دانشگاه پیام نور واحد ایذه

پایان نامه کارشناسی رشته:

مهندسی فناوری اطلاعات

موضوع:

شبکهAd-Hoc

استاد راهنما:

مریم کاووسی

نگارنده:

محمد شاهسوند

نیمسال دوم ۹۲-۱۳۹۱

سپـــاســـگـــذاری:

سپاس بی کران پروردگار یکتا را که هستی مان بخشید و به طریق علم و دانش رهنمونمان شد و به همنشینی رهروان علم و دانش مفتخرمان نمود و خوشه چینی از علم و معرفت را روزیمان ساخت.

در اینجا لازم میدانم از تمام کسانی که مرا در این امر یاری نموده اند، بخصوص استاد ارجمند سرکار خانم مریم کاووسی به دلیل همکاری ها و راهنمایی هایشان، کمال تشکر و قدردانی را نمایم. همچنین امیدوارم که این مجموعه رضایت خاطر ایشان که در طول دوران تحصیل از تجربیات و دانش ایشان نهایت استفاده را برده ام، فراهم آورده باشد.

تقدیم نامه

تقدیم به آن که تقوایش پاسداشت خوبی هاست

و تقدیم به کسانی که دوست داشته می شوند به خاطر خوبی ها

و تقدیم به

پدر و مادر عزیزم که در همه حال محکمترین تکیه‌گاه و بهترین یار زندگی‌ام بوده‌اند.

تقدیر وتشکر:

موضوع این تحقیق مربوط به بررسی شبکه Ad-Hoc می باشد که توسط اینجانب انجام گردیده امید است که توانسته باشم مطالب مفید و ارزنده ای را ارائه داده باشم و از آنجا که هیچ یک از مصنوعات بشر عاری از احتمال خطا واشتباه نیست از هرگونه رهنمود استاد گرامی و دانشجویان گرامی صمیمانه قدردانی می نمایم.

در پایان از استاد گرامی سرکار خانم مریم کاووسی و ریاست محترم دانشگاه ایذه و همچنین از یاری خانم حدیث امیری تشکر و قدردانی می‌نمایم.

محمد شاهسوندی

مهندسی فناوری و اطلاعات

بهار ۱۳۹۲

وزارت علوم، تحقیقات و فناوری

دانشگاه پیام نور واحد ایذه

کد پایان نام وزارت علوم، تحقیقات و فناوری

دانشگاه پیام نور واحد ایذه

کد پایان نامه:

نتیجه ارزشیابی دوره کارشناسی

بدینوسیله گواهی می گردد، پایان نامه آقای محمد شاهسوندی رشته مهنسی فناوری و اطلاعات به شماره دانشجویی ۸۸۰۰۸۴۵۴۶ ازدانشگاه پیام نور واحد ایذه تحت عنوان شبکه Ad-Hoc جهت اخذ مدرک کارشناسی در تاریخ .....موردارزیابی قرار گرفت

و با درجه..... و نمره.....تصویب گردید.

تأیید استاد

تأیید ریاست دانشگاه

تأیید آموزش

تأیید پژوهش

فهرست مطالب

عنوان **صفحه**

فهرست شکل ها و جدول ها

عنوان **صفحه**

پیشگفتار

اصطلاح Ad hoc که از زبان لاتین گرفته شده است به معنای برای "کاربرد اختصاصی" است. این عبارت عموما در مورد راه حلی استفاده می شود که برای حل یک مشکل خاص یا انجام وظیفه ای ویژه طراحی شده باشد و قابل تعمیم به صورت یک راه حل عمومی نباشد و امکان تطبیق دادن آن با مسایل دیگر وجود نداشته باشد.

یک شبکه ادهاک اتصالی است که تنها به مدت یک جلسه برقرار می شود و نیاز به ایستگاه پایه ندارد. در عوض هر دستگاه متصل به شبکه، دیگر دستگاه های واقع در یک محدوده خاص را پیدا می کند و این دستگاه ها یک شبکه بین خود ایجاد می کنند. از سوی دیگر، دستگاه ها با ارسال پیام، گره های هدف را در خارج از محدوده تعریف شده جستجو می کنند. امکان برقراری ارتباط بین چندین گره مختلف وجود دارد. به این ترتیب شبکه های ادهاک گوناگون به یکدیگر متصل می شوند. سپس پروتکل های مسیریابی اتصالات پایداری را بین این گره ها ایجاد می کنند، حتی اگر گره ها متحرک باشند. از جمله کاربران شبکه های ادهاک می توان به پلی استیشن سونی اشاره کرد که از اتصالات ادهاک برای ایجاد شبکه بی سیم بین چند بازیکن (که همگی در یک بازی شرکت می کنند) اشاره کرد. پس از پایان بازی اتصال بی سیم بین کاربران قطع می شود.

شبکه های ادهاک متحرک

شبکه های اجتماعی جدید با استفاده از ترکیبی از محاسبات رایانه ای و ارتباطات مخابراتی ایجاد می شوند. آگاهی از مکان محاسبات P2P و فناوری های شبکه بی سیم ، طراحی شبکه های ادهاک را برای دستگاه های متحرک که مهمترین ابزار ایجاد شبکه های اجتماعی هستند ، امکان پذیر ساخته است.

کاربرد شبکه ادهاک

شبکه های ادهاک در گستره وسیعی از کاربردها، از کاربردهای نظامی تا حفاظت از محیط زیست مورد استفاده قرار می گیرند. با مجهز کردن یک میدان جنگ به دستگاه هایی که از حسگر

لرزش سیستم GPS و حسگر مغناطیسی برخوردارند، می توان عبور و مرور خودروها در محل را کنترل کرد.

هر یک از این ابزارها پس از حس کردن موقعیت جغرافیایی خود با ارسال یک موج رادیویی، ابزارهایی را که در محدوده ای به وسعت ۳۰ متر از آن قرار دارند، یافته و با آنها ارتباط برقرار می کند.

شبکه های ادهاک نقش مهمی در حفاظت از محیط زیست ایفا می کنند.

زیست شناسان با استفاده از گردن آویزهایی که به حس گرهای مکان، دما و دیگر حس گرها مجهز هستند، کیفیت زندگی حیواناتی را که در خطر انقراض قرار دارند، بهبود می بخشد. زمانی که حیوان دارای گردن آویز حرکت می کند، اطلاعات مربوط به حرکت او از حس گرهای مرتبط جمع آوری می شوند و سپس توسط زیست شناسان مورد پردازش قرار می گیرند.

پیش بینی می شود که در آینده شبکه های ادهاک نقشی به سزا در مبادلات بین شبکه ای ایفا کنند.

.

چکیده

شبکه‌های بی‌سیم ادهاک شامل مجموعه‌ای از گره‌های توزیع شده‌اند که با همدیگر به طور بی سیم ارتباط دارند. نودها می‌توانند کامپیوتر میزبان یا مسیریاب باشند. نودها به طور مستقیم بدون هیچگونه نقطه دسترسی با همدیگر ارتباط برقرار می‌کنند و سازمان ثابتی ندارند و بنابراین در یک توپولوژی دلخواه شکل گرفته‌اند. هر نودی مجهز به یک فرستنده و گیرنده می‌باشد. مهم‌ترین ویژگی این شبکه‌ها وجود یک توپولوژی پویا و متغیر می‌باشد که نتیجه تحرک نودها می‌باشد. نودها در این شبکه‌ها به طور پیوسته موقعیت خود را تغییر می‌دهند که این خود نیاز به یک پروتکل مسیریابی که توانایی سازگاری با این تغییرات را داشته، نمایان می‌کند.

مقدمه

شبکه های Ad-hoc به شبکه های آنی و یا موقت گفته می شود که برای یک منظور خاص به وجود می آیند. در واقع شبکه های بی سیم هستند که گره های آن متحرک می باشند. تفاوت عمده شبکه های Ad-hoc با شبکه های معمول بی سیم ۸۰۲.۱۱ در این است که در شبکه های Ad-hoc مجموعه‌ای از گره های متحرک بی سیم بدون هیچ زیرساختار مرکزی نقطه دسترسی و یا ایستگاه پایه برای ارسال اطلاعات بی سیم در بازه ای مشخص به یکدیگر وصل می شوند.

ارسال بسته های اطلاعاتی در شبکه های بی سیم Ad-hoc توسط گره های مسیری که قبلا توسط یکی از الگوریتمهای مسیریابی مشخص شده است، صورت می گیرد. نکته قابل توجه این است که هر گره تنها با گره هایی در ارتباط است که در شعاع رادیویی اش هستند، که اصطلاحا گره های همسایه نامیده می شوند.

پروتکلهای مسیریابی بر اساس پارامترهای کانال مانند تضعیف، انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند. در هنگام طراحی این پروتکلها به امر تضمین امنیت در شبکه های Ad-hoc توجه نشد. در سالهای اخیر با توجه به کاربردهای حساس این شبکه از جمله در عملیاتهای نظامی، فوریتهای پزشکی و یا مجامع و کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در دو حیطه عملکرد و اعتبار پیشنهادات گوناگونی را مطرح کردند و می کنند.

شبکه های بی سیم Ad-hoc فاقد هسته مرکزی برای کنترل ارسال و دریافت داده می باشد و حمل بسته های اطلاعاتی به شخصه توسط خود گره های یک مسیر مشخص و اختصاصی صورت می گیرد. توپولوژی شبکه های Ad-hoc متغیر است زیرا گره های شبکه می توانند تحرک داشته باشند و در هر لحظه از زمان جای خود را تغییر بدهند.

وقتی گره ای تصمیم می گیرد که داده ای را برای گره مورد نظر خود بفرستد. ابتدا با انجام یک پروتکل مسیریابی پخش شونده کوتاهترین مسیر ممکن به گره مورد نظر را بدست می آورد و سپس با توجه به این مسیر داده را ارسال میکند. به هنگام به روز رسانی یا کشف مسیر مورد نظر تمام گره

های واقع بر روی مسیر، اطلاعات مربوط به راه رسیدن به گره مقصد را در جدول مسیریابی خود تنظیم می کنند، تا در هنگام ارسال داده از مبدا، روند اجرای عملیات ارسال داده به درستی از طریق کوتاهترین مسیر ممکن انجام شود.

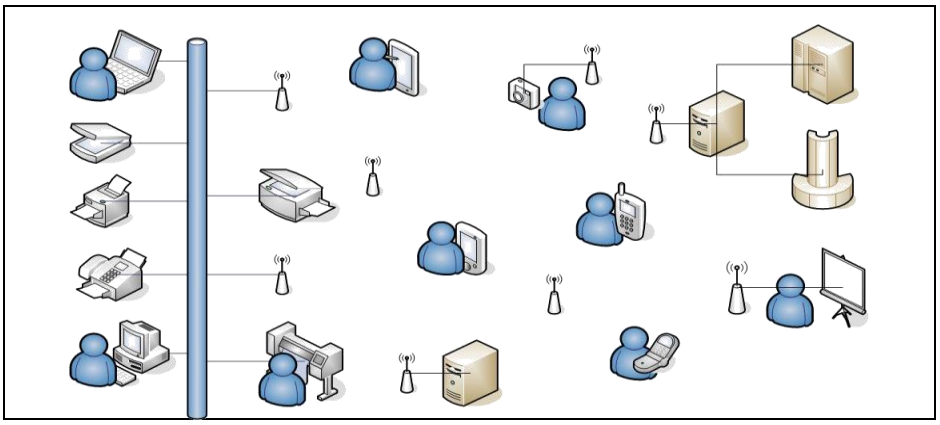
فصل اول: معرفی شبکه ادهاک

۱-۱ پیشینه

شبکه‌های ادهاک عمر ۷۰ ساله دارند و به دلایل نظامی به وجود آمدند. یک مثال کلاسیک از شبکه‌های ادهاک، شبکه جنگنده‌های جنگ و پایگاههای موبایل آنها در میدان جنگ می‌باشد. بعدا مشخص شد در قسمت‌های تجاری و صنعتی نیز می‌توانند مفید واقع شوند. این شبکه‌ها شامل مجموعه‌ای از گره‌های توزیع شده‌اند که بدون پشتیبانی مدیری مرکزی یک شبکهٔ موقت را می‌سازند. طبیعی ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان ایجاد تغییر در ساختار مجازی آنهاست. این ویژگی‌های خاصی که دارند پروتکل‌های مسیریابی و روشهای امنیتی خاصی را می‌طلبد.

۱-۲ مقدمه ای بر شبکه های متحرک بی سیم Ad-hoc

شبکه های اجتماعی جدید با استفاده از ترکیبی از محاسبات رایانه ای و ارتباطات مخابراتی ایجاد می شوند .آگاهی از مکان ،محاسبات P2P و فناوری های شبکه بی سیم طراحی شبکه های ادهاک را برای دستگاههای متحرک که مهمترین ابزار ایجاد شبکه های اجتماعی هستند امکانپذیرساخته است .



شکل ۱-۱ : شبکه ادهاک

۱-۳ معرفی انواع شبکه های Ad-hoc

شبکه‌های حسگر هوشمند: متشکل از چندین حسگر هستند که در محدوده جغرافیایی معینی قرار گرفته‌اند. هر حسگر دارای قابلیت ارتباطی بی سیم و هوش کافی برای پردازش سیگنال‌ها و امکان شبکه سازی است. شبکه‌های موبایل ادهاک :مجموعه مستقلی شامل کاربرین متحرک است که از طریق لینک‌های بی سیم با یکدیگر ارتباط برقرار می‌کنند. برای اتفاقات غیر قابل پیش بینی اتصالات و شبکه‌های متمرکز کارا نبوده و قابلیت اطمینان کافی را ندارند. لذا شبکه‌های ادهاک موبایل راه حل مناسبی است، گره‌های واقع در شبکه‌های ادهاک موبایل مجهز به گیرنده و فرستنده‌های بی سیم بوده و از آنتن‌هایی استفاده می‌کنند که ممکن است از نوع Broad cast و یا peer to peer باشند.

۱-٤ کاربردهای شبکه های Ad-hoc

به طور کلی زمانی که زیرساختاری قابل دسترس نیست و ایجاد و احداث زیرساختار غیرعملی بوده و همچنین مقرون به صرفه نباشد، استفاده از شبکه ادهاک مفید است. از جمله این

کاربردها می‌توان به موارد زیر اشاره نمود : شبکه‌های شخصی تلفن‌های سلولی، کامپیوترهای کیفی، ساعت‌های مچی، ear phone و کامپیوترهای wearable و محیط‌های نظامی.

O سربازها و تانکها و هواپیماها o در نبردهایی که کنترل از راه دور صورت می‌گیرد o برای ارتباطات نظامی o توانایی باقی ماندن در میدان منازعه محیط‌های غیرنظامی o شبکه تاکسی رانی o اتاق‌های ملاقات o میادین یا ورزشگاه‌های ورزشی o قایق‌ها، هواپیماهای کوچک o کنفرانس‌ها جلسات عملکردهای فوری o عملیات جستجو و نجات o موقعیت‌های امدادی برای حادثه‌های بد و فوری o برای ترمیم و بدست آوردن اطلاعات در حوادث بد و غیرمترقبه مانند وقوع بلایای طبیعی چون سیل و طوفان و زلزله محیط‌های علمی در محیط‌های علمی و تحقیقاتی در برخی از مناطق که دانشمندان برای نخستین بار اقدام به بررسی می‌کنند، به علت عدم وجود زیرساختار، شبکه ادهاک بسیار مفید می‌باشد. Sensor webs یک دسته مخصوص از شبکه‌های ادهاک را می‌توان Sensor webs دانست. شبکه‌ای از گره‌های حسگر که یک گره، سیستمی است که دارای باتری می‌باشد. توانایی مخابره بی سیم محاسبات و حس کردن محیط در آن وجود دارد. نقش آن مانیتور کردن و تعامل با محیط و دنیای اطراف است. کاربردهای آن شامل آزمایشا ت اقیانوسی و فضایی می‌باشد.

به طور کلی کاربردهای این شبکه ها را می توان به صورت زیر خلاصه کرد:

- شبکه های رزم آرایی (Tactical Networks)
  - مخابرات نظامی سربازان
  - عملیات و نبردهای خودکار

- شبکه های حسگر (Sensor Networks)
  - مجموعه ای از ادوات حسگر برای جمع آوری اطلاعات آنی (real-time) به منظور خودکار کردن اعمال روزمره
  - سیستم های هواشناسی سیار برای پیش بینی وضعیت هوا
- سرویس های غیرمترقبه (Emergency Services)
  - عملیات امداد و کمک رسانی
  - سیستم های سیار مددرسانی در هنگام زلزله و سیل
- محیط های تجاری (Commercial Environments)
  - تجارت الکترونیکی سیار (پرداخت یا وصول الکترونیکی از هر کجا در هر زمان)
- شبکه های خانگی و اداری (Home and Enterprise Networking)
  - شبکه محلی بی سیم
  - شبکه شخصی بی سیم
- کاربردهای آموزشی (Educational Applications)
  - کلاس های درس مجازی
  - اتاق های کنفرانس مجازی
- سرگرمی (Entertainment)
  - بازی های چندکاربره
  - روبات های خانگی

- سرویس های آگاه از مکان (Location-Aware Services)
  - سرویس های اطلاع رسانی (تبلیغاتی و مسافرتی)

۱-۵ خصوصیات شبکه های Ad-hoc

شبکه‌های بی سیم دارای نیازمندی‌ها و مشکلات امنیتی ویژه‌ای هستند. این مشکلات ناشی از ماهیت و خواص شبکه‌های بی سیم است که در بررسی هر راه حل امنیتی باید به آنها توجه نمود: الف: فقدان زیرساخت : در شبکه‌های بی سیم ساختارهای متمرکز و مجتمع مثل سرویس دهنده‌ها، مسیریابها و... لزوماً موجود نیستند (مثلاً در شبکه‌های ادهاک)، به همین خاطر راه حل‌های امنیتی آنها هم معمولاً غیر متمرکز، توزیع شده و مبتنی بر همکاری همه نودهای شبکه‌است. ب: استفاده از لینک بی سیم: در شبکه بی سیم، خطوط دفاعی معمول در شبکه‌های سیمی (مثلاً فایروال به عنوان خط مقدم دفاع) وجود ندارد. نفوذگر از تمام جهت‌ها و بدون نیاز به دسترسی فیزیکی به لینک، می‌تواند هر نودی را هدف قرار دهد. ج:چند پرشی بودن: در اغلب پروتکل‌های مسیریابی بی سیم، خود نودها نقش مسیریاب را ایفا می‌کنند (به خصوص در شبکه‌های ادهاک)، و بسته‌ها دارای چند hop مختلف هستند. طبیعتاً به هر نودی نمی‌توان اعتماد داشت آن هم برای وظیفه‌ای همچون مسیریابی! د: خودمختاری نودها در تغییر مکان: نودهای سیار در شبکه بی سیم به دلیل تغییر محل به خصوص در شبکه‌های بزرگ به سختی قابل ردیابی هستند. از دیگر ویژگیهای طبیعی شبکه بی سیم که منبع مشکلات امنیتی آن است می‌توان به فقدان توپولوژی ثابت و محدودیت‌های منابعی مثل توان، پردازنده و حافظه اشاره کرد.

