بسم الله الرحمن الرحیم

www.markazpress.ir

دانشگاه جامع
علمی-کاربردی

پایان نامه دوره کاردانی رشته فناوری اطلاعات و ارتباطات

گرایش فناوری اطلاعات و ارتباطات

موضوع

روشهای نشر اطلاعات در شبکه های حسگر بیسیم

استاد راهنما

مهندس حسن زارع

دانشجو

کیاوش مه رو

تیر ماه ۱۳۹۱

www.markazdanesh.ir

دانشگاه جامع
علمی-کاربردی

پایان نامه دوره کاردانی رشته فناوری اطلاعات و ارتباطات

گرایش فناوری اطلاعات و ارتباطات

موضوع

روشهای نشر اطلاعات در شبکه های حسگر بیسیم

استاد راهنما

مهندس حسن زارع

نام استاد راهنما : مهندس حسن زارع

نمره استاد :

www.markazdanesh.ir

چکیده :

علاوه بر نکاتی که تا کنون درباره شبکه های حسگر به عنوان مقدمه آشنایی با این فناوری بیان کردیم، این شبکه ها دارای یک سری ویژگی های عمومی نیز هستند . مهم ترین این ویژگی ها عبارت است از :

۱- بر خلاف شبکه های بی سیم سنتی، همه گره ها در شبکه های بی سیم حسگر نیازی به برقراری ارتباط مستقیم با نزدیک ترین برج کنترل قدرت یا ایستگاه پایه ندارند، بلکه حسگرها به خوشه هایی (سلول هایی) تقسیم می شوند که هر خوشه (سلول) یک سرگروه خوشه موسوم به Parent انتخاب می کند . این سرگروه ها وظیفه جمع آوری اطلاعات را بر عهده دارند. جمع آوری اطلاعات به منظور کاهش اطلاعات ارسالی از گره ها به ایستگاه پایه و در نتیجه بهبود بازده انرژی شبکه انجام می شود . البته چگونگی انتخاب سرگروه خود بحثی تخصصی است که در تیوری شبکه های بی سیم حسگر مفصلاً مورد بحث قرار می گیرد .

۲- پروتکل های شبکه ای همتا به همتا یک سری ارتباطات مش مانند را جهت انتقال اطلاعات بین هزاران دستگاه کوچک با استفاده از روش چندجهشی ایجاد می کنند . معماری انطباق پذیر مش، قابلیت تطبیق با گره های جدید جهت پوشش دادن یک ناحیه جغرافیایی بزرگ تر را دارا است . علاوه بر این، سیستم می تواند به طور خودکار از دست دادن یک گره یا حتی چند گره را جبران کند .

۳- هر حسگر موجود در شبکه دارای یک رنج حسگری است که به نقاط موجود در آن رنج احاطه کامل دارد. یکی از اهداف شبکه های حسگری این است که هر محل در فضای مورد نظر بایستی حداقل در رنج حسگری یک گره قرار گیرد تا شبکه قابلیت پوشش همه منطقه موردنظر را داشته باشد .

یک حسگر با شعاع حسگری r را می توان با یک دیسک با شعاع r مدل کرد. این دیسک نقاطی را که درون این شعاع قرار می گیرند، تحت پوشش قرار می دهد . بدیهی است که برای تحت پوشش قرار دادن کل منطقه این دیسک ها باید کل نقاط منطقه را بپوشانند .

واژه های کلیدی :

شبکه حسگر بیسیم ، مسیر یابی ، پروتکل مسیر یابی ، انتشار اطلاعات

www.markazdanesh.ir

فهرست مطالب

عنوان	صفحه
فصل اول نگاهی به شبکه حسگر بیسیم	۸
مقدمه	۸
۱.۱ تاریخچه	۱۰
۱.۲ساختار کلی شبکه حسگر بیسیم	۱۱
۱.۳ ویژگی ها	۱۵
۱.۴ ویژگی های عمومی یک شبکه	۱۶
۱.۵ ساختار ارتباطی شبکه حسگر	۱۷
۱.۶ فاکتور طراحی	۱۸
۱.۷ نمونه پیاده سازی شده شبکه حسگر	۲۴
۱.۸ سیستم عامل	۲۶
فصل دوم روشهای جمع اوری اطلاعات	۲۸
۲.۱ مقدمه	۲۸
۲.۲ انتشار و جمع اوری	۲۹
۲.۳ رقابت بر سر مسیر یابی	۳۱
۲.۴ استراتژی های مسیر یابی	۳۲
۲.۵ تکنیک مسیر یابی	۳۴
۲.۶ انتشار مستقیم	۳۵
۲.۷ سیل اسا و انواع ان	۳۶
۲.۸ روش شایعه پراکنی	۴۰
LEACH ۲.۹	۴۰
Energy Conversing ۲.۱۰	۴۲
۲.۱۱ پروتکل های ساختار درختی	۴۵
۲.۱۲ پروتکل مبتنی بر مش	۴۵
۲.۱۳ مسیر یابی جغرافیایی	۴۶
۲.۱۴ استراتژی مسیر یابی	۴۷

www.markazdanesh.ir

فهرست مطالب

عنوان	صفحه
۲.۱۵ اصول روتینگمبتنی بر وضعیت	۴۷
۲.۱۶ انتشار توزیع جغرافیایی	۴۹
۲.۱۷ روش های هدایت	۵۰
۲.۱۸ گره های سیار	۵۳
فصل سوم مسیر یابی امن	۵۶
۳.۱ مقدمه	۵۶
۳.۲ پیش زمینه	۵۸
۳.۳ شبکه حسگر در مقابل ad-hoc	۶۱
۳.۴ بیان مشکل	۶۲
۳.۵ حملات روی مسیر یابی شبکه حسگر	۶۶
۳.۶ حملات روی پروتکل های خاص شبکه حسگر	۷۲
۳.۷ ارسال با حداقل هزینه	۷۲
۳.۸ اقدامات متقابل	۷۳
خلاصه اقدامات متقابل	۷۷
نتیجه گیری	۷۸
منابع	۸۰

www.markazdanesh.ir

فهرست شکلها

عنوان | صفحه

۱.۱ حسگر طراحی شده ۱۰
۱.۲ ساختار کلی شبکه ۱۲
۱.۳ ساختار خودکار ۱۳
۱.۴ ساختار نیمه خودکار ۱۳
۱.۵ ساختمان داخلی گره ۱۵
۱.۶ حفره پوششی ۱۷
۱.۷ ساختار متداول یک شبکه حسگر ۱۸
۱.۸ ذره میکا ۲۴
۱.۹ساختار داخلی غبار هوشمند ۲۵
۱.۱۰ دو مدل برنامه نویسی با نقاط ضعف ۲۷
۱.۱۱ مدل برنامه نویسی رویدادگرا ۲۷
۲.۱ برنامه های کاربردی شبکه حسگر ۲۸
۲.۲ داده چندگانه و هدایت پرس و جو ۳۰
۲.۳ پخش Interest ۳۶
۲.۴ Flooding ۳۸
۲.۵ Implosing ۳۹
۲.۶ مسئله رو بهم افتادگی ترافیک در پرو تکل سیل اسا ۳۹
۲.۷ GAF ۴۲
۲.۸ تصمیم ارسال محلی شده و سراسری ۵۱
۲.۹ استراتژی چاهک سیار ۵۲
۲.۱۰ تعدادی چاهک ۵۴
۳.۱ خلاصه ای از حملات علیه پروتکل های مسیر یابی ۵۸
۳.۲ علایم شبکه حسگر ۵۹
۳.۳ یک معماری نمونه برای شبکه حسگر بیسیم ۶۰
۳.۴ حمله SYBIL ۶۹
۳.۵ حمله WORMHOLE ۷۰

