دانشگاه آزاد اسلامی

واحد تهران شمال

دانشکده فنی و مهندسی

گروه مهندسی فناوری اطلاعات

پایان نامه کارشناسی

گرایش فناوری اطلاعات

عنوان :

بررسی جامع الگوریتم های مسیریابی در شبکه های موردی

استاد راهنما :

داریوش ضیایی غفوری

نگارش :

رامین کاشفی

زمان :

نیمسال دوم ۱۳۹۴-۱۳۹۳

www.Prozhe.com

www.Prozhe.com

تقدیم به:

پدر و مادر عزیزم که در زندگی و در تحصیل من زحمات فراوانی را کشیده اند.

www.Prozhe.com

سپاسگزاری:

من در وهله اول از پدر و مادر عزیزم تشکر میکنم و در وهله دوم از استاد گرامی جناب آقای ضیایی تشکر میکنم که در تدوین پایان نامه به من کمک شایانی کرده اند.

www.Prozhe.com

فهرست مطالب

عنوان **صفحه**

www.Prozhe.com

فهرست مطالب

عنوان **صفحه**

www.Prozhe.com

فهرست مطالب

عنوان **صفحه**

www.Prozhe.com

فهرست مطالب

عنوان **صفحه**

www.Prozhe.com

فهرست مطالب

عنوان **صفحه**

www.Prozhe.com

فهرست شکل ها

عنوان **صفحه**

www.Prozhe.com

فهرست جدول ها

عنوان **صفحه**

www.Prozhe.com

فهرست رابطه ها

عنوان **صفحه**

www.Prozhe.com

چکیده

شبکه های موردی شامل مجموعه ای از نود های توزیع شده هستند که به صورت بی سیم با همدیگر در ارتباط می باشند. نودها می توانند کامپیوتر میزبان یا مسیریاب باشند که هر یک مجهز به یک فرستنده و گیرنده بوده و به طور مستقیم بدون هیچگونه نقطه دسترسی با همدیگر ارتباط برقرار می کنند، لذا سازمان ثابتی نداشته و در یک توپولوژی دلخواه شکل گرفته اند. مهمترین ویژگی این شبکه ها نیز وجود همین توپولوژی پویا و متغیر است که نتیجه تحرک نودها می باشد. نودها در این شبکه ها به طور پیوسته موقعیت خود را تغییر میدهند و بنابراین نیاز به یک پروتکل مسیریابی خوب که توانایی سازگاری با این تغییرات را داشته باشد، نمایان تر میشود. در این پایان نامه سعی شده است تا آلگوریتم های مسیریابی موجود در شبکه های موردی مورد بررسی قرار گیرند و کارایی، عملکرد و امنیت آنها با یکدیگر مقایسه شوند.

www.Prozhe.com

مقدمه

شبکه های موردی به علت عدم استفاده از زیر ساخت از پیش بنا شده، می توانند استفاده های گوناگونی داشته باشند .این شبکه ها می توانند به راحتی راه اندازی شوند، مورد استفاده قرار بگیرند و نهایتاً از میان بروند . از موارد استفاده شبکه های موردی می توان به کاربردهای شخصی مانند اتصال laptop ها به یکدیگر،کاربردهای عمومی مانند ارتباط وسایل نقلیه و تاکسی ها، کاربردهای نظامی مانند ارتش و ارتباط ناوگان جنگی و کاربردهای اضطراری مانند عملیات امداد و نجات اشاره کرد .از آنجا که عمل مسیر یابی در شبکه های موردی به عهده خود نود های شرکت کننده در شبکه است، امنیت مسیریابی در این شبکه ها بیش از دیگر شبکه ها خود را نشان می دهد.

www.Prozhe.com

فصل اول

کلیات

www.Prozhe.com

۱-۱)هدف

هدف در این پروژه بررسی و تحلیل الگوریتم ها و پروتکل های مسیریابی در شبکه های ادهاک یا موردی است. الگوریتم هایی که علاوه بر سرعت و کارایی از امنیت قابل توجهی برخوردار باشند تا بتوان به راحتی از آنها استفاده کرد.و در همچنین مزایا و معایب الگوریتم ها بیان شده است تا بتوان الگوریتم ها را ارزیابی کرد و در پروژه های گوناگون از آنها استفاده کرد.

۱-۲)پیشینه کار و تحقیق

اصطلاح Ad hoc که از زبان لاتین گرفته شده است به‌معنای "برای کاربرد اختصاصی" است.این عبارت عموما در مورد راه حلی استفاده می‌شود که برای حل یک مشکل خاص یا انجام وظیفه‌ای ویژه طراحی شده باشد و قابل تعمیم به‌صورت یک راه‌حل عمومی نباشد و امکان تطبیق دادن آن با مسایل دیگر وجود نداشته باشد. یک شبکه ادهاک، اتصالی است که تنها به‌مدت یک جلسه برقرار می‌شود و نیاز به ایستگاه پایه ندارد. در عوض، هر دستگاه متصل به شبکه، دیگر دستگاه‌های واقع در یک محدوده خاص را پیدا می‌کند و این دستگاه‌ها یک شبکه بین خود ایجاد می‌کنند. از سوی دیگر دستگاه‌ها با ارسال پیام، نودهای هدف را در خارج از محدوده تعریف شده جستجو می‌کنند. امکان برقراری ارتباط بین چندین نود مختلف وجود دارد .به این ترتیب، شبکه‌های ادهاک گوناگون به‌یکدیگر متصل می‌شوند. سپس پروتکل‌های مسیریابی، اتصالات

www.Prozhe.com

پایداری را بین این نودها ایجاد می‌کنند، حتی اگر نودها متحرک باشند. از جمله کاربران شبکه‌های ادهاک می‌توان به پلی‌استیشن سونی اشاره کرد که از اتصالات ادهاک برای ایجاد شبکه بی‌سیم بین چند بازیکن (که همگی در یک بازی شرکت می‌کنند) اشاره کرد. پس از پایان بازی، اتصال بی‌سیم بین کاربران قطع می‌شود.

به شبکه adhoc شبکه mesh نیز میگویند. علت این نام گذاری آن است که تمام ایستگاه های موجود در محدوده تحت پوشش شبکهadhoc ،از وجود یکدیگر باخبر بوده و قادر به برقراری ارتباط با یکدیگر می باشند. این امر شبیه پیاده سازی یک شبکه به صورت فیزیکی بر مبنای توپولوژی mesh میباشد.

اولین شبکه adhoc در سال۱۹۷۰ توسط darpa به وجود آمد. این شبکه در آن زمان packet radio نامیده میشد.ولی بعدها متوجه شدند که میتوان در قسمت های تجاری و صنعتی از آنها استفاده کرد.

۱-۳)روش کار وتحقیق

روش کار و تحقیق به شرح زیر است:

۱-جستجوی منابع مرتبط با الگوریتم های مسیریابی شبکه های ادهاک از طریق ابزار و وسایل مختلف مانند کتاب ، مقاله ، پایان نامه، اینترنت و ...

۲- ارزیابی اطلاعات منابع از نظر کمی و کیفی

۳-انتخاب منابع پر محتوا و با ارزش

٤-استخراج اطلاعات از منابع

۵-خلاصه سازی مطالب

www.Prozhe.com

٦-دسته بندی مطالب

۷-ویرایش متن پایان نامه

۸-تجدید نظر در مورد مطالب پایان نامه

www.Prozhe.com

فصل دوم

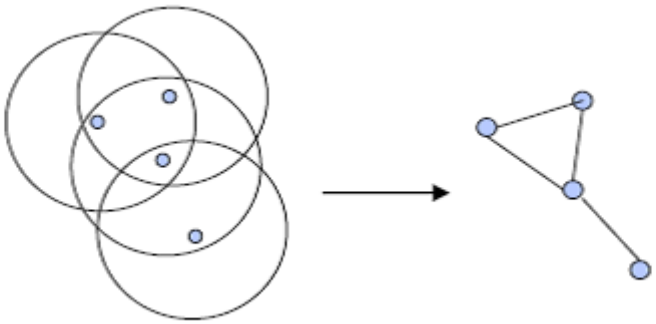
معرفی شبکه های موردی

www.Prozhe.com

۲-۱)شبکه موردی چیست؟

شبکه موردی شبکه ایست که توسط host های بی سیم که می توانند سیار هم باشند تشکیل می شود. شبکه ها(لزوماً) از هیچ زیر ساخت پیش ساخته ای استفاده نمی شود .بدین معنا که هیچ زیر ساختی مانند یک ایستگاه مرکزی، مسیریاب، سوییچ و یا هر چیز دیگری که در دیگر شبکه ها از آنها برای کمک به ساختار شبکه استفاده می شود، وجود ندارد .بلکه فقط تعدادی نود بی سیم هستند که با کمک ارتباط با نود های همسایه، به نود های غیر همسایه متصل می گردند.

در شکل(۲-۱) ساختار یک شبکه موردی نمونه آورده شده است .دایره های کوچک، نشان دهنده نود های بی سیم می باشند .هر دایره بزرگ نشان دهنده برد مفید یک نود است .بدین معنا که هر نود دیگری که در این فاصله قرار داشته باشد، می تواند داده های ارسالی این نود را دریافت کرده و آنها را از نویزهای محیطی تشخیص دهد. برای راحتی کار، این شبکه را با یک گراف متناظر آن نشان می دهند .یالهای گراف بدین معنا هستند که دو راس آن در فاصله ای با یکدیگر قرار دارند که می توانند پیامهای یکدیگر را دریافت کنند .در واقع نود هایی که در فاصله برد مفید یک نود قرار دارند، در نمایش گرافی، با یک یال به آن متصل می شوند.



شکل ۲-۱)ساختار شبکه موردی

www.Prozhe.com

در شبکه های موردی، سیار بودن نود ها ممکن است باعث تغییر مسیر بین دو نود شود .همین امر است که باعث تمایز این شبکه ها از دیگر شبکه های بی سیم می شود. با وجود تمامی این مشکلات، از شبکه های موردی در موارد بسیاری استفاده می شود .دلیل این امر سرعت و آسانی پیاده سازی این شبکه و همچنین عدم وابستگی آن به ساختارهای از پیش بنا شده است .از موارد استفاده شبکه های موردی می توان به کاربردهای شخصی مانند اتصال laptop ها به یکدیگر، کاربردهای عمومی مانند ارتباط وسایل نقلیه و تاکسی ها، کاربردهای نظامی مانند اتصال ارتش و ارتباط ناوگان جنگی و کاربردهای اضطراری مانند عملیات امداد و نجات اشاره کرد.

۲-۲)معرفی انواع شبکه‌های موردی

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، نود های واقع در شبکه‌های ادهاک موبایل مجهز به گیرنده و فرستنده‌های بی سیم بوده و از آنتن‌هایی استفاده می‌کنند که ممکن است از نوع Broadcast و یاpeer to peer باشند.

۲-۳)مزایای شبکه های موردی

۱-سرعت توسعه آن زیاد است.

www.Prozhe.com

۲-به سادگی و به صرف هزینه پایین قابل پیاده سازی می باشد.

۳-مانند سایر شبکه های بی سیم، به زیر ساخت نیاز ندارد.

٤-پیکر بندی خودکار

۵-هر یک از ایستگاه ها به عنوان یک روتر نیز ایفای نقش می کنند.

٦-استقلال از مدیریت شبکه اصلی

۷-انعطاف پذیر بودن به عنوان مثال، دسترسی به اینترنت از نقاط مختلف موجود در محدوده تحت پوشش شبکه امکان پذیر است.

۸-دو ایستگاه موجود در شبکه می توانند به طور مستقل از دیگر ایستگاه ها، با یکدیگر ارتباط برقرار کرده و انتقال اطلاعات بپردازند.

۲-۴) کاربردهای شبکه های موردی

۱-استفاده در شبکه های pan یا personal area network

۲-این نوع شبکه در برگیرنده سیستم های بی سیم که دارای برد و قدرت پایین هستند، می باشد. این نوع شبکه ها معمولا بین افراد و یا در یک دفتر کار و مکان های مشابه ایجاد می گردد. استاندارد مورد استفاده در این محدوده ieee ۸۰۲.۱۵ میباشد. تجهیزات مورد استفاده معمولا laptop,earphone,cell phone و غیره میباشد.

۳-استفاده در عملیات اورژانسی

٤-عملیات جستجو و نجات، اطفاء حریق یا عملیات پلیسی مورد استفاده قرار میگیرد.

۵-استفاده در محیط های غیر نظامی

٦-در شبکه داخلی تاکسیرانی، استادیو ورزشی و ... مورد استفاده قرار می گیرد.

۷-حفاظت از محیط زیست

www.Prozhe.com

۸-زیست شناسان با استفاده از گردن آویزهایی که به حسگرهای مکان، دما و دیگر حسگرها مجهز هستند کیفیت زندگی حیوانات در خطر انقراض را کنترل می‌نمایند.

۹-استفاده در مصارف نظامی

۲-۵)محدودیت های شبکه های موردی

۱-محدودیت پهنای باند دارد.

۲-Multi-hop router نیاز میباشد.

۳-مصرف انرژی یکی از دیگر مشکلات مهم می باشد.

٤-حفظ امنیت در اینگونه از شبکه ها مشکل می باشد.

۵-در شبکه های بزرگتر، ارسال اطلاعات با تاخیر همراه می باشد.

۲-۶)خصوصیات شبکه‌های موردی

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:

۱-فقدان زیرساخت : در شبکه‌های بی سیم ساختارهای متمرکز و مجتمع مثل سرویس دهنده‌ها، مسیریابها و... لزوماً موجود نیستند (مثلاً در شبکه‌های موردی)، به همین خاطر راه حل‌های امنیتی آنها هم معمولاً غیر متمرکز، توزیع شده و مبتنی بر همکاری همه نودهای شبکه‌است.

www.Prozhe.com

۲-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.

۳-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.

٤-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.

www.Prozhe.com

فصل سوم

مسیریابی شبکه های موردی

www.Prozhe.com

۳-۱)چگونگی مسیریابی در شبکه های موردی

مسیریابی در شبکه های موردی به عهده خود نود های موجود در شبکه است.بدین معنا که هیچ دستگاه کمکی شبکه ای مانند سوئیچ، مسیریاب و یا هاب برای مسیریابی وجود ندارد،بلکه این خود host ها یا همان نود های تشکیل دهنده شبکه هستند که عمل مسیریابی را انجام می دهند.اما ممکن است این سوال پیش بیاید که چگونه خود نود ها می توانند عمل مسیریابی در یک شبکه را انجام دهند .برای پاسخ به این سوال به توضیح درباره چند الگوریتم مسیریابی معروف و پرکاربرد در شبکه های موردی پرداخته خواهد شد.هر چند تعداد این الگوریتمها بسیار زیاد است، ولی چند الگوریتم ذکر شده مشهورترین آنها هستند.

استفاده از الگوریتم flooding برای انتقال اطلاعات

ساده ترین راه حل برای حل مشکل مسیر یابی در شبکه های موردی، انتقال اطلاعات از طریق flooding است .این روش بدین صورت است که فرستنده اطلاعات، آنها را برای تمامی نود های همسایه خود ارسال می کند. هر نود که یک بسته اطلاعاتی را دریافت می کند نیز این اطلاعات را برای همسایه های خود می فرستد .برای جلوگیری از ارسال یک بسته توسط یک نود برای بیش از یک بار، از یک شماره توالی برای هر بسته استفاده می شود .بدین ترتیب هر گیرنده، شماره توالی بسته را کنترل می کند و در صورت غیر تکراری بودن آن، بسته را برای همسایگان خود ارسال می کند .با این روش داده به طور حتم به مقصد خواهد رسید ولی بعد از رسیدن اطلاعات به مقصد، عملیات flooding همچنان ادامه پیدا می کند تا بسته، به تمامی نود های موجود در شبکه برسد.

www.Prozhe.com

مزیت اصلی این روش در درجه اول سهولت پیاده سازی آن و در درجه دوم اطمینان از دستیابی بسته به مقصد است .ولی یک اشکال عمده در این طرح این است که بسته های داده غالباً از حجم بالایی برخوردار هستند و داده ها ممکن است مسافتی را بدون آن که لازم باشد طی کنند .برای مثال فرض کنید که یک نود تصمیم دارد تا داده ای را برای نود همسایه خود ارسال کند .حال اگر بخواهیم از روش flooding استفاده کنیم، این بسته در تمامی شبکه پخش خواهد شد .در صورتیکه اگر از همسایگی نود ها اطلاع داشته باشیم می توانیم این انتقال اطلاعات را به شدت کاهش دهیم.

همین افزایش شدید بار شبکه باعث می شود تا از روش flooding برای انتقال اطلاعات استفاده نکنند .ولی این روش در جابجایی سیگنالهای کنترلی به دلیل حجم کوچک این سیگنالها، استفاده فراوانی دارد .بسته های کنترلی بسته هایی هستند که برای به دست آوردن مسیر از آنها استفاده می شود و از مسیرهای به دست آمده برای ارسال داده استفاده می شود.

۳-۲)انواع پروتکل‌های مسیریابی

پروتکل‌های مسیریابی بین هر دو نود این شبکه به دلیل اینکه هر نودی می‌تواند به طور تصادفی حرکت کند و حتی می‌تواند در زمانی از شبکه خارج شده باشد، مشکل می‌باشند. به این معنی یک مسیری که در یک زمان بهینه است ممکن است چند ثانیه بعد اصلا این مسیر وجود نداشته باشد. در ادامه چهار دسته از پروتکل‌های مسیر یابی که با توجه به تصمیم آنها در پیدا کردن یک مسیر به مقصد مشخص میشود، معرفی خواهد شد:

www.Prozhe.com

۳-۲-۱)پروتکل های پیشگیرانه(proactive)

نام دیگر این پروتکل ها ، table driven است.در این روش مسیریابی هرنودی اطلاعات مسیریابی را با ذخیره اطلاعات محلی سایر نودها در شبکه استفاده می‌کند و این اطلاعات سپس برای انتقال داده از طریق نودهای مختلف استفاده می‌شوند. پروتکل های این روش عبارتند از:

۳-۲-۱-۱)پروتکلDSDV

این پروتکل بر مبنای الگوریتم کلاسیک Bellman-Ford بنا شده‌است. در این حالت هر نود لیستی از تمام مقصدها و نیز تعداد پرش‌ها تا هر مقصد را تهیه می‌کند. هر مدخل لیست با یک عدد شماره گذاری شده‌است. برای کم کردن حجم ترافیک ناشی از بروز رسانی مسیرها در شبکه از incremental –packets استفاده می‌شود. تنها مزیت این پروتکل اجتناب از به وجود آمدن حلقه‌های مسیریابی در شبکه‌های شامل مسیریاب‌های متحرک است. بدین ترتیب اطلاعات مسیرها همواره بدون توجه به این که آیا نود در حال حاضر نیاز به استفاده از مسیر دارد یا نه، فراهم هستند.

مزایا و معایب:

این الگوریتم یکی از اولین الگوریتم های موجود بود که برای ایجاد شبکه های adhoc با تعداد نود کم بسیار مناسب بود.اما چون هیچ فرمول مشخصی برای این الگوریتم ارائه نشد،به صورت تجاری پیاده سازی نگردید. Dsdv برای مسیرهای چرخش آزاد (loop-free) تضمین شده است.Dsdv نیاز به بروز رسانی منظم از جداول مسیریابی خود دارد که این باعث استفاده از انرژی باتری و مقدار کمی از پهنای باند می شود. حتی زمانی که شبکه بیکار هست، این انرژی و پهنای باند مصرف می شود. وقتی که توپولوژی شبکه تغییر می کند،لازم است دوباره شماره دهی ترتیبی

www.Prozhe.com

انجام شود تا شبکه همگرایی خود را حفظ کند، در نتیجه dsdv برای شبکه های با پویایی بالا مناسب نیست.

۳-۲-۱-۲)پروتکل 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 نود ، چهار جدول تهیه می‌کند: جدول فاصله، جدول مسیر یابی، جدول هزینه لینک و جدولی در مورد پیام‌هایی که باید دوباره ارسال شوند. تغییرات ایجاد شده در لینک‌ها از طریق ارسال و دریافت پیام میان نودهای همسایه اطلاع داده می‌شوند.

۳-۲-۱-۳)پروتکلcsgr

در این نوع پروتکل نودها 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 ازdsdv به عنوان پروتکل مسیریابی زیر بنایی خود استفاده می‌کند. نیز در این نوع هر نود دو جدول یکی جدول مسیریابی و دیگری جدول مربوط به عضویت در نود های مختلف را فراهم می‌کند.

معایب : نودی که سر(head) 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 نود های سرگروه دچار مشکل شود کل و یا بخشی از شبکه آسیب می‌بیند.

www.Prozhe.com

۳-۲-۱-۴)پروتکلstar

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

۳-۲-۲)پروتکل های واکنش دار(reaction)

نام دیگر این پروتکل ها، on demand است.در این نوع پروتکل ها، مسیرها فقط هنگامی که به وسیله یک نود منبع درخواست می شوند،ایجاد می شوند. هنگامی که یک نود 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 میشود. در الگوریتم های واکنش دار، یک مسیر فقط هنگامی که یک نود بسته ای را برای ارسال به یک نود دارد ایجاد می شود. این نوع از الگوریتم های مسیریابی،پروتکل های مسیریابی(لحظه تقاضا) نامیده می شوند.پروتکل های این روش عبارتند از:

۳-۲-۲-۱)پروتکل ssr

این پروتکل مسیرها را بر مبنای قدرت و توان سیگنال‌ها بین نود ها انتخاب می‌کند. بنابراین مسیرهایی که انتخاب می‌شوند نسبتا قوی تر هستند. می‌توان این پروتکل را به دو بخشDRP 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 نود مربوط به خود را داشته باشد آن را به لایه‌های بالاتر بفرستد.

www.Prozhe.com

۳-۲-۲-۲)پروتکلdsr

در الگوریتم dsr یا dynamic source routing ، نود مبدا یک بسته به نام preq تولید کرده و در آن نود مبدا و مقصد را مشخص می کند و این بسته را به وسیله الگوریتم flooding ارسال می کند .هر نود با دریافت یک بسته preq ، در صورتی که مسیر مقصد را نداند، نام خود را به لیست بسته اضافه کرده و آن را Broadcast می کند .بدین ترتیب وقتی این بسته به مقصد می رسد، یک بسته حاوی اطلاعات نود های مسیر و ترتیب آنها در دست نود مقصد وجود دارد .نود مقصد یک بسته prep ایجاد کرده و آن را از روی لیست موجود در سرآیند بسته preq برمیگرداند. نود های میانی نیز از روی لیست موجود می دانند که بسته را می بایست برای چه کسی ارسال نمایند . بنابراین بسته مسیر را به صورت برعکس طی می کند تا به نود مبدا برسد .این روش اگرچه روش خوبی است و حتما به جواب می رسد ولی بار شبکه را بالا می برد و پهنای باند زیادی را مصرف می کند .زیرا بسته هایی با سرآیند های بزرگ در شبکه منتقل می شوند .افزایش حجم سرآیند ها با افزایش فاصله نود مبدا و مقصد زیاد می شود .این افزایش حجم به دلیل قرار گرفتن نام عناصر میانی شبکه در سرآیند بسته است.بعد از این دیگر فرستنده داده می تواند مسیر مقصد را در سرآیند داده ارسالی قرار دهد تا نود های میانی ازطریق این مسیر، بدانند که باید بسته را به چه کسی ارسال نمایند .به همین دلیل است که این الگوریتم را مسیریابی پویای مبدا می نامند.

هنگامی که یک نود نتواند بسته داده را به نود بعدی ارسال نماید، بسته ای با نام perr تولید نموده و آن را بر روی مسیر باز می گرداند .بدین ترتیب نود های دریافت کننده perr متوجه قطع ارتباط بین آن دو نود میشوند .بنابراین عملیات مسیریابی از سر گرفته می شود.

