روش می‌تواند کارایی بالاتری را برای احراز هویت کلیدهای عمومی در حضور گره‌های بدخواه در مقایسه با دیگر روش‌ها به همراه داشته باشد.

کلمات کلیدی: شبکه اقتضایی، ارزشیابی اعتماد، تعیین اعتبار، گواهی کلید عمومی، روابط اعتمادی، امنیت، PGP

فهرست مطالب

چکیده: I

فهرست مطالب II

فهرست اشکال و جداول V

فصل اول ۱

مقدمه ۱

۱-۱-مقدمه و معرفی طرح ۲

۱-۲-روند ارائه مطالب ۴

فصل دوم: ۵

شبکه اقتضایی ۵

۲-۱-آشنایی با شبکه‌های اقتضایی ۶

۲-۲-کنترل دستیابی به رسانه (MAC) ۸

۲-۳-مسیریابی در شبکه‌های اقتضایی ۱۲

۲-۴-امنیت شبکه‌های اقتضایی ۱۳

۲-۴-۱-چالشهای امنیتی ۱۳

۲-۴-۲-امنیت مسیریابی ۱۴

۲-۴-۳-زیرساخت کلید عمومی ۱۶

فصل سوم: ۱۸

مدیریت کلید عمومی ۱۸

۳-۱-مقدمه: ۱۹

۳-۲-PGP و شبکه درهم تنیده اعتماد ۲۰
۳-۲-۱-Pretty Good Privacy: ۲۰
۳-۲-۲-گواهی کلید عمومی در PGP: ۲۲
۳-۲-۳-فرمت گواهی نامه‌ها: ۲۳
۳-۲-۴-دسته کلید PGP: ۲۳
۳-۲-۵-مدل اعتمادی در PGP: ۲۶
۳-۲-۶-بررسی اعتبار کلید عمومی در PGP ۲۹
۳-۳-مدیریت کلید عمومی در شبکه اقتضایی ۳۱
۳-۳-۱-مدیریت کلید برپایه رمزنگاری آستانه ۳۱
۳-۳-۲-مدیریت کلید خودسازمانده در شبکه اقتضایی ۳۲
۳-۳-۳-سرویس احراز هویت برپایه اعتماد و خوشه‌بندی ۳۴
فصل چهارم: ۳۷
روشهای ارزشیابی اعتماد در شبکه اقتضایی ۳۷
۴-۱-اعتماد و امنیت ۳۸
۴-۲-ارزشیابی اعتماد ۳۹
۴-۲-۱-کمی‌سازی اعتماد در شبکه‌های اقتضایی ۴۰
۴-۲-۲-ارزشیابی اعتماد در شبکه‌های باز ۴۲
۴-۲-۳-ارزشیابی اعتماد برپایه تئوری اطلاعات ۴۳
۴-۲-۴-ارزشیابی اعتماد براساس مسئله مسیر در گرافها ۴۴
فصل پنجم ۵۰
تعیین اعتبار گواهی کلید عمومی با استفاده از اعتماد در شبکه‌های اقتضایی ۵۰
۵-۱-مقدمه ۵۱

۵-۲-برپایی رابطه اعتمادی ۵۳
۵-۳-بکارگیری اعتماد در تعیین اعتبار گواهی‌ها ۵۴
۵-۴-ارزشیابی اعتماد به صادرکنندگان گواهی ۵۷