www.markazdanesh.ir

لیست علایم اختصاری

WSN

Ad-hoc

www.markazdanesh.ir

فصل اول

نگاهی به شبکه‌های بی‌سیم حسگر

مقدمه

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی سیم توانایی طراحی و ساخت حسگرهایی را با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربری‌های گوناگون داده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی (بر اساس نوع حسگر، پردازش و ارسال آن اطلاعات را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه های موسوم به شبکه های بی‌سیم حسگر WSN شده‌اند.

یک شبکه حسگر متشکل از تعداد زیادی گره های حسگری است که در یک محیط به طور گسترده پخش شده و به جمع آوری اط لاعات از محیط می پردازند. لزوماً مکان قرار گرفتن گره های حسگری، از قبل‌تعیین‌شده و مشخص نیست . چنین خصوصیتی این امکان را فراهم می آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم

از طرف دیگر این بدان معنی است که پروتکل‌ها و الگوریتم های شبکه‌های حسگری باید دارای توانایی‌های خودساماندهی باشند. دیگر خصوصیت‌های منحصر به فرد شبکه های حسگری، توانایی همکاری و هماهنگی بین گره‌های حسگری است. هر گره حسگر روی برد خود دارای یک پردازشگر است و به جای فرستادن تمامی اطلاعات خام به مرکز یا به گره‌ای که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را روی اطلاعاتی که به دست آورده است، انجام می‌دهد و سپس داده‌های نیمه پردازش شده را ارسال می‌کند.

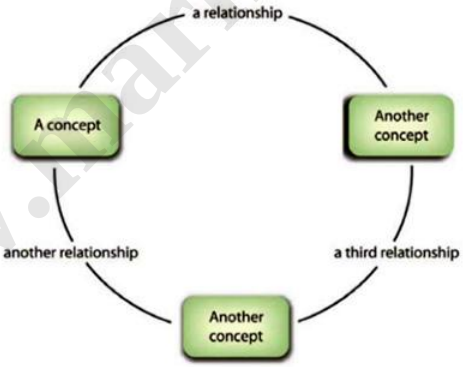
با اینکه هر حسگر به تنهایی توانایی ناچیزی دارد، ترکیب صدها حسگر کوچک امکانا ت جدیدی را عرضه می‌کند. در واقع قدرت شبکه‌های بی‌سیم حسگر در توانایی به کارگیری تعداد زیادی گره کوچک است که

www.markazdanesh.ir

خود قادرند سرهم و سازماندهی شوند و در موارد متعددی چون مسیریابی هم زمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند.

گستره کاربری شبکه‌های بی‌سیم حسگر بسیار وسیع بوده و از کاربردهای کشاورزی، پزشکی و صنعتی تا کاربردهای نظامی را شامل می‌شود. به عنوان مثال یکی از متداول‌ترین کاربردهای این تکنولوژی، نظارت بر یک محیط دور از دسترس است. مثلاً نشتی یک کارخانه شیمیایی در محیط وسیع کارخانه می‌تواند توسط صدها حسگر که به طور خودکار یک شبکه بی‌سیم را تشکیل می‌دهند، نظارت شده و در هنگام بروز نشت شیمیایی به سرعت به مرکز اطلاع داده شود.

در این سیستم ها بر خلاف سیستم های سیمی قدیمی، از یک سو هزینه های پیکربندی و آرایش شبکه کاسته می شود از سوی دیگر به جای نصب هزاران متر سیم فقط باید دستگاه های کوچکی را که تقریباً به اندازه یک سکه هستند (شکل ۱.۱)، را در نقاط مورد نظر قرار داد. شبکه به سادگی با اضافه کردن چند گره گسترش می‌یابد و نیازی به طراحی پیکربندی پیچیده نیست.



شکل۱.۱ - یک حسگر طراحی‌شده برای شبکه‌های WSN که به اندازه یک سکه است.

۱.۱ - تاریخچهٔ شبکه های حسگر

اگرچه تاریخچه شبکه های حس/کار را به دوران جنگ سرد و ایده اولیه آن را به طراحان نظامی صنایع دفاع آمریکا نسبت می دهند ولی این ایده می توانسته در ذهن طراحان ربات های متحرک مستقل یا حتی طراحان شبکه های بی سیم موبایل نیز شکل گرفته باشد.

www.markazdanesh.ir

۱.۲- ساختار کلی شبکه حسگر بی سیم

قبل از ارائه ساختار کلی ابتدا تعدادی از تعاریف کلیدی را ذکر می کنیم.

حسگر : وسیله ای که وجود شیئ رخداد یک وضعیت یا مقدار یک کمیت فیزیکی را تشخیص داده و به سیگنال الکتریکی تبدیل می کند. حسگر انواع مختلف دارد مانند حسگرهای دما , فشار, رطوبت, نور, شتاب سنج, مغناطیس سنج و...

کارانداز : با تحریک الکتریکی یک عمل خاصی مانند باز و بسته کردن یک شیر یا قطع و وصل یک کلید را انجام می دهد

گره حسگر: به گره ای گفته می شود که فقط شامل یک یا چند حسگر باشد.

گره کارانداز: به گره ای گفته می شود که فقط شامل یک یا چند کارانداز باشد.

گره حسگر/کارانداز: به گره ای گفته می شود که مجهز به حسگر و کار انداز باشد.

شبکه حسگر : شبکه ای که فقط شامل گره های حسگر باشد. این شبکه نوع خاصی از شبکه حس/کاراست . در کاربردهایی که هدف جمع آوری اطلاعات و تحقیق در مورد یک پدیده می باشد کاربرد دارد. مثل مطالعه روی گردبادها.