به طور کلی می توان خصوصیات زیر را برای این شبکه ها نام برد:

- ارتباط بی سیم
- تشکیل برحسب اقتضا
- مسیریابی چندپرشی
- خودکار (بی نیاز از زیرساخت)
- قابلیت تحرک در گره ها

۱-٦ لزوم امنیت در شبکه های Ad-hoc

این شبکه‌ها به شدت در مقابل حملات آسیب پذیرند و امروزه مقاومت کردن در برابر حملات از چالش‌های توسعه این شبکه هاست. دلایل اصلی این مشکلات عبارتند از :

- کانال رادیویی اشتراکی انتقال داده
- محیط عملیاتی ناامن
- قدرت مرکزی ناکافی
- منابع محدود
- آسیب پذیر بودن از لحاظ فیزیکی
- کافی نبودن ارتباط نودهای میانی.

۱-۷ منشا ضعف امنیتی و خطرات معمول

ساختار این شبکه‌ها مبتنی بر استفاده از سیگنال‌های رادیوییبه جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی‌نه‌چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس‌دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است : • نفوذگران، با گذر از تدابیر امنیتی‌موجود، می‌توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌ای دست یابند. • حمله‌های DOS به تجهیزات و سیستم‌های بی سیم بسیار متداول است. • کامپیوترهای قابل حمل و جیبی، که امکان استفاده از شبکه بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت. • یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه بی‌سیم در یک سازمان و شبکه سیمی آن (که در اغلب موارد شبکه اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه بی‌سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد.

۱-۸ سه روش امنیتی در شبکه های بی سیم

WEP۱-۸-۱

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می‌آید که مناسب برای شبکه‌های کوچک بوده زیرا نیاز به تنظیمات دستی مربوطه در هر سرویس گیرنده می‌باشد. اساس رمز نگاری WEP بر مبنای الگوریتم ٤RC بوسیله RSA می‌باشد.

SSID۲-۸-۱

شبکه‌های WLAN دارای چندین شبکه محلی می‌باشند که هر کدام آنها دارای یک شناسه یکتا می‌باشند این شناسه‌ها در چندین نقطه دسترسی قرار داده می‌شوند. هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSID مربوطه را انجام دهد.

MAC ۳-۸-۱

لیستی از MAC آدرس‌های مورد استفاده در یک شبکه به نقطه دسترسی مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرس‌ها اجازه دسترسی دارند. به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می‌کند MAC آدرس آن با لیست MAC آدرس مربوطه در نقطه دسترسی مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می‌گیرد. این روش

امنیتی مناسب برای شبکه‌های کوچک بوده زیرا در شبکه‌های بزرگ امکان ورود این آدرس‌ها به نقطه دسترسی بسیار مشکل می‌باشد. در کل می‌توان از شعاع تحت پوشش سیگنال‌های شبکه کم کرد و اطلاعات را رمزنگاری کرد.

فصل دوم: مسیریابی در شبکه ادهاک

۲-۱ مقدمه

آنچه که شبکه های ادهاک را از (شبکه های بی سیمی) متمایز می کند آن است که تمام قواعد طبیعی درخصوص توپولوژی ثابت، همسایه های شناخته شده ثابت، تناظر دائم بین موقعیت فیزیکی و آدرس IP ماشین و مواردی از این قبیل در خصوص (شبکه های ویژه) صادق نیست . مسیریابها در رفت و آمد هستند و ممکن است در هر لحظه از محل جدیدی سر درآورند !در یک شبکه سیمی هرگاه یک مسیریاب، مسیری معتبر به برخی از نقاط مقصد در شبکه داشته باشد آن مسیر تا ابد معتبر خواهد بود (مگر آن که در جایی از سیستم خرابی به وجود بیاید) .در یک شبکه ویژه توپولوژی شبکه به طور دائم در تغییر است لذا اعتبار مسیرها و بهینگی آنها به ناگاه و بی هیچ هشدار قبلی تغییر می کند .آشکار است .که با چنین وضعیتی، مسیریابی در شبکه های ویژه کاملاً متفاوت از شبکه های ثابت می باشد.

۲-۲ دسته بندی الگوریتم های مسیریابی شبکه های ادهاک

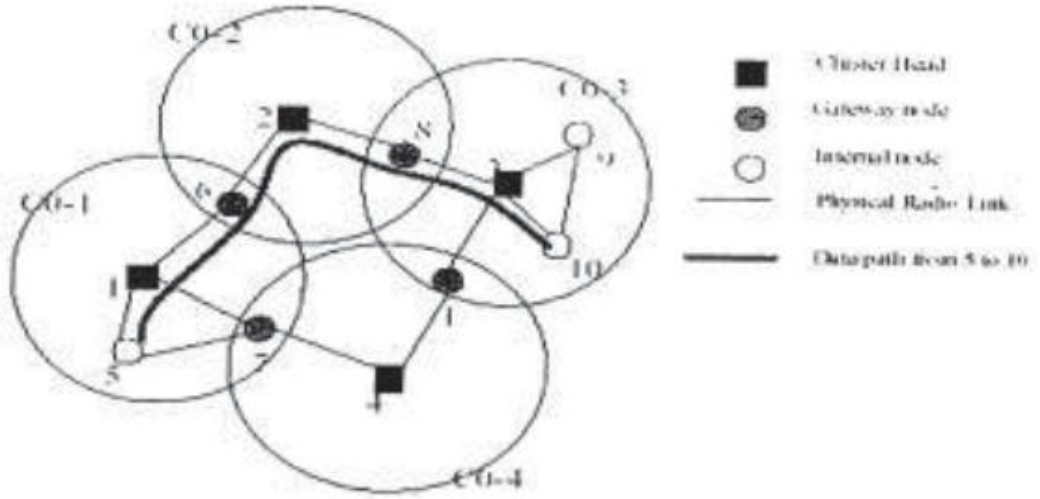
ترکیبی از شبکه های ادهاک نمی تواند دارای یک طرح مسیریابی متمرکز شده باشد .و این ما را نیازمند یک پروتکل مسیریابی توزیع شده می کند که در آن هر گره دارای بخشی از اطلاعات مسیریابی است که آن را به اشتراک می گذارد و در تصمیم گیری و نگهداری مسیریابی نقش دارد . این پروتکلهای مسیریابی توزیع شده می توانند درون دو دسته طبقه بندی شود :اولین دسته با توجه

به چگونگی تعیین توپولوژی شبکه مشخص میشود .دومین دسته با توجه به تصمیم آنها برای پیدا کردن یک مسیر به مقصد مشخص می شود .اولین دسته درون دو دسته مسیریابی(مسطح) و (سلسله مراتبی) تقسیم می شوند .دومین دسته به دو دسته (واکنش دار) و (پیشگیرانه) تقسیم می شوند.

۲-۲-۱ مسیریابی سلسله مراتبی

در الگوریتمهای مسیریابی سلسه مراتبی گره ها درون گروه های مختلف تقسیم بندی می شوند .از هر گروه یک گره به عنوان سرگروه انتخاب می شود .هر گره یا یک سرگروه می باشد و یا یک گام بی سیم می باشد. یک گره ممکن است سرگروه نباشد اما همسایه بیش از چندین سرگروه باشد که به آن (دروازه) می گویند .بسته ها بین سرگروه ها به واسطه این دروازه ها تعیین مسیر می شوند .زیر شبکه شامل دروازه ها و سرگروه ها می باشد که به آن ستون فقرات شبکه نسبت داده می شود .هر سرگروه اطلاعاتی را راجع به دیگر گره های موجود در آن گروه نگهداری می کند .و هر چند وقت یکبار این اطلاعات بین سرگروه های موجود در شبکه مبادله می شوند .بنابراین سرگروه ها اطلاعات توپولوژی شبکه را گردآوری می کنند .یک گره که میخواهد بست های را به گره دیگر ارسال کند اطلاعات مسیریابی را از سرگروهش فراهم می کند.

این روش مسیریابی مسیریابی آگاه از توپولوژی شبکه نامیده م یشود .چندین روش برای پیاده سازی این مسیریابی وجود دارد .اولین امکان این است که هر گره یک مسیر بهینه برای هر گره در سیستم تعیین کند و این اطلاعات را ذخیره کند .یک اتصال بین دو نقطه پایان برقرار می شود و همه بسته ها از این مسیر پیروی می کنند.



شکل ۲-۱ یک مثال از دسته بندی

هر چند که با تغییرات توپولوژی، گره ها می خواهند اطلاعات مسیریابیشان را به روزرسانی کنند و دوباره مسیرهای را که در طول این مکالمه از بین رفته اند برقرار کنند .دومین امکان مسیریابی بدون اتصال می باشد که مسیر برای هر بسته تعیین می شود .در این روش گره ها اطلاعات مسیریابی کمتری را درباره توپولوژی شبکه نگهداری م یکنند .هر چند که هر بسته موجب سرباره مسیریابی می شود.

۲-۲-۲ مسیریابی مسطح

در الگوریتم های مسیریابی مسطح همه گره ها مانند روتر عمل میکنند و مسئولیت هدایت بسته را با دیگرگره ها تقسیم می کنند .از اینرو هیچ انتخاب سرگروهی وجود ندارد و هیچ سازماندهی مجدد دوره ای شبکه لازم نمی باشد .بیشتر الگوریتم های مسطح تلاش م یکنند که یک نسخه توزیع شده از الگوریتم کوتاه ترین مسیر و یا سی لآسا را ارائه کنند که عموماَ فرستنده یک کپی

از پیغام را به هر همسایه ارسال می کند .همسایه ها سپس پیغام را به همه همسایه ها به استثنای همسایه ای که پیغام را از آن دریافت کرده اند ارسال می کنند .این پروسه تا زمانی که تمام شبکه از پیغام غرق شود تکرار می شود .اگر گره مقصد در بخش مشابه منبع باشد، پیغام به طور یقین به مقصد می رسد.

۲-۲-۳ مسیریابی پیشگیرانه

در پروتکلهای پیشگیرانه، گره ها به صورت مداوم اطلاعات مسیریابی را درون شبکه جستجو میکنند.بنابراین هنگامی که یک مسیر مورد نیاز می باشد، مسیر از قبل شناخته شده است .هر گره یک جدول مسیریابی که شامل اطلاعات گام بعدی برای هر گره دیگر در شبکه است نگهداری می کند و از اینرو یک مسیر بین گره مبدأ و گره مقصد همواره وجود دارد .مثالهای از الگوریتمهای پیشگیرانه شامل DSDV و FSR می شوند.

۲-۲-٤ مسیریابی واکنش دار

راندن بر حسب منبع یا پروتکل آغاز شونده منبع، دومین دسته از پروتکل های مسیریابی ادهاک متحرک می باشد .برای آن نوع از پروتکلها، مسیرها فقط هنگامی که به وسیله یک گره منبع درخواست می شوند، ایجاد می شوند .هنگامی که یک گره نیاز به یک مسیر به مقصد دارد یک پروسه کشف مسیر درون شبکه آغاز می شود .این پروسه یک مسیر را که پیدا می کند کامل می کند و یا همه مسیرهای ممکن به صورت جایگشتی آزمایش می شوند .یک مسیر یکبار کشف و برقرار می شود و تا زمانی که مقصد در دسترس نباشد یا مسیر برای مدت طولانی درخواست نشده باشد به

وسیله روال نگهداری مسیر نگهداری می شود. در الگوریتمهای واکنش دار، یک مسیر فقط هنگامی که یک گره بسته ای را برای ارسال به یک گره دارد ایجاد می شود .این نوع از الگوریتمهای مسیریابی، پروتکلهای مسیریابی (لحظه تقاضا) نامیده می شوند .دو مثال برجسته از این نوع الگوریتمها DSR و AODV می باشد .

۲-۳ یک دسته بندی دیگر برای پروتکل های مسیریابی شبکه ادهاک

به طور کلی بسته به اینکه گره ها چگونه مسیرها را ساخته و نگهداری می کنند، پروتکلهای مسیریابی در شبکه های Ad-hoc به دسته های زیر تقسیم میشوند :

۱-راندن بر اساس جدول (پیشگیرانه)Table Driven (Proactive)

مانند DSDV- WRP- CSGR- STAR

۲-راندن در زمان تقاضا (واکنش دار)On-Demand Driven (reaction)

مانند SSR- DSR- TORA- AODV- RDMAR- ABR

۳-پیوندی(Hybrid)

مانند ZRP

٤- مسیریابی بر مبنای موقعیت (Location- based)

۲-۳-۱ پروتکلهای **Proactive**

پروتکلهای مبتنی بر جدول که جداول مسیریابی را با استفاده از اطلاعات گره های همسایه به صورت بروز نگه می دارند.

مسیریابی در چنین پروتکلهایی شامل انتخاب مسیر از مبدأ تا مقصد است به نحوی که گره مبدأ و هر یک از گره های واسط (با استفاده از جستجو در جدول مسیریاب)، گام بعدی را انتخاب میکنند، تا بسته ی داده به مقصد برسد. یکی از ایرادات این پروتکلها، سربار ناشی از نگهداری مسیر و بروزرسانی پیاپی مسیر برای فائق آمدن بر متحرک بودن گرهها می باشد. نمونه ای از این پروتکلها DSDV می باشد.

Destination–Sequenced Distance-Vector : DSDV

یک نسخه ارتقاء یافته از الگوریتم Bellman–Ford توزیعی برای شبکه های mobile ad–hoc است .در این پروتکل هر گره یک جدول مسیریابی را نگهداری می کند که به ازای هرگره در شبکه یک ورودی در آن وجود دارد. هر ورودی تشکیل شده است از : ID مقصد، ID گام بعدی، تعداد گام و یک شماره ی ترتیب برای آن مقصد. شماره ی ترتیب به گره ها کمک می کند تا یک مسیر تازه و جدید (Fresh) به سمت مقصد را نگهداری کنند و از مسیرهای حلقوی اجتناب کنند. برای فائق آمدن به تغییرات مداوم توپولوژی شبکه، گره ها به صورت دوره ای جداول مسیریابی را در سطح شبکه پخش همگانی می کنند.

هنگامی که یک گره، بسته بروزرسانی مسیر را دریافت می کند، اگر شماره ترتیب مقصد در بسته از شماره ترتیب جدول خودش بیشتر باشد (تازهتر باشد)، ورودی های جدول مسیریابی خود را تغییر میدهد. اگر شماره ترتیب ها مثل هم بود، گره مسیری با متریک کمتر را انتخاب میکند (تعداد گام کمتر). برای کاهش ترافیک شبکه ناشی از بسته های بروزرسانی بزرگ DSVD ، دو نوع بروزرسانی را انجام می دهد: نسخه برداری کامل و افزایشی. یک بسته نسخه برداری کامل تولید شده توسط یک گره شامل تمام ورودی های جدول مسیریابی آن گره می شود. در حالی که یک بسته افزایشی تنها شامل ورودی هایی از جدول مسیریابی است که از آخرین نسخه برداری کامل، توسط گره تغییر یافته اند. یک گره زمانی بروزرسانی را انجام می دهد که متریک برای مقصد تغییر کرده باشد یا زمانی که شماره ترتیب تغییر کرده باشد. در مورد دوم، به آن DSVD – SQ گفته میشود.

۲-۳-۲ پروتکلهای **Reactive**

پروتکلهای Reactive پروتکلهای مبتنی بر تقاضا هستند که مسیرها را به صورت on–the–fly و هنگامی که مورد نیاز باشد، پیدا می کنند. در چنین پروتکلهایی برقراری یک مسیر جدید شامل یک فاز اکتشاف مسیر است که خود تشکیل شده است از درخواست مسیر (Flooding) و یک پاسخ مسیر(توسط گره مقصد) گره ها ، تنها مسیرهای فعال را تا یک مدت مطلوب یا تا وقتی که مقصد از طریق هر مسیری از گره مبدأ غیر قابل دسترسی شود، حفظ میکنند. مشکل این چنین پروتکلهایی

تأخیر ناشی از اکتشاف مسیر به صورت on-the-fly میباشد. به طور مختصر در مورد پروتکلهای AODV و DSR بحث خواهیم کرد.

AODV : در AODV یک گره، مسیر به سمت مقصد را فقط هنگامی که مورد نیاز باشد، اکتشاف و حفظ مسیر میکند. گره ها جدول مسیریابی را نگهداری میکنند که شامل مسیریابی در جهت مبدأ به مقصد است و به صورت فعال با یکدیگر در ارتباط خواهند بود. هر ورودی در جدول مسیریابی تشکیل شده است از ID مقصد ، ID گره گام بعدی، تعداد گام و یک شماره ترتیب مربوط به آن مقصد(همانندDSDV) شماره ی ترتیب به گره ها کمک می کند تا یک مسیر تازه به سمت مقصد را داشته باشند و از حلقه های مسیریابی اجتناب کنند. بنابراین، هرگره یک شماره ی ترتیب برای خود و مبدأ (ها) و مقصد(های) مربوطه نگهداری میکند. اگر یک گره، یک درخواست مسیر جدید داشته باشد یا قطع ارتباط با یکی از همسایگانش را تشخیص دهد، شمارهی ترتیب خود را افزایش می دهد. برای برقراری مسیری به مقصد، گره مبدأ، یک بسته ی درخواست مسیر، (RREQ) را در شبکه Broadcast میکند. بسته ی RREQ *شامل* ID *مبدأ* ID مقصد، شمارهی ترتیب مبدأ و آخرین شمارهی ترتیب گره مقصد که گره مبدأ از آن آگاهی دارد، می باشد. وقتی که یک گره، بسته ی RREQ را دریافت می کند، یک ورودی در کَشِ درخواست مسیر می سازد و آدرس گره ای که درخواست را از آن دریافت کرده، به عنوان گام بعدی به سمت مبدأ در جدول مسیریابی خود ذخیره می کند. اگر گره دریافت کننده ی بسته، نود مقصد باشد و یا مسیری تازه به سمت مقصد مورد نظر را داشته باشد، بوسیله ی بسته RREP(پاسخ مسیر) جواب می دهد .در غیراین صورت، بسته ی RREQ را برای همسایگانش Broadcast خواهد کرد. وقتی که یک نود یک بسته ی RREP را دریافت میکند، آدرس نودی را که بسته RREP را از آن دریافت کرده به عنوان گام بعدی در جهت

مقصد در جدول مسیریابی خود ثبت کرده و بسته ی RREP را به نود بعدی در جهت نود مبدأ می فرستد ((unicast می کند). هنگامی که نود مبدأ، بسته ی RREP را دریافت می کند، شروع به ارسال بسته های داده در طول مسیر ردگیری شده بوسیله ی بسته ی RREP می کند. به علت متحرک بودن نودها، مسیر های ساخته شده توسط یک نود مبدأ ممکن است از بین برود. اگر یک نود(نه الزاماً نود مبدأ) برای ارسال داده اقدام کند و اخطارPacket–drop را از لایه ی MAC (کنترل دستیابی به رسانه) دریافت کند، متوجه خرابی مسیر می شود.