مزایا و معایب:

Dsr با استفاده از یک رویکرد واکنشی که نیاز به پیام های دوره ای سیل آسا برای بروز رسانی جدول شبکه عمل می کند که رویکرد جدول محور را حذف می کند. نود های میانی نیز با

www.Prozhe.com

استفاده از اطلاعات مسیرهای موجود در حافظه نهان میزان سربار را کاهش می دهد. از معایب dsr این است که مکانیزم نگهداری مسیر، لینک شکسته شده را به صورت محلی تعمیر نمی کند.تأخیر راه اندازی ارتباط بیشتر از پروتکل های جدول table driven است.

حتی اگر این پروتکل در محیط های ایستا و کم تحرک خوب عمل کند، با افزایش سرعت نود ها میزان کارایی کم می شود. همچنین مکانیزم مسیریابی منبع استفاده شده در dsr سربار قابل توجهی دارد. این سربار مسیریابی مستقیما با طول مسیر در ارتباط است.

۳-۲-۲-۳)پروتکل tora

بر اساس الگوریتم مسیریابی توزیع شده بنا شده است و برای شبکه‌های موبایل بسیار پویا طراحی شده‌است. این الگوریتم برای هر جفت از نود ها 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.

۳-۲-۲-۴)پروتکل aodv

در الگوریتم aodv یا Advanced On-demand Distance Vector بر خلاف الگوریتم قبلی،مسیر را در سرآیند بسته قرار نمی دهد .بلکه هر نود هنگام دریافت preq، از روی جدولی که از قبل دارد آن را کنترل می کند .اگر مسیر نود نهایی را در جدول خود داشته باشد، آنگاه prep صادر میکند. در غیر اینصورت پیغام preq را broadcast می کند. مسلما prepها میتوانند به نود فرستنده preq بازپس فرستاده شوند .برای اینکه یک نود میانی از این موضوع آگاه شود که آیا مسیری که او می داند، جدید تر از درخواست ارسال شده است، از یک شماره توالی در پیامهای

www.Prozhe.com

preq استفاده می شود .بدین ترتیب تنها در حالتی که شماره توالی preq کوچکتر از شماره توالی مسیر دانسته شده باشد، پیام prep توسط نود میانی صادر می گردد.

مزایا و معایب:

مزیت اصلی این پروتکل این است که مسیرهای تأسیس شده برای تقاضا و اعداد ترتیبی مقصد برای پیدا کردن آخرین مسیر به مقصد مورد استفاده قرار می گیرند. تأخیر راه اندازی ارتباط نیز پایین است. یکی از معایب این پروتکل این است که اگر شماره ترتیبی منبع بسیار قدیمی باشد و نود های میانی جدید باشند و شماره های مقصد ترتیبی نباشند،نود های میانی به مسیرهای متناقض می روند و در نتیجه داده های به دست آمده قدیمی می باشند. همچنین بسته های پاسخ مسیرهای متعدد در پاسخ به یک بسته درخواست مسیر می تواند منجر به کنترل سربارهای سنگین شود.یکی دیگر از نقاط ضعف aodv دیده بانی های (کنترل شبکه) دوره ای می باشد که می تواند منجر به مصرف پهنای باندهای غیر ضروری شود.

۳-۲-۲-۵)پروتکلrdmar

این نوع از پروتکل فاصله ی بین دو نود 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.

۳-۲-۳)پروتکل های پیوندی (Hybrid)

ترکیبی از پروتکل های پیشگیرانه و واکنش دار است. این پروتکل‌ها روش مسیریابی بردار فاصله را برای پیدا کردن کوتاه‌ترین به کار می‌گیرند و اطلاعات مسیریابی را تنها وقتی تغییری در

www.Prozhe.com

توپولوژی شبکه وجود دارد را گزارش می‌دهند. هر نودی در شبکه برای خودش یک zone مسیریابی دارد و رکورد اطلاعات مسیریابی در این zone ها نگهداری می‌شود. پروتکل های این روش عبارتند از:

۳-۲-۳-۱)پروتکلZrp

این پروتکل از اکتشاف proactive درون یک همسایگی محلی یک نود استفاده میکند 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 نود های 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»

کارایی zrp بستگی به انتخاب شعاعی دارد که بر اساس 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.

۳-۲-۳-۲)پروتکلZhls

دو سطح مکان شناسی را تعریف میکند.سطح نود و سطح منطقه.مکان شناسی سطح نود میگوید چگونه نود های یک منطقه به طور فیزیکی به یکدیگر متصل میشوند.یک اتصال بی هدف (تصادفی) بین دو منطقه وجود خواهد داشت اگر حداقل یک نود از یک منطقه بطور فیزیکی با دیگر نودها در مناطق دیگر متصل باشد.مکان شناسی سطح منطقه می گوید که چگونه مناطق با یکدیگر در ارتباط هستند.دو نوع پاکت یا بسته ی حالت پیوستگی (lsp node و منطقه lsp)

www.Prozhe.com

وجود دارد. یک نود lsp یک نود شامل اطلاعات نود مجاور آن می باشد و با منطقه ای که به عنوان منطقهLSP شامل اطلاعات این محدوده می شود منتقل و اشاعه می شود و بطور جهانی منشر می گردد. بنابراین هر نود دانش اتصال به نودها در منطقه ی خود وتنها اطلاعات اتصال منطقه درباره مناطق دیگر در شبکه را دارد.بنابراین با ارائه منطقه ی id و node id از یک مقصد ،این بسته یا پاکت مبتنی بر منطقه id ردیابی می شود تا به منطقه درست آن برسد.سپس در آن منطقه براساس شناسه node ردیابی می شود.

۳-۲-۴)پروتکل های موقعیتی (Location)

این پروتکل ها از موقعیت نودها در شبکه استفاده کرده و از اطلاعات توپولوژی کمترین استفاده را میکنند. پروتکل هایی که از چنین طراحی استفاده می کنند، ایرادات ناشی از تغییر مکرر توپولوژی شبکه را از بین می برند. در پروتکلهای مبتنی بر موقعیت،نودها اطلاعات توپولوژی محلی(یک یا دو گام) را به کمک یک پروتکل سلام حفظ می کنند. برای مسیریابی یک بسته به سمت مقصد، نود مبدأ از ارسال حریصانه برای انتخاب گام بعدی به سمت مقصد استفاده می کنند. در ارسال حریصانه،یک نود،گام بعدی در جهت مقصد را طوری انتخاب می کند که در بین همسایگانش به لحاظ جغرافیایی به مقصد نزدیک تر باشد. از آنجایی 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.

دو حالت مسیریابی در این روش وجود دارد : ۱- موقعیت مبدأ و مقصد و یک جدول همسایگی محلی برای هر نود وجود دارد و بسته ها از مبدأ به سمت مقصد ارسال میشوند.۲-هر نود با استفاده از برخی سیستم های موقعیت یاب نظیر GPS موقعیت خودش را تعیین می کند و همچنین موقعیت هر نود دیگر در سیستم را نیز به دست می آورد.

www.Prozhe.com

حالت اول، مسیریابی مبتنی بر موقعیت نام دارد و نمونه هایی چون CFG و GPSR از این نوع اند. مسیریابی مبتنی بر موقعیت معمولا 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 نام دارد و نمونه هایی مانند RLS،GLSو RLS پروتکل های آن هستند که نود ها نیاز ندارند که مسیرها را ساخته و نگهداری کنند و این پروتکلها در مقایسه با پروتکل های proactive و reactive مقیاس پذیری بیشتری دارند.از جمله پروتکل ها عبارتند از:

۳-۲-۴-۱)پروتکلDream

این پروتکل جزو روش های شناخته شده مسیریابی manet(موبایل ادهاک) میباشد در این الگوریتم هر نود مختصات و موقعیت خود را از طریق gps دریافت میکند و سپس نود ها اطلاعات موقعیت خود را از طریق روش های مختلف در اختیار یکدیگر قرار می دهند.جهت به روز کردن جدول های مسیریابی هر نود ، روش های مختلفی بکار برده می شود.

این الگوریتم بر اساس دو نظریه تاثیر فاصله و فرکانس بروزرسانی ساخته شده است؛بدین صورت که دو نود که فاصله بین آنها زیاد است،به نظر می رسد که نسبت به یکدیگر کندتر حرکت میکنند.(یعنی نود دورتر به نظر کندتر حرکت می کند)و نود هایی که کندتر حرکت میکنند نسبت به نود هایی که سریعتر حرکت می کنند نیاز کمتری به بروزرسانی اطلاعات دارند.

چون مسافت و حرکت در این پروتکل نقش مهمی دارند؛این الگوریتم را the distance routing effect algorithm for mobility نامیده اند. در این الگوریتم نیاز نیست که میزان وسیعی از اطلاعات کنترلی را همانند پروتکل های proactive رد و بدل کنیم و همچنین برخلاف

www.Prozhe.com

الگوریتم های reactive، چون هیچ کشف مسیری صورت نمی گیرد،تاخیری جهت مسیریابی به شبکه اعمال نمی شود.

در این الگوریتم،میزان و سرعت تولید پیام های کنترل مطابق با میزان و سرعت حرکت هر نود تعیین و بهینه سازی می شود؛در نتیجه distance effect، پیام های کنترلی اجازه خواهند داشت که در شبکه حرکت کنند قبل از اینکه غیر قابل استفاده شوند که این عمل فقط به مسافت نسبی (جغافیایی) بین نود در حال حرکت و جدول های تعیین مسیر که در حال update شدن است، بستگی خواهد داشت.

در این روش تعداد کپی ها به علاوه تعداد جهش های پیام های کنترل که حرکت خواهند کرد هر دو بدون از دست دادن کیفیت بهینه سازی می شوند. این یعنی اینکه نسبت به پروتکل های موجود، الگوریتم dream از پهنای باند موجود و انرژی در هر نود ، بیشتر برای ارسال پیام های داده استفاده میکند.

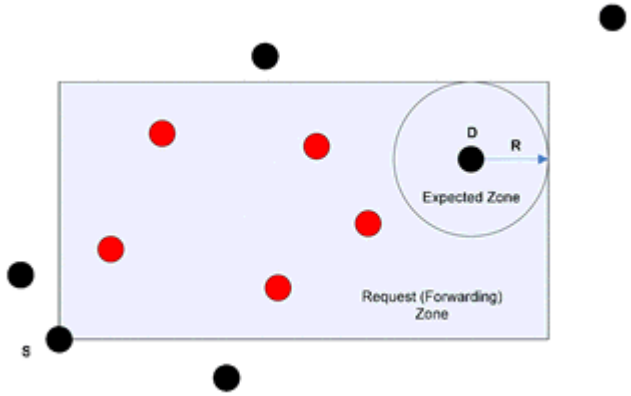
این الگوریتم بصورت ماندگار loopfree است چون پیام های داده دور از منبع خود در یک مسیر ویژه منتشر و زیاد می شوند.با حرکت و جنبش قابل تطبیق است،چون فرکانسی که اطلاعات تعیین مسیر را منتشر می کند، به میزان و سرعت حرکت نود ها وابسته است.

۳-۲-۴-۲)پروتکلLAR

این پروتکل بر مبنای عملکرد پروتکل DSR طراحی شده است. بنابراین یک روش مسیریابی بر اساس مبدا و همچنین مبتنی بر درخواست است. مهمترین بهبودی که این پروتکل نسبت به DSR یافته است این است که در آن به همراه همه بسته ها، اطلاعات مربوط به موقعیت نود های فرستنده و گیرنده را می فرستد. در این روش از اطلاعات مربوط به موقعیت برای ارسال به جلوی بسته ها استفاده نمی شود،بلکه از این اطلاعات برای بهبود عملکرد فاز کشف مسیر در

www.Prozhe.com

الگوریتم مسیریابی استفاده می شود. در روش LAR بجای پخش کردن بسته ها ، تنها در محدوده ارسال این عمل انجام می گیرد. به شکل (۳-۱)توجه شود:



شکل۳-۱)محدوده ارسال lar

دو استراتژی برای فاز کشف مسیر ارائه شده است. در استراتژی اول که نام آن LAR۱ هست، نود ها بررسی می کنند که آیا در محدوده ارسال قرار دارد یا خیر. محدوده ارسال محدوده ای است که با توجه به موقعیت نود مقصد(ناحیه مورد انتظار) و همچنین سرعت تخمینی آن نود ، مشخص می گردد. نحوه محاسبه ناحیه مورد انتظار و ناحیه ارسال، در شکل بالا دیده می شود. شعاع ناحیه مورد انتظار،با داشتن موقعیت قبلی نود مقصد،زمان سپری شده از محاسبه آن و همچنین سرعت تخمینی مقصد،به صورت رابطه (۳-۱) تعیین می گردد:

$$R=V_{avg}\times(t_1-t_0)$$ رابطه۳-۱)شعاع ناحیه مورد انتظار

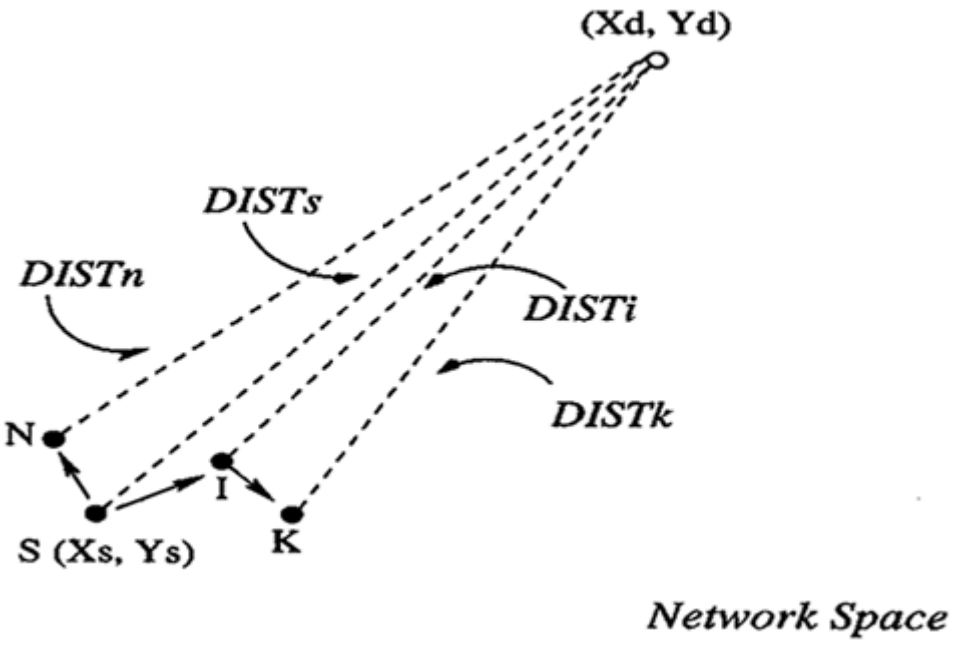
در این رابطه ، t_0 زمانی است که آخرین اطلاعات موقیت نود مقصد بدست آمده است. زمان t_1 هم زمان حال است که به دنبال تخمین موقعیت نود مقصد هست.

اگر نودی،با توجه به موقعیت نود مبدا و همچنین ناحیه مورد انتظار ،تشخیص دهد که در ناحیه ارسال قرار دارد،بسته را به نود های همسایه خود خواهد فرستاد و در غیر اینصورت، بسته

www.Prozhe.com

درخواست مورد نظر را از بین می برد. این روند تا رسیدن بسته به مقصد ادامه می یابد.این دو ناحیه می توانند در طول ارسال دوباره محاسبه شوند و با آخرین شرایط تطبیق پیدا کنند.

در روش دوم که نام آن LAR۲ است، نود میانی تعیین میکند که آیا در محدوده ارسال قرار دارد یا خیر. محدوده ارسال در این روش ، ناحیه ای است که تمامی نود های موجود در آن از نود جاری به مقصد نزدیک ترند. این مکانیزم در شکل (۳-۲) نمایش داده شده است.



شکل۳-۲)مکانیزم lar ۲

در هر دو روش برای کم کردن ناحیه ها، از یک فاکتور به نام فاکتور خطا یا δ استفاده می شود که در رابطه(۳-۲) آورده شده است:

$$LAR۱:R=V_{avg}\times(t_۱-t_۰)+\delta$$ رابطه۳-۲)روش کم کردن ناحیه ها

در هر دو روش پرونکل LAR ، فاز کشف مسیراز دو بخش تشکیل می شوداگر در بخش اول در زمان معینی پاسخ مسیر دریافت نشد، در بخش دوم از ارسال سیل آسای معمولی استاده می شود. اگر جواب تا ۳۰ ثانیه ارسال نشود، مقصد مورد نظر غیر قابل دسترس تلقی می شود.

www.Prozhe.com

۳-۳)دسته بندی دوم الگوریتم های مسیر یابی شبکه های موردی

اینگونه دسته بندی که با توجه به چگونگی تعیین توپولوژی شبکه مشخص می شود، در ادامه به دو دسته از این الگوریتم ها اشاره خواهد شد:

۳-۳-۱) سلسله مراتبی

در الگوریتم های مسیریابی سلسله مراتبی نود ها درون گروه های مختلف تقسیم بندی می شوند. از هر گروه یک نود به عنوان سرگروه انتخاب میشود. ها نود یا یک سرگروه می باشد و یا یک گام بی سیم می باشد. یک نود 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 میشوند. زیر شبکه شامل دروازه ها و سرگروه ها می باشد که به آن ستون فقرات شبکه نسبت داده میشوند. هر سرگروه اطلاعاتی را راجع به دیگر نود های موجود در آن گروه نگهداری میکند. و هر چند وقت یکبار این اطلاعات بین سرگروه های موجود در شبکه مبادله می شوند. بنابراین سرگروه ها اطلاعات توپولوژی شبکه را گردآوری میکنند. یک نود که می خواهد بسته هایی را به نود دیگر ارسال کند اطلاعات مسیریابی را از سرگروهش فراهم می کند.

این روش مسیریابی ، مسیریابی آگاه از توپولوژی شبکه نامیده میشود. چندین روش برای پیاده سازی این مسیریابی وجود دارد. اولین امکان این است که هر نود یک مسیر بهینه برای هر نود 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.

هر چند که با تغییرات توپولوژی ، نود ها می خواهند اطلاعات مسیریابیشان را به روز رسانی کنند و دوباره مسیرهایی 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 نود ها

www.Prozhe.com

اطلاعات مسیریابی کمتری را درباره توپولوژی شبکه نگهداری می کنندوهرچند که هر بسته موجب سرباره مسیریابی می شود. که در ادامه به چند الگوریتم مسیریابی اشاره میشود:

۳-۳-۱-۱)الگوریتم مسیریابی مبتنی بر مورچه متحرک(mabr)

های سن باتل و براون ، این الگوریتم را به عنوان اولین الگوریتم برای manet های(مویایل ادهاک) مقیاس بزرگ بررسی شده با حشرات اجتماعی معرفی کردند که مبتنی بر شبکه مورچه است.این الگوریتم شامل ۳ لایه است:

۱-پروتکل استخراج مکان شناسی: این لایه با استفاده از اطلاعات وضعیتی نود برای تعیین مرکز، شبکه را به محدوده های منطقی گروه بندی می کند. نود های نزدیک به نود فعلی به محدوده ـهای کوچکی گروه بندی میشوند و همین طور که فاصله از نود فعلی افزایش پیدا می کند، بیشتر نود ها با یکدیگر گروه بندی می شوند.

۲- مسیریابی مبتنی بر مورچه سیال(mabr): لایه ی mabr بسته ها را در شبکه سلسله مراتب ساده مسیریابی می کند.هر نود دو ساختار داده را ذخیره می نماید:یک جدول مسیریابی و یک جدول پیوند ارزش هزینه.

جدول مسیریابی این احتمال را ذخیره می کند که یک پیوند خاص به عنوان یک جهش بعدی منطقی برای بسته مورد هدف برای یک محدوده منطقی خاص به کار خواهد رفت.همانطور که بسته ها به شبکه منتقل می شوند این مسیر به وسیله بسته در قسمت فوقانی آن ثبت می شود و برای کشف مسیرهای جدید همان مکانیزم FANT/BANT را که در antnet به کار میرود استفاده می کند یعنی با بروز کردن سطوح فرومون BANT مبتنی بر طول مسیر کشف شده باFANT کشف می ـشود.

www.Prozhe.com

وقتی یک نود به یک بسته ارسال می شود نود تعیین می کند که در محدوده ی منطقی مقصد قرار گرفته است و سپس احتمالاتی را در جدول مسیریابی برای انتخاب یک محدوده منطقی جهش نهایی بکار می برد. از این رو این احتمال وجود دارد که بیش از یک مسیر با امکان غیر صفر وجود داشته باشد.MABR از مسیریابی چند مسیری حمایت می کند.

۳- بسته های مستقیم رو به جلو: این لایه مسئول حرکت رو به جلوی بسته های واقعی از یک نود به دیگری است.این الگوریتم می تواند هر نود را که نسبت به نود فعلی به مقصد نزدیک تر است به عنوان جهش نهایی انتخاب کند یا الگوریتم میتواند یک نود را انتخاب کند که فاصله بین نود فعلی و مقصد را بیشتر کاهش میدهد. الگوریتم mabr یک کار رو به پیشرفت است و هیچ تحقق کاملی از این پروتکل در دسترس نیست.

۳-۳-۱-۲)الگوریتم Sdr اتخاذ شده

این الگوریتم نیز شامل ۳ بخش زیر است:

۱-خوشه بندی بصورت مجموعه: کاسابالیدیس و دیگر همکارانش وقتی در حال کشف مسیرها با استفاده از مکانیزم FANT/BANT بودند متوجه شدند که ترافیک توسط شبکه مورچه (AntNet) وABC ایجاد می شود که در شبکه دارای مقیاس بزرگ بازدارنده بود.علاوه بر این زمانهای حرکت بزرگ توسط FANT که در شبکه های بزرگ محاسبه می شود این احتمال را افزایش می دهد که اطلاعات اجرایی توسط BANT هااز رونق بیفتد. بنابراین این شبکه به مجموعه هایی خوشه بندی می شود.

۲-کشف مسیرها: مکانیزم کشف مسیرها،دو نوع عنصر را بکار می برد که مورچه های مجموعه و مورچه های محلی نامیده می شوند مورچه های مجموعه مسئول کشف مسیرها از یک مجموعه به دیگری هستند،در حالی که مورچه های محلی مسئول کشف مسیرها در بین خوشه ها

www.Prozhe.com

هستند .هر نود دو جدول مسیریابی را حفظ می کند ،یک جدول مسیریابی مجموعه ای و یک جدول مسیریابی محلی که به ترتیب برای بهره وری از مسیریابی بین مجموعه ها و بین نود ها در یک مجموعه است. نود ها به طور دوره ای FANT را به هر نود در مجموعه محلی نود و به یک نود در هر مجموعه خارجی ارسال می کنند.

همانطور که FANT ها به سراسر شبکه منتقل می شوند این مسیر توسط بسته ای ارائه می شود که در قسمت فوقانی بسته ثبت شده است (یک مکانیزم مسیریابی مبدا بکار رفته است).وقتی نود مقصد دریافت می شود یک BANT راه اندازی می شود که مسیر ارائه شده توسط FANT در حال برگشت به نود مبدا را مورد تعقیب قرار می دهد و سطوح فرومون را در این مسیر جدید می کند.