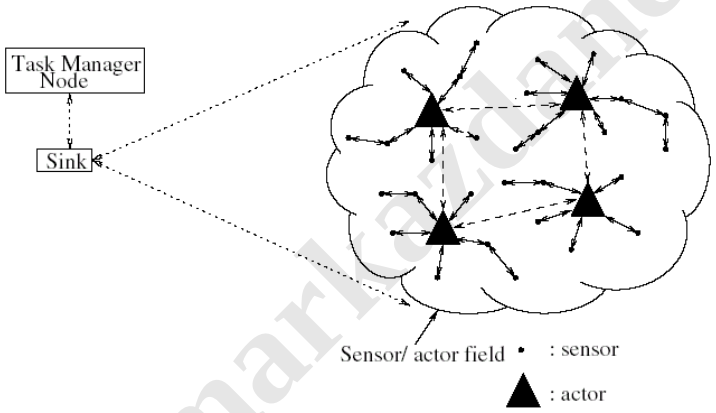
میدان حسگر/کارانداز : ناحیه کاری که گره های شبکه حس/کار در آن توزیع میشوند.

چاهک: گرهی که جمع آوری داده ها را به عهده دارد . و ارتباط بین گره های حس/کار و گره مدیر وظیفه را برقرار می کند.

گره مدیر وظیفه: گرهی که یک شخصی بعنوان کاربریا مدیر شبکه از طریق آن با شبکه ارتباط برقرار میکند. فرامین کنترلی و پرس و جو ها از این گره به شبکه ارسال شده و داده های جمع آوری شده به آن بر میگردد.

www.markazdanesh.ir

شبکه حسگر: شبکه ای متشکل از گره های حسگر و کار انداز یا حسگر/کارانداز است که حالت کلی شبک ه های مورد بحث می باشد. به عبارت دیگر شبکه حس/کارشبکه ای است با تعداد زیادی گره که هر گره می تواند در حالت کلی دارای تعدادی حسگر و تعدادی کارانداز باشد. در حالت خاص یک گره ممکن است فقط حسگر یا فقط کارانداز باشد. گره ها در ناحیه ای که میدان حس /کار نامیده می شود با چگالی زیاد پراکنده می شوند. یک چاهک پایش کل شبکه را بر عهده دارد. اطلاعات بوسیله چاهک جمع آوری می شود و فرامین از طریق چاهک منتشر می شود. مدیریت وظایف میتواند متمرکز یا توزیع شده باشد. بسته به اینکه تصمیم گیری برای انجام واکنش در چه سطحی انجام شود دو ساختار مختلف خودکار و نیمه خودکار وجود دارد. که ترکیب آن نیز قابل استفاده است.شکل(۱.۲) را مشاهده نمایید .

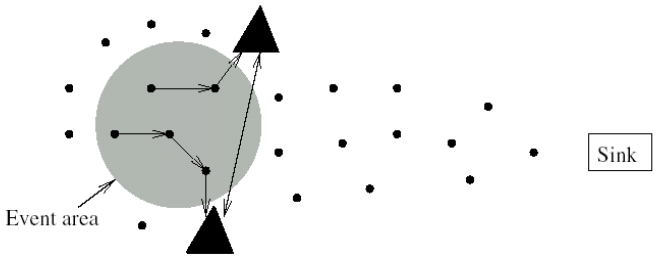


شکل۱.۲- ساختار کلی شبکه حس/کار

ساختار خودکار : حسگر هایی که یک رخداد یا پدیده را تشخیص می دهند داده های دریافتی را به گره های کارانداز جهت پردازش و انجام واکنش مناسب ارسال می کنند. گره های کارانداز مجاور با هماهنگی با یکدیگر تصمیم گیری کرده و عمل می نمایند. در واقع هیچ کنترل متمرکزی وجود ندارد و تصمیم گیری ها بصورت محلی انجام میشود.شکل(۱.۳) را ببینید.

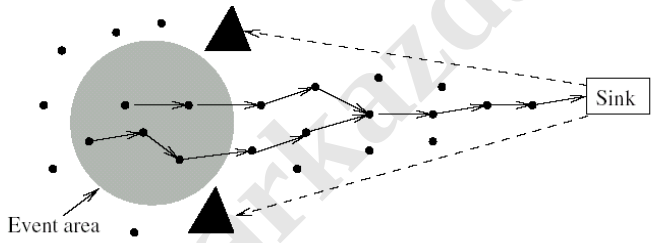
www.marlazdanesh.ir

.



شکل۱.۳ - ساختار خودکار

ساختار نیمه خودکار: در این ساختار داده ها توسط گره ها به سمت چاهک هدایت شده و فرمان از طریق چاهک به گره های کار انداز صادر شود .



شکل ۱.۴- ساختار نیمه خودکار

از طرف دیگر در کاربردهای خاصی ممکن است از ساختار بخش بندی شده یا سلولی استفاده شود که در هر بخش یک سردسته وجود دارد که داده های گره های دستهٔ خود را به چاهک ارسال می کند . در واقع هر سردسته مانند یک مدخل عمل میکند. شکل (۱.۴) را ببینید .

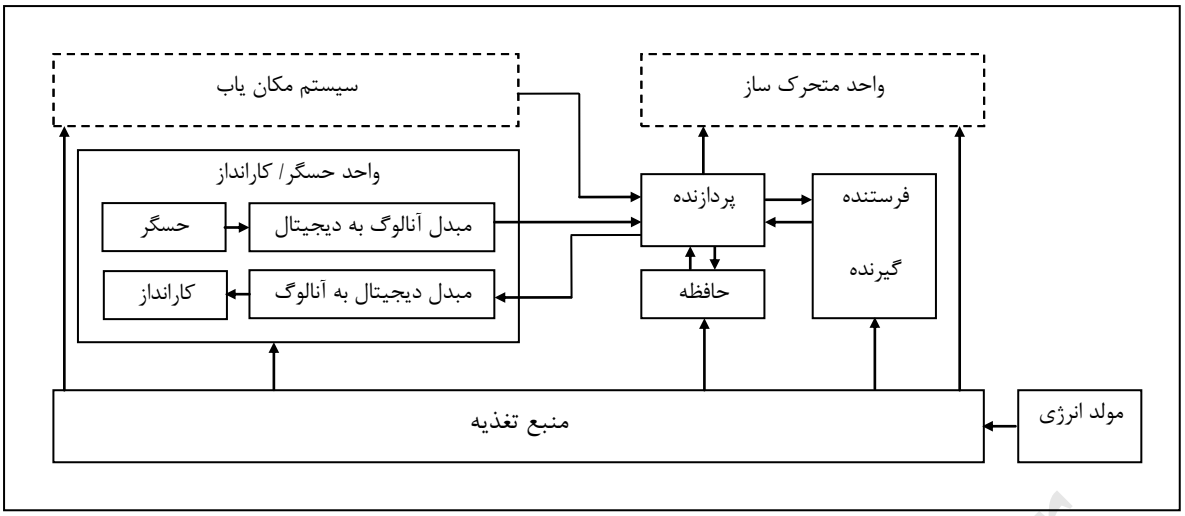
www.markazdanesh.ir

ساختمان گره

شکل(۵) ساختمان داخلی گره حس/کار را نشان می دهد. هر گره شامل واحد حسگر/ کارانداز, واحد پردازش داده ها, فرستنده/گیرنده بی سیم و منبع تغذیه می باشد بخشهای اضافی واحد متحرک ساز , سیستم مکان یاب و تولید توان نیز ممکن است بسته به کاربرد در گره ها وجود داشته باشد.