هنگامی که یک نود متوجه خرابی مسیر می شود، بسته های مربوط به مقصد را نادیده گرفته و یک بسته ی خطای مسیر (*RERR*) برای آن مقصد تولید کرده و به سمت مبدأ می فرستد. به محض دریافت یک RERR نود مبدأ، بسته های داده مربوط به آن مقصد را بافر کرده و مجدداً برای برقراری مسیر به سمت مقصد تلاش می کنند.

DSR : مسیریابی از مبدأ پویا[1] (DSR) یکی از اولین پروتکلهای مسیریابی reactive برای شبکه های ad–hoc می باشد. در DSR نودها از بسته های RREQ،RREP و RERR برای برقراری و حفظ مسیریابی به سمت مقصد استفاده می کنند. با این حال، برخلاف AODV بسته ی RREQ لیستی از ID نودهای طول مسیر مبدأ به سمت مقصد را جمع آوری کرده و بسته ی RREP مربوطه این لیست ID ها را به نود مبدأ برگشت می دهد. وقتی که نود مبدأ بسته ی RREP را دریافت می کند، شروع به ارسال بسته های داده به سمت مقصد می کند، به این صورت که مسیر از مبدأ تا مقصد

[1] Dynamic Source Routing

را در هدر بسته جاگذاری می کند. مسیر قرار گرفته در هدر بسته ی داده به عنوان مسیر از مبدأ شناخته می شود.

هر نود شبکه، مسیر به سمت نودهای دیگر را بوسیله ی نگهداری یک حافظه ی (کَش) مسیر پویا، ذخیره می کند. یک نود مسیرها به سمت دیگر نودها را هنگامی یاد می گیرد که یک بسته ی RREQ برای یک مقصد مشخص م یفرستد و یا زمانی که در یک مسیر فعال به سمت آن مقصد قرار می گیرد. به علاوه، یک نود ممکن است بوسیله ی استراق سمع مبادلات در طول مسیری که بخشی از آن نمی باشد، نیز مسیری را یاد بگیرد.

۲-۳-۳ پروتکلهای **Hybrid**

پروتکلهای ترکیبی، مزایای روشهای مختلف پروتکلهای مسیریابی را به صورت یک پروتکل واحد ترکیب می کنند.

پروتکل مسیریابی منطقه ای[۱] (ZRP) از این دسته پروتکلها است که هر دو روش پروتکلهای مسیریابی reactive و Proactive را ترکیب میکند.ZRP از اکتشاف Proactive درون یک همسایگی محلی یک نود استفاده می کند، و از یک پروتکل reactive برای ارتباط بین این همسایگی ها استفاده می کند. همسایگی های محلی ، Zone ها نامیده می شوند و هر نود ممکن است در چندین Zone هم پوشا قرار گرفته باشد. ZRP از این واقعیت نشأت می گیرد که :« بیشتر ارتباطات، بین نودهای نزدیک به هم اتفاق می افتد. تغییرات توپولوژی در همسایگی یک نود از بیشترین اهمیت برخوردار است. اضافه یا حذف شدن یک نود در دیگر سوی شبکه، تأثیر کمی در همسایگی های محلی دارد.»

[۱] Zone Routing Protocol

کارایی ZRP بستگی به انتخاب شعاعی دارد که براساس آن تصمیم گرفته میشود که از حالت Proactive به حالت reactive تغییر حالت داده شود. با انتخاب محتاطانه ی شعاع، ZRP می تواند به اثربخشی و مقیاس پذیری بهتری نسبت به پروتکلهای Proactive و reactive دست یابد.

۲-۳-٤ پروتکلهای **Location- based**

پروتکلهای مسیریابی بر مبنای موقعیت، از موقعیت نودها در شبکه استفاده کرده و از اطلاعات توپولوژی کمترین استفاده رامی کنند.پروتکلهایی که از چنین طراحی استفاده می کنند، ایرادات ناشی از تغییر مکرر توپولوژی شبکه را از بین می برند. GPSR، DREAM و LAR نمونه هایی از این نوع پروتکل ها می باشند. در پروتکلهای مبتنی بر موقعیت، نودها اطلاعات توپولوژی محلی (یک یا دو گام) را به کمک یک پروتکل سلام[۱] حفظ می کنند. برای مسیریابی یک بسته به سمت مقصد، نود مبدأ از ارسال حریصانه[۲] برای انتخاب گام بعدی به سمت مقصد استفاده می کند. در ارسال حریصانه، یک نود، گام بعدی در جهت مقصد را طوری انتخاب می کند که در بین همسایگانش به لحاظ جغرافیایی به مقصد نزدیکتر باشد. از آنجائی که هیچ مسیر از پیش مشخص شده ای از مبدأ به مقصد وجود ندارد، هر بسته ممکن است بسته به توپولوژی شبکه، یک مسیر متفاوت را دنبال کند.

[۱] Hello protocol
[۲] Greedy forwarding

دو حالت در مسیریابی مبتنی بر موقعیت وجود دارد، (a) موقعیت مبدأ، مقصد و یک جدول همسایگی محلی برای هر نود وجود دارد و بسته ها از مبدأ به سمت مقصد ارسال میشوند و(b) هر نود با استفاده از برخی سیستم های موقعیت یاب نظیرGPS موقعیت خودش را تعیین می کند و همچنین موقعیت هر نود دیگر در سیستم را نیز به دست می آورد.

حالت اول، مسیریابی مبتنی بر موقعیت نام دارد و نمونه هایی چون GFG و GPSR از این نوع اند. مسیریابی مبتنی بر موقعیت معمولاً به صورت ارسال حریصانه می باشد به همراه یک مکانیزم بازیابی برای گیر انداختن بهینه ی محلی در شرایطی که هیچ نودی در همسایگی یک نود واسطه نزدیکتر از نود ارسال کننده نباشد. حالت دوم، سرویس موقعیت [۱]نامیده شده است. برخی نمونه ها عبارتند از: GLS،DLM و RLS. از مزایای این پروتکلها (مبتنی بر موقعیت) این است که نودها نیاز ندارند که مسیرها را ساخته و نگهداری کنند و این پروتکلها در مقایسه با پروتکلهای Proactive و reactive بیشتر مقیاس پذیر [۲] می باشند.

۲-٤ مرور اجمالی بر برخی از الگوریتم های مسیریابی

۲-٤-۱ WRP

این پروتکل بر مبنای الگوریتم path-finding بنا شده با این استثنا که مشکل شمارش تا بینهایت این الگوریتم را برطرف کرده‌است. در این پروتکل هر گره, چهار جدول تهیه می‌کند: جدول فاصله، جدول مسیر یابی, جدول هزینه لینک و جدولی در مورد پیام‌هایی که باید دوباره ارسال شوند.

[۱] Location service
[۲] Scalable

تغییرات ایجاد شده در لینک‌ها از طریق ارسال و دریافت پیام میان گره‌های همسایه اطلاع داده می‌شوند.

CSGR ۲-٤-۲

در این نوع پروتکل گره‌ها به دسته‌ها تقسیم بندی می‌شوند. هر گروه یک سر گروه دارد که می‌تواند گروهی از میزبان‌ها را کنترل و مدیریت کند. از جمله قابلیت‌هایی که عمل دسته بندی فراهم می‌کند می‌توان به اختصاص پهنای باند و دسترسی به کانال اشاره کرد. این پروتکل از DSDV به عنوان پروتکل مسیریابی زیر بنایی خود استفاده می‌کند. نیز در این نوع هر گره دو جدول یکی جدول مسیریابی و دیگری جدول مربوط به عضویت در گره‌های مختلف را فراهم می‌کند. معایب : گره‌ای که سر واقع شده سربار محاسباتی زیادی نسبت به بقیه دارد و به دلیل اینکه بیشتر اطلاعات از طریق این سرگروه‌ها برآورده می‌شوند در صورتی که یکی از گره‌های سرگروه دچار مشکل شود کل و یا بخشی از شبکه آسیب می‌بینند.

STAR ۳-٤-۲

این پروتکل نیاز به بروز رسانی متداوم مسیرها نداشته و هیچ تلاشی برای یافتن مسیر بهینه بین گره‌ها نمی‌کند.

SSR ٤-٤-٢

این پروتکل مسیرها را بر مبنای قدرت و توان سیگنال‌ها بین گره‌ها انتخاب می‌کند. بنابراین مسیرهایی که انتخاب می‌شوند نسبتا قوی تر هستند. می‌توان این پروتکل را به دو بخش DRP و SRP تقسیم کرد. DRP مسئول تهیه و نگهداری جدول مسیریابی و جدول مربوط به توان سیگنال‌ها می‌باشد.SRP نیز بسته‌های رسیده را بررسی می‌کند تا در صورتی که آدرس گره مربوط به خود را داشته باشد آن را به لایه‌های بالاتر بفرستد.

TORA ٥-٤-٢

بر اساس الگوریتم مسیریابی توزیع شده بنا شده و برای شبکه‌های موبایل بسیار پویا طراحی شده‌است. این الگوریتم برای هر جفت از گره‌ها چندین مسیر تعیین می‌کند و نیازمند کلاک سنکرون می‌باشد. سه عمل اصلی این پروتکل عبارتند از: ایجاد مسیر. بروز رسانی مسیر و از بین بردن مسیر.

RDMAR ٦-٤-٢

این نوع از پروتکل فاصله بین دو گره را از طریق حلقه‌های رادیویی و الگوریتم‌های فاصله یابی محاسبه می‌کند. این پروتکل محدوده جستجوی مسیر را مقدار مشخص و محدودی تایین می‌کند تا بدین وسیله از ترافیک ناشی از سیل آسا در شبکه کاسته باشد.

۲-۵ محدودیت‌های سخت افزاری یک گره حسگر

عواملی چون اقتصادی بودن سیستم، قابلیت مورد انتظار، تعداد انبوه گره‌ها و نهایتا عملی شدن ایده‌ها در محیط واقعی، موجب گشته هر گره یکسری محدودیت‌های سخت افزاری داشته باشد. این محدودیت‌ها در ذیل اشاره شده و در مورد هرکدام توضیحی ارائه گردیده‌است :

– هزینه پائین: بایستی سیستم نهایی از نظر اقتصادی مقرون به صرفه باشد. چون تعداد گره‌ها خیلی زیاد بوده و برآورد هزینه هر گره در تعداد زیادی (بالغ بر چند هزار) ضرب می‌گردد، بنابراین هر چه از هزینه هر گره کاسته شود، در سطح کلی شبکه، صرفه جویی زیادی صورت خواهد گرفت و سعی می‌شود هزینه هر گره به کمتر از یک دلار برسد.

– حجم کوچک: گره‌ها به نسبت محدوده‌ای که زیر نظر دارند، بخشی را به حجم خود اختصاص می‌دهند. لذا هر چه این نسبت کمتر باشد به همان نسبت کارایی بالاتر می‌رود و از طرفی در اکثر موارد برای اینکه گره‌ها جلب توجه نکند و یا بتوانند در برخی مکان‌ها قرار بگیرند نیازمند داشتن حجم بسیار کوچک می‌باشند.

– توان مصرفی پائین: منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا بایستی از انرژی وجود به بهترین نحو ممکن استفاده گردد.

– نرخ بیت پائین: به خاطر وجود سایر محدودیت‌ها، عملا میزان نرخ انتقال و پردازش اطلاعات در گره‌ها، نسبتا پایین می‌باشد.

– خودمختار بودن: هر گره‌ای بایستی از سایر گره‌ها مستقل باشد و بتواند وظایف خود را طبق تشخیص و شرایط خود، به انجام برساند.

– قابلیت انطباق: در طول انجام نظارت بر محیط، ممکن است شرایط در هر زمانی دچار تغییر و تحول شود. مثلا برخی از گره‌ها خراب گردند. لذا هر گره بایستی بتواند وضعیت خود را با شرایط بوجود آمده جدید تطبیق دهد.

۲-٦ روشهای مسیریابی در شبکه های حسگر

در مسیریابی در شبکه‌های ادهاک نوع حسگر سخت افزار محدودیت‌هایی را بر شبکه اعمال می‌کند که باید در انتخاب روش مسیریابی مد نظر قرار بگیرند ازجمله اینکه منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا روش مسیریابی پیشنهادی در این شبکه‌ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از منابع گره باشد و اگر گره منابع کافی نداشت بسته را به آن برای ارسل به مقصد نفرستد.

۲-٦-۱ روش سیل آسا

در این روش یک گره جهت پراکندن قسمتی از داده‌ها در طول شبکه، یک نسخه از داده مورد نظر را به هر یک از همسایگان خود ارسال می‌کند. هر وقت یک گره، داده جدیدی دریافت کرد، از آن نسخه برداری می‌کند و داده را به همسایه‌هایش (به جز گرهی که داده را از آن دریافت کرده‌است) ارسال می‌کند. الگوریتم زمانی همگرا می‌شود یا پایان می‌یابد که تمامی گره‌ها یک نسخه

از داده را دریافت کنند. زمانی که طول می‌کشد تا دسته‌ای از گره‌ها مقداری از داده‌ها را دریافت و سپس ارسال کنند، یک دور نامیده می‌شود. الگوریتم سیل آسا در زمان O(d) دور، همگرا می‌شود که d قطر شبکه‌است چون برای یک قطعه داده d دور طول می‌کشد تا از یک انتهای شبکه به انتهای دیگر حرکت کند. سه مورد از نقاط ضعف روش ارسال ساده جهت استفاده از آن در شبکه‌های حسگر در زیر آورده شده‌است : **انفجار** : در روش سنتی سیل آسا، یک گره همیشه داده‌ها را به همسایگانش، بدون در نظر گرفتن اینکه آیا آن همسایه، داده را قبلا دریافت کرده یا خیر، ارسال می‌کند. این عمل باعث بوجود آمدن مشکل انفجار می‌شود. **هم پوشانی**: حسگرها معمولا نواحی جغرافیایی مشترکی را پوشش می‌دهند و گره‌ها معمولا قطعه داده‌هایی از حسگرها را دریافت می‌کنند که با هم هم پوشانی دارند. **عدم اطلاع از منابع**: در روش سیل آسا، گره‌ها بر اساس میزان انرژی موجودی خود در یک زمان، فعالیت‌های خود را تغییر نمی‌دهند در صورتی که یک شبکه از حسگرهای خاص منظوره، می‌تواند از منابع موجود خود آگاهی داشته باشد و ارتباطات و محاسبات خود را با شرایط منابع انرژی خود مطابقت دهد.

۲-۶-۲ روش شایعه پراکنی

این روش یک جایگزین برای روش سیل آسا سنتی محسوب می‌شود که از فرایند تصادف برای صرفه جویی در مصرف انرژی بهره می‌برد. به جای ارسال داده‌ها به صورت یکسان، یک گره شایعه پراکن، اطلاعات را به صورت تصادفی تنها به یکی از همسایگانش ارسال می‌کند. اگر یک گره

شایعه پراکن، داده‌ای را از همسایه اش دریافت کند، می‌تواند در صورتی که همان همسایه به صورت تصادفی انتخاب شد، داده را مجددا به آن ارسال کند.

۲-٦-۳ روش اسپین

روش SPIN خانواده‌ای از پروتکل‌های وقفی است که می‌توانند داده‌ها را به صورت موثری بین حسگرها در یک شبکه حسگر با منابع انرژی محدود، پراکنده کنند. همچنین گره‌های SPIN می‌توانند تصمیم گیری جهت انجام ارتباطات خود را هم بر اساس اطلاعات مربوط به برنامه کاربردی و هم بر اساس اطلاعات مربوط به منابع موجود خود به انجام برسانند. این کار باعث می‌شود که حسگرها بتوانند داده‌ها را با وجود منابع محدود خود، به صورت کارآمدی پراکنده کنند. گره‌ها در SPIN برای ارتباط با یکدیگر از سه نوع پیغام استفاده می‌کنند: – ADV : برای تبلیغ داده‌های جدید استفاده می‌شود. وقتی یک گره SPIN، داده‌هایی برای به اشتراک گذاشتن در اختیار دارد، این امر را می‌تواند با ارسال شبه –داده مربوطه تبلیغ کند. – REQ : جهت درخواست اطلاعات استفاده می‌شود. یک گره SPIN می‌تواند هنگامی که می‌خواهد داده حقیقی را دریافت کند از این پیغام استفاده کند. – DATA: شامل پیغام‌های داده‌ای است. پیغام‌های DATA محتوی داده حقیقی جمع آوری شده توسط حسگرها هستند.