۳- بسته رو به جلو(پیش رونده): بسته های داده با استفاده از احتمالات ایجاد شده بوسیله FANT وBANT های جلورونده از جدول مسیریابی کلونی وجدول مسیریابی محلی برای نودهای بیرونی و درونی مجموعه نود فعلی به ترتیب استفاده می کند.طول صف بسته به صورت یک شاخص سطح فعلی ازدحام در نود جهش نهایی در نظر گرفته می شود و احتمالات جهش بعدی برای نود های جالب با ازدحام پایین تر تنظیم می شود.

این الگوریتم با الگوریتم های شبکه مورچه،حالت پیوسته و فاصله بردار مقایسه شده است. نتایج شبیه سازی نشان می دهد که sdr اتخاذ شده ، زمانهای تاخیر بالاتر،بازده داده های بالاتر و کاهش بسته پایین تر نسبت به الگوریتم های دیگر دارد.

۳-۳-۱-۳)الگوریتم HOPENT

الگوریتمHOPENT شامل کشف فعال محلی در مجاورت نود و ارتباط واکنشگر بین همسایگان است. این شبکه به محدوده هایی تقسیم می شود که همسایه محلی نود هستند.هر نود

www.Prozhe.com

دارای دو جدول مسیریابی است: جدول مسیریابی درون محدوده ای(IntraRT) و جدول مسیریابی بین محدوده ای (InterRT).

IntraRT بطور فعال حفظ می شود بنابراین یک نود می تواند مسیری را برای هر نود در محدوده آن به سرعت به دست اوردInterRT . مسیر را برای یک نود فراتر از محدوده آن ذخیره می کند. این جدول مسیریابی مبدا طبق نیاز تنظیم می شود همانطور که مسیرهای بیرون یک محدوده مورد نیاز است.

کشف مسیر شامل کشف مسیر در یک محدوده و بین محدوده ها است. کشف مسیر در یک محدوده با استفاده از یک جدول ردیابی درون محدوده ای همراه است.وقتی یک نود مبدا می خواهد داده ها را به یک مقصد مشخص ارسال کند،ابتدا IntraRT را مورد بررسی قرار می دهد که آیا مقصد در محدوده آن قرار دارد.اگر مقصد را بیابد پس فرآیند کشف مسیر انجام می شود.در این الگوریتم هر مورچه یک نود را انتخاب می کند که بهترین مسیر تا مقصد است .برای انجام آن یک مورچه تمام ارتباطات مجاور تا یک نود راکشف می کند که هنوز قبل از انتخاب نود ، جهش بعدی را ملاقات نمی کند.اگر چنین نود ملاقات نشده ای وجود نداشته باشد،مورچه برای جهش بعدی تجمع فرومون را بررسی و جستجو می کند.این استراتژی کشف تضمین می کند که هیچ ارتباطی از دست نمی رود.بعد از انتخاب نود با جهش نهایی،فرومون ارتباط انتخابی تقویت می شود و تجمع فرومون روی تمام پیوندهای دیگر صادر می شود. در مسیر برگشت آن به مبدا یک مورچه دوباره تجمع فرومون را جدید و به روز می کند.وقتی یک مبدا می خواهد بسته های داده را به یک مقصد بیرون از محدوده ان ارسال کند اگر یک مسیر در حال حاضر توسط مورد قبلی و بعدی کشف شده باشدInterRT را برای تعیین بررسی می کند.اگر مسیر طی نشده باشد این نود فورا بسته ها را می فرستد .علاوه بر این، نود مورچه های رو به جلو یا پیش رونده خارجی را برای کشف مسیری تا مقصد ارسال میکند.مورچه های پیش رونده خارجی ابتدا بوسیله ی نود به نود های حاشیه ای یا مرزی فرستاده می شوند.

www.Prozhe.com

درحاشیه، نود های مرزی بررسی می شوند تا مشاهده شود آیا مقصد در آن محدوده است .اگر مقصد در آن محدوده نباشد و مسیر طی شده باشد مورچه ها رو به جلو به منطقه بعدی از طریق نود های حاشیه ای دیگر در آن محدوده پیش می روند.این فرآیند ادامه می یابد تا مقصد کشف شود .در مقصد تعداد دفعات مورچه رو به جلو با تعداد دفعات نشان داده شده در جدول برای مقصد مقایسه می شود .اگر مورد اولی بزرگتر باشد پس مورچه رو به جلو تبدیل به مورچه پس رونده می شود و به مبدا فرستاده می شود علی رغم اینکه مورچه از بین می رود.

یک مسیر می تواند بعلت نود ها در طول حرکت مسیر با ارتباط قطع شده غیر معتبر باشد.اگر مسیر اسیب دیده یک مورد داخلی در یک محدوده باشد ان بعد از یک دوره بازیافت خواهد شد زیرا IntraRT به طور فعالی حفظ می شود .اگر یک مسیر درون محدوده ای غیر معتبر باشد نود جریان بالا از محل ارتباط قطع شده یک رویکرد زوج محلی را راه اندازی می کند.با تلاش برای کشف یک مسیر جایگزین تا مقصد در حالی که تمام بسته های ضربه گیر آن را دریافت می کند. اگر نود به طرزی موفق مسیری جدید را تا مقصد پیدا کند.تمام بسته های بافر را تا مقصد از طریق مسیر پیدا شده می فرستد در این فاصله مورچه مورد توجه به مبدایی فرستاده می شود تا اجازه دهد نود مبدا تغییر مسیر را شناسایی کند .اگر چنین مسیر جایگزینی نتواند پیدا شود،یک مورچه دارای خطا به نود مبدا فرستاده خواهد شد .بعد از دریافت مورچه دارای خطا،اگر نود مبدا هنوز نیاز به یک مسیر تا مقصد دارد یک مورچه پیش رونده جدید کشف مسیری تا مقصد را اغاز خواهد کرد.

نتایج مقایسه الگوریتم مربوطه باAODV نشان می دهدکه HOPNET تاخیر انتها به انتها بهتر،قسمت فوقانی کنترل بالاتر و نسبت ارائه بسته پایین تر ازAODV را دارد.

www.Prozhe.com

۳-۳-۲)مسطح

در الگوریتم های مسیریابی مسطح همه نود ها مانند روتر عمل میکنند. از این رو هیچ انتخاب سرگروهی وجود ندارد و هیچ سازماندهی مجدد دوره ای شبکه لازم نمی باشد. بیشتر الگوریتم های مسطح تلاش می کنند که یک نسخه توزیع شده از الگوریتم کوتاه ترین مسیر و یا سیل آسا را ارائه کنند که عموما فرستنده یک کپی از پیغام را به هر همسایه ارسال میکند. 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 نود مقصد در بخش مشابه منبع باشد، پیغام به طور یقین به مقصد میرسد.در ادامه به چند الگوریتم این روش پرداخته می شود:

۳-۳-۲-۱)الگوریتم مسیریابی مبتنی بر لانه مورچه

Antnet یک الگوریتم مسیریابی(ACo) فعال برای بسته ی شبکه های سوئیچ است. الگوریتم مسیریابی مبتنی بر لانه مورچه Ant colony based Routing Algorithm (ARA) که توسط Gunes و همکاران پیشنهاد شد یک الگوریتم ردیابی ACo فعال برای شبکه های اختصاصی موبایل است.این الگوریتم از نظر سادگی ساختار بسیار شبیه سایر الگوریتم های مسیریابی می باشد و شامل سه فاز است:

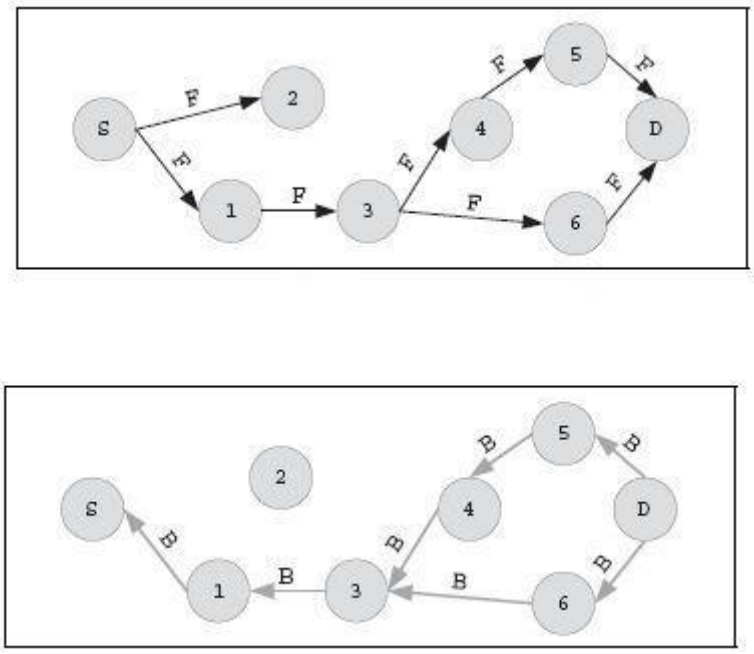
۱-فاز یافتن مسیر

در فاز مسیریابی، مسیرهای جدید ایجاد می شوند. ایجاد مسیر جدید نیازمند استفاده از یک مورچه فوروارد و یک مورچه بک وارد می باشد. مورچه های جلوروونده مشابه بسته های RREQ در AODV است.FANT توسط فرستنده پخش می شوند. نود دریافت FANT برای اولین بار ، یک رکورد در جدول مسیریابی ایجاد می کند.مدخل جدول مسیریاب بر مبنای مفهوم فرمون

www.Prozhe.com

ردیابی می شود. یک مدخل برای یک نود مشخص A شامل تمام همسایه های آن با مقدار فرومون مربوط به آنها است. سپس نود FANT همسایگان خود را تقویت می کند.هنگامی که FANT با تاخیر به مقصد می رسد، این نود اطلاعات را از FANT استخراج و آن را از بین می برد.پس از آن،یک BANT ایجاد می شود که مشابه RREP در AODV است و آن را به نود منبع می فرستد.BAnt در مسیر خود هم مدخل هایی را مجددا در جدول مسیریابی برای مبدا (مقصد اتصال) قرار می دهد.هنگامی که فرستنده BANT را از نود مقصد دریافت می کند، مسیر ایجاد شده و بسته های داده می تواند فرستاده شود. در حالی که راه رفتن مورچه ها در شبکه، غلظت لینک های فرومون $\Delta\varphi$ افزایش می یابد ، این پارامتر تابعی از طول مسیراست.

در شکل (۳-۳)فاز کشف مسیر به وسیله FANT ها و BANT ها مشاهده می شود:



شکل ۳-۳)فاز کشف مسیر FANT و BANT

در شکل بالا مورچه رو به جلو(F) از نود (S) به سمت نود مقصد (D) ارسال می شود. مورچه توسط نود های دیگر،زمانی که جدول مسیریابی آنها و ارزش های فرمون مقداردهی اولیه می شود فرستاده می شود.

www.Prozhe.com

مورچه رو به عقب (B) که مشابه کار مورچه رو به جلو است.که توسط نود مقصد به سمت نود منبع ارسال می شود.

شکل بالا تصویر شماتیکی از فاز کشف مسیر را مجسم کرده است. در مورد تصویر کشیده شده، نود ۳ دارای دو راه برای مسیر ، از طریق نود ٤و نود ٦ است. در این مورد، مورچه رو به جلو تنها یک مسیر فرمون به سمت نود منبع ایجاد می کند،اما مورچه رو به عقب دو بخش فرمونی نسبت به نود مقصد ایجاد کرده است.

۲- فاز نگهداری

این فاز مسئول درست کردن مسیر درحین اتصال است. در این مرحله به محض اینکه FANTها و BANT ها ردپایی از فرومون برای نود مبدا و مقصد به جا می گذارند، بسته های داده بعدی نیز مقدار فرومون را افزایش می دهند.

۳- فاز جابجایی شکست

در مورد شکست مسیر الگوریتم، مسیر خطادار در شبکه را از طریق فقدان یک تصدیق، تشخیص داده ومورچه را بر روی یک مسیر جایگزین هدایت می کند.بدین صورت که اگر یک نود برای یک لینک خاص پیام ROUTE_ERROR را دریافت نماید، در ابتدا با تنظیم مقدار فرومون به صفر، این لینک را غیرفعال می‌کند. سپس نود در جدول مسیریابی خود به دنبال یک مسیر جایگزین می‌گردد. اگر لینک دیگری موجود بود بسته را از طریق این مسیر ارسال می‌کند . در غیر این صورت به نود های مجاور اطلاع می‌دهد، به امید اینکه آنها بتوانند این بسته را انتقال دهند. یا بسته به نود مقصد انتقال می‌یابد یا اینکه پیمایش معکوس تا نود مبنا پیش خواهد رفت. اگر بسته به مقصد نرسد، مورچه به مسیر قبلی بالای جریان باز می گرددو مبدأ بایستی عملیات کشف مسیر جدیدی را آغاز نماید.

www.Prozhe.com

خصوصیات ARA

یک الگوریتم مسیریابی برای شبکه های تلفن همراه adhoc باید شرایط زیر را برآورده کند:

توزیع عملیات: در ara، هر نود دارای مجموعه ای از ۲ عدد فرمون J درجدول مسیریابی برای ارتباط بین گره Vi و VJ است. هنگامی که مورچه ها نود را در جستجوی مسیر ملاقات می کنند، φi هر نود شمارنده فرومون را به طور مستقل کنترل می کند.

حلقه آزاد: نود ها شماره دنباله منحصر به فردی از مسیر بسته کشف شده FANT وBANT را ثبت می کنند، بنابراین آنها تولید حلقه نمی کنند.

عملیات مبتنی بر تقاضا: مسیرها به وسیله دستکاری مقابله با فرمون J ، φi در نود ها تاسیس می شوند. با گذشت زمان، هنگامی که مورچه ها عمل بازدید نود را انجام نمی دهند مقدار فرومون کاهش می یابد تا به صفر برسد. هنگامی که یک فرستنده تقاضایی کند فرآیند پیدا کردن مسیر تنها اجرا می شود.

محل: جدول مسیریابی و اطلاعات آماری بلوکی از یک نود محلی به هر نود دیگر آنها منتقل میشود.

چگونگی کارکرد الگوریتم

در این الگوریتم اگر یک نود بخواهد اتصالی به نود دیگر برقرار کند، یک مورچه جلورونده (FANT) می فرستد، که به طور تصادفی در شبکه حرکت می کند. منظور از تصادفی یعنی اینکه روی هر نود، FANT یکی از همسایه های نود را با احتمال مساوی انتخاب می کند. در ضمن در حرکت از یک نود به نود بعدی ، FANT با گذاشتن یک ردپا مدخلهای جدول مسیریابی در نودهایی که به آنها می رسند از خود به جا می گذارند.همچنین یک مورچه رو به جلو درهر نود میانی ،جهش بعدی را می تواند با استفاده از اطلاعات ذخیره شده در جدول ردیابی آن نود

www.Prozhe.com

انتخاب نماید.نود بعدی با استفاده از احتمال نسبی به درستی آن نود که با مقدار فرومون باقی مانده در اتصال با آن node مقایسه شده انتخاب می شود. این عمل ادامه پیدا می کند تا زمانیکه FANT به مقصد برسد. به محض اینکه به مقصد می رسد، یک مورچه عقب رو(BANT) تولید می شود، که مدخلهای جدول مسیریاب را به سمت عقب طی می کند تا به مبدا برسد.خود BANT هم در مسیرش مدخل هایی را مجددا در جدول مسیریابی برای مبدای آن (مقصد اتصال) قرار می دهد.

در اکثر موارد ما قصد ارسال بیش از یک FANT را در شبکه داریم. ابتدا تصور کنید که یک FANT را ارسال کردیم. کیفیت مسیری که می خواهیم پیدا کنیم، خیلی خوب نخواهد بود. اگر FANT در هیچ حلقه ای نیفتد، BANT هم همین مسیر FANT را برای برگشت انتخاب می کند.

حال اگر یک نود یک FANT دریافت کند باید چه کاری انجام دهد؟یک فلوچارت از این عمل در شکل (۳-٤) نشان داده شده است. با دسترسی نود X به یک FANT ، ابتدا جدول مسیریابی بروز می شود. (هیچ اطلاعاتی راجع به اینکه این نود به کجا خواهد رفت در جدول مسیریاب گذاشته نخواهد شد.)

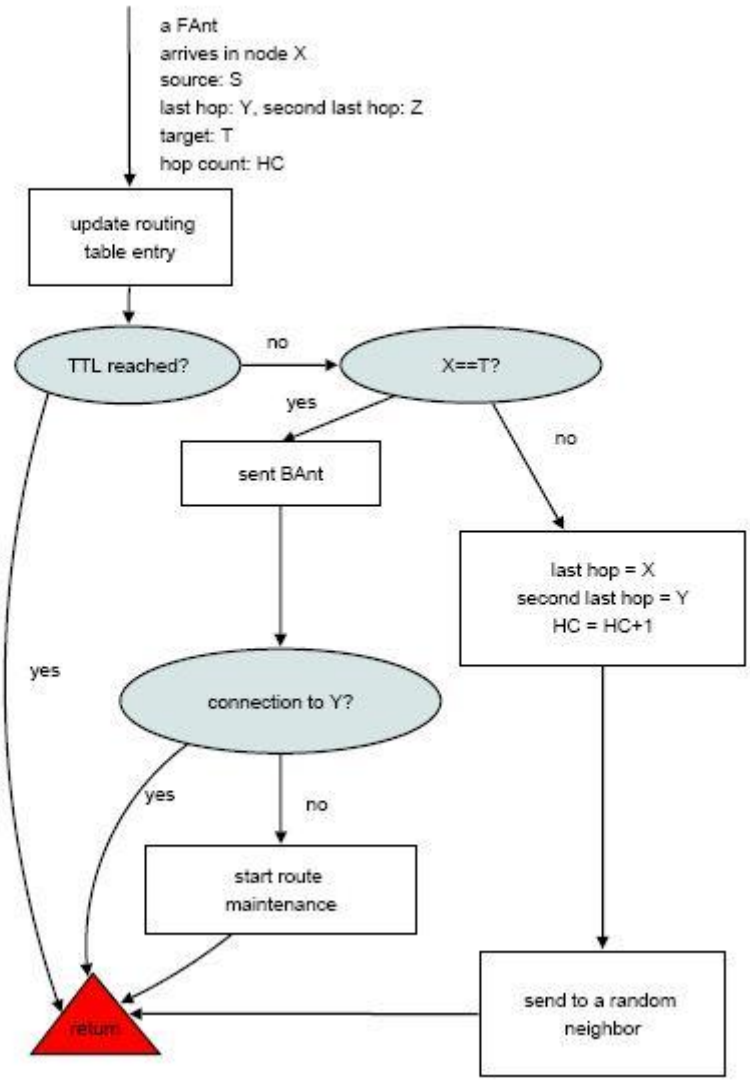
پس از اینکه آن تست شد، اگر FANT به انتهای عمرش در این حالت برسد، مورچه از بین خواهد رفت. اگر نود X هنوز نود مقصد نباشد ، FANT آخرین هوپ ، دومین آخرین هوپ و تعداد هوپ را در بدنه اش بروز می کند. اگر به مقصد برسد ، یک BANT را به سمت مبدا بر می گرداند. در حالت ایستا و "شرایط خوب" ، الگوریتم بدون هیچ مشکلی کار می کند.اگر شبکه پویا باشد، همسایه Y می ـتواند از شعاع اتصال ان نود خارج شود. که مفهوم نگهداری مسیری را که برای رفع این مشکل در الگوریتم به کار برده شده است معرفی خواهد شد.

نکته:به دو دلیل به ازاء هر پیغامی که به نود X می رسد،آن نود باید مدخل جدول مسیریاب را برای مبدائی که از آنجا می آید بسازد:۱)پیغام از یک مبدا می اید. بنابراین نود X جدیدترین

www.Prozhe.com

اطلاعات را راجع به مسیرش تا مبدا دارد. ۲) به دلیل پویایی شبکه ی موبایل مسیرهای ما همیشه معتبر نیستند.

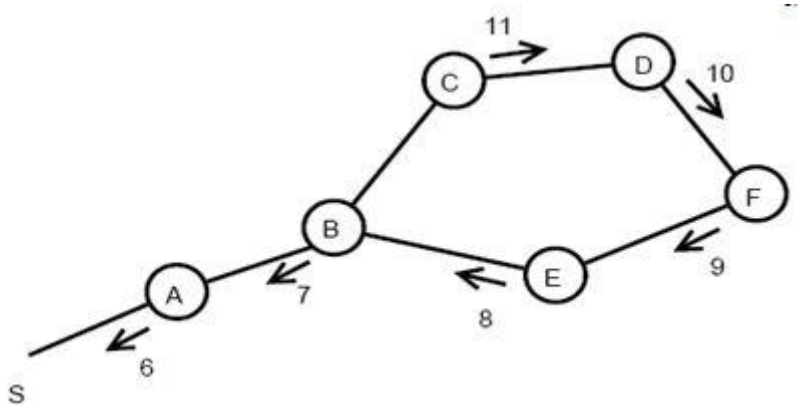
شکل (۳-٤)فلوچارت یک FANT را نشان میدهد.



شکل۳-٤) فلوچارت یک FANT

حال فرض کنید که یک FANT در مسیر خود با یک حلقه برخورد می کند برای مشخص شدن این مشکل و جلوگیری از آن شکل(۳-۵)را در نظر بگیرید:

www.Prozhe.com



شکل۳-۵)تصویری از چگونگی ایجاد حلقه

فرض کنید FANT مسیر ABEFDC را طی می کند و در هر نود مدخل جدول مسیریابی را مانند آنچه در شکل نشان داده شده می نویسد. با دوباره رسیدن به B هنگامی که مدخل موجود را بازنویسی می کنیم به مشکل ایجاد شدن حلقه بر می خوریم. اگر یک BANT برگشتی به یکی ازآن نودها برخورد کند و مدخل های ایجاد شده را ادامه دهد، در یک حلقه افتاده و هرگز به مبدا نمی رسد. ایده اصلی در کنار این مفهوم به این صورت است : هنگامی که یک FANT به یک همسایه مشخص می رسد،FANT اجازه ندارد که یک مدخل جدول مسیریابی را بسازد.برای فهمیدن این موضوع هنگامی که یک FANT به نود B می رسد ، نود را چک می کند که یک مدخل جدول مسیریابی موجود باشد. اگر قبلی بهتر بوده باشد، نود اتصال بین C وB را بلاک کرده و دیگر اجازه نمی دهد که FANT های بعدی از این اتصال عبور کنند تا مدخل های جدول مسیریاب را بسازند. در شکل نود B ، به FANT ها اجازه نمی دهد تا از C بروند.