واحد پردازش داده شامل یک *پردازندهٔ* کوچک و یک *حافظه* با ظرفیت محدود است داده ها را از حسگرها گرفته بسته به کاربرد پردازش محدودی روی آنها انجام داده و از طریق فرستنده ارسال می کند . واحد پردازش مدیریت هماهنگی و مشارکت با سایر گره ها در شبکه را انجام می دهد . واحد فرستنده گیرنده ارتباط گره با شبکه را برقرار می کند. واحد حسگر شامل یک سری حسگر و مبدل آنالوگ به دیجیتال است که اطلاعات آنالوگ را از حسگرگرفته و بصورت دیجیتال به پردازنده تحویل می دهد. واحد کارانداز شامل کارانداز و مبدل دیجیتال به آنالوگ است که فرامین دیجیتال را از پردازنده گرفته و به کارانداز تحویل می دهد. واحد تامین انرژی, توان مصرفی تمام بخشها را تامین می کند که اغلب یک باطری با انرژی محدود است. محدودیت منبع انرژی یکی از تنگناهای اساسی است که در طراحی شبکه های حس /کار همه چیز را تحت تاثیر قرار می دهد. در کنار این بخش ممکن است واحدی برای تولید انرژی مثل سلول های خورشیدی وجود داشته باشد در گره های متحرک واحدی برای متحرک سازی وجود دارد. مکان یاب موقعیت فیزیکی گره را تشخیص می دهد. تکنیکهای مسیردهی و وظایف حسگری به اطلاعات مکان با دقت بالا نیاز دارند . یکی از مهمترین مزایای شبکه های حس/کار توانایی مدیریت ارتباط بین گره های در حال حرکت می باشد.

www.markazdanesh.ir



شکل ۱.۵- ساختمان داخلی گره حسگر/کارانداز

۱.۳- ویژگی ها

وجود برخی ویژگی ها در شبکه حسگر/ کارانداز, آن را از سایر شبکه های سنتی و بی سیم متمایز می کند . از آن جمله عبارتند از:

- تنگناهای سخت افزاری شامل محدودیتهای اندازهٔ فیزیکی, منبع انرژی , قدرت پردازش , ظرفیت حافظه
- تعداد بسیار زیاد گره ها
- چگالی بالا در توزیع گره ها در ناحیه عملیاتی
- وجود استعداد خرابی در گره ها
- تغییرات توپولوژی بصورت پویا و احیانا متناوب
- استفاده از روش پخش همگانی در ارتباط بین گره ها در مقابل ارتباط نقطه به نقطه
- داده محور بودن شبکه به این معنی که گره ها کد شناسایی ندارند

www.markazdanesh.ir

۱.۴- ویژگی‌های عمومی یک شبکه حسگر

علاوه بر نکاتی که تا کنون درباره شبکه‌های حسگر به عنوان مقدمه آشنایی با این فناوری بیان کردیم، این شبکه‌ها دارای یک سری ویژگی‌های عمومی نیز هستند. مهم‌ترین این ویژگی‌ها عبارت است از:

۱. بر خلاف شبکه های بی سیم سنتی، همه گره ها در شبکه های بی سیم حسگر نیازی به برقراری ارتباط مستقیم با نزدیک ترین برج کنترل قدرت یا ایستگاه پایه ندارند، بلکه حسگرها به خوشه هایی (سلول‌هایی) تقسیم می‌شوند که هر خوشه (سلول) یک سرگروه خوشه موسوم به Parent انتخاب می‌کند.

این سرگروه‌ها وظیفه جمع‌آوری اطلاعات را بر عهده دارند. جمع‌آوری اطلاعات به منظور کاهش اطلاعات ارسالی از گره‌ها به ایستگاه پایه و در نتیجه بهبود بازده انرژی شبکه انجام می شود. البته چگونگی انتخاب سرگروه خود بحثی تخصصی است که در تئوری شبکه‌های بی‌سیم حسگر مفصلاً مورد بحث قرار می‌گیرد.

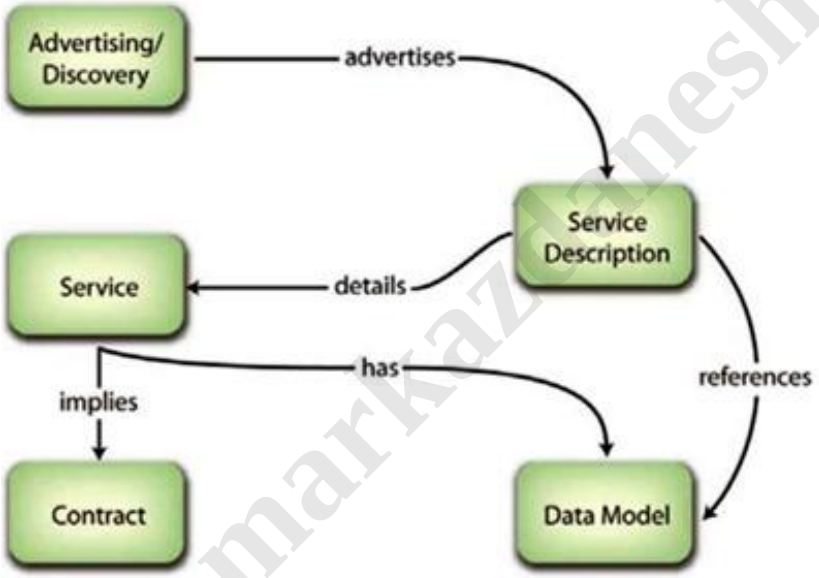
۲. پروتکل‌های شبکه ای همتا به همتا یک سری ارتباطات مش مانند را جهت انتقال اطلاعات بین هزاران دستگاه کوچک با استفاده از روش چندجهشی ایجاد می کنند. معماری انطباق‌پذیر مش، قابلیت تطبیق با گره‌های جدید جهت پوشش دادن یک ناحیه جغرافیایی بزرگ‌تر را دارا است. علاوه بر این، سیستم می‌تواند به طور خودکار از دست دادن یک گره یا حتی چند گره را جبران کند.

۳. هر حسگر موجود در شبکه دارای یک رنج حسگری است که به نقاط موجود در آن رنج احاطه کامل دارد . یکی از اهداف شبکه های حسگری این است که هر محل در فضای مورد نظر بایستی حداقل در رنج حسگری یک گره قرار گیرد تا شبکه قابلیت پوشش همه منطقه موردنظر را داشته باشد.