۲-٦-٤ روش انتشار هدایت شده

در این روش منابع و دریافت کننده‌ها از خصوصیات، برای مشخص کردن اطلاعات تولید شده یا موردنظر استفاده می‌کنند و هدف روش انتشار هدایت شده پیدا کردن یک مسیر کارآمد چندطرفه بین فرستنده و گیرنده هاست. در این روش هر وظیفه به صورت یک علاقه مندی منعکس

می‌شود که هر علاقه مندی مجموعه‌ای است از زوج‌های خصوصیت–مقدار. برای انجام این وظیفه، علاقه مندی در ناحیه موردنظر منتشر می‌شود. در این روش هر گره، گره‌ای را که اطلاعات از آن دریافت کرده به خاطر می‌سپارد و برای آن یک گرادیان تشکیل می‌دهد که هم مشخص کننده جهت جریان اطلاعات است و هم وضعیت درخواست را نشان می‌دهد (که فعال یا غیرفعال است یا نیاز به بروز شدن دارد). در صورتی که گره از روی گرادیان‌های قبلی یا اطلاعات جغرافیایی بتواند مسیر بعدی را پیش بینی کند تنها درخواست را به همسایه‌های مرتبط با درخواست ارسال می‌کند و در غیر این صورت، درخواست را به همه همسایه‌های مجاور ارسال می‌کند. وقتی یک علاقه مندی به گره‌ای رسید که داده‌های مرتبط با آن را در اختیار دارد، گره منبع، حسگرهای خود را فعال می‌کند تا اطلاعات موردنیز را جمع آوری کنند و اطلاعات را به صورت بسته‌های اطلاعاتی ارسال می‌کند. داده‌ها همچنین می‌توانند به صورت مدل خصوصیت–نام ارسال شوند. گرهی که داده‌ها را ارسال می‌کند به عنوان یک منبع شناخته می‌شود. داده هنگام ارسال به مقصد در گره‌های میانی ذخیره می‌شود که این عمل در اصل برای جلوگیری از ارسال داده‌های تکراری و جلوگیری از به وجودآمدن حلقه استفاده می‌شود. همچنین از این اطلاعات می‌توان برای پردازش اطلاعات درون شبکه و خلاصه سازی اطلاعات استفاده کرد. پیغام‌های اولیه ارسالی به عنوان داده‌های اکتشافی برچسب زده می‌شوند و به همه همسایه‌هایی که به گره دارای داده، گرادیان دارند ارسال می‌شوند یا می‌توانند از میان این همسایه‌ها، یکی یا تعدادی را برحسب اولویت جهت ارسال بسته‌های اطلاعات انتخاب کنند. (مثلا همسایه‌هایی که زودتر از بقیه پیغام را به این گره ارسال کرده‌اند) برای انجام این کار، یرنده یا سینک همسایه‌ای را جهت دریافت اطلاعات ترجیح می‌دهد تقویت می‌کند. اگر یکی از گره‌ها در این مسیر ترجیحی از کار بیفتد، گره‌های شبکه به طور موضعی مسیر از کار افتاده را بازیابی

می‌کنند. در نهایت گیرنده ممکن است همسایه جاری خود را تقویت منفی کند در صورتی که مثلا همسایه دیگری اطلاعات بیشتری جمع آوری کند. پس از ارسال داده‌های اکتشافی اولیه، داده‌های بعدی تنها از طریق مسیرهای تقویت شده ارسال می‌شوند. منبع اطلاعات به صورت متناوب هر چند وقت یکبار داده‌های اکتشافی ارسال می‌کند تا گرادیان‌ها در صورت تغییرات پویای شبکه، بروز شوند.

فصل سوم: توپولوژی و طراحی الگوریتم های مسیریابی

۳-۱ مقدمه

شبکه بی سیم Adhoc یا به طور ساده تر یک شبکه Adhoc مجموعه ای ازنودهای پراکنده از نظر جغرافیایی است که با یکدیگر از طریق یک بستر بی سیم ارتباط دارند. یک شبکه Adhoc با شبکه cellular (سلولی) تفاوت دارد و تفاوتش این است که هیچ چارچوب سیم کش ای وجود ندارد و ارتباطات شبکه از طریق نیروی باطری ها محدود می شوند . یک نمونه کلاسیک از شبکه هایAdhoc شبکه جنگنده ها در جنگ در میدان رزم است . به علاوه توانایی بررسی های جدید در این حوزه شامل توسعه شبکه های packet radio (PRNS) و شبکه های رادیویی ماندگار است . از آنجا که حوزه های کاربردی نظامی هنوز اصلی ترین حوزه مطالعاتی را در شبکه هایAdhoc در بر می گیرد ولی توسعه سریع تلفن های موبایل و افزایش کامپیوترهای دستی ، موضوع جدیدی در مطالعات تجاری شبکه های Adhoc به وجود آورده است برای مثال بلایای زندگی ، کنفرانس ها ، شبکه های خانگی ، شبکه های حسی ، شبکه های محلی شخصی و...

فقدان یک چارچوب ثابت در شبکه های Adhoc مشخص می کند که هر محاسبه درشبکه ، نیاز به انجام در یک حالت غیر متمرکز دارد . به علاوه بسیاری از مشکلات اساسی که در شبکه های Adhoc وجود ندارد به عنوان مشکلات محاسبات توزیع شده معرفی شده است.

البته شبکه هایAdhoc ویژگی های به خصوصی دارند که مطالعه آنها را متمایز از سایرشبکه ها می سازد در این فصل ما به بعضی ویژگی های شبکه های Adhoc ، مشکلات ویک نمونه بررسی شده می پردازیم. ما به **۲** حوزه مشکل توجه داریم :

۱- کنترل شکل Topologyمحاسبه و پشتیبانی از نودهای به هم متصل در شبکه و مسیریابی.

۲- مدل سازی شبکه های Adhoc <Modeling Adhoc ned works> : یک شبکهAdhoc را می توان یک مجموعه ای از نقاط در فضای۲بعدی (یا سه بعدی) اقلیدسی در نظر گرفت که هر نقطه یک نود شبکه را نمایش می دهد . هر نود می تواند به وسیله قدرت محاسباتی و ارتباطی اش شناسایی شود . قدرت محاسباتی یک نود عبارت است از سطح کد گذاری و رمزنگاری ای که نود می تواند انجام دهد ،**۲** کار کلیدی در شبکه های بی سیم و خصوصیات ارتباطی شبکه ها به وسیله ویژگی های کانال رادیویی و محیط و قدرت باطری و کنترل نیروی نودهای اختصاصی مدیریت می شود.

۲-۳ توسعه رادیویی و موانع

مدلسازی کانال رادیویی بی سیم کار پیچیده ای است محیط انتقال بی سیم به .pathloss مسیر ، صدا ، کانه و قفل شدن به دلیل مشکلات فیزیکی حساس است pathloss نسبت به قدرت دریافت به قدرت ارسال است . آن بر کیفیت سیگنال های دریافتی تاثیر می گذاردو تابع فاصله ارسال است اگرPR قدرت دریافت سیگنال وPTقدرت ارسال باشد سپس در فضای آزاد (پاک و در خط مستقیم) خواهیم داشت:

فرمول شماره ۱

$$P_R = O\left(\frac{P_T}{d^{\alpha}}\right)$$

ثابت پنهان علامت بزرگ big-oh است که در فرمول بالا وابسته به دست آوری آنتن وفرکانس کاری است و a=2 **است.**

همچنین توجه کنید که مقادیر مشخص ثابت های پنهان همچنین به بخش هایی که پارامترهای مختلف تاثیر دارد (مثل d,p'T,p'R) محیط مطلوب تنها فضای باز نیست بلکه شامل بازخورد ، تشعشع و پراکنده سازی ساختمان ها ، زمان و ناحیه و سایر اجسام موجود در محیط است .اغلب مدل انتشار ، که α در آن از ۲تا٤ تغییر می کند برای مدلسازی چنین محیط هایی کاملا مناسب است.

به علاوه درPath loss نرخ بیت خطا در ارسال و افزایش کیفیت دریافت در هر نود ، به قدرت نویز و قدرت ارسال و مکان سایر نودها در جوار vتاثیر دارند . ما در ادامه به ۳ مدل ساده که وقتی ارسال شده در مقصد با موفقیت دریافت شد توصیف می کنیم.

$\{X_K, K \in T\}$ مجموعه نودهایی را که در واحد زمان ، همزمان ارسال می کنند را مشخص می کند سپس در مدل فیزیکی ، ارسال به وسیله یک نودXi توسط۲با موفقیت دریافت می شود اگر:

فرمول شماره**۲**

$$\frac{\frac{pi}{d(xi,2)^{\alpha}}}{N+\sum_{K\in T,K\neq i}\frac{p_k}{d(x_k,2)^{\alpha}}}\geq\beta$$

که β مقدار آستانه برای سیگنال ثبت تصادم برای دریافت کننده های موفق و N سطح قدرت نویز است و β عموما بین ۱/. و ۱۰در حال تغییر است و به تکنولوژی انتقال بی سیم مورد استفاده بستگی دارد اغلب با دسی بل مشخص می شود در این جا به βکمترین مقدار لگاریتم ده دهی سمت چپ معادله**۲ است** مقدار β به شکل کد گذاری و ماژول بندی نیز بستگی دارد معادله ۲حالتی از یک مدل انتقال بدبین را نشان می دهد که فرض می کند که سیگنال های تمام نودهای $2X_K : K \neq i$ به صورت مخربی با سیگنال xi برخورد کند . در عمل سیگنال هایی که به هم برخورد می کنند یکدیگر را نابود می کنند و تاثیرشان کوچک می شود ، حتی در مقایسه با سیگنال های noise.

یک مدل بهینه تر سطح بالا ، مدلی است که فقط به تصادم های جفت جفت توجه دارد درزیر گفته شده در product modle چیزی که نود xi ارسال کرده توسط نود دریافت می شود اگر

فرمول شماره۳

$$\frac{pi}{d(xi,y)^{\alpha}}\geq(1+\Delta)\frac{p_k}{d(x_k,y)^{\alpha}}$$

برای هر نود دیگرxk ارسال همزمان روی یک پهنای باند که در آن $\Delta > 0$ یک محیط پایدار پروتکل مشخص را برای جلوگیری از تصادم ارسال دوری می کند.

اگر فرض کنیم که قدرت انتقال هر نود ایده آل و ثابت است در این صورت معادله۳ می تواند به عنوان نیاز یک باند پایین تر در نسبت $d(x_k,2)$ و $d(x_i,2)$.

در حالت دیگری از معادله۳ فرض می شود که ارسال توسط نود xi با قدرت pi تمام نودهایی را که با قدرت $(1+\Delta)pi$ از x_i قابل دسترسی اند را قفل می کند black می کند از کار می اندازد .

mohility ۳-۳

۲روش برای مدلسازی mohility قابلیت سیار بودن در شبکه های adhoc وجود دارد یک روش که اغلب در شبیه سازی استفاده می شود مدل سازی حرکت یک نود فلش حرکت است که جهت و سرعت نود را نشان می دهد هر نود به طور مستقل فلش حرکتی را که حرکتش را در زمان تعریف می کند برای خود انتخاب می کند مدل ها برای حرکت های گروهی جایی است که گروه نودها ممکن است هم جهت با هم باشند انتخاب می شوند .

برای یک آنالیز تئوریکی ، مدلهای جزئی تر حرکت ، چنانچه در بالا گفته شد بسیار مشکل خواهد بود به جای این mobility می تواند با تغییراتی که در گراف انتقال مخصوص mobility خواهد بود به جای این صورت می گیرد نمایش داده می شود برای مثال ما می توانیم قدرت پروتکل

مسیریابی در شبکه Adhoc را با توجه به میزان کاری که مورد نیاز است انجام شود وقتی یک تغییر ابتدایی در گراف انتقال صورت می گیرد آنالیز کنیم که عبارت است از حذف یک یال یا اضافه شدن یا تغییراتی که در همجواری راس گراف صورت می گیرد.

مدل جالب دیگر برای فهمیدن حرکت نود ، مدل شبکه ای adversarial گفته شده اخیر است که در آن دشمن ممکن است گراف را به حالتی غیر قابل پیش بینی تغیر دهد. حرکت خود سرانه یک نود می تواند با تغییرات رقابتی در شکل نشان داده شود .

٤-٣ topology control کنترل شکل (topology)

نبود یک چارچوب متمرکز باعث می شود که یک شبکه Adhoc یک topology مشخص و خاص نداشته باشد به علاوه یک کار مهم در شبکه Adhoc که از نودهای پراکنده جغرافیایی تشکیل شده است مشخص نمودن یک topology معین با استفاده ازپروتکل های مسیریابی سطح بالا است که تعریف شده اند در این بخش به کنترل topology مسئله تعیین یک topology در شبکه Adhoc می پردازیم.

اگرv مجموعه نودها را مشخص کند و G گراف V باشد در آن بین نودهای V,U یکیال وجود دارد اگر و تنها اگرVبتواند به طور مستقیم با V ارتباط برقرار کند.

Tتوپولوژی ای که توسط الگوریتم کنترل توپولوژی به دست می آید نشان می دهد

کیفیت توپولوژیTمی تواند بر اساس بعضی مشخصه ها مانند اتصال کارآیی انرژی بازده و قدرت درmobility ارزیابی شود در ادامه توصیف جزئی این معیارها می پردازیم

۳.-٤-۱ اتصال و کارآیی انرژی **energy – efficiency**

شاید نیاز اساسی یک توپولوژی اتصال است صریحا ما نیاز داریم هر۲نودی که در گراف Gبه هم متصل اند درTنیز به هم متصل باشند. از آنجا که توپولوژیTشبکه مشخص پروتکل مسیریابی را نشان می دهد باید راه هایکارآیی که انرژی بین جفت هایی که به یکدیگر پیام ارسال می کنند باشد یکی از نکات مورد توجه برای کارآیی انرژی فاکتور توسعه انرژی است که تعریف خواهیم کرد انرژی نیاز است و انرژی مصرفی برای انتقال ازVبهVتابعی Polynomial خطی از فاصله U و V است . انرژی استفاده شده برای دریافت یک پکت در طول یک مسیر به صورتجمع انرژی مصرفی یال های بین U و V است برای مثال نودهای U,V یعنی EG(U,V) انرژی مصرفی در کمترین مسیر انرژی (Minimum energy path) بینV و U در G تعریف می شود.

حالا فاکتورenergy stretch در آرا ماکسیمم تعریف می کنیم برای هر UوV $\frac{E_G(U,V)}{E_T(U,V)}$ ما می خواهیم اتصال وenergy efficiency را با استفاده از یک توپولوژی ساده که پشتیبانی از آن Easy آسان است .فراهم کنیم از آنجا که یک راه مشخص برای فرموله ساختنsimplicity و maintainability وجود ندارد بعضی مسائلی که بر این اهداف تاثیر می گذارند اندازه توپولوژی است که ناشی از تعداد یال ها در T و بیشترین درجه هر نود در T است.

اتصال درجه و اندازه معیارهای معمول ارزشیابی در هر شبکه ای (چه سیمی و چه بی سیم) هستند فاصله بین ۲ نود طول کوتاه ترین مسیر بین ۲ نور است مشکل طراحی توژولوژی با فاکتور laws retch توسط طراحان شبکه بسیار مورد بررسی قرار گرفته. یکی از مناسب ترین ها در این حوزه تصور آچار (spanner) است. گراف G مجموعه ای از نودها داده شده است یک spanner زیر گراف H از G است که فاصله بین هر ۲ نود در آن فاکتور ثابتی از فاصله بین۲ نود در G است. با این تفاوت که فاکتور distance stretch در spanner از درجه o(۱) است . اگر ما مدل را که در بخش۲توصیف شد استفاده کنیم با افزایش مسافت نیرو رقیق تر کمتر می شود پس می توان نشان داد که یک توپولوژی با یک فاکتور distance stretch o(۱) فاکتور energy stretch O(۱) نیز دارد.

چیزی که مسائل کنترل توپولوژی را درAdhoc از سایر طراحی های شبکه مجزا می سازد این است که ما باید توپولوژی را در یک محیط کاملا توزیع شده معین کنیم . تعدادی از الگوریتم های کنترل topology اخیرا ارائه شده اند .

این الگوریتم ها بر مبنای تکنیک های محاسبات جغرافیایی طراحی شده اند که توپولوژی های اتصال را در فضای گوش توصیف می کنند این تکنیک ها و توپولوژی ها در سطح سادگی ، کیفیت توپولوژی و مناسب بودن آنها برای طراحی در فضاهای توزیع شده با یکدیگر تفاوت دارند . حالا به بررسی بعضی ساختارهای جغرافیایی و توپولوژی هایی که توسط آنها ارائه می شوند می پردازیم.

ب)رای نودهایی که در فضای اقلیدسی (euclidoam) اند تعدادی گراف ابتدایی ارائه شده است این ها شامل گراف های همجوار و گراف های Garbriel هستند v مجموعه relative neigh) (RNG)

borhood Gra) یالی بین ۲نود V,U هست اگر هیچ نودی مثل d(v,w)}< d(u,v) max{d(u,w وجود نداشته نباشد گراف Garbriel (GG) یالی بین نودهای V,U دارد و اگر و تنها اگر هیچ نود W ای که d2(v,w) , d2(u,w)}< d2(u,v) وجود نداشته باشد .هم RNG و هم GG با استفاده از الگوریتم های محلی (local algoritm) ساده است.

مجموعه ای از نودها در فضای ۲ بعدی نشان داده شده فرض کنید فضای دور هر نود به مجموعه sector هایی با زوایای (angle) ثابت و نود را به نزدیکترین همسایه اش در هر sector ربط می دهیم اگر هر sector زاویه ای $\theta < \mu/3$ داشته باشد گراف حاصل به نام $\theta - graph$ (گراف θ) نامیده می شود و به صورت گراف همبند با stretch $1/(1-2\sin(\theta/2))$ است که گراف θ یک panner است.

۳-٤-۲ بازده **throughput**

علاوه بر همبندی و energy efficiency ما دوست داریم یک توپولوژی با ظرفیت بالا یا بازده باید مسیریابی در آن صورت بگیرد در توپولوژی بر اساس ویژگی های شبکه که مطالعه می شود و الگوهای ترافیک مورد توجه می توان بازده یک شبکه Adhoc را به صورت های مختلف تعریف کرد.

در[۲۱] Gupth و kumar بازده شبکه Adhoc را بر مبنای فیزیکی و مدل های پروتکل انتشار که آنها بازده را با مفهوم ارسال بیت توصیف کرد هاند فرض کنید که در شبکه ارسال bid – meter این گونه تعریف می شود که وقتی۱ بیت مسافت ۱ متر را طی می کند. بنابراین بازده یک شبکه می

تواند به این صورت تعریف شود که تعداد bid – meter هایی که در هر ثانیه منتقل می شوند . در این موضوع نمایش داده شده که برای n ود ایده آل که به صورت تصادفی در یک محیط پراکنده شده اند هر نود از رنج انتقال ثابتی استفاده می کند بازده تعریفی برای هر منبع با bid-distance محاسبه می شود که نسبت معکوسی با $\sqrt{n \log n}$دارد نشان داده شده که اگر نودهایی که به عنوان منبع و مقصد انتخاب می شوند نیز به صورت بهینه انتخاب شوند ماکسیمم نرخ bid-distance که توسط شبکه در هر زمان وجود دارد $\theta(\sqrt{n})$ خواهد بود علاوه میانگین bid-distance با $\sqrt{n}$ نسبت معکوس دارد نتایج به دست آمده نشان می دهد تصور در مورد الگوهایترافیک با مکان میانگین بازده برای هر کاربر با افزایش تعداد کاربران کاهش می یابد.