اما چه موقع یک مسیر بهتر از مسیر دیگر است؟ هرگز نباید اساس تصمیم گیری خود را روی تعداد هوپ ها بگذاریم.بر این اساس یک طول عمر برای مدخل های جدول مسیریاب و اتصالات بلاک شده معرفی شده است.

www.Prozhe.com

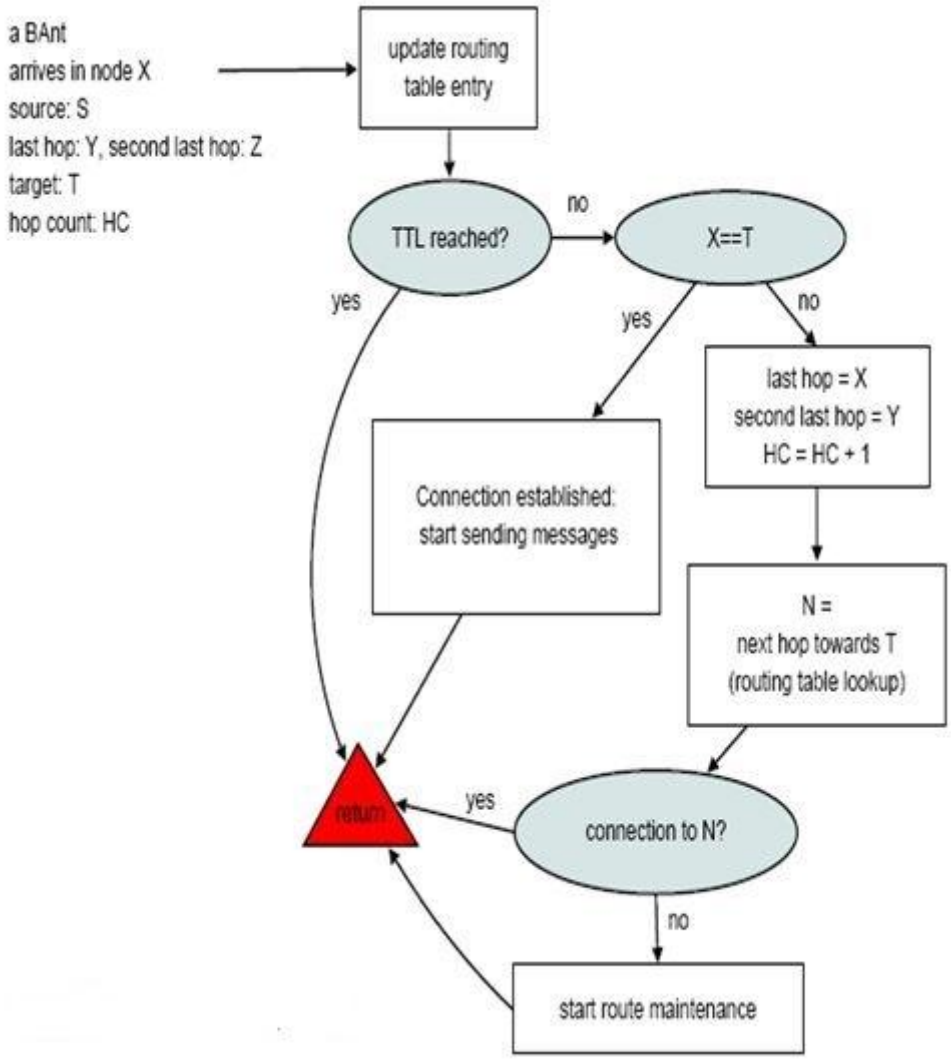
الگوریتم ممکن است بعد از مدت کوتاهی لبه غلط را بلاک کند، اما با توجه به طول عمر پس از مدتی که مدخل ها نامعتبر شدند، پروسیجر مجددا از ابتدا شروع به اجرا می کند. برای استنتاج مسئله ایجاد مدخل های جدول مسیریابی ، به مدخل نود F واقع در جدول(۳-۱)توجه شود.

جدول۳-۱)مدخل نود F

target	next hop	after next hop	hops to target	lifetime
S	E	B	9	8

همانطور که گفته شد، اگر FANT به مقصد برسد، یک BANT به سمت مبدا بر می گرداند.فلوچارت شکل(۳-٦)نشان می دهد که چطور یک نود، یک BANT را مدیریت می کند.

www.Prozhe.com



شکل۳-٦)فلوچارت یک BANT

رویه خیلی شبیه رویه FANT می باشد.ابتدا با رسیدن به نود X، یک BANT ابتدا جدول مسیریاب را ویرایش کرده و یک مدخل جدول مسیریاب جدید ایجاد می شود. سپس تست می شود که BANT به انتهای طول عمرش نرسیده باشد. در این حالت مورچه از بین خواهد رفت. اگر به مقصد رسیده باشیم، اتصال برقرار می شود. اگر نود X هنوز نود مقصد نباشد، BANT آخرین جهش ، دومین آخرین جهش و تعداد جهش ها را در هدرشان بروز می کند. سپس نود در جدول مسیریابی اش به دنبال هوپ بعدی جلوی مبدا می گردد. سپس نود سعی می کند تا پیغامی

www.Prozhe.com

را به این نود بفرستد. اگر نود به دلیل جابجایی دیگر در دسترس نباشد، رویه نگهداری مسیر را آغاز می کند.

سربار ARA

سربار مورد انتظار در آرا بسیار کوچک است، زیرا هیچ جدول مسیریابی که شامل مبادله بین نودها باشد وجود ندارد.بر خلاف الگوریتم های مسیریابی دیگر، بسته FANT و BANT مقدار اطلاعات مسیریابی را انتقال نمی دهد،بلکه تنها یک دنباله منحصر به فرد شماره در مسیریابی بسته را انتقال می دهد. بیشتر نگهداری مسیر از طریق بسته های داده انجام شده، در نتیجه آنها مجبور به انتقال اطلاعات اضافی مسیریابی نیستند . ARA تنها به اطلاعات موجود در عنوان IP از بسته های داده نیاز دارد.

۳-۳-۲-۲)الگوریتم موریانه

رات و ویکر یک الگوریتم ارائه کردند که مرتبط با ARA است،و ازهمان اصول مسیریابی بردار فاصله استفاده می کند.اما از نظرکشف مسیر و بازیابی شکست با ARA متفاوت است.

کشف مسیر در موریانه به وسیله ارسال یک بسته RREQ انجام می شود. بسته RREQ پخشی نیست، نود منبع به صراحت تعدادی از بسته های RREQ که قصد ارسال دارند تولید می کند. هر بسته RREQ هوپ نود بعدی را انتخاب کرده و از توزیع یکنواخت تابع تصمیم تصادفی استفاده می کند. این "راه رفتن تصادفی" بسته همچنان ادامه می یابد تا زمانی که بسته یا حذف شده، و یا یک مسیر به نود مقصد مورد نظر بیابد. از آنجا که بسته ها به صورت تکی به نود های همسایه خاص هستند، این الگوریتم نیاز به استفاده از پیام سلام برای ایجاد ارتباط اولیه بین نود های همسایه دارد.

www.Prozhe.com

موریانه فقط بسته های سلام را زمانی که جدول مسیریابی یک نود خالی است انتقال می دهد، و انتقال پیام های سلام تا زمانی که جدول مسیریابی خود را دوباره خالی کند متوقف می شود.اگر یک بسته RREQ یک نود با یک مسیر در نود مقصد را بیابد، نود یک بسته RREP تولید می کند،و آن را به نود منبع برمی گرداند.در نتیجه یک مسیر برای بسته های داده ایجاد می شود. RREP و بسته های داده تصمیم های احتمالی در هر نود مربوط به مقصد بعدی هوپ خود را می گیرند.احتمال برای هر یک از نود همسایه با استفاده از رابطه (۳-۳) محاسبه می شود:

$$p_{\mathrm{nd}} = \frac{(p_{\mathrm{nd}}+\mathrm{K})^{\mathrm{F}}}{\Sigma_{\mathrm{i}\epsilon N_k(t)}(p_{\mathrm{nd}}+\mathrm{K})^{\mathrm{F}}}$$

رابطه ۳-۳) احتمال نود همسایه

هنگامی با احتمال قوی است که یک بسته با نود مقصدD، نود N را به عنوان مقصد هوپ بعدی انتخاب می کند، مجموعه همسایگان شناخته شده از نود K و در زمان t ، است. همچنین مقدار فرومون مرتبط با گذر از نود فعلی به نود n برای یک بسته با نود مقصد D میباشد،K یک ثابت است که حساسیت محاسبات احتمالی به مقدار کمی از فرومون را تعیین می کند، همچنین F یک ثابت است که بر تفاوت بین میزان فرومون بر روی سطوح پیوند تأکید دارد.

هنگامی که بسته فرمون ذخیره شده، مقدار فرومون ثابت از پیش تعیین شده است و سطح فرمون در هر یک ثانیه کاهش می یابد. وقتی که یک خطا در ارسال بسته داده ها رخ می دهد، اگر هیچ مسیری درحذف بسته پیدا نشود الگوریتم تلاش می کند یک مسیر کشف کند.

۳-۳-۲-۳)الگوریتم مسیریابی اورژانس احتمالاتی(pera)

در این روش،کشف آغازین و موارد مجاور توسط پیامهای تک جهشی سلام پخش شده صورت می گیرد که بطور دوره ای منتقل می شوند. ایجاد اولین مورچه رو به جلو در یک نود

www.Prozhe.com

برای نمونه مبدا باعث می شود ورودی های جدول مسیریابی با احتمالات۱/N برای هر همسایه بعنوان جهش بعدی برای مقصد به ترتیب شروع می شود جاییکه تعداد همسایه های نود N است جدول مسیریابی تایید شده است. علاوه براین در جدول مسیریابی هر نود فهرستی از آمار و رقام را برای هر مقصد حفظ می کند که یک مورچه پیش رونده یا رو به جلو قبلا فرستاده شده است میانگین و واریانس برای مسیرهای بین نود منبع S و نود مقصد d است.

وقتی یک نود مسیری تا مقصد مشخص ندارد،یک مورچه پیش رونده آن را ایجاد کرده و به تمام مورچه های مجاورش پخش می کند اگر مورچه پیش رونده به یک نود تکراری برسد تخریب می شود. در این مورد مهم مورچه های رو به جلو روی همان صف ها یا ردیف ها به عنوان بسته های اطلاعاتی حرکت می کنند.از این رو همان تاخیر و ازدحام را به عنوان داده ها تجربه می کند.وقتی مورچه ای پیش رونده به مقصد می رسد نود اطلاعات آن را استخراج کرده و یک مورچه پس رونده یا در حال حرکت به عقب را ایجاد می کند .مورچه پس رونده اطلاعات موجود در مورچه ی پیش رونده را در مسیری معکوس جهت تغییر توزیع احتمالی در هر نود بکار می برد و جداول ردیابی را برای انعکاس حالت فعلی شبکه بطور دقیق تر به روز در می آورد .این عامل به سبک یا مدل تک حالتی برگشت تا نود مبدا حرکت می کند و روی ردیف های بالاتر پیش می رود. توجه شود که در این الگوریتم عامل تقویت فرومون بعنوان تابع متریک یا ترکیبی از متریک ها تعیین می شود.

این الگوریتم باAODV مقایسه شده است و نتایج نشان داده است که در حرکت یا جنبش پایین کل ورودی درست برای هر دو الگوریتم بالاست اما در حرکت بالا ورودی درست PERA پایین تر از AODV است.در سرعت پایین تر بازده یا عملکرد برای هر دو الگوریتم مشترک است با این وجود در سرعت بالاتر بازده در برخی موارد برای PERA کمی کمتر است.هر دو الگوریتم یک تاخیر ابتدایی عمده را نشان می دهند که برای تنظیم مسیرها مورد نیاز است .در نتیجه AODV تاخیر زیادی را دوباره در موقعیتهای دارای حرکت بالا نشان می دهد. از سوی دیگر PERA تاخیر پایین در تمامی موارد را نشان می دهد.

www.Prozhe.com

۳-۳-۲-۴)الگوریتم مسیریابی فوری ویژه(eara)

EARA یک الگوریتم مسیریابی چند مسیر مورد تقاضا است .هر نود که این الگوریتم را به کار می برد یک جدول ردیابی احتمالی را در بر می گیرد.در ابتدا یک همسایه مجاور برای هر نود با استفاده از پیامهای تک جهشی سلام ساخته می شود .علاوه بر این جدول مسیریابی هر نود همچنین یک جدول فرومون را در بر میگیرد که مقداری از فرومون در هر محل اتصال مجاور بر جای می ماند.

سه ارزش آستانه وجود دارد که کنترل کننده ی پیوندها از طریق فرومون در جدول است.آنها فرومون بالاتر U ،فرومون پایین تر L و فرومون اولیه هستند که وقتی یک مسیر جدید پیدا می شود مشخص می شود .ارزش احتمالی مسیریابی (درستی نود j بعنوان جهش بعدی d)بصورت رابطه (۳-٤) محاسبه می شود:

$$P_{i,j,d} = \frac{[\tau_{i,j,d}]^{\alpha}\,[\eta_{i,j}]^{\beta}}{\sum_{l\in N_i}[\tau_{i,l,d}]^{\alpha}[\eta_{j,l}]^{\beta}} \qquad \tau_{i,j,d} > l$$

رابطه ۳-٤)ارزش احتمالی مسیریابی

دراینجا α و β دو پارامتر هماهنگ هستند که وزن نسبی فرومون بر جای مانده و ارزش اکتشافی موارد مجاور یا همسایگان بعنوان جهش بعدی تا مقصد d هستند .ارزش یک مقیاس تراکم یا شلوغی در یک نود است.مشارکت ارزش اکتشافی در محاسبه ردیابی باعث می شود این الگوریتم در بردارنده خاصیت اگاهی از ازدحام باشد.

هر وقت یک منبع ترافیک نیاز به مسیری برای یک مقصد مشخص داشته باشد آن، بسته های (RQ) موردنیاز مسیر را در عرض شبکه پخش می کند. نود میانی در حال دریافت یک بسته RQ است که مسیرهای معکوس تا مبدا را به وسیله ثبت آدرس و نود جهش قبلی در نهانگاه پیام تنظیم کند.اگر یک مسیر معتبر تا مقصد موجود باشد نود میانی یک پاسخ مسیر RQ را ایجاد می کند که

www.Prozhe.com

به صورت رو به عقب تا مبدا را از طریق مسیرهای بر عکس مسیریابی می کند.علی رغم این RQ پخش مجدد است.

وقتی نود مقصد،RQ را دریافت می کند ان یک RP را به تمامی همسایگانی که یک RQ را می بینند ارسال می کند.برای حفظ مسیرهای چندتایی با میدان یا حلقه های باز در هر نود میانی این نود باید تمامی مسیرهای رو به جلو جدید را ثبت کند که آخرین عدد ردیف را در بر می گیرد،اما یک محاسبه جهش را در جدول ردیابی حفظ می کند و نیز یک RP را به تمام همسایگان ارسال می کند که یک RQ مشاهده می کند.در طول مرحله ردیابی بازگشت RP تا مبدا یک ارزش فرومون اولیه تا نود مجاور مربوطه را علامت گذاری می کند که مسیر معتبر تا مقصد را نشان می دهد.

بعد از اینکه نود مقصد به ترافیک داده ها رسید توسط نود مبدا فرستاده می شود، سپس در مواقعی که مسیرهای درست و جدید را شناسایی کرد با ارسال پاکت های سیگنال تقویت RS بعضی همسایگان مجاور را تقویت می کند.وقتی یک نود یک RS را دریافت می کند می داند که ان دارای یک پیوند کنار رونده نسبت به مقصد است و فعلا یک مسیر درست را اعمال کرده است. درنتیجه این نود ورودی جدول فرومون را با ارزش و نسبت به پاکت RS برای انتخاب همسایه محلی مبتنی بر پیام مخفی به روز در می اورد.

در یک شبکه پویا مثل MANET (موبایل ادهاک)تغییرات مکان شناسی شبکه،فرصتهایی را برای مسیرهای جدید جهت ظهور ایجاد می کند.به منظور استفاده از این خاصیت این الگوریتم مورچه های درحال جستجوی محلی (LFA) را که در جستجوی مسیرهای جدید هستند بطور دوره ای به کمک می طلبد وقتی تمام فرومون از یک نود به سمت مقصد زیر آستانه یا مدخل می رود . LFA یک پیاده روی اتفاقی از نود اولیه آن است و آدرس نود ها را که به مجموعه ی حافظه ی آن برگشته ترسیم می کند.اگر LFA بتواند یک نود دارای فرمون را دریافت کند، بیشتر

www.Prozhe.com

لانه ی اولیه را جستجو می کند،که به آشیانه اش در پی مجموعه حافظه آن برگشته و علی رغم اینکه به سادگی از بین می رود مسیرهای مربوطه را با مسیرهای جدید عوض می کند.

۳-۳-۲-۵)الگوریتم مورچه aodv

شیوانجای،تام و سرینیواسان یک پروتکل فعال واکنش های ترکیبی که ترکیب عناصری از AntNet و پروتکل مسیریابی AODV است پیشنهاد کردند.پروتکل مسیریابی مورچه AODV حفظ جمعیتی از مورچه های جلورونده که کشف شبکه با یک لیست منبع مسیریابی از نود های بازدید شده در عنوان بسته است،می باشد. علاوه بر این،هنگامی که یک نود نیاز به یک نود خاص در یک مسیر دارد ممکن است بسته های اطلاعاتی RREQ واکنش گرایانه را راه اندازی کند،هر چند مشخص نیست که آیا بسته RREQ که از منبع و یا بردار فاصله مسیریابی استفاده می کند راه اندازی شده است.

این پروتکل همچنین به پیام های مکرر سلام اجازه می دهد که نود ها به طور مداوم و آگاه از همسایه های آنها، و نود هشدار از شکست پیوند استفاده کنند .نود های جداول مسیریابی بردار فاصله را با مقصد/هوپ بعدی جفت و تعداد هوپ مرتبط و شماره توالی برای هر مسیر را حفظ می کند.

۳-۴)مسیریابی شبکه های حسگر

پروتکل‌های بسیاری در شبکه‌های حسگر به موضوع مسیریابی پرداخته‌اند و این پروتکل‌ها برای برخی از موضوعات دیگر در این شبکه مانند موضوع خوشه‌بندی، انتخاب لیدر و ... برنامه دارند. در ادامه دسته‌بندی‌های ارائه شده درباره پروتکل‌های مسیریابی بیان خواهد شد.

www.Prozhe.com

۳-۵)روشهای مسیر یابی شبکه های حسگر

مسیریابی در شبکه های ادهاک نوع حسگر سخت افزار محدودیت هایی را بر شبکه اعمال می کند که باید در انتخاب روش مسیریابی مد نظر قرار بگرند از جمله اینکه منبع تغذیه در نود ها محدود می باشد و در عمل،امکان تعویض یا شارژ مجدد آن مقدور نیست؛لذا روش مسیریابی پیشنهادی در این شبکه ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از منابع نود باشد و اگر نود منابع کافی نداشت بسته را به آن برای ارسال به مقصد نفرستد. پروتکل‌های مسیریابی در شبکه‌های حسگر بیسیم می‌توانند از دید ساختار شبکه به سه دسته مسیریابی مسطح، سلسه مراتبی و مبتنی بر مکان تقسیم شوند. در مدل مسطح همه‌ی نود ها نقش یا کار مساوی دارند، اما در مدل سلسله مراتبی نود ها نقش‌های مختلفی را در شبکه بازی می‌کنند. در مدل مبتنی بر مکان نیز از موقعیت نود های سنسور برای مسیردهی داده در شبکه استفاده می شود. این پروتکل‌ها هم می‌توانند به صورت چند مسیری (Multi path)، پرس و جو و رقابت و غیره که به عملکرد پروتکل بستگی دارد دسته‌بندی شوند.

۳-۵-۱)مسیریابی مسطح

مسیریابی مسطح اولین رده از پروتکل‌های مسیریابی است. در این دسته نود ها نقش یکسانی دارند و سنسورها با هم برای یک عمل حس کردن کار می‌کنند. به علت تعداد زیاد این قبیل نود های سنسور امکان دادن شناسه سراسری برای هر سنسور وجود ندارد و این مسئله باعث میشود که مسیریابی در این شبکه‌ها به‌جای برمبنای ادرس (Address-based) برمبنای داده (Data-Centric) باشد، که ایستگاه اصلی یکسری پرس‌وجو به یک ناحیه مشخص می‌فرستد و منتظر داده‌هایی از سنسورهای نواحی انتخاب شده می‌شود. از آنجایی که داده از طریق پرس‌وجوها درخواست می‌شود، نامگذاری مبتنی بر صفت برای تعیین خصوصیات داده نیاز است. کارهایی

www.Prozhe.com

روی مسیریابی Data-Centric مثل SPIN و انتشار مستقیم برای ذخیره‌سازی انرژی از طریق انتقال داده و حذف داده اضافی انجام شده است.

۳-۵-۱-۱)روش سیل آسا

در این روش یک نود 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 نود ، داده جدیدی دریافت کرد، از آن نسخه برداری می‌کند و داده را به همسایه‌هایش (به جز نود ی که داده را از آن دریافت کرده‌است) ارسال می‌کند. الگوریتم زمانی همگرا می‌شود یا پایان می‌یابد که تمامی نود ها یک نسخه از داده را دریافت کنند. زمانی که طول می‌کشد تا دسته‌ای از نود ها 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 شبکه است چون برای یک قطعه دادهd 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 شده است :

۱-انفجار : در روش سنتی سیل آسا، یک نود 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.

۲-هم پوشانی: حسگرها معمولاً نواحی جغرافیایی مشترکی را پوشش می‌دهند و نود ها معمولاً قطعه داده‌هایی از حسگرها را دریافت می‌کنند که با هم هم پوشانی دارند.

۳-عدم اطلاع از منابع: در روش سیل آسا، نود ها بر اساس میزان انرژی موجودی خود در یک زمان، فعالیت‌های خود را تغییر نمی‌دهند در صورتی که یک شبکه از حسگرهای خاص منظوره،

www.Prozhe.com

می‌تواند از منابع موجود خود آگاهی داشته باشد و ارتباطات و محاسبات خود را با شرایط منابع انرژی خود مطابقت دهد.

۳-۵-۱-۲)روش شایعه پراکنی

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

۳-۵-۱-۳)روش اسپین(spin)

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 نودهای 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. نود ها در spin برای ارتباط با یکدیگر از سه نوع پیغام استفاده می‌کنند:

adv-۱: برای تبلیغ داده‌های جدید استفاده می‌شود. وقتی یک نودspin ، داده‌هایی برای به اشتراک گذاشتن در اختیار دارد، این امر را می‌تواند با ارسال شبه -داده مربوطه تبلیغ کند.

www.Prozhe.com

۲-req : جهت درخواست اطلاعات استفاده می‌شود. یک نودspin می‌تواند هنگامی که می‌خواهد داده حقیقی را دریافت کند از این پیغام استفاده کند.

۳-data : شامل پیغام‌های داده‌ای است. پیغام‌هایdata محتوی داده حقیقی جمع آوری شده توسط حسگرها هستند.

۳-۵-۱-۴)روش انتشار هدایت کننده

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 می شود. در این روش هر نود ، نودی 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 نود 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 نود ی رسید که داده‌های مرتبط با آن را در اختیار دارد، نود 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. نود ی که داده‌ها را ارسال می‌کند به عنوان یک منبع شناخته می‌شود. داده هنگام ارسال به مقصد در نود های 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

www.Prozhe.com

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 نود 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 نود ارسال کرده‌اند) برای انجام این کار، سینک همسایه‌ای را جهت دریافت اطلاعات تقویت می‌کند. اگر یکی از نود ها در این مسیر ترجیحی از کار بیفتد، نود های 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.

از جمله پروتکلهای این روش عبارتند از:

GBR-۱ : این پروتکل یک روش تغییریافته از پروتکل انتشار مستقیم است. وقتی که درخواست ایستگاه پایه در کل شبکه پخش می شود، هر نود سنسور تعداد گام های مورد نیاز برای رسیدن به ایستگاه پایه را اندازه گیری می کند و بدین وسیله می تواند کمترین تعداد گام برای رسیدن به ایستگاه پایه را که ارتفاع آن سنسور نامیده می شود را بدست اورد. اختلاف بین ارتفاع سنسورهای همسایه به عنوان گرادیان مسیر بین انها در نظر گرفته می شود. داده های هر سنسور توسط مسیرهایی که بالاترین گرادیان را دارند به ایستگاه پایه فرستاده می شوند .در واقع این روش تلاش می کند تا با تعداد گام های کمتر داده را به ایستگاه پایه برساند. برای توزیع یکنواخت ترافیک روی شبکه در این پروتکل دو تکنیک ترکیب داده ها و پخش ترافیک به کار گرفته شده است. حسگرهایی که از چندین مسیر داده دریافت می کنند می توانند کار ترکیب

www.Prozhe.com

داده ها را انجام دهند .تکنیک های پخش ترافیک نیز به قرار زیر می باشند:

روش اتفاقی : اگر دو یا چند مسیر با گرادیان یکسان وجود داشته باشند، انتخاب مسیر به صورت تصادفی خواهد بود .