فصل ششم ۶۲

شبیه‌سازی ۶۲

۶-۱-پیش فرضها ۶۳
۶-۲- نتایج و تحلیل ۶۴
۶-۳-مقایسه نتایج ۶۷

فصل هفتم ۷۰

نتیجه‌گیری و پیشنهادات ۷۰

۷-۱-نتیجه‌گیری: ۷۱
۷-۲-زمینه‌های تحقیقاتی آتی ۷۲
مراجع ۷۴

فهرست اشکال و جداول

شکل ۲-۱: شبکه‌های بی‌سیم دارای زیرساخت (بالا) و شبکه بی‌سیم اقتضایی (پایین) ۷

شکل ۲-۲: مشکل ترمینال مخفی ۹

شکل ۲-۳: مشکل ترمینال درمعرض ۱۰

شکل ۲-۴: نمودار زمانی CSMA/CA و تشخیص حامل مجازی ۱۱

شکل ۳-۱: ترکیب رمزنگاری متقارن و نامتقارن در PGP ۲۱

شکل ۳-۲: به رمز درآوردن کلید خصوصی در دسته کلید ۲۴

شکل ۳-۳: مدل اعتمادی به هم تنیده ۲۷

شکل ۳-۴: مسیر گواهی در PGP ۳۰

شکل ۳-۵: گراف گواهی نمونه به همراه مسیرهای گواهی بین دو گره u و v پس از ترکیب مخازن به‌هنگام ۳۴

شکل ۴-۱: بکارگیری رابطه ۴-۳ روی یک گراف اعتمادی نمونه ۴۳

شکل ۵-۱: یک مسیر اعتمادی نمونه از گره مبداء s به صادرکننده گواهی مقصد، t ۵۲

شکل ۵-۲: نظارت محلی بر یک صادرکننده گواهی کلید عمومی ۵۴

شکل ۵-۳ :بکارگیری اعتماد در تعیین اعتبار گواهی‌های کلید عمومی ۵۶

شکل ۵-۴: گراف مسیرهای گواهی و اعتماد در شبکه اقتضایی ۵۸

شکل ۵-۵: ارزشیابی اعتماد برای توصیه‌کنندگان دست اول و صادرکنندگان گواهی ۵۹

جدول ۶-۱: پارامترهای شبیه‌سازی شبکه اقتضایی ۶۴

شکل ۶-۱: نرخ موفقیت، شکست و ناتوانی در تعیین اعتبار گواهی‌های کلید عمومی بواسطه اعمال نیم‌حلقه اعتمادی بدبینانه معادله (۵-۳) (با ۱۰٪، ۵۰٪ و ۷۰٪ گره‌های بد و آستانه اعتمادی ۰،۸) ۶۵

شکل ۶-۲: مقایسه نرخ موفقیت، شکست و ناتوانی در تعیین اعتبار گواهی‌های کلید عمومی بواسطه اعمال نیم-حلقه اعتمادی خوش‌بینانه معادله (۵-۱) و بدبینانه معادله (۵-۳) ۶۷

شکل ۶-۳: نرخ موفقیت، شکست و ناتوانی در تعیین اعتبار گواهی‌های کلید عمومی در روشهای مختلف ۶۸

فصل اول

مقدمه

۱-۱-مقدمه و معرفی طرح

علاقه به ارتباطات بی‌سیم متحرک بدلیل کاربرد آسان و خصوصیت حضور همه‌جایی سرویس آن باعث توجه زیادی طی دهه‌های اخیر در این بخش شده است. از طرفی مشکلات و چالش‌های ارتباطات بی‌سیم، علی‌الخصوص در شرایطی که گره‌ها سیار می‌باشند، همواره سدی بلند در برابر کیفیت سرویس دهی شبکه‌های مبتنی بر این تکنولوژی بوده است. این عوامل سرمایه‌گذاری وسیعی را برای تجاری سازی شبکه‌های بی‌سیم متحرک طلب می‌کرده است.

بطور مرسوم ارتباطات بی‌سیم بر زیرساخت‌های ثابتی استوار بوده‌اند که وظیفه مدیریت تحرک و ارایه سرویس‌های شبکه را برعهده داشتند. در این شبکه‌ها ابزار موبایل نقطه انتهایی[1] ارائه سرویس می‌باشد و کاربر از طریق آن به شبکه دسترسی خواهد داشت. نوع دیگری از شبکه‌های بی‌سیم که در اینجا مدنظر می‌باشد شبکه‌های اقتضایی هستند که در آن هیچ زیرساخت و مرکزیت ثابتی موجود نیست. این خصوصیت باعث می‌شود شبکه‌های اقتضایی حضور همه‌جایی[2] مناسب‌تری نسبت به شبکه‌های بی‌سیم دارای زیرساخت داشته باشند. با این حال تمامی سرویس‌های شبکه مانند مدیریت تحرک، مسیریابی و امنیت باید توسط گره‌ها انجام شود.