یک حسگر با شعاع حسگری r را می‌توان با یک دیسک با شعاع r مدل کرد. این دیسک نقاطی را که درون این شعاع قرار می گیرند، تحت پوشش قرار می دهد. بدیهی است که برای تحت پوشش قرار دادن کل منطقه این دیسک‌ها باید کل نقاط منطقه را بپوشانند.

www.markazdanesh.ir

با این که توجه زیادی به پوشش کامل منطقه توسط حسگرها می شود، احتمال دارد نقاطی تحت پوشش هیچ حسگری قرار نگیرد. این نقاط تحت عنوان حفره های پوششی نامیده می‌شوند. اگر تعدادی حسگر به علاوه یک منطقه هدف داشته باشیم، هر نقطه در منطقه باید طوری توسط حداقل n حسگر پوشش داده شود که هیچ حفره پوششی ایجاد نشود این موضوع لازم به ذکر است که مسأله حفره پوششی بسته به نوع کاربرد مطرح می گردد. در برخی کاربرده ا احتیاج است که درجه بالایی از پوشش جهت داشتن دقت بیشتر داشته باشیم.



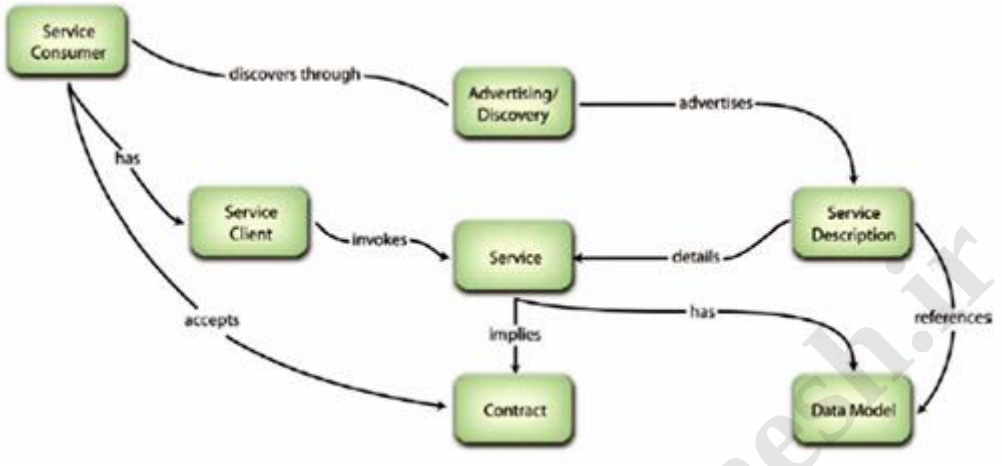
شکل۱.۶- الف) حفره پوششی، ب) استفاده از حسگری اضافی (با ناحیه پوششی پررنگ) جهت حذف حفره پوششی

۱.۵- ساختار ارتباطی شبکه‌های حسگر

گره‌های حسگری همانند شکل ۱.۲ در یک منطقه پراکنده می شوند. همان‌طور که قبلاً هم اشاره کردیم گره‌های حسگری دارای توانایی خودساماندهی هستند . هر کدام از این گره‌های پخش‌شده دارای توانایی جمع‌کردن اطلاعات و ارسال آنها به پایانه‌ای موسوم به sink است. این اطلاعات از یک مسیر چند مرحله‌ای

www.markazdanesh.ir

که زیرساخت مشخصی ندارد به سینک فرستاده می‌شوند و سینک می‌تواند توسط لینک ماهواره یا اینترنت با گره task manager ارتباط برقرار کند.



شکل ۱.۷- ساختار متداول یک شبکه حسگری

طراحی یک شبکه تحت تأثیر فاکتورهای متعددی است . این فاکتورها عبارتند از : تحمل خرابی، قابلیت گسترش، هزینه تولید، محیط کار، توپولوژی شبکه حسگری، محدودیت های سخت‌افزاری، محیط انتقال و مصرف توان که در زیر به شرح آنها می‌پردازیم.

۱.۶- فاکتورهای طراحی

فاکتورهای بیان‌شده در بالا از اهمیت فراوانی در طراحی پروتکل های شبکه‌های حسگر برخوردار هستند؛ در ادامه درباره هر یک از آنها توضیحات مختصری ارائه می‌کنیم.

www.markazdanesh.ir

۱.۶.۱- تحمل خرابی : برخی از گره های حسگری ممکن است از کار بیفتند یا به دلیل پایان توانشان، عمر آنها تمام شود، یا آسیب فیزیکی ببینند و از محیط تأثیر بگیرند. از کار افتادن گره‌های حسگری نباید تأثیری روی کارکرد عمومی شبکه داشته باشد. بنابراین تحمل خرابی را "توانایی برقرار نگه داشتن عملیات شبکه حسگر علی‌رغم از کار افتادن برخی از گره‌ها" تعریف می‌کنیم .در واقع یک شبکه حسگر خوب با از کار افتادن تعدادی از گره های حسگری، به سرعت خود را با شرایط جدید (تعداد حسگرهای کمتر) وفق داده و کار خود را انجام می‌دهد.

۱.۶.۲- قابلیت گسترش : تعداد گره های حسگری که برای مطالعه یک پدیده مورد استفاده قرار می‌گیرند، ممکن است در حدود صدها و یا هزاران گره باشد. مسلماً تعداد گره‌ها به کاربرد و دقت موردنظر بستگی دارد؛ به طوری که در بعضی موارد این تعداد ممکن است به میلیون ها عدد نیز برسد. یک شبکه باید طوری طراحی شود که بتواند چگالی بالای گره‌های حسگری را نیز تحقق بخشد. این چگالی می‌تواند از چند گره تا چند صد گره در یک منطقه که ممکن است کمتر از ۱۰ متر قطر داشته باشد، تغییر کند.

۱.۶.۳- توپولوژی: توپولوژی ذاتی شبکه حس /کار توپولوژی گراف است. بدلیل اینکه ارتباط گره ها بی سیم و بصورت پخش همگانی است و هر گره با چند گره دیگر که در محدوده برد آن قرار دارد ارتباط دارد. آلگوریتم های کارا در جمع آوری داده و کاربردهای ردگیری اشیاء شبکه را درخت پوشا در نظر می گیرند. چون ترافیک اصولا بفرمی است که داده ها از چند گره به سمت یک گره حرکت می کند . مدیریت توپولوژی باید با دقت انجام شودیک مرحله اساسی مدیریت توپولوژی راه اندازی اولیه شبکه است گره هایی که قبلا هیچ ارتباط اولیه ای ندشته اند در هنگام جایگیری و شروع بکار اولیه باید بتوانند با یکدیگر ارتباط برقرار کنند . الگوریتم های مدیریت توپولوژی در راه اندازی اولیه باید امکان عضویت گره های جدید و حذف گره هایی که بدلایلی از کار می افتند را فراهم کنند . پویایی توپولوژی از خصوصیات

www.markazdanesh.ir

شبکه های حس/کار است که امنیت آن را به چالش می کشد. ارائه روشهای مدیریت توپولوژی پویا بطوری که موارد امنیتی را هم پوشش دهد از موضوعاتی است که جای کار زیادی دارد