روش انرژی : وقتی که انرژی یک سنسور از یک استانه معین پایین تر می اید، ارتفاع خود را افزایش می دهد و بدین وسیله به سنسورهای دیگر می فهماند که تا حد امکان از این سنسور برای انتقال داده کمتر استفاده شود.

روش جریان داده : این روش تلاش می کند تا مسیرهایی که در حال حاضر برای انتقال داده ها استفاده می شوند، برای مسیرهای جدید به کار گرفته نشوند.

با بکارگیری روش های بالا ترافیک در کل شبکه پخش می شود و در نتیجه طول عمر شبکه افزایش پیدا می کند، همچنین این روش ها را می توان در پروتکل های دیگر نیز به کار برد. نتایج شبیه سازی ها نشانگر آن است که GBR از نظر مصرف انرژی موثرتر از Directed Diffusion کار می کند.

EAR-۲ : در این روش از یک سری مسیرهای زیربهینه جهت افزایش طول عمر شبکه استفاده می‌شود. این مسیرها به واسطه‌ی یک تابع احتمال، که به مصرف انرژی در آن مسیرها بستگی دارد، انتخاب می‌شوند. مهمترین پارامتری که در طراحی این پروتکل مدنظر گرفته شده-است بقای شبکه می‌باشد. نظر به اینکه استفاده دائمی از مسیری که کمترین انرژی در ان تلف می-شود، باعث تخلیه‌ی انرژی سنسورهای موجود در آن مسیر می‌شود، در این روش به جای استفاده از مسیر بهینه، چند مسیر زیربهینه در نظر گرفته می‌شوند که با استفاده از یک تابع احتمال فقط یکی از آنها انتخاب شده و برای مدتی از آن مسیر استفاده می‌شود. این پروتکل از سه فاز تشکیل شده است:

فاز راه اندازی: در این فاز با استفاده از پروتکل سیل‌آسا محلی، مسیرها تا مقصد شناسایی شده و جدول‌های مسیریابی ایجاد می‌شوند. در طی این عملیات، تابع هزینه‌ی انرژی برای هر

www.Prozhe.com

سنسور حساب می‌شود. برای مثال، اگر درخواست از سنسور به سنسور فرستاده شود، سنسور تابع هزینه مسیر را به‌صورت رابطه (۳-۵) حساب می‌کند.

$$C_{N_j N_i} = Cost(N_i) + Metric(N_j \cdot N_i)$$

رابطه۳-۵)تابع هزینه مسیر

در این رابطه متریک انرژی، خود تابعی از هزینه‌ی ارسال و دریافت و همچنین مقدار انرژی باقیمانده‌ی سنسورها در طول مسیر است. مسیرهایی که هزینه بسیار بالایی داشته باشند در نظر گرفته نمی‌شوند. در این روش انتخاب سنسورها بر مبنای نزدیکی آن‌ها به مقصد می‌باشد. هر سنسور به هر یک از همسایه‌های خود که در جدول ارسال آن وجود دارد، یک احتمال نسبت می دهد. این احتمال که با معکوس هزینه رابطه مستقیم دارد، در رابطه (۳-٦) نشان داده شده است.

$$P_{N_j N_i} = \frac{1/C_{N_j N_i}}{\sum_{k \in FT_j} 1/C_{N_j N_i}}$$

رابطه ۳-٦)احتمال همسایه سنسور

فاز انتقال داده‌ها: هر سنسور داده‌ی خود را به یکی از همسایه‌های خود که در جدول ارسال وجود دارد با توجه به احتمال اختصاص داده شده به ان همسایه می‌فرستد.

فاز نگهداری مسیرها: هر چند وقت یکبار، یک داده به‌صورت سیل‌آسا محلی فرستاده می‌شود تا از سالم بودن مسیرها اطمینان حاصل شود.

این پروتکل با پروتکل انتشارمستقیم در نحوه‌ی پیداکردن مسیرها از ایستگاه پایه تا حسگرها مشترک است. در انتشارمستقیم از بین چند مسیر، تنها مسیری انتخاب می‌شود که نرخ داده ، ۲۱/۵٪ در مصرف انرژی و ٤٤٪ در افزایش EAR مسیر انتخابی بواسطه تابع احتمال برگزیده می

www.Prozhe.com

شود. نتایج شبیه‌سازی‌ها حاکی از آن است که EAR بیشتری بواسطه آن دریافت می‌شود. اما در طول عمر شبکه نسبت به انتشارمستقیم بهتر عمل می‌کند. از طرفی مثل انتشارمستقیم وقتی مسیر انتخاب شده به هر دلیلی از کار بی‌افتد، دچار مشکل نمی‌شود زیرا علاوه بر مسیرEAR اصلی مسیرهای دیگری را نیز در اختیار دارد.

۳-۵-۲)مسیریابی سلسله مراتبی

مسیریابی سلسله مراتبی یا مبتنی بر خوشه در ابتدا برای شبکه های سیم دار پیشنهاد شد که تکنیک های معروفی دارد و مزایای اصلی آن مربوط به مقیاس پذیری و ارتباطات کارا هستند.همین طور مفهوم مسیریابی سلسله مراتبی برای انجام مسیریابی که به صورت کارآمد از انرژی استفاده می کند در شبکه های سنسور بیسیم به کار می رود. در معماری سلسله مراتبی از نود های با انرژی بالاتر می توان برای پردازش و فرستادن سیگنال استفاده کرد. در حالی که نود های با انرژی پایین تر را می توان برای انجام عملیات حسگری در نزدیکی هدف به کار برد. این موضوع به این معنی است که ایجاد خوشه ها و تخصیص وظایف خاص به لیدرها(Cluster head یا سرخوشه) می تواند به طور مهمی روی مقیاس پذیری سیستم، طول عمر و کارآیی انرژی تاثیر بگذارد. مسیریابی سلسله مراتبی با انجام تراکم داده و ترکیب داده ها برای کاهش تعداد پیام های منتقل شده به ایستگاه اصلی یک روش کارآمد برای مصرف انرژی پایین تر در یک خوشه است.

مسیریابی سلسله مراتبی در اصل مسیریابی دولایه ای است که لایه اول برای انتخاب لیدر و لایه دیگر برای مسیریابی استفاده می شود. در این قسمت برخی پروتکل های مهم در این رابطه بیان شده است. البته برخی از پروتکل های این بخش برای انتخاب لیدر از توزیع احتمال تصادفی بین دیگر سنسورها استفاده می کنند؛ یعنی برنامه خاصی ندارند و برخی دیگر دارای روش ویژه ای برای انتخاب لیدر هستند.

www.Prozhe.com

۳-۵-۲-۱)پروتکل LEACH

در بین پروتکل‌های ارتباطی ارائه شده پروتکل LEACH به دلایل زیر از اهمیت ویژه‌ای در نزد محققان برخوردار است:

اول اینکه خوشه‌های شبکه به‌صورت تصادفی، تطبیقی و خودپیکربندی شده تشکیل می‌شوند. شرح این ویژگی‌ها به‌صورت زیر است:

تصادفی : به این معنی که در هر دور،تعداد مشخصی از نودها به صورت تصادفی خود را به عنوان سرخوشه انتخاب می‌کنند و نود های خاصی از قبل به عنوان سرخوشه در نظر گرفته نشده است. مزیت این ویژگی سربار کم روش انتخاب سرخوشه است. این روش سریع‌ترین روش انتخاب سرخوشه است.

تطبیقی : نود هایی که در دور فعلی نقش سرخوشه را به عهده داشته‌اند، در دور بعدی دیگر نمی توانند برای بر عهده گرفتن این نقش کاندیدا شوند، بنابراین در هر دور، با توجه به دور قبلی کاندیداهای سرخوشه مشخص می‌شوند. به این ترتیب انتظار می‌رود که در پایان تعداد مشخصی از دورها، تمامی نود ها سرپرست خوشه شوند.

خودپیکربندی شده : نود ها دراین پروتکل بدون کمک هر عامل خارجی و یا نود خاصی در شبکه، تشکیل خوشه می‌دهند و این به مقیاس‌پذیری این پروتکل کمک می‌کند.

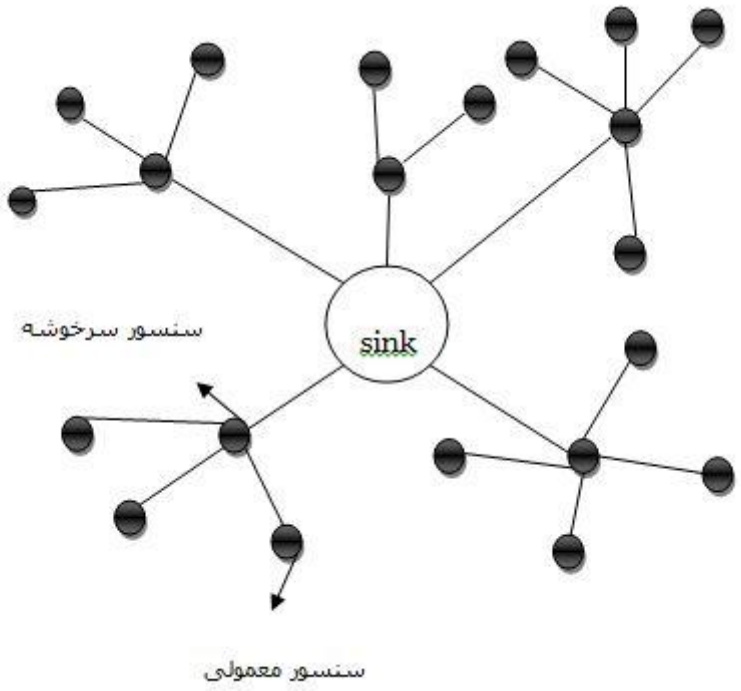
دومین اهمیت اینکه در LEACH انتقال اطلاعات از نود های یک خوشه به سرخوشه و از سرخوشه‌ها به ایستگاه sink با کنترل محلی انجام می‌شود و نیازی به کمک یک عامل خارجی و یا نود خاصی در شبکه برای انتقال اطلاعات نیست.

سوم اینکه پروتکل MAC استفاده شده در LEACH با استراحت دادن به نود ها در انرژی مصرفی صرفه‌جویی می‌کند.

www.Prozhe.com

همان‌طور که قبلا گفته شد،LEACH از روش ترکیب داده‌های هر خوشه و ارسال داده‌ی فشرده شده به ایستگاه پایه استفاده می‌کند. بدین ترتیب هم تعداد ارسال و دریافت‌ها در شبکه کاهش می‌یابد و هم داده‌های زاید که به علت نزدیکی سنسورهای یک خوشه به یکدیگر ایجاد می‌شوند، پیش از ارسال به sink حذف می‌گردند. نوع ترکیب داده‌ها در LEACH ثابت نیست و بستگی به کاربرد شبکه سنسور بیسیم دارد. هدف این پروتکل ایجاد توازن در مصرف انرژی در نود ها است. گزینه‌های کلاسیک مانند DT و MTE تعادل انرژی بین نود ها را تضمین نمی‌کنند. در DTچون نود ها مستقیماً داده را به sink ارسال می‌کنند انرژی نود های دورتر، زودتر تخلیه می‌شود و در نتیجه زودتر می‌میرند. در MTE داده از کم هزینه‌ترین مسیر هدایت می‌شود. در جایی که معیار هزینه مصرف توان است، چون نود های نزدیک به sink عمل انتقال داده‌های نود های دورتر را نیز انجام می‌دهند، در نتیجه زودتر می‌میرند. پس بخش زیادی از محیط در مدت زمان زیادی از عمر شبکه قابل نظارت نخواهد بود. یک راه‌حل استفاده از پروتکل LEACH است که مصرف انرژی را با خوشه‌بندی و انتخاب پویای خوشه ها توزیع می‌کند، بدین ترتیب که سنسورها به ناحیه‌هایی تقسیم می‌شوند که هر ناحیه دارای یک سرخوشه است و پس از اتفاق یک رویداد سنسورهای هر ناحیه، اطلاعات خود را به سرخوشه ارسال می‌کنند و سرخوشه این اطلاعات را مستقیم به sink می‌رساند.به شکل (۳-۷)توجه شود:

www.Prozhe.com



شکل ۳-۷)خوشه بندی در شبکه های بیسیم

الگوریتم LEACH به انتخاب شدن سرخوشه‌ها به صورت تصادفی و با یک احتمال ثابت تاکید دارد) .تمام نود ها از احتمالی یکسان برای سرخوشه شدن برخوردارند.) نود ها همگن فرض می‌شوند (نود ها دارای انرژی اولیه یکسانی هستند). در این الگوریتم سنسورها به‌صورت تصادفی در یک ناحیه توزیع می‌شوند. سنسورها ثابت در نظر گرفته می‌شوند. آنها در گروه‌ها یا خوشه‌هایی دسته‌بندی می‌شوند و هر گروه یک سردسته دارد، که هر ناحیه از طریق سرخوشه‌اش با sink که در مرکز شبکه قرار دارد به صورت مستقیم ارتباط برقرار می‌کند. به این ترتیب هم تعداد ارسال و دریافت‌ها در شبکه کاهش می‌یابد و هم داده‌های زاید که به علت نزدیکی سنسورهای یک خوشه به یکدیگر تولید می‌شوند حذف می‌شوند .عملکرد پروتکل از دوره‌هایی متشکل از چندین دور تشکیل شده است. احتمال بهینه سرخوشه شدن نود ها برابر P_{opt} است و ثابت در نظر گرفته می‌شود. تعداد بهینه خوشه ها بر اساس توزیع مناسب بین تمام سنسورها و کمینه نمودن مصرف انرژی انتخاب می‌شود. هر دوره از $1/P_{opt}$ دور تشکیل شده است. در صورتی

www.Prozhe.com

که نود در دور فعلی سرخوشه شود تا انتهای دوره دیگر سرخوشه نخواهد شد. نود برای سرخوشه شدن یک عدد تصادفی در بازه $[0,1]$ انتخاب و عدد تصادفی موردنظر را با حد آستانه $T(s)$ مقایسه میکند. در صورتی که عدد انتخابی کوچک‌تر از حد آستانه باشد نود در دور فعلی سرخوشه می‌شود. اگر سنسور در این دور سرخوشه نشود احتمال سرخوشه شدن خود را افزایش می‌دهد و این کار را تا زمانی ادامه می‌دهد که در دور آخر این احتمال به ۱ برسد . به این معنی که اگر نود تا دور آخر سرخوشه نشده باشد، حتما در دور آخر سرخوشه خواهد شد. نود هایی که هنوز در دوره فعلی سرخوشه نشده اند متعلق به مجموعه G هستند ودر هر دور احتمال سرخوشه شدن آنها افزایش می‌یابد. رابطه (۳-۷) احتمال سرخوشه شدن سنسور را نشان میدهد.

$$T(s)=\begin{cases}\dfrac{p_{opt}}{1-p_{opt}\cdot\left(r \bmod \frac{1}{p_{opt}}\right)} & if\ s\in G\\ 0 & otherwise\end{cases}$$

رابطه۳-۷)احتمال سرخوشه شدن سنسور

در این رابطه r مشخص کننده دور فعلی است و مقدار اولیه آن صفر است. انتخاب این رابطه در پروتکل LEACH به صورتی بوده که نود هایی که اخیرا سرخوشه نبوده‌اند در دور فعلی سرخوشه شوند؛ زیرا می‌توان انتظار داشت که این نود ها نسبت به نود هایی که اخیرا وظیفه سرخوشه بودن را (که انرژی زیادی مصرف می‌کند) بر عهده داشته اند، انرژی بیشتری دارند. میتوان انتظار داشت که در هر دور $N/\mathrm{K_{opt}}$ ، هر نود به طور متوسط یک بار سرخوشه شود.

وقتی یک نود سرخوشه می‌شود، احتمال سرخوشه شدن سنسور تا دوره بعدی صفر شده و احتمال نود هایی که در دور فعلی سرخوشه نشده‌اند افزایش می‌یابد .

www.Prozhe.com

مجموعه G شامل سنسورهایی است که تا کنون سرخوشه نشده‌اند و در زمان t قابلیت سرخوشه شدن را دارند. احتمال سرخوشه شدن آنها از طریق رابطه (۳–۸) بدست می‌اید.

$$E[G] = N - K_{opt} \times (r \bmod \frac{N}{K_{opt}})$$

رابطه۳–۸)احتمال سرخوشه شدن مجموعه

LEACH دارای چهار مرحله عملیاتی پیشنهاد، تشکیل گروه، ایجاد زمانبندی و انتقال داده است، در مرحله پیشنهاد سرخوشه با یک پیام خود را به نود های دیگر معرفی می‌نماید. سنسورها از این پیشنهادها، نزدیک‌ترین سرخوشه را انتخاب نموده و درخواست عضویت را برای آن ارسال می‌کنند. نود سرخوشه یک زمانبندی برای اعضا ایجاد و انرا به سنسورهای عضو ارسال می‌کند. نود ها در زمانبندی اعلام شده داده‌های خود را به سرخوشه ارسال می‌کنند و سرخوشه با جمع-آوری و ترکیب داده‌ها ان را به sink ارسال می‌کند. مصرف انرژی نود های سرخوشه به دلیل جمع‌آوری اطلاعات گروه‌های عضو، ترکیب و ارسال داده ترکیب شده به sink که در فاصله دورتری قرار دارد بیشتر از نود های عضو است. با انتخاب تصادفی سرخوشه و در نتیجه چرخش نقش سرخوشه بین نود ها، مصرف انرژی بین انها به خوبی توزیع می‌شود.

مهمترین کاربرد LEACH این است که برای جمع‌آوری داده‌ها استفاده می‌شود و با توجه به اینکه، به جدول مسیریابی سنگین نیازی ندارد دارای سربار پایینی است و یکی از پروتکل‌های موفق در نوع خود است. مزیت ناهمگن بودن نود ها (وجود سنسورهایی با انرژی بیشتر) کاهش هزینه توسعه سیستم است؛ زیرا می‌توان همین عمل را با افزایش تعداد نود های همگن در ابتدای کار انجام داد ولی با توجه به این نکته که هزینه افزودن نود جدید به‌جای قرار دادن باتری اضافه روی بعضی از سنسورها ده برابر بیشتر است، پس ناهمگن بودن نود ها و استفاده مطلوب از ان می‌تواند هزینه را به‌طور چشمگیری کاهش دهد.

اشکالاتی که بر پروتکل LEACH وارد است نیز عبارتند از:

www.Prozhe.com

۱-هر سنسور در این الگوریتم با تولید یک عدد تصادفی تصمیم می‌گیرد که سرخوشه باشد یا نباشد. با توجه به انتخاب تصادفی سرخوشه‌ها این احتمال وجود دارد که در برخی از زمان‌ها قسمتی از شبکه سرخوشه نداشته باشد و در قسمت دیگری چگالی سرخوشه‌ها زیاد باشد. در مجموع هیچ قاعده منطقی بر پایه تغییرات توپولوژیکی و انرژی باقیمانده سنسورها وجود ندارد که بر انتخاب شدن نود ها به عنوان سرخوشه تاثیر می‌گذارد. LEACH توانسته تنها به نحوی انتخاب سرخوشه را در شبکه میسر سازد.

۲-پروتکل‌های کلاسیک (همچنین پروتکل LEACH) فرض را بریکسان بودن انرژی نود ها گذاشته و در نتیجه در صورت ناهمگنی نود ها از نظر انرژی، مزایای کامل خود را ارائه نمی‌کنند. ناهمگنی نود ها دلایل زیادی دارد که می‌توان به تنظیم اولیه متفاوت، عملکرد شبکه یا افزودن نود های جدید به سنسورهای قبلی اشاره نمود. در صورتی که نود ها ناهمگن باشند پروتکل به درستی عملیات مطلوب خود را انجام نمی‌دهد و به ویژه از زمان مرگ اولین نود، عملکرد شبکه ناپایدار خواهد شد.

۳-پروتکل LEACH فرض می‌کند که همه نود ها می‌توانند با توان کافی برای رسیدن به ایستگاه اصلی درصورت نیاز، انتقال داشته باشند و اینکه هر نود توان محاسباتی برای حمایت پروتکل‌های مختلف MAC دارد. بنابراین گسترش شبکه به نحوی بزرگ قابل اجرا نیست. همچنین فرض می‌کند که نود ها داده برای ارسال دارند و نود هایی که نزدیک به هم هستند داده وابسته به هم دارند. معلوم نیست چطور تعداد لیدر از پیش تعیین شده به‌صورت یکنواخت در شبکه توزیع می‌شود. بنابراین این امکان وجود دارد که لیدرهای انتخاب شده در یک بخش از شبکه متمرکز شود. بعضی نود ها ممکن است هیچ لیدری در مجاورت خود نداشته باشند. به-علاوه، برای رفع این مشکل فکر خوشه‌بندی پویا سربار ایجاد می‌کند.

جدول (۳-۲)مقایسه تکنیک‌های مسیریابی LEACH،SPIN و انتشار مستقیم را بر طبق تعدادی پارامتر مختلف نشان می‌دهد.

www.Prozhe.com

جدول۳-۲)مقایسه تکنیک های مسیریابی

	انتشارمستقیم	SPIN	LEACH
طول عمر شبکه	خوب	خوب	بسیار خوب
استفاده از Meta-data	بله	بله	خیر
اگاهی منبع	بله	بله	بله

برای مثال، تغییرات سرآیند اعلان و غیره، ممکن است بهره‌وری در مصرف انرژی را کاهش دهد. همچنین پروتکل، فرض می‌کند که همه نودها با یک میزان ظرفیت انرژی در هر دور انتخابی شروع می‌کنند. فرض شود که یک لیدر تقریبا همان میزان انرژی را برای هر نود مصرف کند. پروتکل بایستی گسترش پیدا کند تا برای نودهای انرژی غیر یکنواخت یعنی استفاده آستانه مبتنی بر انرژی هم کار کند.

در الگوریتم دیگری بنام HEED نیز چهار هدف افزایش طول عمر شبکه، اتمام فاز خوشه بندی پس از طی تعداد متناهی و مشخصی از تکرار، حداقل کردن سربار کنترلی و توزیع متناسب خوشه‌ها در سطح شبکه دنبال می‌شود. هر نود با احتمالی متناسب با میزان انرژی باقیمانده خود تصمیم می‌گیرد که آیا لیدر خوشه باشد یا نه. این تصمیم‌گیری موقتی است و پس از گذشت چندین تکرار نهایی می‌شود. نود هایی که خود را به‌عنوان لیدر خوشه برگزیده‌اند، به همسایگان خود این مسئله را اطلاع می‌دهند. هر یک از همسایگان، در صورتی که پیش از این عضو خوشه ای نشده باشد، عضو این خوشه می‌شود. در صورتی که همسایه‌ای پیش از این عضو خوشه دیگری باشد که انرژی باقیمانده سرخوشه آن نسبت به انرژی باقیمانده لیدر خوشه جدید پایین‌تر باشد، همسایه به خوشه جدید ملحق می‌شود.