۳-٤-۳ قدرت **Robustness to mobility**

یک چالش دیگر در طراحی الگوریتم های کنترل توپولوژی اطمینان حاصل کردن از قدرت mobility نودهاست یک معیار از قدرت توپولوژی توسط بیشترین تعداد نودها است که نیاز به تغییر اطلاعات توپولوژی نشان دارند که نتیجه اش تغییر مکان یک نود است. این تعداد که از آن با عنوان adaptability یاد می شود به تعداد همسایه های نود V و مکان نودهای وابسته بستگی دارد .الگوریتم های کنترل توپولوژی بر مبنای گراف های تخمینی است از آنجا که یک تغییر مکان یک نود فقط نیاز دارد که همسایه های آن یال هایشان را در توپولوژی پیدا کنند هم همسایگان جدید و هم همسایگان قدیم نود تغییر یافته . توپولوژی Gaottal پیچیده تر است چون بر مبنای دسته بندی سلسله مراتبی نودها صورت می گیرد . آنها نشان داده اند که تعداد نودهایی که نیاز به update شدن در گراف را در اثر تغییر دارند وابسته به تعداد نودهایی اند که در حال حاضر همسایه نود mobile هستند که زمان به

روز رسامی هر نود ثابت است علاوه بر پشتیبانی توپولوژی mobility مستلزم تغییراتی در مسیرهای مسیریابی است.

۳-۵ Routing product پروتکل های مسیریابی

در بخش قبلی ما در مورد توپولوژی هایی که ویژگی های دلخواهی در مورد اتصال ،

کفایت انرژی و بازده دارند صحبت کردیم حالا در مورد طراحی الگوهای مسیریابی که این خصوصیات را به کار می گیرند بحث می کنیم.

چگونه ما کیفیت پروتکل مسیریابی شبکهAdhoc را می سنجیم ؟ یک چارچوب آنالیز هزینه درخواست های شخصی مسیریابی براساس معیارهای از جمله میزان تطبیق سازی و حافظه overhead است.

حافظه overhead اندازه بیت ها از تمام ساختارهای داده ای است که در پروتکل مسیریابی استفاده می شود و در مورد توازن (trade off) میان معیارهای کارآیی بحث خواهیم کرد.

۳-۵-۱ پروتکل های مسیریابی مسطح **flat routing protocols**

برای یک شبکه Adhoc توپولوژی ارائه شده که با گراف بدون جهت(V,E) =G الگوی مسیریابی باید راه بیم۲ نقطه را به صورتی که در شبکه های سیم کشی انجام می دهد اجرا کند۲ نمونه که در پروتکل مسیریابی دیده می شود بردار فاصله (DV) (vector Distance) و حالت لینک

(LS) (link state) هستند هم الگوریتم های DV و هم LS تیاز به تعویض مداوم اطلاعات مسیریابی کلی در تمام شبکه دارند این نودهای اختصاصی امکان پشتیبانی از نقشه شبکه را در هر حالتی می دهد برای شبکه های Adhoc پروتکل های مسیریابی Proactive از نمونه های LS یاDV استفاده می کنند و تلاش می کنند تا اطلاعات مسیریابی را برای تمام نودها به روز نگه دارند . وقتی توپولوژی یک شبکه Adhoc تحت تغییراتی پی در پی همیشگی است LS تغییرات فراوانی در حالت های ارتباطات ایجاد می کند ولی الگوریتم های DV اغلب از به روز نبودن حالت ها (به روز نشدن حالات ارتباط ها) رنج می برند اندازه شبکه و Mobility نودها ۲ عنصر موثر در طراحی پروتکل های مسیریابی هستند . در مقابل در الگوریتم های proactive پروتکل های مسیریابی reactive اطلاعات توپولوژیی و به روز رسانی اطلاعات را در صورت درخواست ارائه می کنند (on-demand) پروتکل های reactive از هزینه بالای پشتیبانی اطلاعات مسیریابی و به سبک proactive به دوراند و در عمل به خوبی کار می کنند مثال هایی از پروتکل های reactive عبارتند از :

dynamic source routing (DSR) و dynamic source routing (DSR) و TORA و Vector routing (AODV).

پیوند پروتکل های reactive وproactive مثل پروتکل Zone routing product نیز ارائه شده که از دسته بندی (clustering) و حفظ اطلاعات مسیریابی به صورت update در یک cluster در حالی که برای جمع آوری اطلاعات از نودهای دیگر دورتر distance از نمونه reactive استفاده می شود. بیشترین clustering دسته بندی ای که در حوزه شبکه های Adhoc استفاده می شود بر مبنای دسته

های مسلط (dominating sets) قرار دارد در گراف بدون جهت G=(V,E) یک دسته مسلط D از G یک زیر مجموعه از V است که به ازای هر نود $V \in V$ یا $V \in D$ یا نودی مثل $V \in D$ وجود داشته باشد که $(U,V) \in E$ باشد.

مجموعه D از مسلط ها (Dominators) مجموعه ای از cluster ها را مشخص می کند که در cluster از یک نود در D و نودهای مجاور ان را تشکیل شده است.

Dominators مسلط ها نقش رهبر دسته ها را دارند که اطلاعات عمومی مسیریابی را در خود ذخیره می کنند برای کاهش هزینه به روز رسانی پایگاه داده عمومی بر اساس تغییرات شبکه انتخاب cluster به صورت کوچکتر مطلوب است . مسئله یافتن کوچکترین cluster یک مسئله بهینه NP-Complete است.

در حوزه شبکه های Adhoc ما به الگوریتم های توزیع شده برای یافتن مجموعه کوچک cluster ها علاقه مندیم kutten و pleg یک الگوریتم توزیع شده که دارای زمان O (log) n در تمام شبکه هاست ارائه می دهند با این فرض که محاسبات شکل همزمان اند که در آن هر نود می تواند با هر همسایه ای در هر مرحله ای پیغام رد و بدل کند.

۳-۵-۲ پروتکل های مسیریابی سلسله مراتبی

نظریه custering یک سطحی به راحتی می تواند برای یک ساختار چند سطحی سلسله مراتبی طراحی شود به علاوه یک مفهوم قدیمی در ارتباطات شبکه ای است که به v0 بر می گردد. با

اینکه بسیاری از پروتکل های سلسله مراتبی اصولا برای شبکه های ثابت طراحی شده اند آنها با یکسری تغییرات مناسب می تواند برای شبکه های Adhoc مورد استفاده قرار گیرد .ایده اصلی در مسیریابی سلسله مراتبی اداره به صورت سلسله مراتبی از دسته های نود است . سطح l ام دسته ها با هم برای تعداد مشخصی از سطح l+1 ام با هم گروه می شوند $i \geq 0$ در اکثر دسته های اولیه فرض می شود که همه دسته های l ام همسایه اند بسیاری از پروتکل های مسیریابی از دسته های هم پوشان برای فراهم کردن تحمل خطا fault – tolerance تطابق پروتکل با تغییرات دینامیکی شبکه استفاده می کنند. یک ساختار کنترلی سلسله مراتبی باعث یک آدرس دهی سلسله مراتبی در شبکه می شودکه می تواند لایه الگوی مسیریابی را ایجاد کند . در اکثر الگوهای مسیریابی هر دسته یک رهبر مشخص برای خود در cluster انتخاب می کند که اطلاعات حالات شبکه را به صورت چند سطحی نمایش دهند و جمع آوری کنند.

شامل نود مقصد است با کاهش مقدار l تا جایی که پکت به دسته سطح 0 صفر که نود مقصد در آن است که خود نود مقصد است صورت می گیرد پر.وتکل های مسیریابی دردقت مکانیزهایی که در آنها اطلاعات جمع آوری می شوند و مسیر مشخصی که در فرآیندمسیریابی از آن استفاده می شود با هم تفاوت دارند.

ساختارهای کنترل سلسله مراتبی پروتکل های مسیریابی مختلف بر مینای تفاوت شان درتعداد سطوح سلسله مراتبی m اندازه و شعاع cluster ها در سطوح مختلف و میزان هم پوشانی سطوح استوارند . انتخاب های مختلف باعث توازن میان حافظه overhead و فاکتور توزیع می شوند . بسیاری از این

پروتکل ها بر مبنای هیوریستک ها هستند . از دیدگاه تئوریکی پروتکل گفته شده در توازن مناسبی میان حافظه overhead ایجاد می کنند .پروتکل مسیریابی برای شبکه هایی که ارتباطات ثابت دارند.

۳-۵-۳ پروتکل های مسیر جغرافیایی **Geographical rouding protocols**

یک روش اخیر برای طراحی پروتکل های ساده این است که overhead را کوچک می کند تا از امکان جغرافیایی شبکه Adhoc استفاده کنند در پروتکل perimeday statelass graeady (GPSR) هر نود فقط از اطلاعات در مورد همسایه شان که عبارت است از مجموعه ای از نودها که در نود مورد نظر مستقیما با آنها در ارتباط است پشتیبانی می کند با استفاده از اطلاعات مکان نود منبع به طور هرسانه پکت مورد نظر را به همسایه اش که نزدیک تر از سایرین به آن است ارسال می کند اگر ارسال هرسانه ناممکن باشد پکت به صورت قطری محل را طی می کند تا به مقصدش برسد .در حالی که GPSR اتصال را ممکن می سازد بهترین توسعه باند هر پروتکل خواهد بود GPSR با Node mobiling مطابق است چون نود فقط از اطلاعات همسایگان پشتیبانی می کنند. حتی ساده ترین روش ها نسبت به GPSR از G-graph استفاده می کنند G-graph نه تنها یک توپولوژی تعریف می کند بلکه یک پروتکل مسیریابی ساده با گسترش (Stretch) حافظه overhead G(1) نشان می دهد این روش در نشان داده شده بدترین حالت تطابق الگوهای مسیریابی حداقل مقدار ماکزیمم در درجه یک گراف است که ممکن است بزرگ باشد . که کوچک حرکت نود ممکن است احتیاج به تغییرات فراوان در گراف داشته باشد.

بدبختانه وقتی الگوریتم های کنترل توپولوژی که بر مبنای این متغیرها درست شده اند مسیرمورد نظر را مشخص می کند به عنوان یک مکانیزم سازنده برای محاسبه مسیر در حالت های توزیع شده ای که شناخته شده نیستند.

۳-۵-٤ **Adversarial modle** مدل تهاجمی

دومین چارچوب برای آنالیز الگوریتم های مسیریابی شبکه های Adhoc مدل adversary است که در توسعه یافته در حوزه شبکه های Adhoc می توانیم حرکت و الگوهای ترافیکی را با استفاده از یک adversary مدل کنیم mobility می تواند به وسیله اجازه دادن به adversary برای فعال / غیر فعال کردن یال های شبکه مدل شود . الگوهای ترافیکarbitrary می توانند با اجازه داده به adversary به منظور تعیین نرخ دریافت پکت و جفت های مبدا مقصد برای هر پکت محاسبه شوند . در عمده ترین مدل adversarir بررسی شده در این مدل به adverser این امکان داده شده که پکت را در نودها در فرمان های متناوب تزریق می کنند و می توانند مقدار یال های ورودی و خروجی را به ماکسیمم مقدار Δبرای هر نود برسانند مقصد هر پکت توسط adversary انتخاب می شود. محدودیت دیگری نیز وجود دارد که اندازه با فرد هر نود یک مقدار محدود مثل B خواهد بود اگر در هر زمانی تعداد پکت های موجود با فراز B بیشتر شود، پکتهای اضافی باید بیرون انداخته شوند .توپولوژی شبکه ای adversarial در برابر طبیعت دینامیک یک شبکه adhoc مطابقت می کند، که در آن یال ها ممکن است در هر زمان ظاهر شوند و یا از بین بروند .فرض می کنیم هیچ پکتی کم نشود، کنترل تزریقی پکت adversarial دینامیک بودن و طبیعت غیر قابل پیش بینی ترافیک شبکه را مدل می کند.

کارآیی الگوریتم مسیریابی گفته شده می توانند به وسیله یه چارچوب آنالیز رقابتی ارزیابی شود .برای رشته ی از ارسال پکتها و فعالیت یالها، OPTB ماکسیمم تعداد پکتهایی را که توسط A با در نظر گرفتن اندازه B برای بافر، دریافت شده نشان می دهد .ما A(C,S) را رقابتی می دانیم اگر برای هر 6 B, داشته باشیم. ASB(6)>C.OPTB(6)- r

برای مقادیر $r \geq 0$ که مستقل از (٦)OPTB می باشند.

بهترین نتیجه ای که برای مدل adversarial گفته شده بدست آمده الگوریتم ساده local balancing است که پکتها را از نودهایی که load بالا دارند به نودهایی که load پایین دارند می فرستد load (بارگذاری) در یک نود به وسیله ارتفاع بافر آن مشخص می شود. برای الگوریتم گفته شده در دارای پیچیدگی درجه $T \geq B + 2(\Delta - 1)$ است که L میانگین طول مسیرهایی است $0(1 - 4{,}1 + (1 + (T + \Delta)/\mathbf{B})\, L/4)$ که توسط پکتها در راه حل بهینه طی شده اند؛ عموماً درجه Δ ثابت است، پس الگوریتم درجه خواهد داشت .یک سوال مهمع حل نشده این است که چگونه کمترین مقدار S را که در الگوریتم رقابتی برای مقادیر $0<S<1$ پیدا شود.

Concluding remarles ٦-٣

از روی ایده پروتکل های مسیریابی شبکه های ثابت برای شبکه های Adhoc طراحی شده است.

فصل چهارم: امنیت در شبکه ادهاک

٤-١ مقدمه

شبکه های Ad- Hoc نمونه هایی جدیدی برای میزبان های سیار (mobile hosts) هستند. برخلاف شبکه های بی سیم موبایل قدیمی شبکه های Ad-Hoc بر مبنای هیچ ساختاری استوار نیستند(یعنی ساختارمشخصی ندارند) به جای آن، میزبان ها برای متصل نگه داشتن شبکه به یکدیگر وابسته اند.

تاکتیک های نظامی و سایر مسائل امنیتی هنوز اصلی ترین کاربرد شبکه هایAd-Hoc است با این وجود برای استفاده از این شبکه ها برای کاربردهای تجاری درخواستها و تمایلات فراوانی وجود دارد.

یکی از مهمترین دغدغه های در طراحی این شبکه ها آسیب پذیری آنها در حمله های امنیتی است.

در این بخش، ما در مورد حملاتی که یک شبکه Ad-Hoc را تهدید می کنند و اهداف امنیتی که به آنها دست یافته ایم بحث خواهیم کرد. ما چالشهای جدید و فرصتهایی که توسط این محیط شبکه ای ایجاد می شود و به دنبال روشهای جدید برای روابط امن می گردد بخصوص ما از تکرار ذاتی موجود در شبکه های Ad-Hoc استفاده می کنیم برای حمایت از مسیریابی در مقابل حمله های سرویس همچنین از رمزنگاری، مثل رمزنگاری آستانه برای

ایجاد سرویس مدیریت با دسترسی بالا و ایمن که هسته چارچوب امنیتی مان را تشکیل می دهند استفاده می کنیم.

٤-٢کمبود ایمنی در شبکه های Ad-Hoc:

ساختار شبکه Ad-Hoc طوری مجسم می شود که در آن جا پشتیبانی دستیابی بی سیم یا پشتیبان سیم دار، میسر نیست – شبکه تک کاره ، هیچ پایه و اساس از پیش تعریف شده ندارد و تمام خدمات شبکه ای در موقع اجرا پیکر بندی می شود و به وجود می آیند. از این رو بدیهی است که با فقدان پشتیبانی زیر بنایی و حملات لینک بی سیم آسیب پذیر، ایمنی در شبکه-Ad Hocنقطه ضعف ذاتی است، دستیابی به ایمنی در داخل شبکه سازی Ad-Hoc بنا به دلایل زیر مشکل آفرین است:

- توپولوژی دینامیکی و عضویت:

  توپولوژی شبکه ای Ad-Hoc خیلی دینامیک است به طوریکه متحرک بودن گروهها یا عضویت گره ها خیلی تصادفی و سریع است این امر به دینامیکی بودن نیاز برای راه حل های ایمن تاکید می کند.

- لینک بی سیم آسیب پذیر:

  حملات لینک فعال/غیر فعال نظیر استراق سمع، کلک زدن، انکار خدمات رسانی، تقلید و جعل هویت امکان پذیر هستند.

- پرسه زدن در محیط خطرناک:

هرگونه بدرفتاری بدخواهی می تواند سبب ایجاد حملات خصمانه شود یا تمام گروهها را از فراهم نمودن خدمات محروم کند.

گره های موجود در محیط متحرک با دستیابی به لینک رادیویی مشترک در تنظیم Ad-Hoc infrastructu به آسانی مشارکت می کنند. اما ارتباطات ایمن در میان گره ها مستلزم ایجاد ارتباط در لینک ارتباطات ایمن است. قبل از تعیین لینک ارتباطات ایمن، گره باید بتواند گره دیگر را شناسایی کند. در نتیجه گره، گره هویت خود و نیز مدارک مربوطه به گره دیگر را فراهم می سازد.

اما مدارک و احراز هویت ارائه شده باید مورد تایید و حفاظت قرار گیرند به طوری که اصالت یکپارچگی مدارک و هویت ارائه شده را نمی توان طبق گره گیرنده مورد سوال قرار داد هر گره می خواهد مطمئن شود که مدارک و هویت ارائه شده به گروههای دریافت کننده تطبیق داده نمی شود. از این رو لازم است ساختار ایمن برای شبکه ایی سازی تک کاره و ایمن فراهم شود.

مساله هویت فوق الذکر فورا به مساله خصوصی سازی منجر می شود بطور کلی گره سیار از انواع هویت ها استفاده می کند و آن از سطح لینک تا سطح کاربر/کاربر تغییر می کند همچنین در محیط سیار بصورت مکرر گره سیار آماده نیست تا مدارک یا هویتش را به گره سیار دیگر از نقطه نظر خصوصی سازی آشکار سازد هر گونه هویت سازگار شده باعث می شود که حمله کننده ها تهدید و خصوصی سازی برای دستگاه کاربر ایجاد کند متاسفانه استانداردهای سیار جاری هیچ گونه خصوصی سازی ممکن فراهم نمی کند و در بسیاری از موارد آشکار ساختن

هویت برای تولید لینک ارتباطات اجتناب ناپذیر است از این رو حفاظت خصوصی سازی بی درز برای مهار کردن کاربرد شبکه ای سازی تک کاره مورد نیاز است.