۱.۶.۴- تنگناهای سخت افزاری: هرگره ضمن اینکه باید کل اجزاء لازم را داشته باشد باید بحد کافی کوچک, سبک و کم حجم نیز باشد بعنوان مثال در برخی کاربردها گره یاید به کوچکی یک قوطی کبریت باشد و حتی گاهی حجم گره محدود به یک سانتیمتر مکعب است و از نظر وزن آنقدر باید سبک باشد که بتواند همراه باد در هوا معلق شود . در عین حال هر گره باید توان مصرفی بسیار کم , قیمت تمام شده پایین داشته و با شرایط محیطی سازگار باشد. اینها همه محدودیتهایی است که کار طراحی و ساخت گره های حس/کار را با چالش مواجه میکند. ارائه طرح های سخت افزاری سبک و کم حجم در مورد هر یک از اجزای گره بخصوص قسمت ارتباط بی سیم و حسگرها از جمله موضوعات تحقی قاتی است که جای کار بسیار دارد. پیشرفت فن آوری ساخت مدارات مجتمع با فشردگی بالا و مصرف پایین , نقش بسزایی در کاهش تنگناهای سخت افزاری خواهد داشت.

۱.۶.۵- قابلیت اطمینان: هر گره ممکن است خراب شود یا در اثر رویدادهای محیطی مثل تصادف یا انفجار بکلی نابود شود یا در اثر تمام شده منبع انرژی از کار بیفتد. منظور از تحمل پذیری یا قابلیت اطمینان این است که خرابی گره ها نباید عملکرد کلی شبکه را تحت تاثیر قرار دهد. در واقع می خواهیم با استفاده از اجزای غیر قابل اطمینان یک شبکه قابل اطمینان بسازیم. برای گره k با نرخ خرابی λ_k قابلیت اطمینان با فرمول(۱) مدل می شود. که در واقع احتمال عدم خرابی است در زمان t بشرط اینکه گره در بازهٔ زمانی (0,t) خرابی نداشته باشد. به این ترتیب هرچه زمان می گذرد احتمال خرابی گره $R_k(t) = e^{-\lambda_k t}$ بیشتر می شود.

۱.۶.۶- مقیاس پذیری :

شبکه باید هم از نظر تعداد گره و هم از نظر میزان پراکندگی گره ها , مقیاس پذیر باشد. بعبارت دیگر شبکه حس/کار از طرفی باید بتواند با تعداد صدها, هزارها و حتی میلیون ها ها, هزارها و حتی میلیون ها

www.markazdanesh.ir

گره کار کند و از طرف دیگر , چگالی توزیع متفاوت گره ها را نیز پشتیبانی کند . چگالی طبق فرمول (۲) محاسبه می شود . که بیانگر تعداد متوسط گره هایی است که در برد یک گره نوعی (مثلادایره ای با قطر۱۰ متر) قرار می گیرد. A: مساحت ناحیه کاری N:تعداد گره در ناحیه کاری و R: برد ارسال رادیویی است. در بسیاری کاربردها توزیع گره ها اتفاقی صورت می گیرد و امکان توزیع با چگالی مشخص و یکنواخت وجود ندارد یا گره ها در اثر عوامل محیطی جابجا می شوند . بنابراین چگالی باید بتواند از چند عدد تا چند صد گره تغییر کند. موضوع مقیاس پذیری به روشها نیز مربوط می شود برخی روشها ممکن است مقیاس پذیر نباشد یعنی در یک چگالی یا تعداد محدود از گره کار کند . در مقابل برخی روشها مقیاس پذیر هستند

$$\mu(R) = (N \cdot \pi R^2) / A$$

۱.۶.۷- هزینه تولید : از آنجایی که شبکه های حسگری از تعداد زیادی گره‌های حسگری تشکیل شده‌اند، هزینه یک گره در برآورد کردن هزینه کل شبکه بسیار مهم است. اگر هزینه یک شبکه حسگری گران‌تر از هزینه استفاده از شبکه‌های مشابه قدیمی باشد، در بسیاری موارد استفاده از آن مقرون به صرفه نیست. در نتیجه قیمت هر گره حسگری تا حد مم‌کن باید پایین نگه داشته شود .

۱.۶.۸- رسانه ارتباطی: در شبکه های حس /کار ارتباط گره ها بصورت بی سیم و از طریق رسانه رادیویی, مادون قرمز, یا رسانه های نوری دیگر صورت می گیرد. اکثرا از ارتباط رادیویی استفاده می شود. البته ارتباط مادون قرمز ارزانتر و ساختنش آسانتر است ولی فقط در خط مستقیم عمل می کند.

۱.۶.۹- توان مصرفی گره ها: گره های شبکه حس/کار باید توان مصرفی کم داشته باشند . گاهی منبع تغذیه یک باتری ۱/۲ ولت با انرژی ۵/. آمپر ساعت است که باید توان لازم برای مدت طولانی مثلا ۹ ماه را تامین کند. در بسیاری از کاربردها باتری قابل تعویض نیست. لذا عمر باطری عملا عمر گره را مشخص می

www.markazdanesh.ir

کند. بعلت اینکه یک گره علاوه بر گرفتن اطلاعات(توسط حسگر) یا اجرای یک فرمان (توسط کارانداز) بعنوان مسیریاب نیز عمل می کند بد عمل کردن گره باعث حذف آن از توپولوژی شده و سازماندهی مجدد شبکه و مسیردهی مجدد بسته عبوری را در پی خواهد داشت . در طراحی سخت افزار گره ها استفاده از طرح ها و قطعاتی که مصرف پایینی دارند و فراهم کردن امکان حالت خواب برای کل گره یا برای هر بخش بطور مجزا مهم است.

۱.۶.۱۰- ارتباط بلادرنگ و هماهنگی : در برخی کاربردها مانند سیستم تشخیص و جلوگیری از گسترش آتش سوزی یا سیستم پیش گیری از سرقت سرعت پاسخگویی شبکه اهمیت زیادی دارد . در نمایش بلادرنگ فشار بر روی مانیتور بسته های ارسالی باید بطور لحظه ای روزآمد باشند. برای تحقق بلادرنگ یک روش این است که برای بسته های ارسالی یک ضرب العجل تعیین شود و در لایه کنترل دسترسی رسانه بسته های با ضرب العجل کوتاهتر زودتر ارسال شوند مدت ضرب العجل به کاربرد بستگی دارد . مسئلهٔ مهم دیگر تحویل گزارش رخدادها به چاهک, یا کارانداز ناحیه, به ترتیب وقوع آنهاست در غیر این صورت ممکن است شبکه واکنش درستی انجام ندهد . نکته دیگر هماهنگی کلی شبکه در ارتباط با گزارشهایی است که در مورد یک رخداد از حسگرهای مختلف به کاراندازهای ناحیه مربوطه داده می شود . بعنوان مثال در یک کاربرد نظامی فرض کنید حسگرهایی جهت تشخیص حضور یگان های پیاده دشمن و کاراندازهایی جهت نابودی آن در نظر گرفته شده چند حسگر حضور دشمن را به کار اندازها اطلاع می دهند شبکه باید در کل منطقه, عملیات را به یکباره شروع کند. در غیر این صورت با واکنش اولین کارانداز, سربازان دشمن متفرق شده و عملیات با شکست مواجه می شود. بهرحال موضوع بلادرنگ و هماهنگی در شبکه های حس/کاربخصوص در مقیاس بزرگ و شرایط نامطمئن از مباحث تحقیقاتی است.