به‌علاوه، درصورتی که همسایه‌ای خود لیدر باشد، پس از مقایسه میزان انرژی باقیمانده خود با میزان انرژی باقیمانده لیدر خوشه معرفی شده، تصمیم می‌گیرد که همچنان لیدر باقی بماند یا به خوشه‌ی جدید منتقل شود. هر لیدر، در صورتی که برای ملحق شدن به خوشه دیگری تصمیم

www.Prozhe.com

نگرفته باشد، مقدار احتمال خود را دو برابر کرده و مجددا خود را به عنوان سرخوشه به p همسایگانش معرفی می‌کند. اگر مقدار p در نودی بزرگ‌تر از ۱ شد، آن نود خود را به عنوان سرخوشه نهایی برمی‌گزیند. در این صورت، همسایگان این نود نیز، عضو خوشه‌ای نهایی خواهند شد که دیگر تغییری در آن به وجود نمی‌اید. در این مرحله، در صورتی که نودی، هیچ پیام معرفی خوشه‌ای را دریافت نکرده باشد، خود تصمیم می‌گیرد که راس خوشه‌ای جدید باشد.

۳-۵-۲-۲)پروتکل SEP

Sep پروتکل توسعه یافته LEACH است که هدف اصلی آن بهره گیری از سنسورهای ناهمگن در های سنسور بی سیم است. این پروتکل عملکردی مانند LEACH دارد با این تفاوت که پروتکل SEP بر مبنای احتمال وزن دار انتخاب نود ها به عنوان سرخوشه بر مبنای انرژی باقیمانده عمل می کند. در این پروتکل فرض بر این است که درصدی از سنسورها انرژی بیشتری دارند(برای مثال انرژی ده درصد سنسور ها دو برابر بقیه است.) و نود ها به صورت یکنواخت در محیط پراکنده شده اند. با توجه به این نکته که دو نوع سنسور معمولی و توسعه یافته در شبکه وجود دارد، هر کدام از این دو نوع نود احتمال های متفاوتی برای سرخوشه شدن هستند. احتمال سرخوشه شدن نود های معمولی با P_{normal} و احتمال سرخوشه شدن نود های توسعه یافته با $P_{advanced}$ مشخص میشود. در مدل همگن تعداد بهینه سرخوشه ها برابر $n \times p$ است. در مدل ناهمگن میانگین تعداد خوشه ها برابر $n(۱+\alpha \times m) \times p$ است . نود های معمولی در هر دور سر خوشه می شوند و نود های دارای انرژی بیشتر $۱+\alpha$ بار در هر دور سرخوشه میشوند و این تعادل انرژی را تضمین می کند.α ضریب انرژی افزونه و m درصد سنسورهای با انرژی اولیه اضافه را مشخص می کند. نود های مجازی معادل یک سنسور نرمال در نظر گرفته می شود. برای مثال در یک شبکه نا همگن معادل $n+a \times m \times n=n(۱+a \times m)$ نود مجازی وجود دارد و از یک شبکه ناهمگن انتظار می رود که عملکردی مشابه شبکه ای با نود های همگن ولی با تعداد

www.Prozhe.com

سنسورهای مجازی داشته باشد. در صورتی که نسبت ضریب مورد نظر هنگام عملکرد شبکه تغییر کند SEP عملکرد مطلوبی از خود نشان نمی دهند و با گذشت مدت زمانی از عملکرد شبکه دیگر این تناسب برای توزیع انرژی وجود ندارد و تناسب جدیدی خواهیم داشت، ولی چون پروتکل SEP از تناسب جدید آگاه نیست به خوبی نمی تواند مصرف انرژی را توزیع نماید احتمال های مربوط به هر یک از نود های معمولی و پیشرفته به ترتیب از روابط(۳-۹) و (۳-۱۰)محاسبه می شود.این احتمال ها در ابتدای عملکرد شبکه تنظیم می شود. احتمال مربوط به سرخوشه شدن نود های معمولی از رابطه(۳-۱۱)به دست می آید.

سنسورهای معمولی که در دوره فعلی سرخوشه نشده اند عضو مجموعه G_{normal} هستند . احتمال سنسورهای پیشرفته از رابطه(۳-۱۲)به دست می آید. $G_{advanced}$ مجموعه نود های پیشرفته ای را شامل می شود که تا دور فعلی سرخوشه نشده اند.

$$P_{normal} = \frac{p}{1+a\times m} \qquad \text{رابطه ۳-۹}$$

$$P_{normal} = \frac{p}{1+a\times m} \times (1+a) \qquad \text{رابطه ۳-۱۰}$$

$$T(i) = \begin{cases} \dfrac{P_{normal}}{1-P_{normal}\cdot\left(r \bmod \frac{1}{P_{normal}}\right)} & \text{if } i \in G_{normal} \\ 0 & \text{otherwise} \end{cases} \qquad \text{رابطه ۳-۱۱}$$

$$T(i) = \begin{cases} \dfrac{P_{advanced}}{1-P_{advanced}\cdot\left(r \bmod \frac{1}{P_{advanced}}\right)} & \text{if } i \in G_{advanced} \\ 0 & \text{otherwise} \end{cases} \qquad \text{رابطه ۳-۱۲}$$

پروتکل SEPدوره پایداری شبکه (زمان مرگ اولین نود) و میانگین گذردهی اطلاعات را در همه حال در شبکه افزایش می دهد. دوره پایداری رابطه مستقیم با قابلیت اعتماد شبکه دارد. پروتکل SEP به صورت ایستا عمل می کند و برای مواردی مناسب است که در ابتدا از تاثیر انرژی متفاوت روی احتمال سرخوشه شدن نود ها آگاه باشد و این تنظیم در ابتدای کار انجام می

www.Prozhe.com

شود.برای مثال نود هایی که انرژی آنها دو برابر نود های معمولی است احتمال سرخوشه شدن آنها نیز دو برابر در نظر گرفته می شود. شاید مهمترین دلیل ناهمگنی نود ها مصرف انرژی نود ها در حین کار شبکه باشد که به دلایلی از جمله فاصله ارتباطی متفاوت نود ها و وقایع تصادفی مانند خرابی خطوط ارتباطی و شرایط محیط باشد که پروتکل SEP به این پارامترها آگاه نیست.

۳-۵-۲-۳)پروتکل PEGASIS

این پروتکل برای بهبود پروتکل LEACH یشنهاد شد و بسیار شبیه پروتکل مبتنی بر زنجیره بهینه است. هدف اصلی این پروتکل این است که برای گسترش طول عمر شبکه، نود ها نیاز دارند فقط با نزدیک ترین همسایه هایشان ارتباط برقرار کنند و در ارتباط با ایستگاه اصلی گردش داشته باشند. وقتی یک دور ارتباط همه نود ها با ایستگاه اصلی به پایان رسید، دور جدید آغاز خواهد شد و همین طور الی آخر. این انرژی برای انتقال داده به ازای هر دور نیاز است به طوری که Energy Draining به طور یکنواخت روی همه نود ها منتشر خواهد شد.

بنابراین PEGASIS دو هدف اصلی دارد؛ اول، افزایش طول عمر هر نود با استفاده از تکنیک-های شراکتی و در نتیجه طول عمر شبکه افزایش خواهد یافت. دوم، برای اینکه پهنای باند مصرف شده در ارتباطات کاسته شود، به نود هایی که به هم نزدیک هستند فقط اجازه هماهنگی محلی بین خودشان داده می شود. بر خلاف پروتکل LEACH، PEGASIS جلوی فرم خوشه را می گیرد و فقط از یک نود در یک زنجیره برای انتقال به ایستگاه اصلی بجای چندین نود استفاده می کند. برای تعیین مکان نزدیک ترین نود همسایه در PEGASIS ، هر نود از شدت سیگنال برای اندازه گیری فاصله همه نود های همسایه استفاده می کند و سپس شدت سیگنال را طوری تنظیم می کند که فقط یک نود می تواند بشنود.

www.Prozhe.com

زنجیره در PEGASIS شامل نود هایی است که به هم نزدیک ترین هستند و فرم یک مسیر به ایستگاه اصلی است. فرم متراکم داده به ایستگاه اصلی با هر نود در زنجیره ارسال می شود. ساخت زنجیره در یک سبک حریصانه انجام می شود. نتایج شبیه سازی نشان می دهد که PEGASIS توانایی افزایش طول عمر شبکه را دو برابر بیشتر از طول عمر شبکه تحت پروتکل LEACH دارد. این قبیل کسب کارایی از طریق کاهش سرباری که در LEACH به خاطر فرم خوشه پویا وجود دارد و کاهش تعداد انتقال ها و دریافت با استفاده از تراکم داده به دست می اید. گرچه جلوی سربار حاصل از خوشه گرفته شد، اما PEGASIS هنوز نیاز به تنظیم توپولوژی پویا دارد. یک نود سنسور برای اینکه بداند داده هایش را کجا مسیردهی کند نیاز به آگاهی درباره وضعیت انرژی همسایه هایش دارد. این قبیل تنظیم توپولوژی می تواند سربار قابل توجهی به ویژه برای شبکه های مورد استفاده زیاد تولید کند. به علاوه PEGASIS فرض می کند که نود سنسور می تواند به طور مستقیم با ایستگاه اصلی ارتباط برقرار کند. در عمل نود های سنسور از ارتباط چند گام برای رسیدن به ایستگاه اصلی استفاده می کنند.

بنابراین پروتکل PEGASIS فرض می کند که همه نود ها یک پایگاه داده کامل را درباره مکان همه نود ها در شبکه نگهداری می کنند. به علاوه،PEGASIS فرض می کند که همه نود های سنسور یک سطح انرژی دارند و مثل هم در یک زمان از کار خواهند افتاد. توجه داشته باشید که PEGASIS تاخیر زیادی را برای نود های دوردست در زنجیره تولید می کند. این پروتکل عقیده دارد یک لیدر تنها می تواند گلوگاه شود. همچنین اگرچه در بیشتر طرح ها، سنسورها ثابت یا بدون تحرک خواهند بود، اما در این پروتکل فرض شده بعضی از نود ها ممکن است متحرک باشند و برای همین روی عملکرد پروتکل تاثیر می گذارد. نسخه گسترش یافته PEGASIS ، مدل سلسه مراتبی آن است که با هدف کاهش تاخیر برای بسته ها در طول انتقال به ایستگاه اصلی تولید شده است.

www.Prozhe.com

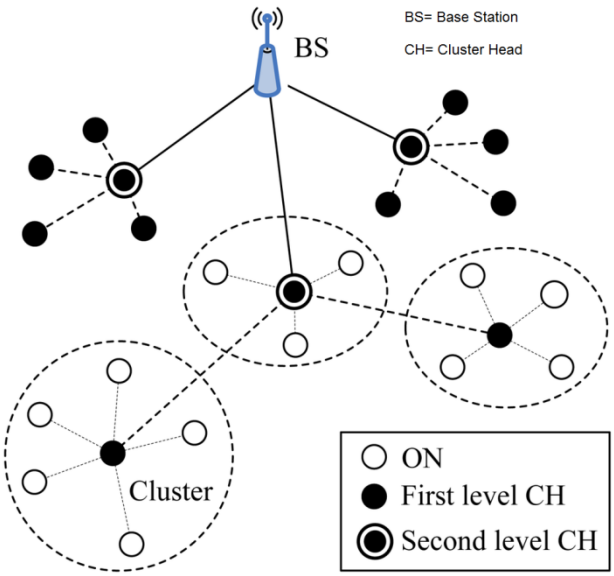
۳-۵-۲-۴)پروتکل TEEN و APTEEN

دو پروتکل مسیریابی سلسه مراتبی TEEN (پروتکل شبکه سنسور موثر در انرژی حساس به آستانه)و APTEEN (تناوب فعالانه TEEN) برای کاربردهای بحرانی از نظر زمان پیشنهاد شده اند. در TEEN نود های سنسور به صورت پیوسته حسگری می کنند، اما انتقال داده کمتر اتجام می شود. یک سنسور لیدر به بخش خودش یک سیگنال آستانه قوی تر می فرستد، که مقدار آستانه صفت حس شده است و یک آستانه ضعیف، که یک تغییر کوچک در مقدار صفت حس شده است و نود را در حالت سوییچ روی انتقال دهنده و انتقال نگه می دارد.

به این ترتیب آستانه قوی سعی می کند تعداد انتقال ها را کاهش دهد؛ و یعنی نود ها مجازند تا وقتی که فقط صفت حس شده در محدوده Interest است انتقال داشته باشند. آستانه ضعیف نیز تعداد انتقال ها را درصورتی کاهش می دهد که صفت حس شده تغییر کمتر داشته باشد یا بدون تغییر باشد.

یک مقدار کوچک تر آستانه ضعیف می تواند در هزینه افزایش مصرف انرژی تصویر دقیق تری بدهد؛ به این صورت که کاربر تعادل بین بهره وری انرژی و صحت داده را کنترل کند. وقتی لیدرها در حال تغییر هستند مقدار جدید برای پارامترهای بالا منتشر می شود. اشکال اصلی طرح مذکور این است که اگر آستانه ها دریافت نشوند، نود ها هرگز ارتباط برقرار نخواهند کرد و کاربر هیچ داده ای را از شبکه نخواهد گرفت.شکل (۳-۸) نحوه خوشه بندی در این پروتکل را نشان می دهد.

www.Prozhe.com



شکل۳-۸)نحوه خوشه بندی در پروتکل TEEN

APTEEN یک پروتکل ترکیبی است که تناوب یا مقادیر آستانه استفاده شده در پروتکل TEEN را بر طبق نیازهای کاربر و نوع کاربردها تغییر می دهد. در APTEEN ، لیدرها پارامترهای زیر را منتشر می کنند:

صفت ها: مجموعه ای از پارامترهای فیزیکی است که کاربر علاقه مند است اطلاعاتی را درباره آن به دست آورد.

آستانه ها: این پارامتر شامل آستانه قوی و استانه ضعیف است.

زمانبندی: شامل یک زمانبندی TDMA است که به هر نود یک برش زمانی اختصاص می دهد.

شمارش زمان : ماکزیمم دوره زمانی بین دو گزارش متوالی ارسال شده توسط کاربر است.

نود محیط را به صورت پیوسته حس می کند و فقط آن نود هایی که مقدار داده را در آستانه شدید یا فراتر از آن حس کرده اند منتقل می کنند. برای یک بار که یک نود یک مقدار را فراتر از آستانه قوی حس می کند، آن داده را فقط وقتی منتقل می کند که مقدار آن صفت با یک مقدار

www.Prozhe.com

بزرگ تر یا مساوی آستانه ضعیف تغییر می کند.اگر یک نود داده را برای یک دوره زمانی برابر با شمارش زمان ارسال نکند، مجبور است حس کند و دوباره داده را منتقل کند.

یک زمانبندی TDMA استفاده شده و هر نود خوشه، یک برش زمانی برای انتقال داده می گیرد. از این رو APTEEN از زمانبند TDMA تغییر یافته برای پیاده سازی شبکه ترکیبی استفاده می کند. ویژگی های اصلی این پروتکل سیاست ترکیب Reactive و Proactive است. آزمایش ها نشان می دهند که کارایی APTEEN ها در اتلاف انرژی و طول عمر شبکه چیزی بین LEACH و TEEN است.TEEN با کاهش تعداد انتقالات بهترین کارایی را ارائه می دهد. اشکال اصلی این دو روش سربار و پیچیدگی مربوط به شکل گیری خوشه ها در چندین سطح، روش های پیاده سازی توابع مبتنی بر آستانه و رسیدگی به نحوه نامگذاری مبتنی بر صفت و پرس و جوها است.

۳-۵-۲-۵)پروتکل SOP

یک پروتکل خود سازمانده است و برای سنسورهای ناهمگن کاربرد دارد. این سنسورها می توانند متحرک یا ساکن باشند. بعضی از سنسورها پس از بررسی محیط، داده را به یک مجموعه معین شده از نود ها ارسال می کنند که مثل لیدرها عمل می نمایند. نود های لیدر ساکن هستند و ستون فقرات یا زیرساختی برای ارتباطات می باشند. داده جمع اوری شده از طریق لیدرها به ایستگاه اصلی قوی تری ارسال می شود. هر نود حس کننده برای اینکه بخشی از شبکه باشد باید بتواند به یک لیدر دسترسی داشته باشد.

در این پروتکل یک معماری مسیریابی که به آدرس دهی هر نود سنسور نیاز دارد پیشنهاد شده است. نود های حس کننده از طریق ادرس یک نود لیدر که به آن متصل شده اند قابل شناسایی هستند. معماری مسیریابی سلسله مراتبی است که یک گروهی از نود ها در صورت نیاز مرتب و

www.Prozhe.com

ادغام شده اند. و برای پشتیبانی تحمل پذیری خرابی و به عنوان ابزار همه پخشی استفاده شده است.

در این روش، نود های سنسور می توانند اساسا در معماری مسیریابی آدرس داده شوند. از این رو معماری مسیریابی مناسب کاربردهایی است که ارتباط به یک نود ویژه نیاز است. به علاوه این الگوریتم هزینه کمی برای نگهداری جدول مسیریابی و نگهداری یک مسیریابی سلسله مراتب متعادل دارد. همچنین انرژی مصرف شده برای یک پیام، کمتر از پروتکل SPIN است، اما مشکل این پروتکل این است که سربار اضافی تولید می کند. موضوع دیگر نیز در مورد ساخت سلسله مراتب زمانی اتفاق می افتد که تعداد زیادی حفره در شبکه وجود داشته باشد و از این رو احتمال اعمال دوباره فاز سازماندهی افزایش می یابد که یک عمل پرهزینه خواهد بود.

نویسندگان این پروتکل نه تنها پروتکل خود سازمانده را توصیف می کنند، بلکه یک رده بندی از موارد کاربرد سنسور را هم توسعه داده و مطرح می کنند. بر اساس چنین رده بندی، آنها اجزای معماری و زیر ساختار ضروری برای ساختن و موارد کاربرد سنسور را پیشنهاد و ارائه داده اند. این معماری از سنسورهای ناهمگن حمایت می کند که می توانند سیار یا ثابت باشند. برخی از سنسورها محیط را جستجو می کنند و داده را با مجموعه ای معین از نود ها جلو برده و انتقال می دهند که به عنوان عمل می کنند.

نود های لیدر ثابت هستند و ستون فقرات ایجاد ارتباط را تشکیل می دهند. داده های جمع آوری شده از طریق سرخوشه ها به نود های Sink منتقل می شوند. هر نود حس کننده برای اینکه بخشی از شبکه باشد باید برای مسیریاب قابل دسترس باشد. معماری تعیین مسیر که مستلزم آدرس دادن نود سنسور است نیز پیشنهاد شده است. معماری مسیریابی دارای سلسله مراتبی است که در آن نود هایی از نود ها تشکیل می شوند و موقعی که لازم باشد با هم ادغام می شوند. به منظور تایید و حمایت از تحمل پذیری خطا، الگوریتم حلقه های محلی مارکف، که یک مسیر تصادفی بر روی درخت های پوشا گراف را اجرا می کند برای پخش و منتشر کردن به کار میرود.

www.Prozhe.com

الگوریتم خود سازماندهی نود های مسیر و ایجاد جدول مسیریابی دارای چهار مرحله است:

۱-مرحله کشف: نود های همسایگی هر سنسور کشف می شوند.

۲-مرحله سازمان: گروه ها تشکیل می شوند و با تشکیل سلسله مراتب با هم ادغام می شوند. هر نود بر اساس وضعیت و موقعیت خود در ان سلسله مراتب به ادرسی اختصاص داده می شود. جداول مسیریابی برای هر نود تولید و ایجاد می شوند .درخت های همه پخشی که همه نود ها را پوشش می دهند ساخته می شوند.

۳-مرحله حذف و نگهداری: به هنگام کردن(به روز نگهداشتن) جداول مسیریابی و سطوح انرژی نود ها در این مرحله ایجاد و ساخته می شود. هر نود ، همسایه ها را در مورد جدول مسیریابی و سطح انرژی خود مطلع می سازد.

٤-مرحله خودسازماندهی مجدد: در صورت بروز تقسیم نود و یا خطاهای آن، سازماندهی مجدد گروهی به اجرا در می آید. این الگوریتم از نود های لیدر برای حفظ همه سنسورهای متصل شده با تشکیل مجموعه ای حاکم استفاده می کند .چنین رویکردی شبیه ایده شبکه مجازی مورد استفاده در پروتکل مسیریابی GAF است . هر دو رویکرد از طریق استفاده از زیر مجموعه واحد و محدودی از نود ها به صرفه جویی در انرژی می رسند. از آنجا که می توان نود های سنسور را به صورت انفرادی در معماری مسیریابی آدرس داد، این الگوریتم برای شبکه هایی مناسب است که در آنها ایجاد ارتباط با نودی ویژه مورد نیاز است.

مزیت عمده و اصلی استفاده از این الگوریتم هزینه بسیار کم برای حفظ جداول مسیریابی و متعادل نگهداشتن سلسله مراتب مسیریابی است. علاوه بر این، انرژی مصرفی برای پخش پیام کمتر از میزان مصرف شده در پروتکل SPIN است که ناشی از درخت های همه پخشی مورد استفاده در این الگوریتم است .امتیازات در فاز سازماندهی الگوریتم است، که مبتنی بر درخواست نیست و بنابراین سربار زیادی را ایجاد و عرضه می کند.

www.Prozhe.com

۳-۵-۲-۶)پروتکل Sensor Aggregates Routing

در این پروتکل الگوریتمی برای ساخت و نگهداری خوشه های سنسور پیشنهاد شده است که هدف از آن نظارت در یک محیط مشخص (کاربردهای ردیابی هدف) است. خوشه آن دسته از نود هایی در شبکه است که یک گروه بندی را برای شرکت در کار پردازش ارائه می کند. پارامترهای این خوشه بستگی به کار و نیازمندی های منبع دارد. سنسورها در فیلد سنسور بر اساس شدت سیگنالشان به خوشه ها تقسیم شده اند، به طوری که به ازای هر خوشه فقط یک نقطه اوج وجود دارد. سپس لیدرهای خوشه های انتخاب شده اند. یک نقطه اوج ممکن است یک هدف را نشان دهد و همچنین در حالتی که نقطه اوج توسط نویز منابع تولید می شود، هدفی را نشان ندهد. برای انتخاب لیدر، بین سنسورهای همسایه تبادل اطلاعات نیاز است .اگر یک سنسور بعد از تبادل بسته ها با همه همسایه های یک گام خودش، متوجه شود که از همه همسایه های یک گام خودش در ناحیه سیگنال بالاتر است، خودش را به عنوان یک لیدر اعلام می کند. این الگوریتم مسیریابی مبتنی بر لیدر فرض می کند سرخوشه منحصر به فرد، ناحیه جغرافیایی همکاری را می داند.

برای این پروتکل سه الگوریتم پیشنهاد شده است. در اولین روش مدیریت تراکم توزیع شده DMA است که برای شکل دهی خوشه های الگوریتم و نظارت بر هدف است. دومین الگوریتم نظارت فعال مبتی بر انرژی است که سطح انرژی در هر نود را با محاسبه ضربه سیگنال ناحیه ارزیابی می کند و سومین الگوریتم EMLAM اتلاف انرژی ثابت یا مساوی هدف را حذف نموده و از نتیجه ارزیابی برای پیش بینی امکان نحوه ترکیب سیگنال های اهداف در هر سنسور استفاده می کند .این فرآیند تکرار می شود تا ارزیابی به قدر کافی مطلوب شود. طرح مدیریت شروع ردیابی توزیع شده، با الگوریتم ردیابی مبتنی بر لیدر توصیف شده و یک سیستم مقیاس پذیر را شکل می دهد. سیستم در ردیابی چندین هدف وقتی به خوبی کار می کند که اهداف مزاحم نیستند.

www.Prozhe.com

۳-۵-۲-۷)پروتکل VGA

VGA یک الگوریتم مسیریابی موثر در انرژی است که برای بیشینه کردن طول عمر شبکه، تراکم داده و پردازش درون شبکه به کار می‌رود . برای نود ثابت و خیلی کم تحرک در بسیاری از کاربردها در شبکه های سنسور بیسیم یک روش مرتب کردن نودها در یک توپولوژی ثابت است. یک روش GPS-free برای ساخت خوشه‌ها که ثابت، مساوی و مجاور هستند و هم پوشانی ندارند با اشکال منظم استفاده شده است. همچنین خوشه های مربع برای به دست اوردن یک توپولوژی مجازی مستقیم الخط استفاده شده است.