٤-٣ مسائل و چالشهای اصلی:

٤-٣-١ ایمنی سطح لینک:

در محیط بی سیم لینک ها نسبت به حملاتی که استراق سمع کننده به آسانی می تواند ارتباطات پیوسته را دست اندازد آسیب پذیر هستند چون هیچ حفاظتی نظیر فایروال ها یا کنترل دستیابی از شبکه Ad-Hoc وجود ندارد هر گره نسبت به حملاتی که از هر جهت یا هر گروه بدست می آیند آسیب پذیر می باشد نتایج این حملات شامل دست اندازی و هویت گره، دستکاری کردن مدارک گره، آشکار ساختن اطلاعات محرمانه یا جعل هویت گره است این نوع حملات به آسانی می توانند با جنبه های اصلی ایمنی نظیر خصوصی بودن، یکپارچگی، دسترس پذیری و محرمانگی گره سازگار شوند.

٤-٣-٢ مسیریابی ایمن:

پروتوکل های مسیر یابی پیشنهاد شده در شبکه Ad-Hoc در زمانی که هر دستگاه بصورت رله ها عمل می کند نسبت به حملات آسیب پذیر تر هستند هر گونه دستکاری کردن اطلاعات مسیر یابی می تواند کل شبکه را سازگار کند هر حمله کننده می تواند اطلاعات کاذب در اطلاعات ردیابی جایگزین کند یا با نمایش دادن مجدد اطلاعات ذخیره شده یا ثبت شده حملات

نوع سرویس را تکذیب کند همچنین گره سازگار می تواند اطلاعات نامناسب را به گره های دیگر ردیابی کند که سبب بروز خسارات جدی می شود اما راه حل های مسیر یابی پیشنهاد شده می تواند با توپولوژی دینامیکی عمل کند اما بر حسب اندازه ایمن راه حل های جزئی یا هیچ گونه راه حلی ارائه نمی دهند از این رو پیاده سازی پروتوکل مسیریابی ایمن یکی از مسائل مربوط به شبکه Ad-Hoc است.

٤-٣-٣ به طور کلی اهداف ایمنی در شبکه های **Ad-Hoc** از طریق مکانیسم‌های رمزنگاری نظیر رمزنگاری کلید مهری یا امضای دیجیتالی بدست می آیند این مکانیسم ها از طریق مدیریت کلید متمرکز را پشتیبانی می شوند. که در این جا مسئول گواهی نامه کلید عمومی را برای گره های سیار فراهم می کند بنابر این گره ها می توانند اعتماد دو طرفه بین یکدیگر ایجاد کنند هر گونه دستکاریCA می تواند ایمنی کل شبکه را به آسانی سازگار سازد.

مکانیسم های پیشنهادی بکار رفته برای هویت نظیر راز مشترک، رمزنگاری کلید عمومی، تاییدیه طرف سوم راه حل های جزئی فراهم می کنند. به طوری که آنها حساس هستند یا قادر نیستند مقیاس بندی کنند. تمام راه حل های پیشنهادی مستلزم آن است که کاربران سیار از کلید های رمزنگاری شده در شبکه Ad-Hoc بدست نمی آید که این امر به علت متحرک تصادفی گره ها است که در آن جا اتصال پیوسته حفظ نمی شود.

٤-٣-٤ خصوصی سازی:

دستکاری هویت یا هرگونه اطلاعات خصوصی باعث ایجاد تهدیدهای خصوصی سازی می شود و بعدهای مهندسی می شود تا اینکه حملات DOS به وجود می آورند از این رو خصوصی سازی یکی از مسائل اصلی در مورد شبکه ایی سازی ویژه است.

٤-٤ اهداف ایمنی:

امنیت مهمترین مقوله برای شبکه های Ad-Hoc است به خصوص برای کاربردهای که به امنیت بسیار حساس هستند برای امن سازی یک شبکه Ad-Hoc ما گزینه های زیر را در نظر گرفته ایم:

قابلیت دسترسی، محرمانگی، جامعیت تصدیق هویت

a ⟶ b

قابلیت دسترسی بقای سرویس های شبکه ای را در برابر حملات سرویسی تضمین می کند مقاومت در برابر حملات به سرویس می تواند در هر لایه ای از شبکه Ad-Hoc وجود داشته باشد در لایه های فیزیکی و کنترل دستیابی یک دشمن می تواند از گیرها و کمبودها برای دخالت در ارتباطات از طریق کانالهای فیزیکی استفاده کند. در لایه های بالاتر دشمن می تواند پروتکل مسیریابی را قطع کند و شبکه را قطع کند. در لایه های بالاتر دشمن می تواند کیفیت سرویس های سطح بالا را پایین آورد چنین هدفی اصلی ترین مدیریت سرویس است. ضروریترین سرویس برای هر چارچوب امنیتی است.

محرمانگی تضمین می کند که اطلاعات مشخصی هیچ گاه برای موجودیت های بدون مجوز قابل دسترسی نخواهند بود انتقال اطلاعات حساس از طریق شبکه مثل اطلاعات استراتژیکی یا اطلاعات تاکتیکی نظامی نیاز به محرمانگی دارند کسری از چنین اطلاعاتی می تواند برای دشمنان مفید باشد.

مسیریابی اطلاعات نیز باید در موارد مشخصی محرمانه بماند زیرا اطلاعات می توانند برای دشمن به منظور شناسایی و مشخص سازی مکان آنها درموضع هاشان در میدان جنگ کمک کنند. یکپارچگی تضمین می کند که به پیغام هیچ گاه منحرف نمی شود یک پیغام می تواند به دلیل خرابی مثل خرابی در گسترش رادیویی یا حملات بداند نشانه به شبکه اتفاق افتد احراز هویت به یک نود اجازه می دهد تا هویت نودی را که با آن ارتباط برقرار می کند شناسایی کند. بدون ابزار هویت دشمن می تواند یک نود را وارد شبکه کند و آن را به عنوان یک نود از شبکه جابرنند و به اطلاعات سری دست پیدا کنند و یا با سایر نودها ارتباط برقرار کنند.

سرانجام قابلیت عدم انکار (non-requdiation) این امکان را می دهد که منبع ارسال پیغام نمی تواند ارسال پیغام مشخصی را انکار کند و بگوید این پیغام را نفرستاده ام.

قابلیت عدم انکار برای مشخص سازی مکان نودهای موجود در شبکه بسیار مفید خواهد بود وقتی نود a یک پیغام نادرست از نودb دریافت می کند می تواند شهادت دهد که b آن پیغام را فرستاده و سایرین را نیز متقاعد سازد که b دارای مشکل یا.... است.

اهداف امینتی دیگر نیز وجود دارد که ما در اینجا به آنها نمی پردازیم.

٤-٥ چالش ها (دغدغه ها)

موارد مهم و برجسته ای که در شبکه های Ad-Hoc مطرح است و مشکلات و هم چالش ها در دستیابی به این اهداف امنیتی است.

استراق سمع پیام ها و پاسخ آنها ممکن است به دشمن امکان دسترسی به اطلاعات سری را بدهد. حملات active ممکن است به دشمن امکان از بین بردن پیام و ثانیا نودهایی که دارای حفاظ امنیتی فیزیکی کم هستند که در محیط دشمن گردش می کنند(مثلا در یک جبهه) احتمال خرابی بالایی دارند بنابراین ما فقط نباید نگران حملات خصمانه از بیرون از شبکه باشیم بکله ممکن است یک نود از داخل نیز باعث مختل شدن سیم شود بنابراین برای دستیابی به survivability، شبکه های Ad-Hoc باید یک معماری توزیع شده بدون موجودیت های متمرکز داشته باشند با ارائه هر موجودیت متمرکز به راه حل امنیتیمان، با عث آسیب پذیری سیستم خواهیم شد چنانچه این موجودیت متمرکز صدمه بیند تمام شبکه نابود خواهد شد.

سوما، یک شبکه Ad-Hoc دینامیک است و به دلیل تغییراتی که هم در شکل و هم عضویت نودها وجود دارد(مثلا نودها مداوم به شبکه اضافه می شوند و یا خارج می شوند) ارتباط میان نودها نیز تغییر می کند برای مثال وقتی نودهای مشخصی برای عضویت در شبکه پیدا می شوند برخلاف سایر شبکه های موبایل بی سیم مثل IP سیار،نودها در شبکه Ad-Hoc ممکن است به صورت دینامیک به هم بپیوندد راه حل های و تنظیمات ثابت کافی نخواهند بود. بنابراین یک مکانیزم امنیتی که با این تغییرات در پرواز باشد بسیار مناسب خواهد بود. در پایان یک شبکه

Ad-Hoc ممکن است از صدها یا هزاران نود تشکیل شده باشد مکانیزم های امنیتی باید طوری باشد که بتواند چنین شبکه های را مدیریت کنند.

-scope and roadmap

مکانیزمهای امنیتی مثل پروتکل های تصدیق هویت امضای دیجیتالی و رمزنگاری هنوز نقش مهمی در دستیابی به اطمینان یکپارچگی و قابلیت عدم انکار در ارتباطات شبکه های Ad-Hoc ایفا می کنند همچنین این مکانیزم ها به تنهایی کافی نخواهند بود.

ما بر ۲ اصل زیر تاکید خواهیم داشت اول از تکرار در شکل شبکه برای مثال چندین مسیر بین نودها، برای دستیابی به قابلیت دسترسی استفاده می کنیم دومین اصل انتشار واقعیت است با این وجود در شبکه Ad-Hoc نود تنها نداریم بلکه می توان نام شبکه Ad-Hoc را بر مجموعه ای نودها گذاشت.

در این مقاله ما توجه به حملات سرویسی به لایه فیزیکی و datalink را رد نمی کنیم و معیارهای اندازه گیری لایه های فیزیکی مشخص مثل شعاع انتشار بسیار مطالعه شده اند. (مثلا(٤٤و٦و٤٢و٧)).

٤-٦ secure routing:مسیریابی امن

برای دستیابی به قابلیت دسترسی پروتکل های مسیریاب باید هم برای تغییرات دینامیکی شکل شبکه و حملات دشمن مقاوم باشد پروتکل های مسیریابی هم برای (۳۵و۲۳) که برای شبکه های ad-hoc استفاده شده اند.

همچنین هیچ کدام از آنها برای اطلاعات ما با مکانیزم های مقابله با حملات وفق داده نشده اند پروتکل های مسیریابی برای شبکه های Ad-Hoc تحت مطالعه است در حال حاضر پروتکل مسیریاب مشخص استانداردی برای این شبکه ها وجود ندارد. بنابراین تصمیم داریم تهدیدات معمولی که این شبکه ها را تحت تاثیر قرار می دهد مشخص کنیم و راه حل هایی برای پروتکل های مسیریابی امن ارائه دهیم.

در اکثر پروتوکل های مسیریابی روترها اطلاعات را در شبکه ردو بدل می کنند تا بین نودها ارتباط برقرار شود چنین اطلاعاتی هدف مناسبی برای دشمنانی است که می خواهید شبکه را مختل کنند.

۲ منبع تهدید در پروتکل های مسیریابی وجود دارند اولی ناشی از حملات خارجی است با وارد کردن اطلاعات مسیریابی اشتباه تکرار اطلاعات مسیریابی قبلی یا ایجاد تغییر شکل در اطلاعات مسیریابی حمله کننده با موفقیت می تواند یک شبکه را تکه تکه کند یا ترافیک ورودی به شبکه را بالا ببرد و کارآیی شبکه را کاهش می دهد.

دومین و سخت ترین نوع حملات از سوی نودهای سازش پذیر داخلی صورت می گیرد که ممکن است اطلاعات مسیریابی اطلاعات مسیریابی اشتباهی به سایر نودها بفرستد. مهم و پیدا

کردن چنین اطلاعات اشتباهی مشکل است چون نودهای سازش پذیر امضاهای معتبری را با استفاده از کلیدهای اختصاصی شان تولید می کنند که اطلاعات فرستاده شده را معتبر می سازند.

برای مقابله با حملات نوع اول نودها می توانند از اطلاعات مسیریابی همانند داده های ترافیکی مثلا با استفاده از رمزنگاری مثل امضاهای دیجیتال و ... محافظت کنند. این مقابله در مورد نودهای داخلی امکان پذیر نخواهد بود. شناخت نودهای سازش پذیر به دلیل توپولوژی دینامیک و در حال تغییرشان بسیار مشکل است: وقتی بخشی از اطلاعات مسیریابی نامعتبر شناخته شد یا از سوی یک نود سازش پذیر بوده یا اینکه به دلیل تغییرات شکل topology نامعتبر شناخته شده تفکیک کردن ۲ نمونه گفته شده مشکل خواهد بود.

از سوی دیگر ما می توانیم از ویژگی های مشخص شبکه های Ad-Hoc برای رسیدن به مسیریابی ایمن استفاده کنیم توجه کنید که پروتکل های مسیریابی برای شبکه های Ad-Hoc باید اطلاعات مسیریابی اشتباهی را زمانی کند تا با تغییرات شکل شبکه مطابقت کند.

اطلاعات مسیریابی اشتباهی که توسط نودهای داخلی فرستاده می شود تا حدودی اطلاعات خارج از زمان محسوب می شود. چنانچه نودهای درست زیادی وجود دارند پروتکل مسیریابی باید بتواند مسیرها را در میان این نودهای سازگار پیدا کند این قابلیت پروتکل مسیریابی معمولا بر مبنای تکرارهای ذاتی استوار است چندگانگی سهولت جدایی، مسیرها بین نودها در شبکه های Ad-Hoc اگر پروتکل های مسیریابی چندین مسیر پیدا کنند مثل پروتکل AODV،TORA،DSR،ZRP نودها می توانند به روت (مسیر) تبدیل شوند.

Diversting Coding از چندین راه بصورت موثری بدون نیاز به فرستادن دوباره پیغام استفاده می کنند برای مثال اگر n مسیر غیر متصل بین ۲ نود وجود دارند ما می توانیم از n-r کانال برای انتقال دیتا استفاده کنیم و از r کانال دیگر برای ارسال اطلاعات اضافی استفاده کنیم حتی اگر مسیرهای مشخصی پیدا شوند گیرنده ممکن است بتواند پیام ها اعتبار سنجی کند و پیام ها را از خطاها با استفاده از اطلاعات اضافی از r کانال دیگر آمده تشخیص دهد.

۷-٤ key management service

ما از شکل های رمزنگاری، مثل امضاهای دیجیتالی برای حفاظت اطلاعات مسیریابی و دیتاهای ترافیک استفاده می کنیم استفاده از چنین شکل هایی معمولا نیاز به سرویس مدیریت کلید دارد.key managment service

از یک ساختار کلید عمومی به دلیل برتری اش در مورد انتشار کلید و دستیابی به یکپارچگی و عدم انکار(non-repudiation) استفاده می کنیم شکل های کلید مخفی کافی برای ارتباطات ام و پس از آنکه نودها هویت شناسی شدند وقتی کلیدهای خصوصی برای نودهای اختصاصی حفظ شوند استفاده می شوند و یک کلید اشتراکی سری می سازند.

در ساختار کلید عمومی هر نود یک جفت کلید عمومی/اختصاصی (public/prirade) دارد کلید عمومی می تواند به سایر نودها فرستاده شود در حالی که کلید های اختصاصی باید برای نودهای اختصاصی محافظت شود. یک موجودیت مطمئن به نام(CA) Certification authority برای مدیریت کلید وجود دارد. CA یک جفت کلید عمومی/اختصاصی دارد که

کلید عمومی اش برای تمام نودها شناخته شده است و کلید های عمومی الزامی هویت را به نودها اختصاص می دهد.

CA باید آن لاین بماند تا بر binding موجود تاثیر گذارد چون binding ها می توانند هر زمان تغییر کنند: کلید عمومی باید پس از آنکه یک نود از شبکه خارج شد پس گرفته شود و یک نود ممکن است جفت کلیدهایش را درباره های زمانی refreshکند تا احتمال حمل به کلید عمومی اش در شبکه کاهش یابد.

ایجاد یک سرویس مدیریت کلید با استفاده از یک CA در شبکه های Ad-Hoc مشکل خواهد بود CA مسئول امنیت شبکه هست اگر CA غیر قابل دسترسی باشد نودها نمی توانند کلید های عمومی اخیر را از سایر نودها بگیرند یا ارتباطی امن با سایر نودها ایجاد کنند. اگر CA سازش پذیر باشد و کلید عمومی را به یک دشمن لو دهد دشمن می تواند از آن برای ارسال پیام ها و .... معتبر استفاده کند.

یک روش استاندارد برای بالا بردن قابلیت دسترسی یک سرویس، تکثیر است ولی یک تکثیر ابتدایی و پیش پا افتاده از CA سرویس را آسیب پذیرتر می سازد: صدمه به هر یک از نسخه ها که کلید عمومی سرویس را prossess کند ممکن است باعث خرابی و ویرانی کل سیستم شود.

٤-٧-١ مدل سیستم: **System models**

سرویس مدیریت کلیدها برای شبکه های Ad-Hoc ای که آسنگرون اند قابل اجرا است چون آن یک شبکه بدون حد و مرز در دریافت پیغام و زمان پردازش پیغام است. ما همچنین فرض می کنیم که لایه شبکه گفته شد، دارای لینک های واقعی است سرویس تماما یک جفت

کلید خصوصی/عمومی دارد تمام نودها دراین سیم کلید عمومی را می دانند و هر سند موثقی را با استفاده از این کلید عمومی شناسایی می کنند نودها مثل clientها بفرستد واز آنها بخواهند که کلید عمومیشان را برای نود ارسال کنند یا پیغام درخواست به روز رسانی به آنها ارسال تا کلید عمومیشان تغییر دهند.

از داخل ، سرویس مدیریت کلیدها با یک(n،t+1) تنظیم شده (n≥3t+1) از n نود مخصوص تشکیل شده که ما آنها را server می نامیم در یک شبکه Ad-Hoc نمایش داده می شود هر سرور جفت کلید خودش را دارد و کلیه کلیدهای عمومی نودهای موجود در شبکه را ذخیره می کند عموما هر سرور کلید عمومی سرورهای دیگر را می داند بنابراین سرورها می توانند ارتباطات امنی میان خودشان برقرار کنند. ما فرض می کنیم که دشمن می تواند به t سرور در هر بازه زمانی صدمه بزند اگر یک سرور صدمه ببیند دشمن می تواند به اطلاعات محرمانه ای که در آن ذخیره شده دست یابد. سرور صدمه دیده ممکن است دیگر قابل استفاده نباشد یا رفتار Byzantine از خود نشان دهد ما همچنین فرض می کنیم دشمن قدرت محاسباتی را برای شکستن شکل رمزنگاری ای که ما استفاده کرده ایم کاهش می دهد.