۱.۶.۱۱- امنیت و مداخلات : موضوع امنیت در برخی کاربردها بخصوص در کاربرد های نظامی یک موضوع بحرانی است و بخاطر برخی ویژگی ها شبکه های حس/کار در مقابل مداخلات آسیب پذیر ترند . یک مورد بی سیم بودن ارتباط شبکه است که کار دشمن را برای فعالیت های ضد امنیتی و مداخلات آسانتر می کند. مورد دیگر استفاده از یک فرکانس واحد ارتباطی برای کل شبکه است که شبکه را در

www.markazdanesh.ir

مقابل استراق سمع آسیب پذیر می کند. مورد بعدی ویژگی پویایی توپولوژی است که زمینه را برای پذیرش گره های دشمن فراهم می کند. اینکه پروتکل های مربوط به مسیردهی , کنترل ترافیک و لایه کنترل دسترسی شبکه سعی دارند با هزینه و سربار کمتری کار کنند مشکلات امنیتی بوجود می آورد مثلا برای شبکه های حسگر در مقیاس بزرگ برای کاهش تأخیر بسته هایی که در مسیر طولانی در طول شبکه حرکت می کنند یک راه حل خوب این است که اولویت مسیردهی به بسته های عبوری داده شود . همین روش باعث می شود حمله های سیلی مؤثرتر باشد. یکی از نقاط ضعف شبکه حس/کارکمبود منبع انرژی است و دشمن می تواند با قرار دادن یک گره مزاحم که مرتب پیغام های بیدار باش بصورت پخش همگانی با انرژی زیاد تولید می کند باعث شود بدون دلیل گره های همسایه از حالت خواب خارج شوند. ادامهٔ این روند باعث به هدر رفتن انرژی گره ها شده و عمر آنها را کوتاه می کند. با توجه به محدودیت ها باید دنبال راه حل های ساده و کارا مبتنی بر طبیعت شبکه حس/کار بود. مثلا اینکه گره ها با چگالی بالا می توانند توزیع شوند و هر گره دارای اطلاعات کمی است یا اینکه داده ها در یک مدت کوتاه معتبرند از این ویژگی ها می توان بعنوان یک نقطه قوت در رفع مشکلات امنیتی استفاده کرد. اساسا چالشهای زیادی در مقابل امنیت شبکه حس/کاروجود دارد. و مباحث تحقیقاتی مطرح در این زمینه گسترده و پیچیده است.

۱.۶.۱۲- عوامل پیش بینی نشده: یک شبکه حسگر کارانداز تابع تعداد زیادی از عدم قطعیت هاست . عوامل طبیعی غیر قابل پیش بینی مثل سیل زلزله, مشکلات ناشی از ارتباط بی سیم و اختلالات رادیویی, امکان خرابی هر گره , کالیبره نبودن حسگرها, پویایی ساختار و مسیردهی شبکه , اضافه شدن گره های جدید و حذف گره های قدیمی, جابجایی گره ها بطور کنترل شده یا در اثر عوامل طبیعی و غیره . سؤالی که مطرح است این است که در این شرایط چگونه میتوان چشم اندازی فراهم کرد که از دیدگاه لایه کاربرد شبکه یک موجودیت قابل اطمینان در مقیاس بزرگ دارای کارایی عملیاتی مشخص و قابل اعتماد باشد. باتوجه به اینکه شبکه های حسگر کارانداز تا حدود زیادی بصورت مرکزی غیر قابل کنترل هستند و بصورت خودکار یا حداقل نیمه خودکار عمل میکنند باید بتوانند با مدیریت مستقل بر مشکلات غلبه کنند از این رو باید ویژگی های خود بهینه سازی خود سازماندهی و خود درمانی را داشته باشند. اینها از جمله

مواردی هستند که بحث در مورد آنها آسان ولی تحقق آن بسیار پیچیده است . بهرحال این موضوعات ازجمله موارد تحقیقاتی می باشند.

۱.۷- نمونه ی پیاده سازی شده شبکه حسگر

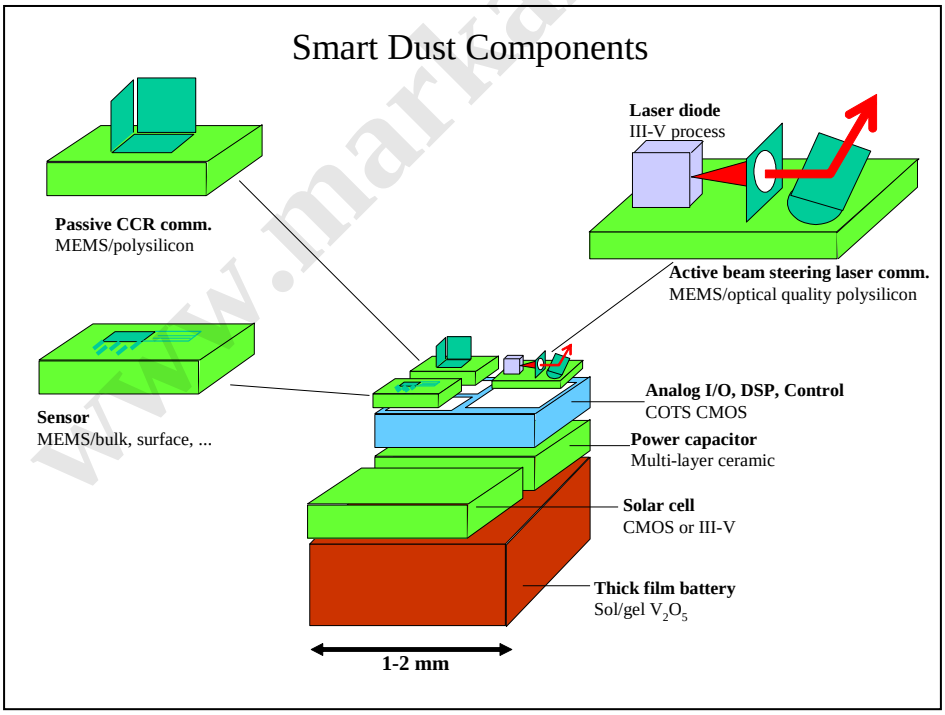
۱.۷.۱- ذره ی میکا

یک نمونه از پیاده سازی سخت افزاری گره های حسگر ذره میکا دانشگاه برکلی امریکا است .این نمونه, یک واحد حس/کار کوچک (چندین اینچ مکعب) با یک واحد پردازنده مرکزی,منبع تغذیه,رادیو و چندین عنصر حسگر اختیاری می باشد. پردازشگر آن یک پردازنده ۸- بیتی از خانواده ی اتملی باشد همراه با ۱۲۸ کیلو بایت حافظه ی برنامه , ۴کیلوبایت RAM برای داده ۵۱۲کیلوبایت حافظه ی فلش .این پردازنده فقط یک کمینه از مجموعه دستورالعمل های ریسک (RISK)را بدون عمل ضرب , شیفت با طول متغیر و چرخش پشتیبانی می کند.رادیوی آن یک رادیوی مصرف پایین ۹۱۶ مگاهرتز با پهنای باند ۴۰ کیلو در ثانیه روی یک کانال تسهیم شده منفرد با محدوده ی نزدیک به ۱۲ متر می باشد. رادیو در حالت دریافت ۴.۸ میلی آمپر, در حالت ارسال تا ۱۲میلی آمپر ودر حالت خواب ۵ میکرو آمپر مصرف می کند .