نبود امنیت بطور ذاتی در پروتکل‌های ارائه شده برای شبکه‌های کامپیوتری و به تبع آن شبکه‌های بی‌سیم و مهمتر از آن نبود زیرساخت در شبکه‌های اقتضایی در کنار محدودیت‌ها و تهدیدات ویژه مرتبط با این نوع شبکه‌های بی‌سیم باعث پدید آمدن حوزه تحقیقاتی گسترده‌ای شده‌است. توجه روزافزون محققین و پژوهشگران به این حوزه تحقیقاتی از این رو می‌باشد. یکی از روشهای اصلی امن‌سازی ارتباطات کامپیوتری استفاده از رمزنگاری کلید عمومی است که قادر خواهد بود امنیت

---

[1] End Point

[2] Ubiquitous

انتها به انتها را بگونه‌ای مقیاس‌پذیر بین کاربران بوجود آورد. با این حال بدون تکیه بر یک سیستم مدیریت کلید عمومی نمی‌توان بطور موثر از رمزنگاری کلید عمومی استفاده کرد.

مهمترین سرویس ارائه شده توسط سیستم مدیریت کلید، احراز هویت کلید عمومی است که به کاربران در مورد صحت کلید عمومی یکدیگر اطمینان خاطر می‌دهد. منشاء چنین اطمینانی، اعتماد کاربران به سیستم مدیریت کلید عمومی است. اعتماد و امنیت دو مفهوم به‌هم پیوسته در شبکه‌ها می‌باشند. مثالی از چنین پیوستگی نیاز به روشی قابل اعتماد برای حصول کلید عمومی در کاربرد رمزنگاری نامتقارن هنگام برقراری ارتباط امن می‌باشد؛ این درحالیست که سیستمی برای معاوضه کلید که قابلیت اعتماد آن نزد کاربران بالا باشد بدون استفاده از سرویسهای امنیتی مناسب که غالبا برپایه رمزنگاری بنانهاده شده‌اند، امکان‌پذیر نیست [۱].

سیستم مدیریت کلید خودسازمانده برای شبکه اقتضایی [۳]، بر مسیری از گواهی‌ها که هر یک قادر به اعتبارسازی برای گواهی بعدی در یک زنجیره می‌باشند برای تعیین اعتبار گواهی کلید عمومی بهره می‌برد. از طرفی چنین طرحی در مواجهه با گره‌های بدخواه که قادر به صدور گواهی‌های نامعتبر هم باشند کارایی خود را از دست می‌دهد. از این رو در اینجا طرحی پیشنهاد شده است تا به کمک آن بتوان صحت گواهی‌های کلید عمومی در شبکه اقتضایی در حضور گره‌های بدخواه را بررسی کرد. این کار با تکیه بر ارزشیابی اعتماد[1] که محاسبات آن در گره بررسی کننده و برپایه اطلاعاتی - توصیه‌های اعتمادی- که از رفتار دیگر گره‌ها به آن گره رسیده است، انجام می‌گیرد. این رویکرد به بررسی صحت گواهی‌های کلید عمومی، بدلیل توجه روزافزون به مقوله اعتماد در ایجاد امنیت برای شبکه‌های باز مدنظر قرار گرفته است.

در طرح پیشنهادی برای تعیین اعتبار گواهی‌های کلید عمومی، روابط اعتمادی باتوجه به فعالیت‌ی که این روابط برای آن برپا می‌شوند، در دوسطح مجزا تعریف شده‌اند. گره بررسی کننده اعتبار

---

[1] Trust Evaluation

گواهی کلید عمومی، با استفاده از روش ارزشیابی اعتماد مبتنی بر مسئله مسیر در گراف وزن‌دار جهت‌دار به همراه ترکیب دوسطح روابط اعتمادی متمایز، یک مقدار قابل استناد برای اعتماد به صادرکننده گواهی در حال بررسی بدست می‌آورد. این مقدار اعتمادی معیاری برای رد یا پذیرش گواهی کلید عمومی بادرنظر گرفتن کاربردی خاص ویا خط‌مشی‌های موجود بدست می‌دهد.