سرویس درست خواهد بود اگر ۲ حالت زیر همواره برقرار باشند:

- (قدرت) سرویس همواره قادر به پردازش درخواست ها و به روزرسانی درخواست های آمده از سویclient هاست. هر query همیشه آخرین کلید عمومی به روزرسانی شده را در جواب درخواست client بر میگرداند با این فرض که در این رویداد هیچ به روزرسانی همزمانی رخ نمی دهد.

- (قابلیت اعتماد) کلید عمومی سرویس هیچ گاه به روی یک دشمن بسته نیست. بنابراین یک دشمن هیچ وقت قادر به انتشار اسنادی که توسط کلید خصوصی سرویس ها نشانه گذاری شده نیست.

٤-٧-٢ رمزنگاری آستانه **threshold cryptography**

انتشار واقعیت در سرویس مدیریت کلید ما با استفاده از رمزنگاری آستانه کامل شده یک شکل (n،t+1)از رمزنگاری آستانه به nبخش اجازه به اشتراک گذاری قابلیت اجرای یک عمل رمزنگاری را می دهد. بنابراین هر t+1 بخش این کار را به صورت متصل به هم انجام می دهد در حالی که این کار برای بیش از t بخش غیر قابل انجام است. برای سرویس تحمل t سرور صدمه دیده، ما از یک (n،t+1)شکل رمزنگاری آستانه استفاده می کنیم و کلید عمومی k را به n بخش تقسیم می کنیم(s_1 ،s_2 ،s_3 ،.... ،s_n)و هر سهم را به یک سرور می دهیم. به (s_1 ،s_2 ،s_3 ،.... ،s_n)نام (n،t+1)سهم k را نسبت می دهیم.

سرویس نشانه گذاری یک سند هر سرور پاره ای امضاء را برای رسمی کردن استفاده از کلید عمومی تقسیم شده اش تولید می کند و امضای بخشی را به یک ترکیب کننده می فرستد.

با t+1 تکه امضاء ها ترکیب کننده قادر خواهد بود که امضای سند را محاسبه کند. همچنین سرورهای صدمه دیده (حداکثر t تا از آنها) نمی توانند سندها را به تنهایی نشانه گذاری کنند، چون آنها می توانند حداکثر t بخش امضاء تولید کنند شکل ۳ نشان می دهد که چگونه سرورها یک امضاء با استفاده از یک شکل (۲و۳) امضاء تولید می کنند.

در زمان اعمال رمزنگاری آستانه باید در مقابل سرورهای صدمه دیده از خود دفاع کنیم برای مثال یک سرور صدمه دیده می تواند یک بخش امضای نادرست تولید کند استفاده از این امضا موجب ایجاد یک امضای غیر معتبر می شود خوشبختانه یک ترکیب کننده می تواند اعتبار یک امضای محاسبه شده را با استفاده از سرویس کلید عمومی بسنجد. اگر تصدیق با شکست روبه رو شد ترکیب کننده$t+1$ تکه امضای دیگر را امتحان می کند این فرآیند ادامه می یابد تا وقتی که ترکیب کننده امضای درست ر ا از $t+1$ تکه امضا بدست آورد.روش های ترکیب کردن قوی تری وجود دارد. این شماها از تکرار ذاتی در تکه های امضاها استفاده می کنند (که به یاد داشته باشید$t+1$ تکه امضای درست، کلیه اطلاعات امضای نهایی را شامل می شود)و از تصحیح خطا برای پوشش تکه امضاها استفاده می کند.

۳-۷-٤ **proacity security and adaptability**:

علاوه بر امضاهای آستانه ای threshold signature سرویس مدیریت کلید ما از share refreshing(به روز رسانی اشتراکی) برای تحمل دشمن متحرک مطابقت سازی تنظیمات با تغییرات در شبکه استفاده می کند. Mobile adverarioes برای اولین بار توسط ostrovsky،rung برای توصیف شخصیتی دشمنان که بطور موقتی یک سرور را مورد حمله قرار می دهند و سپس به قربانی دیگر منتقل می شوند معرفی شد دراین مدل دشمن ممکن است بتواند به تمام سرورها را در مدت زمان زیادی صدمه بزند.

حتی اگر سرورهای صدمه دیده از سرویس خارج شود از سرویس دادن محروم میشوند دشمن هنوز می تواند tتکه از کلید عمومی را از سرورهای درحال سرویس دهی بدست

آورد. این به دشمن امکان تولید هر نوع سند معتبری که با کلید عمومی نشانه گذاری شده را میدهد.

شکل هایproactive(۹و۱۰و۱۹و۲۰و۲٤) به عنوان مقابل متضاد برای دشمنان mobile محسوب می شود. یک شکل رمزنگاری آستانه ی proactive از به روز رسانی اشتراکی استفاده می کنند که به سرورها این امکان را می دهد تا بخشهای جدید را از قدیمیها در همکاری بدون بستن کلید عمومی سرویس به روی سایر سرورها بدست آورد.بعد ازrefresh شدن سرورها بخشهای قدیمی را پاک می کنند و از تکه های جدید برای تولید امضاهای ناقص استفاده می کنند چون تکه های جدید مستقل از قدیمیها هستند دشمن نمی تواند با استفاده از ترکیب قدیمی ها با جدید ها کلید عمومی سرویس را بدست آورد بنابراین دشمن سعی می کند تا با t+1 سرور در یک بازه زمانی حمله کند. به روز رسانی اشتراکی بر مبنای خصوصیات homorophic زیر استوار است. اگر(s_1 ، s_1^{1} ،....، s_n) ، s_2 ،s_3 ،....، s_n ، s_1 ،(n،t+1)تکه از k1 و (s_1 ، s_2 ،s_3 ،....، s_n) ، (n،t+1) تکه از k2 باشد پس (s_1 ، s_2 ،s_3 ،....، s_n)، (n،t+1) تکه از k1+k2 خواهد بود اگر k2 صفر 0 باشد ما یک تکه (n،t+1) تایی از k1 را به دست خواهیم آورد.

Nسرور داریم فرض کنیم (s_1 ، s_2 ،s_3 ،....، s_n) یک(n،t+1)تایی که از کلید عمومی k از سرویس باشد که سرور i با s_i مشخص شده فرض می کنیم تمام سرورها سالم اند به روزرسانی اشتراکی به صورت زیر خواهد بود:

اول هر سرور به صورت random (تصادفی)،(s_n،...، s_{i2}، s_{i1}) را تولید می کند یک (n،t+1) تایی تکه از 0(صفر) ما این تازه تولید شده ها s ها را زیر بخش می نامیم پس هر زیر بخش s_{ij} از طریق یک لینک ارتباطی امن به ijام فرستاده می شود وقتی ijام زیر بخش s s_{nj}،...، s_{2j}، s_{ij} را دریافت کرد.

یک بخش جدید(share) تکه با استفاده از زیر بخش ها و بخشها ی قدیمی تولید می کند.

Share refreshing باید تحمل نبود یکسری زیر بخش ها و خطاهای آنها از سرورهای صدمه دیده ناشی می شود داشته باشد یک سرور صدمه دیده ممکن است هیچ زیر تکه ای ارسال نکند بنابراین به محض اینکه سرورها سالم بر سر تکه ها برای استفاده توافق کردند آنها می توانند تکه های جدیدی با استفاده از همان زیر بخش های t+1 سرور ایجاد کنند.

تنوع به روز رسانی اشتراکی تکه ها به سرویس مدیریت کلید اجازه می دهد تا تنظیماتش را از (n،t+1) به (n'،t'+1) تغییر دهد به این صورت که سرویس مدیریت کلید می تواند خودش را تطبیق دهد در پرواز با تغییرات در شبکه: اگر فهمید یک سرور صدمه دیده سرویس باید سرور صدمه دیده را از دور خارج کند و تکه تولید شده را به روزرسانی کند واگر یک سرور دیگر قابل استفاده نباشد یا سرور جدید به شبکه اضافه شود سرویس باید تنظیماتش را بر آن اساس تغییر دهد برای مثال یک سرویس مدیریت کلید ممکن است از (۳و۷)شروع کند. اگر بعد از مدتی یک سرور به عنوان یک سرور صدمه دیده شناخته شود و سرور دیگری بیش از آن قابل استفاده نباشد سرویس باید تنظیماتش را به (۲و۵) تغییر دهد

اگر ۲ سرور بعدها به شبکه اضافه شود سرویس می تواند تنظیماتش را به (۳و۷) برگرداند و سرورهای جدید را نیز در نظر بگیرد.

تنها تفاوتی که وجود دارد این است که مجموعه سرورهای اصلی موجود subshare زیر بخش هایی را بر اساس تنظیمات جدید سرویس ها تولید می کنند برای مجموعه t+1 از n سرور قدیمی موجود هر سرور l در این مجموعه یک ($n^{'}$،$t^{'}$+1) زیر بخش s_n،...،s_{i2}،s_{i1} .

همزمانی ای، یک سرور نمی تواند زیر تکه هایش را برای تمام سرورهای سالم با یک کانال ارسال کند. همچنین، ما فقط نیاز به زیر بخشها برای فراهم کردن یا محاسبه تمام زیر بخشهایی که ارسال شده اند داریم.

این مکانیزم مهم استفاده از چند امضایی برای سرورهای سالم برای پیدا کردن و رد کردن پیام های خطایی است که از سرورهای صدمه دیده فرستاده می شوند. یعنی، مانیاز داریم که پیام های مشخصی همراه با تصدیق از سوی سرورهای فرستاده شوند. اگر یک پیغام که شامل امضاهای دیجیتالی که از تعداد مشخصی سرور دریافت می شود، اعتبار سنجی شود، حداقل یک سرور سالم باید یک امضا داشته باشد.

ما یک نمونه اولیه از چنین سرویس مدیریت کلیدی را طراحی کرده ایم. نتایج اولیه نشان دهنده امکان پذیر بودن آن است. بنابر محدودیتهای این مقاله، مانتوانستیم توصیفی جزئی از این سرویس ارائه دهیم.

٤-٨ related work کارهای مربوطه

٤-٨-١ secure routingمسیریابی امن

مسیریابی ایمن در شبکه ها مثل اینترنت به صورت گسترده ای مطالعه شده. بسیاری از راه های ارائه شده برای مسیریابی ایمن در شبکه های Ad-Hoc قابل استفاده هستند. با در نظر گرفتن جملات خارجی، الگوهای استاندارد مثل امضای دیجیتالی برای تصدیق هویت و یکپارچگی مورد توجه قرار گرفته اند. برای مثال، kent،sirios از یک تابع hashe که کلید یکطرفه دارد با یک پنجره از pada که برای یکپارچگی در ارتباطات poind to poind استفاده می شوند برای حفاظت از پیام ها استفاده می کنند.

٤-٨-٢ replicadedsecare service سرویس های تکرار امن

Reiter و سایرین با موفقیت از ابزار rampart در ساختن یک سرویس مدیریت کلید کپی (replict) استفاده کرده اند، که از رمزنگاری استانه (threshold crypdoghraph) نیز استفاده می کنند. یکی از اشکال های rampart این است که ممکن است سرورهای کند ولی سالم از گروه خارج کند.چنین حذفی ممکن است سیستم را آسیب پذیر کند. تغییرات در عضویت ها هزینه بر خواهد بود. به همین دلیل، rampart بیشتر برای شبکه های tghly coupled مناسب است تا برای شبکه های Ad-Hoc.

Gongاز مرکز توزیع کلید (key disdribuction center)استفاده می کند، موجودیت مرکزی مسئول مدیریت کلید در یک ساختار کلید سری است. در راه حل او، یک گروه از

سرورهای به هم متصل نقشKDC را عمل می کنند، که هر سرور یک کلید سری یکتا را با هر client به اشتراک می گذارد.

در phalanx،reiter،malkhi را ارائه می دهند، یک سرویس واکنش دادن که خرابی را در یک سیستم غیر همزمان کنترل می کنند. ذات phalamx سیم پاسخ اکثریت است که در آن سرورهای یک گروه ویژگی های یکسان دارند. این سرویس از خواندن و نوشتن بهره می گیرد و قرار داد می کند که یک عمل خواند همیشه آخرین چیز نوشته را بر می گرداند. به جای اینکه هر سرور سالم یک عمل را انجام دهد، مجموعه سرورهای اکثریت این کار را انجام می دهند.

در lishov،casdro روشsdade-machine را برای دستیابی به کنترل خطای در Byzantine به کار می گیرند. آنها از یک پروتکل 3 فازی استفاده می کنند.

٤-٨-٣ امنیت در شبکه های **Ad-Hoc**

در رفتارهای امنیتی که یک شبکه Ad-Hoc با آن مواجه است توصیف میکنیم الگوی گرفته شده فرمت پیام ها را توضیح می دهد، بعلاوه پروتوکل هایی که تصدیق هویت را فراهم می کند. معماری می تواند از الگو های مختلف تصدیق هویت استفاده کنند. سرویس مدیریت کلیدی ما یک پیش نیاز برای چنین معماری های امنیتی است.

فصل پنجم: manet

۵-۱ مقدمه

سیستم های بی سیم از حدود سال های۱۹۸۰ مورد استفاده بوده و ما تا کانون شاهد نسل های اول، دوم و سوم این تکنولوژی بوده ایم. این نوع سیستم ها بر اساس یک ساختار مرکزی و کنترل شده مثل access point عمل می کنند. نقاط دسترسی به کاربرین امکان می دهند با تغییر مکان خومد هم چنان بتوانند به شبکه متصل بمانند. اما با این حال به دلیل حضور چنین نقاط ثابتی در شبکه محدودیتهایی بروز می کنند. به عبارتی در مکان هایی که امکان برقراری ساختار ثابت و همیشه پایدار وجود ندارد این نوع تکنولوژی نمی تواند پاسخ گو باشد. پیشرفتها و دست آوردهای اخیر بشری و به وجود آمدن blue tooth, نوع جدیدی ازسیستم های بی سیم یعنی شبکه های Mobile ad hoc را معرفی کردند. شبکه های Mobile ad hoc که آنها زا گاهی شبکه های "short live" نیز می نامند می توانند در غیاب ساختار ثابت و متمرکز عمل کنند. بدین ترتیب در مکان هایی که امکان به راه اندازی سریع یک شبکه ی ثابت وجود ندارد کمک بزرگی محسوب مکی شوند. شایان ذکر است که واژه ی ad-hoc لاتین بوده و به معنی " فقط برای این منظور" می باشد.

شبکه ی Mobile ad hoc سیستم خودکاری متشکل از Nodeهای موبایل و یا متحرکی است که توسط لینک های بی سیم به یکدیگر متصل شده اند. هر node هم به عنوان end-system و هم به عنوان مسیریاب برای بقیه node های موجود در شبکه به کار می رود. در چنین شبکه ای هر

کاربری می تواند در حالی که با node یا node های دیگری در حال ارتباط است مکان خود را تغییر دهد.

مسیر بین هر جفت از کاربرین ممکن است دارای لینک های چندگانه بوده و نیز رادیوی بین آنها ناهمگن باشد.

پروتوکل معروف IEEE 802.11 قادر به تامین امکانات شبکه های Ad hoc در مواقعی که access point وجود ندارد اما در سطح پلیین تری می باشد. در این حالت node ها می توانند اطلاعات را در شبکه ارسال و دریافت کنند اما قادر به مسیریابی نیستند. شبکه های Mobile ad hoc یا به صورت مجزا و ایزوله و یا در ارتباط با بقیه شبکه ها همچون اینترنت عمل می کنند. این شبکه ها توانسته اند رویای اتصال به شبکه در هر مکان و هر زمانی را به واقعیت بدل کنند. یکی از کاربردهای بسیار واضح این نوع شبکه در محل های گرد آمدن افراد با laptop است که به راحتی می توانند تشکیل شبکه بدهند.

انواع شبکه های بیسیم:

شبکه های بی سیم بر ۳ نوع هستند:

۱- شبکه های infrastructure-based

۲- Wireless LANs: معمولا از لینکهای رادیویی (۸۰۲.۱۱) و یا اشعه ی مادون قرمز استفاده می کنند. انعطاف پزیری بالایی در محدوده ای که این امکان در آن قرار داده شده است ایجاد کرده و پهنای باند کمتری نسبت به شبکه های سیمی دارند.

۳- شبکه های Ad hoc: زمانی که ساختار infra structure موجود نیست گزینه ی مناسبی به شمار می روند و نسبت به دو نوع قبل گران تر هستند.

شبکه های بی سیم Ad hoc خود بر ۲ نوع می باشند:

۱- smart sensor Networks: متشکل از چندین sensor هستند که در محدوده ی جغرافیا یی معینی قرار گرفته اند. هر sensor دارای قابلیت ارتباطی بی سیم و هوش کافی برای پردازش سیگنال ها و امکان شبکه سازی است.

۲- Mobile ad hoc networks(MANET): مجموعه ی مستقلی شامل بر کاربرین متحرک است که از طریق لینک های بی سیم با یکدیگر ارتباط برقرار می کنند. برای اتفاقات غیر قابل پیش بینی اتصالات و شبکه های متمرکز کارا نبوده و قابلیت اطمینان کافی را ندارند. لذا MANET را ه حل مناسبی است. Node های واقع درMANET مجهز به گیرنده و فرستنده های بی سیم بوده و از آنتن هایی استفاده می کنند که ممکن است از نوع Broad cast و یا peer to peer باشند.

۲-۵ شبکه ی Mobile ad hoc (MANET):

MANET مجموعه ای است ازNode های موبایل یا متحرک مجهز به گیرنده و فرستنده به منظور برقراری ارتباطات بی سیم. Node های موبایل به دلیل وجود محدودیت هایی در فرستنده و گیرنده های خود نمی توانند با تمام Node ها ارتباط مستقیم برقرار کنند. به همین دلیل لازم است در مواردی که امکان برقراری چنین ارتباط مستقیمی وجود ندارد داده ها از طریق بقیه Node ها که در

این حالت نقش مسیریابرا ایفا می کنند منتقل شوند. با این حال متحرک بودن Node ها باعث شده شبکه مدام در حال تغییر بوده و مسیرهای مختلفی بین دو Node به وجود آید. عوامل دیگری همچون Multi hopping , اندازه ی بزرگ شبکه, و ناهمگونی انواع host ها و تنوع نوع و ساختار آنها و محدودیت توان باتری ها طراحی پروتوکل های مسیریابی مناسب را به یک مشکل جد ی بدل کرده است. برای این منظور بایستی از پروتوکل های مناسب و امنی استفاده شود که در ادامه به آنها خواهیم پرداخت.