در داخل هر ناحیه، یک نود به صورت بهینه به عنوان لیدر انتخاب می‌شود .تراکم داده در دو سطح محلی و سپس سراسری انجام می‌شود. مجموعه‌ای از لیدرها به عنوان متراکم کننده های محلی (LA)مطرح هستند و تراکم محلی را انجام می‌دهند، در حالی که یک زیر مجموعه از این متراکم کننده‌های محلی برای انجام تراکم سراسری استفاده می‌شوند. هدف الگوریتم‌ها انتخاب تعدادی نود سنسور متراکم کننده اصلی (MA)خارج از سنسورهای متراکم کننده محلی (LA)برای بیشینه کردن طول عمر شبکه است.

۳-۵-۲-۸)پروتکل HPAR

این الگوریتم مسیریابی شبکه را به گروه هایی از سنسورها تقسیم می کند. هر گروه از سنسورهای مجاور هم با هم به عنوان یک ناحیه خوشه شده اند و هر ناحیه به عنوان موجودیت مستقل عمل می کند. برای انجام مسیریابی هر ناحیه تصمیم گیری می کند که چگونه یک پیام سلسله مراتبی از میان ناحیه های دیگر به طوری مسیردهی می شود که عمر باتری این نود ها در سیستم بیشترین باشد .مسئله دشوار الگوریتم اساسا تعادل بین کم کردن انرژی و بیشتر کردن طول عمر شبکه است. از این رو الگوریتم سعی می کند تا به یک مسیر Max-Min با محدود کردن

www.Prozhe.com

مصرف انرژی ان به صورت زیر کمک کند. اول، الگوریتم مسیر با حداقل مصرف انرژی را با استفاده از الگوریتم مسیریابی دایکجسترا پیدا می کند. دوم، الگوریتم مسیری را که منجربه مصرف انرژی کمتری می شود پیدا می کند. الگوریتم پیشنهاد شده سعی می کند تا معیارهای هر دو راه حل را بهینه کند.

الگوریتم دیگر، مسیریابی مبتنی بر ناحیه نامیده می شود. مسیریابی مبتنی بر ناحیه یک روش سلسله مراتبی است که ناحیه پوشیده شده توسط شبکه سنسور به تعدادی ناحیه کوچک تر تقسیم شده است. برای ارسال یک پیام از طریق محل ناحیه یک مسیر سراسری از یک ناحیه به ناحیه دیگر پیدا می شود. سنسورها در یک ناحیه به صورت خودگردان مسیریابی محلی را هدایت می کنند و در ارزیابی سطح انرژی ناحیه سهیم می شوند. هر پیام از طریق نواحی با استفاده از اطلاعات درباره براورد انرژی ناحیه مسیردهی می شود.

۳-۵-۲-۹)پروتکل TTDD

پروتکل TTDD روشی است که ارسال داده به چندین ایستگاه اصلی متحرک را فراهم می‌کند. در TTDD ، هر منبع داده به صورت Proactive یک ساختار شبکه توری را می‌سازد که برای ارسال داده به Sink های متحرک با فرض اینکه نود های سنسور ثابت و آگاه از مکان هستند، استفاده شده است. در این پروتکل نود های سنسور ثابت و آگاه از مکان هستند، در حقیقت Sinkها ممکن است مکانشان را به صورت پویا تغییر دهند. وقتی یک رویداد اتفاق می‌افتد، سنسورها آن فرآیند را با سیگنال احاطه می‌کنند و یکی از آنها به عنوان منبع شروع به تولید گزارش می‌کنند و نود های سنسور نیز از ماموریت خود آگاه هستند.

برای ایجاد ساختارGrid ، یک منبع داده خودش را به عنوان نقطه شروع انتخاب می‌کند و یک پیام اعلان داده را به چهار نقطه مجاورش با استفاده از ارسال جغرافیایی حریصانه ساده می‌فرستد.

www.Prozhe.com

در طول این فرآیند هر نود میانی اطلاعات منبع را ذخیره می‌کند و در ادامه پیام را به همسایه مجاورش به جز یکی که پیام از آنجا می‌اید ارسال می‌کند. این فرآیند تا زمانی که پیام در لبه شبکه متوقف شود ادامه پیدا می‌کند. نود هایی که پیام منبع را ذخیره کرده‌اند به عنوان نقاط توزیع اطلاعات انتخاب می‌شوند. بعد از این فرآیند، ساختار Grid به دست می‌آید. با استفاده از Grid ، یک ایستگاه اصلی می‌تواند یک پرس و جو را ارسال کند که به نزدیک‌ترین نقطه در سلول محلی برای دریافت داده ارسال خواهد شد. سپس پرس و جو از طریق نقاط توزیع اطلاعات دیگر به صورت جریان به منبع ارسال می‌شود. در ادامه داده تقاضا شده در مسیر عکس به سمت Sink ارسال می‌شود. گرچه TTDD یک روش مسیریابی کارآمد است،یک سری مسائل مربوط به اینکه الگوریتم چگونه مکان اطلاعات را به دست آورند وجود دارد که برای تنظیم و راه‌اندازی ساختار Grid نیاز است.

طول مسیر ارسال در TTDD نسبت به طول کوتاه‌ترین مسیر بیشتر است. نویسندگان پروتکل TTDD معتقدند که بهینگی کمتر در طول مسیر در تقویت مقیاس‌پذیری با ارزش است. نحوه کار این پروتکل هنوز یک سوال قابل بحث است. مقایسه نتایج بین TTDD و انتشار مستقیم نشان می‌دهد که TTDD می‌تواند طول عمر بیشتر و تاخیرهای ارسال داده را به دست آورد، اما سربار حاصل از نگهداری و محاسبه دوباره شبکه به عنوان تغییرات توپولوژی شبکه ممکن است بالا باشد. گذشته از این، پروتکل TTDD در دسترس بودن موقعیت‌یابی خیلی دقیق فرض شده که هنوز برای شبکه‌های سنسور بیسیم در دسترس نیست. به جدول (۳-۳)توجه شود:

www.Prozhe.com

جدول۳-۳)مقایسه مسیریابی سلسله مراتبی و مسطح

مسیریابی سلسله مراتبی	مسیریابی مسطح
اجتناب از تصادم	سربار تصادم به وجود می‌اورد
تراکم داده توسط Clusrer head	نود ها در مسیر Multi hopداده ورودی از همسایه‌ها را متراکم می‌کنند
سربار اطلاعات مربوط به خوشه‌ها در سرتاسر شبکه	مسیرها فقط در نواحی که داده برای انتقال دارند شکل می‌گیرند
اتلاف انرژی یکنواخت است	اتلاف انرژی به الگوی ترافیک بستگی دارد
اتلاف انرژی کنترل نمی شود	اتلاف انرژی با الگوی ترافیک سازگار است
ساده اما بدون مسیریابی بهینه	مسیریابی با یک مقدار پیچیدگی اضافی می‌تواند بهینه شود

۳-۵-۳)مسیریابی مبتنی بر مکان

در این نوع مسیریابی نودهای سنسور به وسیله مکانشان ادرس دهی شده‌اند .فاصله بین نودهای همسایه می‌تواند بر اساس شدت سیگنال‌های ورودی تخمین زده شود. هماهنگی نسبی نودهای همسایه می‌تواند با تبادل این قبیل اطلاعات بین همسایه ها به دست اید. همچنین مکان نودها ممکن است به طور مستقیم با ارتباط با یک ماهواره یا استفاده از GPS ، در صورتی که نودها به یک دریافت کننده GPS کم مصرف مجهز شده باشند در دسترس باشد. برای ذخیره انرژی، بعضی از طرح‌های مبتنی بر مکان‌یابی می‌خواهند که نودها در صورتی که فعالیتی ندارند به خواب روند. ذخیره‌سازی انرژی بیشتر می‌تواند با نود های خوابیده بیشتر در شبکه تا حد ممکن به دست آید.

www.Prozhe.com

۳-۵-۳-۱)پروتکل GAF

GAF یک الگوریتم مسیریابی آگاه از انرژی و متنی بر مکان است که در اصل برای شبکه های متحرک موردی طراحی شده است، ولی برای شبکه های سنسور هم به خوبی قابل کاربرد است. ناحیه شبکه در ابتدا به نواحی ثابت تقسیم می شود و به صورت شبکه مجازی در می آید. داخل هر ناحیه، نود ها با هم برای انجام کارهای مختلف همکاری می کنند.
برای مثال، نود ها یک سنسور را برای بیدار ماندن برای یک دوره مشخص از زمان انتخاب می کنند و سپس آنها به خواب می روند. این نود مسوول نظارت و گزارش داده به ایستگاه اصلی از طرف نود های موجود در ناحیه خواهد بود. از این رو با خاموش کردن نود های غیرضروری در شبکه بدون اینکه روی میزان صحت مسیریابی تاثیر بگذارد میزان مصرف انرژی را کاهش می دهند. هر نود از GPS نشان دهنده مکان خودش برای اینکه خودش را به یک نقطه در شبکه مجازی ارتباط دهد استفاده می کند. نود های مرتبط با همان نقطه در شبکه در هزینه مسیریابی بسته معادل فرض شده اند.

پروتکل GAF در واقع می تواند طول عمر شبکه را افزایش دهد، در نتیجه تعداد نود ها افزایش می یابد. سه حالت در GAF تعریف شده است. این حالت ها برای تعیین همسایه ها در شبکه، شراکت فعال در مسیریابی و خواب سنسورها تعریف شده است.

همسایه های خوابیده زمان خوابشان را برای نگهداری مسیریابی به صورت دقیق تنظیم می کنند. قبل از زمان خارج شدن از زمان انقضای نود های فعال، نود های خوابیده بیدار شده و یکی از آنها فعال می شود. GAF هم برای نود های غیرمتحرک (GAF اولیه) و هم برای نود های متحرک (GAF سازگار با تحرک) پیاده سازی شده است. اگر سیگنال فاصله بین دو سنسور در خوشه افقی و یا عمودی مجاور هم که بتوانند به طور مستقیم با هم ارتباط برقرار کنند را طی می کند، وقوع یک ارتباط افقی و عمودی تضمین می شود.

www.Prozhe.com

بحث درباره نحوه قوانین زمانبندی است به صورتی که نود ها به عنوان سرخوشه ها عمل کنند است. یک لیدر می تواند از نود های سنسور در خوشه خودش بخواهد تا فعال شوند و در صورتی که یک شی را حس کردند شروع به جمع آوری داده کنند. سپس لیدر برای دریافت داده خام از دیگر نود ها در خوشه خودش و ارسال ان به ایستگاه اصلی مسوول است. فرض می شود که نود های سنسور می توانند مکانشان را با استفاده از کارت های GPS بدانند که با تکنولوژی حاضر قابل تصور نیست. GAF سعی می کند تااتصال شبکه را با یک نود نماینده که همیشه در حالت فعال برای هر ناحیه در شبکه مجازی خودش است، حفظ کند. نتایج شبیه سازی نشان می دهد که GAF حداقل به خوبی یک پروتکل مسیریابی شبکه های موردی در مورد تاخیر و اتلاف بسته کار می کند و طول عمر شبکه را با ذخیره سازی انرژی افزایش می دهد.

گرچه GAF یک پروتکل مبتنی بر مکان است، ممکن است به عنوان یک پروتکل سلسله مراتبی نیز مطرح شود که خوشه ها بر اساس مکان جغرافیایی باشند. برای هر ناحیه، یک نود نماینده به عنوان لیدر برای انتقال داده به نود های دیگر عمل می کند. نود لیدر، هیچ تراکم یا ترکیب را مثل دیگر پروتکل های مسیریابی سلسله مراتبی بحث شده انجام نمی دهند.

۳-۵-۳-۲)پروتکل GEAR

این مسیریابی در مورد استفاه از اطلاعات جغرافیایی در حین انتشار پرس و جوها به نواحی مناسب است. پروتکلGEAR ، که بر پایه آگاهی از انرژی و همسایه عمل مسیریابی را انجام می دهد، هدف اصلی محدود کردن تعداد Interest ها در انتشار مستقیم فقط با توجه به یک ناحیه مشخص نسبت به ارسال Interest ها به همه شبکه است. GEAR می تواند انرژی بیشتری را نسبت به انتشار مستقیم ذخیره کند.

هر نود در GEAR هزینه برآوردی و فراگیری را از طریق همسایه هایش نگهداری می کند. هزینه برآوردی ترکیبی از انرژی باقیمانده و فاصله با مقصد است. هزینه فراگیری پالایش هزینه،

www.Prozhe.com

برآوردی است که برای مسیریابی موجود در شبکه محاسبه می شود .یک حفره زمانی ایجاد می شود که یک نود هیچ همسایه نزدیک تری به ناحیه مقصد نسبت به خودش ندارد. اگر هیچ حفره ای نباشد هزینه برآوردی برابر است با هزینه فراگیری. هزینه فراگیری یک گام به عقب منتشر می شود، در هر زمان یک بسته به مقصد می رسد به خاطر اینکه برپایی مسیر برای بسته بعدی تنظیم خواهد شد.

دو فاز در الگوریتم وجود دارد:

۱-ارسال بسته ها به سمت ناحیه هدف: به محض دریافت یک بسته، یک نود همسایه هایش را بررسی میکند، اگر بیش از یک همسایه بود که نسبت به خودش به ناحیه هدف نزدیک تر بود متوجه می شود. اگر بیش از یک همسایه وجود داشت، نزدیک ترین همسایه به ناحیه هدف به عنوان گام بعدی انتخاب می شود. اگر همه آنها فاصله شان نسبت به خود نود بیشتر است بدین معنی است که یک حفره در شبکه موجود است. در این حالت، یکی از همسایه ها برای ارسال بسته بر اساس تابع هزینه برآوردی انتخاب می شود. سپس این انتخاب می تواند بر طبق هزینه فراگیری در طول ارسال بسته ها انتخاب شود.

۲-ارسال بسته ها داخل ناحیه: اگر بسته به ناحیه رسید، می تواند در آن ناحیه با ارسال جغرافیایی بازگشتی و یا سیل آسا به طور محدود شده، منتشر شود .سیل آسای محدود شده وقتی سنسورها به صورت متراکم گسترش یافته اند خوب است .در شبکه های با چگالی بالا، سیل آسای جغرافیایی بازگشتی بهره وری انرژی بیشتری نسبت به سیل آسای محدود شده دارد. در این حالت، ناحیه به چهار زیر ناحیه تقسیم شده و چهار کپی از بسته ایجاد می شود. فرآیند انشعاب (چند دسته ای شدن) و ارسال تا زمانی که ناحیه هایی فقط با یک نود ایجاد شود ادامه پیدا می کند.

www.Prozhe.com

فصل چهارم

امنیت شبکه های موردی

www.Prozhe.com

۴-۱)مشکلات امنیتی در مسیر یابی شبکه های موردی

حملات بر علیه شبکه های موردی را می توان از چند دیدگاه دسته بندی نمود. در دیدگاه اول دسته بندی میتواند به صورت حملات خارجی و حملات داخلی باشد .حملات داخلی حملاتی است که توسط نود های مجاز داخل شبکه انجام می شود و غالباً جلوگیری از آنها کاری مشکل است. حملات خارجی حملاتی هستند که توسط یک یا چند نود از خارج از شبکه انجام می شوند و اکثر اقدامات امنیتی در مقابل اینگونه حملات اعمال می شوند .دیدگاه دیگر دسته بندی بر حسب فعال و یا غیر فعال بودن حمله است .حملات غیر فعال حملاتی هستند که در آنها حمله کننده تنها به داده های عبوری گوش داده و آنها را استراق سمع می کند ولی در حملات فعال حمله کننده این داده ها را به نفع خود تغییر می دهد .دیدگاه بعدی دسته بندی از جهت لایه های شبکه ای مورد حمله می باشد .یعنی حمله می تواند بر روی لایه های فیزیکی ،MAC ،شبکه و یا کاربرد صورت پذیرد.

مشکلات امنیتی در مسیریابی در شبکه های موردی به سه دسته عمده تقسیم می شود تغییر، جعل هویت و جعل . البته گونه های دیگری از حملات که منجر به حملات ممانعت از سرویس می شوند مانند شرکت نکردن در عملیات مسیریابی یا قطع ارتباط وجود دارند که در تمامی پروتکلهای مسیریابی وجود دارند و تنها راه جلوگیری از آنها پیدا کردن نود متخاصم می باشد .در ادامه به بررسی هر سه دسته از حملات فوق پرداخته خواهد شد:

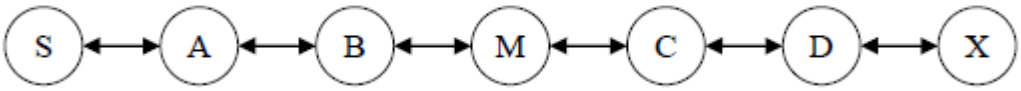
www.Prozhe.com

۴-۱-۱)حملات مبتنی بر Modification

یک نود متخاصم می تواند با تغییر فیلدهای یک بسته مسیریابی، باعث شود تا یک مسیر به اشتباه بنا نهاده شود .این کار به گونه های مختلفی می تواند صورت پذیرد .در زیر به توضیح درباره روشهای مختلف modification برای دستیابی به مقاصد مختلف پرداخته شده است:

۱-تغییر مسیر به وسیله تغییر شماره توالی

برخی از الگوریتمهای مسیریابی مانند AODV برای تصحیح مسیر از پیش ساخته شده از یک شماره توالی در پیامهای RREQ استفاده می کنند .شکل(٤-١) یک شبکه موردی نمونه را نشان می دهد که فرض شده نود متخاصم M یک پیام RREQ را از نود B دریافت کرده است.



شکل ٤-١) یک شبکه موردی

این پیام RREQ از طرف S برای پیدا کردن مسیری به X صادر شده است .حال اگر نود M یک RREP با شماره توالی بسیار بزرگتر از شماره توالی RREQ ارسالی، ایجاد کند می تواند مسیر را به نفع خود تغییر دهد .زیرا نود B ، RREP های ارسالی از نود های دیگر را به دلیل کوچکتر بودن شماره توالی آنها نمی پذیرد .این اشکال تنها زمانی رفع می شود که یک RREP یا RREQ معتبر با شماره توالی بزرگتر از RREP ارسالی توسط M ،به B برسد.

۲-تغییر مسیر به وسیله تغییر تعداد HOP

در الگوریتمهایی مانند AODV از روشهای مختلفی برای پیدا کردن کوتاه ترین مسیر از بین مسیرهای پیدا شده استفاده می کنند .یکی از این روشها که بسیار استفاده می شود، استفاده از شمارنده hop است .بدین ترتیب که هر نود که RREQ را به گره بعدی ارسال می کند، یک واحد

www.Prozhe.com

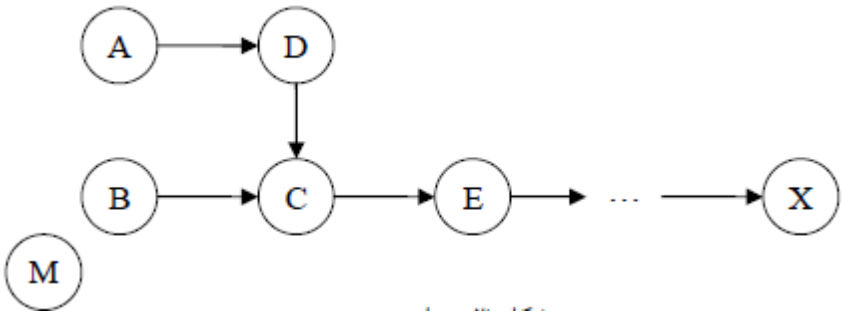
به شمارنده hop اضافه می کند. در نهایت، از روی کمترین مقدار hop count می توان به کوتاه ترین مسیر پی برد .حال یک نود متخاصم می تواند با صفر کردن مقدار hop count یک RREQ ، باعث شود تا مسیر نهایی با احتمال بسیار زیادی از خود آن نود عبور کند. و یا اینکه با بینهایت قرار دادن مقدار آن، خود را از قرار گرفتن در مسیر کنار بکشد.

۳-ممانعت از سرویس به وسیله تغییر مسیر مبدأ

الگوریتمهایی مانند DSR ،مسیر پیدا شده را در سرآیند بسته های ارسالی قرار می دهند .حال یک نود متخاصم می تواند مسیر داخل سرآیند یک بسته را تغییر دهد تا آن بسته به مقصد خود دست نیابد .بدین ترتیب می تواند از رسیدن بسته به مقصد درست، جلوگیری نماید.

۴-۱-۲)حملات مبتنی بر Impersonation

یکی دیگر از ضعفهای موجود، امکان جعل هویت افراد است .بدین ترتیب که یک نود در بسته های خروجی خود، IP یا آدرس MAC نود دیگری را قرا دهد .بدین وسیله یک نود می تواند خود را به جای یک نود دیگر جا بزند .یک نمونه از این حملات را که منجر به ایجاد یک حلقه می شود در شکل (٤-۲) آورده شده است.



شکل٤-۲)جعل هویت

www.Prozhe.com

در شکل بالا یک شبکه نمونه نمایش داده شده است. مسیرهای نشان داده شده توسط یک درخواست مسیریابی توسط الگوریتم AODV بنا شده است .حال اگر نود M به نزدیکی نود B رفته و با MAC نود A خود را به جای او جا بزند و RREPی را با hop count صفر برای B ارسال کند، B مسیر را به سمت A تغییر می دهد .در مرحله بعد نود M جای خود را عوض کرده و به سمت C می رود و با MAC متعلق به B یک RREP با hop count صفر برای C ارسال می کند .بنابراین C نیز مسیر خود را به سمت B تغییر میدهد .در این مرحله است که یک حلقه (A,D,C,B,A) ایجاد می شود.

یکی دیگر از راههای دسته بندی حملات مسیریابی به صورت زیر است .این حملات را می توان به دو دسته حمله های شکست مسیریابی و حمله های مصرف مسیریابی تقسیم می شوند .در دسته اول از حمله ها، حمله کننده سعی می کند تا بسته های خود را به عنوان بسته های قانونی بر روی شبکه ارسال نماید تا این بسته ها در راههای غیر کارا صرف شوند .در دسته دوم، حمله کننده سعی می کند تا با ارسال بسته ها به گونه ای سبب شود تا منابع شبکه مانند پهنای باند و یا منابع نود مانند حافظه یا توان محاسباتی، مصرف شوند .از دید لایه کاربرد هر دوی این حملات در دسته حملات ممانعت از سرویس قرار می گیرند.

در ادامه به بررسی چند حمله مشهور که خاص شبکه های موردی هستند پرداخته می شود:

۴-۱-۳)حمله سوراخ کرم

یکی از حملات بسیار مشهوری که خاص شبکه های موردی است، حمله سوراخ کرم می باشد . در این حمله دو نود متخاصم با همکاری یکدیگر، یک اتصال کوتاه را در توپولوژی شبکه ایجاد می کنند .حمله مذکور به ترتیب زیر اجرا می شود .درخواست مسیریابی از جانب یک نود ، به یکی از نود های متخاصم می رسد .حال این نود متخاصم درخواست را از طریق یک شبکه خصوصی برای

www.Prozhe.com

نود دوم ارسال می کند .حال اگر این دو نود مقدار شمارنده hop درخواست مسیر را عوض نکنند، مقداری زیادی از مسیر توسط این شبکه خصوصی بدون افزایش مقدار hop طی شده است .بدین ترتیب ممکن است به جای دهها hop،تنها با دو hop، بسته به مقصد برسد .در این حالت، مطمئناً این مسیر به عنوان کوتاهترین مسیر انتخاب می شود.