۱-۲-روند ارائه مطالب

در فصل دوم به معرفی و آشنایی با شبکه‌های اقتضایی و مباحث مربوط به آن پرداخته شده است. در فصل سوم مدیریت کلید عمومی مورد توجه می‌باشد که زیربنای کار این پایان نامه را تشکیل می‌دهد. در این فصل ابتدا مدیریت کلید در PGP مورد بررسی قرار گرفته است و سپس چند سیستم پیشنهادی برای مدیریت کلید در شبکه‌های اقتضایی معرفی شده‌اند. فصل چهارم به اعتماد در شبکه‌های اقتضایی اختصاص داده شده است. ابتدا با ارائه مفهوم اعتماد و تاثیر آن در برپایی امنیت، به کارکرد آن در ارتقاء امنیت شبکه‌های اقتضایی خواهیم پرداخت و سپس در ادامه چندین روش برای ارزشیابی اعتماد در شبکه‌های اقتضایی مورد مطالعه قرار خواهد گرفت. کار پیشنهادی برای تعیین اعتبار گواهی‌های کلید عمومی با استفاده از ارزشیابی اعتماد در فصل پنجم بطور کامل تشریح شده‌است. در نوشتن این فصل سعی شده‌است وابستگی نسبت به دیگر فصول پایان نامه در حد امکان پایین باشد. بگونه‌ای که خواننده قادر باشد تنها به مطالعه این بخش در صورت علاقه مبادرت نماید. فصل ششم شبیه‌سازی طرح پیشنهادی و نتایج حاصل از آن ارائه می‌دهد. در نهایت این کار با نتیجه گیری در فصل ۷ به پایان می‌رسد

فصل دوم:

شبکه اقتضایی

۲-۱-آشنایی با شبکه‌های اقتضایی

شبکه موبایل اقتضایی یک معماری شبکه‌ای است که می‌تواند بدون اتکا به هیچ زیرساخت از پیش مفروضی و به سرعت به خدمت گرفته شود. در این شبکه تعدادی گره (که ممکن است متحرک باشند) وجود دارد که با همکاری یکدیگر بین خود ارتباطی بی‌سیم بر قرار می‌کنند. بر قراری این ارتباط بسته به وسعت شبکه ممکن است یک جهشی[1] یا چند جهشی[2] باشد. در ارتباط یک جهشی یک گره تنها با همسایگان خود که قادر است سیگنال رادیویی را به آنها برساند ارتباط برقرار می‌کند اما در ارتباط چند جهشی بسته‌های اطلاعاتی به کمک گره‌های دیگر که نقش واسط را انجام می‌دهند به مقصد رسانده می‌شوند. در شکل ۲-۱ ساختار شبکه‌های اقتضایی در کنار شبکه‌های مرسوم بی‌سیم دارای زیرساخت نمایش داده شده است. سرویسها و پروتکل‌ها در شبکه اقتضایی بصورت توزیع شده و غیر متمرکز عمل می‌کنند. از این رو توپولوژی شبکه اقتضایی می‌تواند بصورت دینامیک تغییر کند و گره‌ها قادر هستند به دلخواه خود در شبکه وارد و یا از آن خارج شوند و این عمل غالبا تخریبی به ارتباطات دیگر گره‌ها وارد نخواهد کرد.

ایده شبکه‌های موبایل اقتضایی به اوائل دهه ۱۹۷۰ و پروژه‌های PRNET, SVRAN در مرکز تحقیقات پیشرفته دفاعی آمریکا باز می‌گردد. امروزه این شبکه‌ها در کاربردهای جدید غیر نظامی مورد توجه قرار گرفته اند. بعضی از موارد استفاده از شبکه‌های اقتضایی موبایل (MANET) به صورت زیر می‌باشد [۲]:

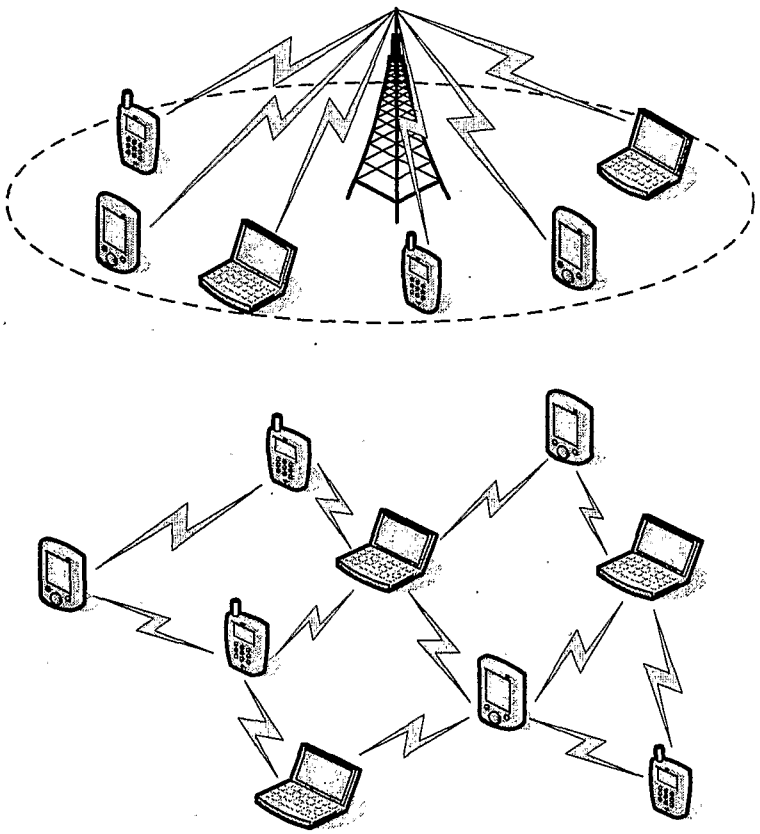
- عملیات تاکتیکی: با توجه به عدم وجود زیر ساخت در حین بکارگیری نیروهای نظامی در خاک دشمن کاربرد ابتدایی و اصلی شبکه‌های موبایل اقتضایی در برقراری ارتباط سریع هنگام عملیات تاکتیکی بوده است.

---

[1] One-Hop

[2] Multi-Hop

- عملیات امداد: برقراری ارتباط بی سیم بین امدادگران در بحرانهای طبیعی و غیر طبیعی مختلفی که پوشش مخابراتی مناسبی وجود ندارد یا زیرساختهای ارتباطی آسیب دیده اند. (بر اثر جنگ، زلزله، سیل و ....)
- کاربرد تجاری: جهت برپایی ارتباطات درون سالن‌های کنفرانس، نمایشگاههای بزرگ، فروشگاهها و ....
- آموزش: برقراری ارتباط در کلاسهای درسی یا پیاده سازی کلاسهای مجازی.
- شبکه‌های سنسور: برای ایجاد ارتباط بین گروهی از سنسورهای هوشمند که روی یک بستر متحرک قرار گرفته اند. مانند سیستمهای الکترومکانیکال کوچک[1] (MEMS).



شکل ۲-۱: شبکه‌های بی‌سیم دارای زیرساخت (بالا) و شبکه بی‌سیم اقتضایی (پایین)

[1] Micro Electro Mechanical Systems

دسته ای از گره‌ها که هدف مشترکی را داشته باشند یا وظیفه مشخص به آنها محول شده باشند می‌توانند تشکیل گروهی داده و با یکدیگر جابجا شوند، همانند یک واحد نظامی در عملیاتی خاص. یک شبکه موبایل اقتضایی شبکه نقطه به نقطه‌ای[1] است که در آن امکان ارتباط بین هر دو گره وجود دارد، البته در صورتیکه امکان رسیدن سیگنال رادیویی از یک گره به گره دیگر و باالعکس وجود داشته باشد. اگر یک اتصال مستقیم بین دو گره مبدا و مقصد وجود نداشته باشد، مسیر دهی چند جهشی استفاده می‌شود که در آن گره‌های واسط وظیفه به پیش راندن بسته‌ها از مبدا به مقصد را بر عهده دارند. بدین منظور پروتکل‌ها و الگوریتم‌های مسیریابی مناسبی در گره‌ها بکار گرفته می‌شوند که وظیفه بررسی وجود یا عدم وجود مسیر و کشف بهترین مسیر را بر عهده دارند. ازاین رو قابلیت تحرک آزادانه گره‌ها در یک شبکه اقتضایی، در قسمتی از فضا، تا آنجایی امکان پذیر است که یک گره حداقل با یک گره دیگر شبکه بتواند تماس خود را حفظ کند.