همچنین Node ها هیچ دانش پیشینی نسبت به توپولوژی شبکه ای که در محدوده ی آنها برقرار است ندارند و بایستی از طریقی پی به آن ببرند . روش رایج این است که یک Node جدید بایستی حضوذر خود را اعلام کرده و به اطلاعات broad cast شده از همسایگان خود گوش فرا دهد تا بدین ترتیب اطلاعاتی در مورد Node های اطراف و نحوه ی دسترسی به آنها به دست آورد.

دیگر مسائل, مشکلات و محدودیت های موجود در این شبکه ها:

* خطاهای ناشی از انتقال ودر نتیجه packet loss فراوان.

* حضور لینکهای با ظرفیت متغیر.

* قطع و وصل شدن های زیاد و مداوم

* پهنای باند محدود

* طبیعت broad cast ارتباطات.

* مسیرها و توپولوژی های متغیر و پویا

* طول کم شارژ باتری ابزار متحرک

* ظرفیت ها و قابلیت های محدود Node ها

* نیاز به application های جدید (لایه ی Application)

* کنترل میزان تراکم و جریان داده ها (لایه ی Transport)

* روش های آدرس دهی و مسیریابی جدید (لایه ی Network)

*تغییر در وسایل و لبزار آلات اتصالی (لیه ی Link)

* خطاهای انتقال (لایه ی physical)

* انجام عملیات محاسباتی توزیع شده و مشارکتی

* در وقوع حوادث نگوار همچون زمین لرزه, سیل و ... که امکان آسیب دیدگی stationهای ثابت وجود دارد. (در شبکه با ساختار ثابت در صورت آسیب دیدن station اصلی ممکن است کل شبکه از کار بیافتد.)

* عملیات جستجو و نجات

* و موارد نظامی

۳-۵ پروتوکل های مسیریابی (Routing Protocols):

همان طور که پیش از این نیز اشاره شد در شبکه های Mobile ad hoc عمل مسیریابی به دلایلی همچون متحرک بودن و نبود سیستم کنترلی متمرکز از اهمیت بالایی برخوردار بوده و مطالعه و بررسی بیشتری را می طلبد. قبل از بررسی این پروتوکل ها باید توجه کنیم که هدف از الگوریتم ها و استراتژی های مسیریابی جدید کاهش سربار ناشی از مسیریابی در کل شبکه, یافتن مسیرهای کوتاه تر و انتقال صحیح داده ها و اطلاعات می باشد.

تقسیم بندی های مختلفی در مورد پروتوکل های مسیرهای شبکه های Mobile ad hoc وجود دارد که از این میان می توان به ۲ نوع زیر اشاره کرد:

تقسیم بندی اول:

* pro active(Table driven)

* Reactive(On demand)

* Hybrid(Table driven&On demand)

تقسیم بند یدوم:

* Fiat routing protocols

* Hierarchal routing approaches

* GPS Augmented geographical routing approaches

در اینجا به توضیحاتی در مورد پروتوکل های تقسیم بندی اول می پردازیم:

۱. Pro active- Table driven:

در پروتوکلهای از این نوع, Node ها مدام در حال جستجوی اطلاعات مسیریابی جدید درون شبکه هستند به صورتی که حتی با تغییر مکان Node ها در صورت نیاز به راحتی می توان مسیر مناسبی را یافته و برای ارسال و دریافت اطلاعات بین هردو Node ی استفاده کرد. به عبارت بهتر می توان گفت که در این شبکه ها مسیرها از قبل موجود هستند و به محض آنکه Node ی اقدام به ارسال داده به Node دیگری کند قادر خواهد بود مسیر موجود را از روی اطلاعات از قبل جمع آوری شده شناسایی کرده و مورد استفاده قرار دهد و لذا تاخیری در این مورد متوجه Node نیست.

* DSDV: این پروتوکل بر مبنای الگوریتم کلاسیک Bellman-Ford بنا شده است. در این حالت هرNode لیستی از تمام مقصدها ونیز تعداد hopها تا هر مقصد را تهیه می کند. هر مدخل لیست با یک عدد شماره گزاری شده است . برای کم کردن حجم ترافیک ناشی از به روز رسانی مسیر ها در شبکه از incremental packets استفاده می شود. تنها مزیت این پروتوکل اجتناب از به وجود آمدن حلقه های مسیریابی در شبکه های مسیریاب های متحرک است. بدین ترتیب اطلاعات مسیرها همواره بدون توجه به این که آیا Node در حال حاضر نیاز به استفاده از مسیر دارد یا نه فراهم هستند.

معایب: پروتوکل DSDV نیازمند پارامترهایی از قبیل بازه ی زمانی به روز رسانی اطلاعات و تعداد به روز رسانی مورد نیاز می باشد.

* WRP: این پروتوکل بر مبنای الگوریتم path-finding بنا شده با این استثنا که مشکل count-to-infinity این الگوریتم را برطرف کرده است. در این پروتوکل هرNode , ٤ جدول تهیه می کند: جدول فاصله, جدول مسیریابی, جدول link-cost و جدولی در مورد پیامهایی که باید دوباره ارسال شوند. تغییرات ایجاد شده در لینکها ار طریق ارسال ودریافت پیام میان Node های همسایه اطلاع داده می شوند.

* CSGR: در این پروتوکل Node ها به دسته ها یا cluster هایی تقسیم بندی می شوند. هر گروه یک Cluster head دارد که می تواند گروهی از host ها را منترل و مدیریت کند. از جمله قابلیت هایی که عمل Clustering فراهم می کند می توان به اختصاص پهنای باند و Channel access اشاره کرد. این پروتوکل از DSDV به عنوان پروتوکل مسیریابی زیر بنایی خود استفاده می کند. نیز

در این نوع هر Node دو جدول یکی جدول مسیریابی و دیگری جدول مربوط به عضویت در Node های مختلف را فراهم می کند.

معایب: Node ی که head واقع شده سربار محاسباتی زیادی نسبت به بقیه دارد و به دلیل اینکه بیشتر اطلاعات از طریق این head ها برآورده می شوند در صورتی که یکی از Node های head دچار مشکل شود کل و یا بخشی از شبکه آسیب می بیند.

* STAR: این پروتوکل نیاز به به روز رسانی متداوم مسیرها نداشته و هیچ تلاشی برای یافتن مسیر بهینه بین Node ها نمی کند.

۲. Reactive- On demand:

در این نوع پروتوکل مسیرها تنها زمانی کشف می شوند که مبدا اقدام به برقراری ارتباط با Nodeدیگری کند. زمانی که یک Node بخواهد با Node دیگری ارتباط برقرار کند بایستی فرایند کشف مسیر (Route Discovery Process) را در شبکه فراخوانی کند. در این حالت قبل از بر قرار شدن ارتباط, تاخیر قابل توجهی مشاهده می شود.

* SSR: این پروتوکل مسیرها را بر مبنای قدرت و توان سیگنالها بین Node ها انتخاب می کند. بنابراین مسیرهایی که انتخاب می شوند نسبتا قوی تر هستند. می توان این پروتوکل را به ۲ بخش DRP(Dynamic Routing Protocol)و SRP(Static Routing Protocol) تقسیم کرد.

DRP مسئول تهیه و نگهداری جدول مسیریابی و حدول مربوط به توان سیگنال ها می باشد. SRP نیز Packet های رسیده را بررسی می کند تا در صورتی که آدرس Node مربوط به خود را داشته باشد آن را به لایه های بالاتر بفرستد و در غیر این صورت به شبکه.

* DSR: در این نوع Node های موبایل بایستی Cache هایی برای مسیرهایی که از وجود آنها مطلع هستند فراهم کنند. دوفاز اصلی برای این پروتوکل در نظر گرفته شده است: کشف مسیر و به روزرسانی مسیر. فاز کشف مسیر از rout request/reply packet ها و فاز به روز رسانی مسیر از acknowledgement ها و errorهای لینکی استفاده می کند.

TORA: بر اساس الگوریتم میریابی توزیع شده بنا شده و برای شبکه های mobile بسیار پویا طراحی شده است. این الگوریتم برای هر جفت از Node ها چندین مسیر تعیین می کند و نیازمند clock سنکرون می باشد. ۳ عمل اصلی این پروتوکل عبارتند از : ایجاد مسیر، به روز رسانی مسیر و از بین بردن مسیر.

* AODV: بر مبنای الگوریتم DSDV بنا شده با این تفاوت که به دلیل مسیریابی تنها در زمان نیاز میزان broad casting را کاهش می دهد. الگوریتم کشف مسیر تنها زمانی آغاز به کارمی کند که مسیری بین Node2 وجود نداشته باشد.

* RDMAR: این نوع از پروتوکل فاصله ی بین Node2 را از طریق حلقه های رادیویی و الگوریتم های فاصله یابی محاسبه می کند. این پروتوکل محدوده ی جستجوی مسیر را مقدار

مشخص و محدودی تایین می کند تا بدین وسیله از ترافیک ناشی از flooding در شبکه کاسته باشد.

۳. Hybrid(Pro- active/Reactive) :

این مورد با ترکیب دو روش قبلی سعی در کاهش معایب کرده و از ویژگی های خوب هر دو مورد بهره می برد. این پروتوکل جدیدترین کلاس پروتوکل ها در این راستا می باشد. معروفترین پروتوکل از این نوع می توان به ZRP(Zone Routing Protocol) اشاره کرد. این پروتوکل از ویژگی های نوع Pro active برای مسیریابی Node های نزدیک به هم و از ویژگی های نوع Reactive برای مسیریابیNode های دورتر استفاده می کند.

* ZRP: نوعی از Clusteringاست با این تفاوت که در این پروتوکل هر Node خود head بوده و به عنوان عضوی از بقیه ی Cluster ها می باشد. به دلیل hybrid بودن کارایی بهتری دارد.

٤-٥ امنیت در شبکه های Mobile ad hoc:

شاید بتوان شبکه های ad hoc را آسیب پذیرترین شبکه ها از لحاظ امنیتی و ضعیفترین در مقابل حملات نفوذگران دانست. به همین دلیل برخورد با این مسئله و رفع مشکلات مربوطه از مهمترین دغدغه های شخصی است که اقدام به راه اندازی چنین شبکه ای می کند. از جمله مواردی که منجر به نا امن شضدن این شبکه ها شده است می توان به موارد زیر اشاره کرد:

* کانال رادیویی از نوع broad cast به اشتراک گزارده شده.

* محیط عملیاتی نا امن

* نبود شناسایی (authentication) متمرکز.

* دسترسی محدود به منابع.

* مشکلات و آسیب پذیری های فیزیکی.

زمانی که در مورد امنیت شبکه بحث می شود معمولا به عناوین چندی توجه می شود:

* Availability: بدین معنی که شبکه در تمام زمان ها حتی در مواردی که دچار حمله شده بتواند به عمل خود ادامه بدهد.

* Confidentiality: اطمینان از اینکه اطلاعات مشخص و معینی در اختیار کاربران خاصی قرار نگیرد.

* Authentication: توانایی یک node در شناسایی و تشخیص node ی که با وی در ارتباط است.

* Integrity: تضمین اینکه یک پیام پس از منتشر شدن تخریب نشده و از بین نمی رود.

* Non-repudiation: فرستنده ی پیام نتواند ارسال خود را انکار کنند.

یک شبکه ی ad hoc به دلیل نداشتن ساختار ثابت و مشخص و نیز ارتباطات پویا بین node ها نیازمند ملاحظات امنیتی بیشتری نسبت به انواع دیگر شبکه است.

همان طور که قبلا نیز بیان شد در این شبکه ها هر node ی هم مسیریاب است و هم end system. بدین ترتیب node ها از هم متمایز نیستند و به این دلیل نیاز یک پروتوکل مسیریابی امن حس می شود. که در این راستا معمولا پروتوکل های multi hop بث کار گرفته می شوند.

نتیجه گیری

شبکه‌های ادهاک موبایل در واقع آینده شبکه‌های بی سیم می‌باشند به دلیل اینکه آنها ارزان، ساده، انعطاف پذیر و استفاده آسانی دارند. ما در جهانی زندگی می‌کنیم که شبکه‌ها در آن پیوسته تغییر می‌کنند و توپولوژی خودشان را برای اتصال نودهای جدید تغییر می‌دهند به همین دلیل ما به سمت این شبکه‌ها می‌رویم. علی رغم مشکلات امنیتی که دارند کاربردهای زیادی دارند در واقع روز به روز بر کارآیی آنها افزوده شده و از قیمتشان کاسته می‌شود به همین دلیل در بازار طرفداران زیادی دارند.

پیشنهادها

- ارتقاء پروتکل های ارائه شده از نظر امنیت و عملکرد
- ارزیابی و مقایسه علمی بین انواع پروتکل های مسیریابی امن
- بدست آوردن مدلی برای مشکلات امنیتی مسیریابی امن
- منطق طراحی یک پروتکل امن برای شبکه های بی سیم اقتضایی
- طراحی بهینه پروتکل مسیریابی با توجه به بده بستان امنیت و عملکرد

منابع

[1] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, “ARAN: A Secure Routing Protocol for Ad Hoc Networks”, UMass Tech Report 02-32, 2002

[2] Y. Hu, D. B. Johnson, A. Perrig, “ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc Networks”, in proceedings of MOBICOM 2002

[3] C. E. Perkins, E. M. Royer, and S. R. Das, Ad-hoc On-demand Distance Vector (AODV) routing, IETF MANET Group, Jan 2002

[4] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks, IETF MANET Group, Feb 2002

[5] S. Lee and M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks”, Proc. of IEEE ICC, Vol.10, pp.3201-3205, May 2001

[6] "A review of routing protocols for mobile ad-hoc networks". Mehran Abolhasan a, Tadeusz Wysocki a, Eryk Dutkiewicz : Ad Hoc Networks 2 (2004) 1–22

[7] "Strategies for enhancing routing security in protocols for mobile ad-hoc networks". Lakshmi Venkatraman and Dharma P. Agrawal : J. Parallel Distrib. Comput. 63 (2003) 214–227

[8] "SEAD-secure efficient distance vector routing for mobile wireless ad-hoc networks". Yih-Chun Hu , David B. Johnson , Adrian Perrig. s.l. : Ad Hoc Networks, 2003, Vol. 1, pp. 175–192.

[9] "Secure position-based routing protocol for mobile ad-hoc networks". Joo-Han Song , Vincent W.S. Wong , Victor C.M. Leung. s.l. : Ad Hoc Networks, 2007, Vol. 5, pp. 76–86.

[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, “ARAN: A Secure Routing Protocol for Ad Hoc Networks”, UMass Tech Report 02-32, 2002

[11] Y. Hu, D. B. Johnson, A. Perrig, “ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc Networks”, in proceedings of MOBICOM 2002

[12] C. E. Perkins, E. M. Royer, and S. R. Das, Ad-hoc On-demand Distance Vector (AODV) routing, IETF MANET Group, Jan 2002

[13] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks, IETF MANET Group, Feb 2002

[14] S. Lee and M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks”, Proc. of IEEE ICC, Vol.10, pp.3201-3205, May 2001

[15] P. Papadimitratos and Z.J. Haas, “Secure Message Transmission in Mobile Ad Hoc Networks,” submitted for publication.

[16] P. Papadimitratos, “Secure Routing: Methods for Protecting Routing Infrastructures – A Survey,” work in progress.

[17] L. Lamport, R. Shostak, M. Pease, “The Byzantine Generals Problem,” ACM Trans. Program. Languages, Vol. 4, no. 3, pp. 382-401, July 1982.

[18] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[19] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks,” Security Protocols, 7th International Workshop, LNCS, Springer- Verlag, 1999.

[20] IEEE Std. 802.11, “Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications,” 1999.

[21] R. Zucceratto, and C. Adams, “Using Elliptic Curve Diffie- Hellman in the SPKM GSS-API,” Internet Draft, IETF, Aug. 1999.

[22] D. B. Johnson et al, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks,” Internet Draft, IETF MANET Working Group, March 2nd, 2001.

[23] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February 1997.

[24] N. Asokan, P. Ginzboorg, “Key Agreement in Ad Hoc Networks,” Computer Communications 23 (17): 1627-1637 Nov. 1 2000.

[25] Alfred Menezes, Paul van Oorschot and Scott Vanstone, “Handbook of Applied Cryptography,” CRC Press, October 1996 – 5th reprinting, Aug. 2001.

[26] W. Diffie, M.E. Hellman, “New directions in cryptography,” IEEE Transactions in Information Theory, 1976.

[27] Z.J. Haas, M. Perlman, P. Samar, “The Interzone Routing Protocol (IERP) for Ad Hoc Networks,” draft-ietf-manetzone- ierp-01.txt, IETF MANET Working Group, June 1st, 2001.

[28] Z. J. Haas, M. Perlman, “The Performance of Query Control Schemes of the Zone Routing Protocol” IEEE/ACM Transactions on Networking, vol. 9, no. 4, pp. 427-438, Aug. 2001.

[29] C.K. Toh, ”Associativity-Based Routing for Ad-Hoc Mobile Networks, ” Wireless Personal Communications, Vol. 4, No. 2, pp. 1-36, Mar. 1997.

[30] C.E. Perkins, E.M. Royer, S.R. Das, “Ad hoc On-Demand Distance Vector Routing,”, draft-ietf-manet-aodv-08.txt, IETF MANET Working Group, June 1st, 2001.

[31] S. Yi, P. Naldurg, R. Kravets, “Security-Aware Ad-Hoc Routing for Wireless Networks,” UIUCDCS-R-2001-2241 Technical Report, Aug. 2001.

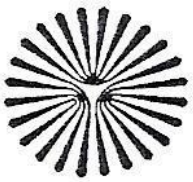
[32] M. Guerrero, “Secure AODV”, Internet draft sent to manet@itd.nrl.navy.mil mailing list, Aug. 2001.

[33] R. Rivest, A. Shamir, L. Adleman, “A method for obtaining Digital Signatures and Public Key Cryptosystems,” Comm. of ACM, 21 (2), pp. 120-126, Feb. 1978.

[34] L. Lamport, “Password Authentication with Insecure Communication,” Comm. of ACM, 24 (11), pp. 770-772, Nov. 1981.

[35] R. Droms, “Dynamic Host Configuration Protocol,” IETF RFC 2131, Mar. 1997.

[36] M. Hattig, Editor, “Zero-conf IP Host Requirements,” draft-ietf-zeroconf-reqts-09.txt, IETF MANET Working



Payame Noor University

Ad-Hoc Networks

A Project Report
Presented to:

Department of Information Technology
Payame Noor University

In Partial Fulfilment of the Requirement for the degree of
Bachelor of Science in

Information_ Technology

Advisor:
Kavoosi

By:
Mohammad shahsavandi

Summer 20