یک راه برای جلوگیری از حمله سوراخ کرم استفاده از قلاده های بسته است. این روش توسط Yih Chun Hu و Adrian Perrig ارائه شد. قلاده های بسته به دو قسمت تقسیم می شوند:

۱-قلاده های زمانی:

این تکنیک مبتنی بر همزمانی دقیق دو نود مبدا و مقصد و همچنین استفاده از مهر زمانی در بسته ها است. بدین ترتیب با کاهش مقدار مهر زمانی از زمان دریافت بسته، مدت زمانی که بسته در راه بوده است تخمین زده می شود و از این طریق می توان در مقابل تعداد hop هایی که زمان از اندازه معقول بزرگتر است، جلوگیری کرد .یعنی با توجه به زمان در راه بودن بسته و سرعت انتقال بسته در رسانه، تخمین زد که حدوداً چه تعداد hop ی می بایست توسط بسته طی شده باشد . بنابراین می توان در مقابل حمله سوراخ کرم ایستادگی کرد.

۲-قلاده های مکانی:

این تکنیک مبتنی بر اطلاعات مکانی است. نود مقصد می تواند با توجه به محدود بودن سرعت نود ها، فاصله تقریبی نود مبدا تا خود را اندازه گیری کند و بنابراین از مسیرهای غیر معقول جلوگیری نماید.

۴-۱-۴)حمله هجوم

یکی از حملاتی که در شبکه های موردی وجود دارد حمله هجوم است .این حمله در برابر تمامی پروتکلهای on-demand ی که برای شبکه های موردی مطرح شده است (شامل

www.Prozhe.com

الگوریتمهای امن)کاربرد دارد دارد .در یک پروتکلon-demand زمانی که یک نود بخواهد مسیری را به یک نود مقصد بداند، بسته درخواست مسیر را برای تمامی نود های همسایه ارسال می کند .برای کاهش بار این flooding ، هر نود که دریافت کننده این درخواست مسیر است، فقط برای یک بار آن را به سمت جلو ارسال می کند .در تمامی پروتکلها همانند SRP، ARAN ، SAODV، Ariadne، LAR، AODV،DSR و غیره تنها اولین درخواست مسیر دریافت شده منتشر می گردد و درخواستهای مسیر بعدی از همان اکتشاف مسیر، نادیده گرفته می شوند .در حمله توسط نود های همسایه نود مقصد باشد .در این صورت تمامی درخواستهای دیگر که بعداً به دست این نود های هجوم همین روش عملکرد مورد استفاده قرار می گیرد.

فرض شود در طی یک عملیات اکتشاف مسیر، بسته های دریافتی از سوی مهاجمین، اولین بسته دریافتی توسط نود های همسایه نود مقصد باشد .در این صورت تمامی درخواستهای دیگر که بعداً به دست این نود های می رسد نادیده گرفته خواهد شد و تنها بسته درخواست مسیری که مهاجم فرستاده است را به مقصد ارسال می نماید .همین امر باعث می شود تا مسیرهای به دست آمده به گونه ای باشد که حتماً در آن مسیرها یک نود مهاجم وجود داشته باشد.

بنابراین اگر مهاجم درخواست خود را بسیار سریعتر از نود مجاز ارسال نماید، به طور حتم بسته او دریافت خواهد شد و مورد پذیرش قرار خواهد گرفت و مهاجم می تواند با احتمال زیادی مسیری را بنا کند که خود او در آن مسیر وجود دارد .نود مهاجم برای انجام این عمل به منابع زیادی احتیاج ندارد .زیرا اصولاً تأخیری که در فرستادن رو به جلوی بسته های درخواست ایجاد می شود ناشی از دو علت است. علت اول مشغول بودن رسانه است .به عنوان مثال اگر از سیستم CDMA برای ارسال اطلاعات بر روی رسانه استفاده می شود، در صورت اشغال بودن رسانه، نود می بایست برای خالی شدن رسانه منتظر بماند .دوم اینکه برای جلوگیری از تلاقی اطلاعات بر روی رسانه، هر نود می بایست به میزان یک عدد تصادفی منتظر بماند و سپس اطلاعات خود را بر روی رسانه منتشر کند .حال اگر مهاجم هیچکدام از این زمانها را صرف نکند و بلافاصله پس از دریافت

www.Prozhe.com

درخواست، آن را ارسال کند، با احتمال زیادی درخواست او زودتر از بقیه درخواستها به نود های همسایه نود مقصد می رسد.

یک روش دیگر برای این کار این است که مهاجم نود های همسایه را مشغول نگاه دارد تا در هنگام دریافت یک درخواست مسیر، آنها فرصت پاسخگویی به آن را نداشته باشند .برای مثال در یک شبکه که از تصدیق اصالت برای پیامهای درخواست مسیر استفاده می شود، نود مهاجم می تواند با ارسال پیامهای درخواست مسیر جعلی، نود های همسایه را سرگرم تصدیق اصالت آنها کند . در این حالت پس از دریافت درخواست مسیر مجاز از یک نود دیگر، خود نود مهاجم آن را به سمت جلو ارسال می کند .در صورتی که نود های همسایه فرصتی برای کنترل آن را ندارند و این کار را به تأ خیر می اندازند.

راه دیگری که برای این کار وجود دارد این است که مهاجم، توان ارسال بسته درخواست را بالا ببرد .بنابراین بسته با توان بیشتری بر روی رسانه منتشر می شود و با تعداد hop کمتری به مقصد می رسد .بنابراین در زمانهایی که در طول این رفت و آمد در نود ها صرف پردازش بسته ها می شد، صرفه جویی می شود.

یک مهاجم قدرتمند تر ممکن است از حمله سوراخ کرم برای پیاده سازی حمله هجوم استفاده کند .در این روش، مهاجم از طریق یک کانال باسیم که سرعت انتقال آن سریعتر از سرعت انتقال بسته ها در شبکه موردی است، بسته درخواست به سمت یک نود مهاجم دیگر ارسال کرده و بدین ترتیب باعث حمله هجوم در شبکه موردی می شود.

تمامی پروتکلهای on-demand موجود در مقابل حمله هجوم دچار ضعف هستند. زیرا این پروتکلها می بایست تعداد درخواستهای ارسالی تکراری را به منظور کاهش بار شبکه، کم کنند . بنابراین یک مهاجم زیرک می تواند از این مسأله استفاده ببرد.

۴-۲)نیازمندیهای امنیتی شبکه های موردی

www.Prozhe.com

یک الگوریتم مسیریابی خوب در شبکه موردی می بایست بتواند یک مسیر را به درستی بنا کند و از آن نگهداری نماید .بدین معنا که اجازه ندهد تا نود های متخاصم از ساخت یا نگهداری صحیح مسیر جلوگیری نمایند. در مجموع اگر یک الگوریتم نکات زیر را رعایت کند می توان آن را یک الگوریتم امن نامید. اصولاً در یک الگوریتم امن باید موارد زیر رعایت شود:

۱-سیگنالهای مسیریابی نمی توانند جعل شوند.

۲-سیگنالهای دستکاری شده نتوانند به داخل شبکه تزریق شوند.

۳-پیامهای مسیریابی در طی انتقال به جز در روند عادی پروتکل تغییر پیدا نکنند.

٤-حلقه های مسیریابی در طی فعالیتهای خصم آمیز ایجاد نشوند.

۵-کوتاه ترین مسیرها توسط نود های متخاصم تغییر پیدا نکند.

موارد بالا نیازهای یک محیط باز را برآورده می کنند .برای یک محیط باز مدیریت شده مورد زیر نیز می بایست رعایت شود.

٦- نود های غیر مجاز می بایست از شبکه کنار گذاشته شوند .این مورد با این فرض صورت می گیرد که مدیریت شبکه در راه اندازی و توزیع کلید و ... نقش داشته باشد.

همچنین یک محیط متخاصمانه مدیریت شده تعریف می شود که در آن علاوه بر موارد فوق مورد زیر نیز در نظر گرفته می شود.

۷-توپولوژی شبکه نباید توسط مدیر شبکه به هیچ کدام از نود های مجاز و یا متخاصم نشان داده شود .زیرا نود های متخاصم می توانند از طریق آن برای تخریب شبکه اقدام کنند.

۴-۳)الگوریتم های امن مسیریابی شبکه های موردی

به دلیل ضعف امنیتی که الگوریتم های مسیریابی موردی داشته اند پروتکل هایی جهت امنیت آنها معرفی شده اند که به چند مورد آنها اشاره شده است:

www.Prozhe.com

۴-۳-۱)پروتکل ARAN

این الگوریتم توسط kimiya sanzgiri و همکارانش در سال ۲۰۰۲ ارائه شد.این الگوریتم بر پایه رمزنگاری با کلید عمومی و همچنین استفاده از گواهی بنا شده است.پروتکل ARAN جهت ارائه امنیت مسیریابی،گواهی های رمزنگارانه را به کار می گیرد.چنین گواهی هایی در حال حاضر به عنوان بخشی از شبکه های تک hop ۸۰۲.۱۱ به کار گرفته شده اند.

پروتکل aran شامل یک فرآیند صدور گواهی مقدماتی است که توسط یک فرآیند نمونه سازی مسیر دنبال می شود و تصدیق اصالت انتها به انتها را تضمین می کند. این پروتکل در مقایسه با اکثر پروتکل های مسیریابی موردی غیر امن ،ساده به نظر می رسد. کشف مسیر aran توسط یک پیام کشف مسیر انتشار یافته از یک نود مبدأ انجام می گیرد که به حالت unicast توسط نود مقصد پاسخ داده می شود، به طوریکه پیامهای مسیریابی هم در طول مسیر مبدأ به مقصد،در هر hop تصدیق اصالت می شوند و هم در مسیر عکس(از مقصد به مبدأ)

۴-۳-۲)پروتکل Ariadne

این پروتکل برخلاف aran بر ایمن سازی الگوریتم dsr تکیه میکند. در این پروتکل به جای استفاده از کلید عمومی، از رمزنگاری متقارن استفاده می شود. برای تصدیق اصالت پیامها نیز یک کد تصدیق اصالت پیام مورد استفاده قرار می گیرد. این کد تصدیق اصالت توسط یک تابع درهم سازی بر روی hash پیام دریافتی و همچنین شناسه خود گره فرستنده ساخته می شود. بنابراین هر دریافت کننده ای میتواند از اصیل بودن پیام دریافتی اطمینان حاصل نماید.

www.Prozhe.com

۴-۳-۳)پروتکل saodv

این پروتکل همانند اسم آن برای ایجاد امنیت در الگوریتم aodv ساخته شده است. در این پروتکل از توابع hash استفاده می شود. به طوری که hn-۱=H(hn) در این الگوریتم از hop count برای اندازه گیری تعداد hop ی که بسته تاکنون طی کرده است استفاده می گردد. اگر hop count از یک مقدار max count بیشتر شود،این بسته نادیده گرفته می شود. برای عدم تغییر مقدار hop count و اطمینان از صحت مقدار آن،از توابع hash استفاده می شود.

۴-۳-۴)پروتکل srp

مبنای این پروتکل بر این اساس است که یک نود مبدأ برای مسیریابی،می تواند پاسخ های دریافتی برای این عملیات را تشخیص داده و در صورت تشخیص نادرست بودن، آنها را نادیده بگیرد. برای این منظور یک وابستگی امنیتی بین نود مبدأ و نود مقصد در نظر گرفته می شود. اینsa می تواند به عنوان مثال به وسیله دانستن کلید عمومی طرف مقابل مطرح شود. حال طرفین می توانند به وسیله یک پروتکل تبادل کلید مانند الگوریتم خم بیضوی دیفی هلمن، یک کلید مشترک خصوصی را بین خود به اشتراک بگذارند.

وجود وابستگی امنیتی قطعی است، زیرا میزبان های نهایی ، یک طرح ارتباطی ایمن را به کار برده اند و در نتیجه باید قادر باشند که یکدیگر را تصدیق اصالت کنند. به عنوان مثال ،چنین گروهی از نود ها میتواند یک تبادل کلید امن را انجام دهد. با وجود این ، وجود وابستگی امنیتی میان هر یک از نود های میانی ضروری نمی باشد. در نهایت می بایست که نود های نهایی قادر باشند که از حافظه ایستا یا فناناپذیر استفاده کنند.

نود های متخاصم ممکن است برای مختل کردن عملکرد شبکه رفتاری خودسرانه،byzantine، در پیش گیرند. آنها قادر به خراب کردن،اجرای مجدد و همچنین ساختن بسته های مسیریابی می

www.Prozhe.com

باشند. این نود ها ممکن است به هر روشی در صدد منحرف کردن بسته ها از مسیر خود باشند و عموما نمی توان توقع داشت که به درستی پروتکل مسیریابی را اجرا کنند. علی رغم اینکه مجموعه ای از نود های متخاصم ممکن است به طور همزمان، حملاتی را برعلیه پروتکل ایجاد کنند، فرض ما بر این است که نود ها قادر به همکاری در یکی از مراحل اجرای پروتکل نمی باشند، یعنی در زمان انتشار یک درخواست و دریافت پاسخ های مربوطه هیچ عملی انجام نمی دهند.

در این پروتکل پیوندها دوطرفه هستند که نیاز اکثر پروتکل های کنترل دسترسی رسانه ارائه شده را برآورده میکند به خصوص پروتکل هایی که گفتگوی rts/cts را به کار میبرند. همچنین انتظار می رود که یک نگاشت یک به یک میان کنترل دسترسی رسانه و آدرس های ip وجود دارد. در آخر، خاصیت انتشاری کانال رادیویی متعهد می شود که هر ارسال، توسط تمام همسایگانی که در حالت نامنظمی قرار دارند، دریافت می شود.

۴-۳-۵)پروتکل sead

این پروتکل بر اساس dsdv بنا شده است. در این پروتکل در هر نود یک جدول مسیریابی وجود دارد که در آن لیستی از تمامی مقاصد ممکن در شبکه وجود دارد. در هر قسمت جدول، آدرس مقاصد، نزدیک ترین فاصله دانسته شده آن ها(که metric نامیده میشود)و نود های همسایه که با hop بعدی می توان به آن مقصد دست یافت، ذخیره شده است. این metric ها معمولا برحسب تعداد hop در جدول نوشته می شوند. هر نود برای به روز در آوردن جدول مسیریابی خود هر از چند گاهی یک پیام درخواست مسیر را برای تمامی همسایگان خود ارسال می کند تا بتواند مسیرهای جدید را در جدول خود قرار دهد. اولین پیشرفت امنیتی که sead در dsdv انجام داده است،اضافه کردن شماره توالی به هر عنصر جدول مسیریابی است. این شماره توالی ها از ایجاد حلقه هایی که ممکن است از به روزآوری خارج از موقع مسیرها ایجاد

www.Prozhe.com

شود،جلوگیری میکند.این پروتکل از زنجیره توابع درهم سازی یک طرفه به جای توابع رمزنگاری غیر متقارن استفاده میکند.

۴-۳-۶)پروتکل spaar

این پروتکل برای بهبود بخشیدن کارآیی و امنیت،اطلاعات موقعیت را به کار می گیرد و در عین حال این اطلاعات را از نود هایی که تصدیق اصالت نشده اند،محافظت می کند. برای اینکه پروتکلهای مسیریابی شبکه های موردی به سطح بالایی از امنیت دست یابند، به نود ها تنها این اجازه داده می شود که پیام های مسیریابی را از همسایگان تک hop خود بپذیرند.

در spaar ، به کمک اطلاعات موقعیت،یک نود می تواند همسایگان تک hop خود را پیش از قرار دادن آنها در پروتکل مسیریابی،شناسایی کند. از نیازهای spaar این است که هر دستگاه بتواند موقعیت خود را تعیین کند.دریافت کننده های gps تقریبا ارزان و سبک هستند،بنابراین منطقی است که فرض کنیم تمام دستگاه ها در شبکه ما به یکی از آن ها مجهز هستند.

درspaar ، نود مبدأ باید موقعیت جغرافیایی تقریبی مقصد را نیز بداند،که می تواند آن را از روی اطلاعات آخرین موقعیت و آخرین سرعت ذخیره شده در جدول مقصد نود مبدأ،محاسبه نمود. اگر این اولین تلاش نود مبدأ برای برقراری ارتباط با یک مقصد خاص باشد،ممکن است موقعیت مقصد را نداشته باشد. در این حالت می توان از یک سرویس موقعیت استفاده کرد.اگر هیچ سرویس موقعیتی در دسترس نبود،می توان برای دستیابی به مقصد و دریافت اطلاعات موقعیتی آن، یک الگوریتم flooding انتخابی را به کار گرفت.

www.Prozhe.com

فصل پنجم

بحث و نتیجه گیری

www.Prozhe.com

۵-۱) نتیجه گیری

در این قسمت نتایج بررسی ها به طور خلاصه اعلام خواهد شد. از جمله نتایج عبارتند از:

۱-در شبکه های ادهاک، نودهای شبکه دانش قبلی از توپولوژی شبکه ای که درآن قرار دارند، ندارند به همین دلیل مجبورند برای ارتباط با سایر نودها، محل مقصد را در شبکه کشف کنند.

۲-مسیریابی در شبکه های ادهاک نوع حسگر محدودیت هایی را بر شبکه اعمال می کند که باید در انتخاب روش مسیریابی دقت شود ازجمله اینکه منبع تغذیه در نود ها محدود می باشد و در عمل، امکان تعویض یا شارژ مجدد آن نیست.

۳-شبکه های حسگر بی سیم قادر به انجام کارهایی هستند که تا پیش از این امکان پذیر و عملی نبوده است. و چون مصرف انرژی نقش مهی پیدا کرده است در آینده شاهد بکارگیری بیشتر شبکه های حسگر بی سیم خواهیم بود. کاربردهای حسگر بی سیم شامل: سیستم های کنترل انرژی ، حراست و نظارت توربین های بادی است.پایش های زیست محیطی خدمان پشتیبانی در محل و نیز مراقبت های بهداشتی و پزشکی است.

٤-بر خلاف سیستم های مخابراتی جاری در شبکه های سیار ادهاک ، یک کاربر از طریق چند hop با کاربر دیگر ارتباط برقرار می کند(در حالیکه در سیستم های کنونی کاربر تنها در یک hop با ایستگاه مرکزی ارتباط دارد.)

www.Prozhe.com

۵-شبکه های ادهاک ارزان،ساده،انعطاف پذیر هستند و استفاده از آنها راحت است. این شبکه ها پیوسته تغییر می کنند و توپولوژی خودشان را برای اتصال نود های جدید تغییر می دهند به همین دلیل ما به سمت آنها می رویم. علی رغم مشکلات امنیتی که دارند کاربردهای زیادی دارند در واقع روز به روز بر کارایی آنها افزوده شده و از قیمتشان کاسته می شود .به همین دلیل در بازار طرفداران زیادی دارند.

٦-یکی از مهمترین و جالب ترین بخش ها در شبکه های حسگر بیسیم در نظر گرفتن حسگرهای متحرک در شبکه است. در اکثر پروتکل های فعلی فرض می شود که حسگرها در شبکه ثابت هستند. اما در بعضی از شرایط نیاز است که حسگرها متحرک باشند .در این موارد به روز کردن اطلاعات مسیریابی و انتقال اطلاعات مسیریابی در کل شبکه باعث مصرف زیاد انرژی می شود. راه حل های مناسب برای استفاده از حسگرهای متحرک در شبکه به شدت مورد بررسی و تحقیق است.

۷-همچنین تحقیقات آینده می تواند در مورد اتصال شبکه های حسگر بیسیم به شبکه های امروزی مانند اینترنت باشد. در بسیاری از کاربرها مانند کاربردهای حفاظتی و کنترل محیط، نیاز به این است تا داده ها از حسگرها جمع آوری شده و به یک ایستگاه پایه جهت بررسی و آنالیز فرستاده شود. از طرف دیگر، درخواست های کاربر از طریق اینترنت صادر می شود در نتیجه فراهم ساختن این امکان، امری لازم و اجتناب ناپذیر می باشد.

۸- با توجه به ضعف شبکه های ادهاک ، الگوریتم های امنیتی ارائه شده با اینکه از لحاظ کارایی قابل قبول هستند ولی هنوز برخی از مشکلاتی امنیتی در آنها وجود دارد که برای رفع اینگونه مشکلات ، بسط هایی ارائه شده است ولی کارایی شبکه آنها را دچار مشکل میکند. پس بنابراین الگوریتم هایی که دو جنبه امنیت و کارایی شبکه را در بر بگیرد بسیار ضروری است.

www.Prozhe.com

۵-۲) پیشنهادات

با توجه به مطالب گفته شده ، پیشنهادات به شرح زیر است:

۱)ارتقای پروتکل های ارائه شده از نظر امنیت و کارایی

۲)ارزیابی و مقایسه علمی بین انواع پروتکل های مسیریابی امن

۳)بدست آوردن مدلی برای مشکلات امنیتی مسیریابی امن

٤)طراحی پروتکل های امن برای شبکه های بی سیم

۵)بهینه سازی پروتکل ها و الگوریتم های ارائه شده

www.Prozhe.com

منابع و ماخذ

منابع فارسی

۱)موسی پور ،م،۱۳۸٤،امنیت مسیریابی در شبکه های موردی،سمینار دوره کارشناسی ارشد،دانشگاه صنعتی امیرکبیر

۲)حمیدی،ر،۱۳۹۱،شبکه های موردی **manet** و شبکه های حسگر بی سیم،پایان نامه دوره کاردانی،دانشگاه آزاد اسلامی واحد مهدیشهر

۳)شاهسوند،م،۱۳۹۲،شبکه **adhoc** ،پایان نامه دوره کارشناسی،دانشگاه پیام نور واحد ایذه

٤)کریمی،ن،۱۳۹۲،شبکه های موردی و شبکه های حسگر بی سیم و مسیریابی بین آنها،پایان نامه دوره کاردانی،دانشگاه فنی و حرفه ای آموزشکده فنی الزهرا تبریز

۵)براتی کلر،ج،۱۳۹۰، ارزیابی الگوریتم های هوشمند در مسیریابی شبکه های موبایل،پایان نامه دوره کاردانی،دانشگاه پیام نور مشهد

٦)علیزاده،س،۱۳۹۱، مسیریابی در شبکه های حسگر بیسیم،پایان نامه دوره کارشناسی،دانشگاه پیام نور مشهد

۷)آذرمی،مهدی،۱۳۸۵،بهبود الگوریتم های مسیریابی مبتنی بر موقعیت گره ها در شبکه های موردی سیار،پایان نامه کارشناسی ارشد،دانشگاه صنعتی امیرکبیر

www.Prozhe.com

ABSTRACT

Ad hoc networks include a set of distributed nodes that are wirelessly connected together. Nodes can be computer hosts or routers that equipped with a transceiver and communicate with each other directly without any access points, therefore they have not a fixed organization and formed in an arbitrary topology. So the most important feature of these networks is their dynamic topology that is the result of mobility. Nodes in this network are constantly changing their positions and therefore the need for a good routing protocol that can adapt to these changes, has become more visible. In this thesis, routing algorithms in Ad hoc networks will be considered and their performance, efficiency and security will be compared with each other.

www.Prozhe.com

ISLAMIC AZAD UNIVERSITY

North Tehran Branch

B.Sc.Thesis

On Information Technology Engineering

Research Title:

An Exhaustive Study of Routing Algorithms in Adhoc Networks

Advisor:

Dariush Ziaei Ghafouri

Prepare By:

Ramin Kashefi

Spring ۲۰۱۵

www.Prozhe.com