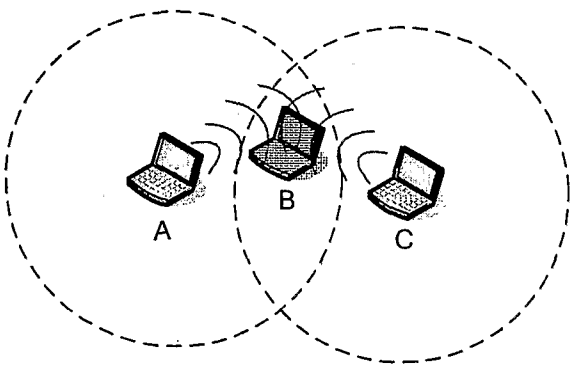
عدم وجود یک مرکزیت در شبکه‌های MANET بکارگیری پروتکل‌های توزیع شده را می‌طلبد. در حقیقت تفاوت عمده بین MANET با WLAN و یا شبکه‌های بی‌سیم سلولی، عدم وجود مداخل دارای مرکزیت در شبکه MANET می‌باشد که در شبکه‌های بی‌سیم مرسوم وظیفه هماهنگی و مدیریت شبکه را بر عهده دارند. الگوریتم‌ها و پروتکل‌های شبکه MANET بصورت توزیعی چنین عملیاتی را انجام می‌دهند. به طور خاص استفاده از مدیریت تحرک مبتنی بر HLR/VRL و پروتکل‌های زیر لایه MAC مبتنی بر وجود Base Station در شبکه‌های سلولی، دیگر در شبکه-های MANET امکان پذیر نیست.

۲-۲-کنترل دستیابی به رسانه (MAC)

[1] Peer to Peer

با توجه به اینکه در شبکه MANET گره‌ها از رسانه مشترکی استفاده می‌کنند در نتیجه امکان برخورد بسته‌ها و رقابت بر سر رسانه[1] بین گره‌ها حتمی است. به علاوه مشکلاتی مانند ترمینال مخفی[2]، ترمینال درمعرض[3] و ابزارهای رادیویی یک طرفه-که بطور همزمان قادر به ارسال و دریافت نیستند- استفاده از پروتکل‌های خاص در زیرلایه MAC برای تعیین اینکه چه گرهی می‌تواند به رسانه دسترسی داشته باشد را الزامی می‌کند. زیرا پروتکل مرسوم CSMA/CD که در شبکه‌های LAN کاربرد دارد قادر به برآوردن چنین نیازی نمی‌باشد.

مشکل ترمینال مخفی هنگامی رخ می‌دهد که دو گره (گره A و C در شکل ۲-۲) که می‌خواهند با B ارتباط بر قرار کنند قادر به دیدن یکدیگر نباشند. در این حالت دو گره C, A فارغ از احتمال برخورد بسته‌ها شروع به ارسال به B می‌کنند و این تداخل باعث از بین رفتن داده‌ها در سمت B می‌شود.



شکل ۲-۲: مشکل ترمینال مخفی

در مشکل ترمینال درمعرض که در شکل ۲-۳ نشان داده شده است گره B در حال ارسال داده به A می‌باشد اما گره C هم که در رنج رادیویی آن قرار دارد این سیگنال را دریافت می‌کند و از ارسال به D خودداری خواهد کرد. این در حالی است که ارسال اطلاعات از C به D بدلیل عدم دریافت سیگنال C در A هیچ تداخلی را در ارتباط A,B موجب نمی‌گردد.

---

[1] Media

[2] Hidden Terminal

[3] Exposed Terminal