شکل۱.۸- ذره میکا

www.markazdanesh.ir

ذره میکا در اندازه های مخ تلف وجود دارد ,کوچکترین آن اغلب به عنوان غبار هوشمند شناخته می شود .طرح پژوهشی غبار هوشمند که به وسیله ی پروفسور پیتستروکان رهبری و هدایت می شود موفق به دستیابی حدی برای اندازه ومصرف توان در گره های حسگر خود مختار شده است .کاهش اندازه برای ساختن گره های ارزان و البته تسهیل گسترش آن بسیار مهم است .گروه تحقیقاتی امیدوارند که ضمن حفظ موثر توانایی های حسگری وارتباطی می توانند موارد لازم حسگری , مخابره اطلاعات و محاسبات سخت افزاری همراه با منبع تغذیه را در اندازه ای در حدود چند میلیمتر مکعب فراهم کنند . این گره میلیمتر مکعبی غبار هوشمند نام دارد که حقیقتاً قلمرو چیزهای ممکن شدنی است .چنان که نمونه های آتی آن می تواند به قدری کوچک باشد که معلق در هوا باقی مانده و به وسیله جریان هوا شناور شود و برای ساعت ها یا روزها موارد حس شده را ارسال کند . غبار هوشمند می تواند اطلاعات را با استفاده از یک تکنولوژی بازتابنده ی نوری جدید , به صورت غیر فعال ارسال کند این یک راه معقول وارزان برای پراب یک سنسور یا تایید دریافت اطلاعات را فراهم می کند ارسال نوری فعال نیز ممکن است اما اتلاف انرژی بیشتری دارد.



شکل۱.۹ ساختار داخلی غبار هوشمند

www.markazdanesh.ir

۱.۸- سیستم عامل

سیستم عامل های که برای شبکه های بی سیم حسگر طراحی شده اند به طور معمول دارای پیچیدگی کمتری نسبت به سیستم عامل های که برای اهداف معمول توسعه یافتند، هستند . که این پیچیدگی کم بخاطر دو مورد زیر است:

۱. نیازمندیهای خاص برنامه های شبکه های بی سیم حسگر
۲. محدودیت های منابع در پلات فرم های سخت افزاری شبکه های حسگر

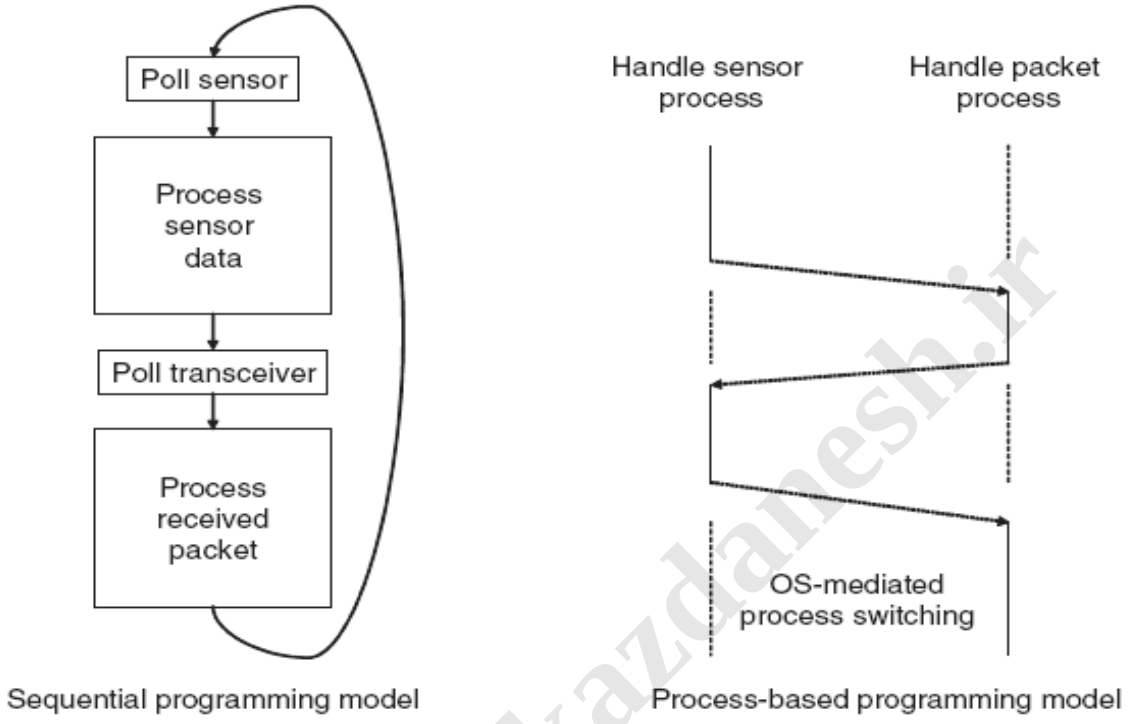
برای مثال، طرز تعامل برنامه های شبکه های حسگر با برنامه ها در یک PC متفاوت است. بخاطر اینکه در این نوع سیستم عامل ها، نیازی به پیشتبانی از واسط کاربری نیست . علاوه بر اینها، محدودیت های منابع مانند حافظه و پشتبانی سخت افزاری از نگاشت از حافظه، مکانیزم های مانند حافظه مجازی را غیر ضروری یا پیاده سازی آنرا غیر ممکن می سازد.

سخت افزار شبکه های حسگر، تفاوتی با سخت افزار سیستم های جاسازی شده ندارد و بنابراین استفاده از سیستم عامل های مانند eCos یا uC/OS که برای سیستم های جازسازی شده طراحی شده اند، برای شبکه های حسگر میسر است. اما باید توجه شود که، سیستم عامل های مخصوص سیستم های جاسازی شدهریال درای ویژگی real-time هستند، در حالیکه سیستم عامل های که به طور خاص برای شبکه های حسگر طراحی شده اند، ویژگی real-time را پشتبانی نمی کنند.

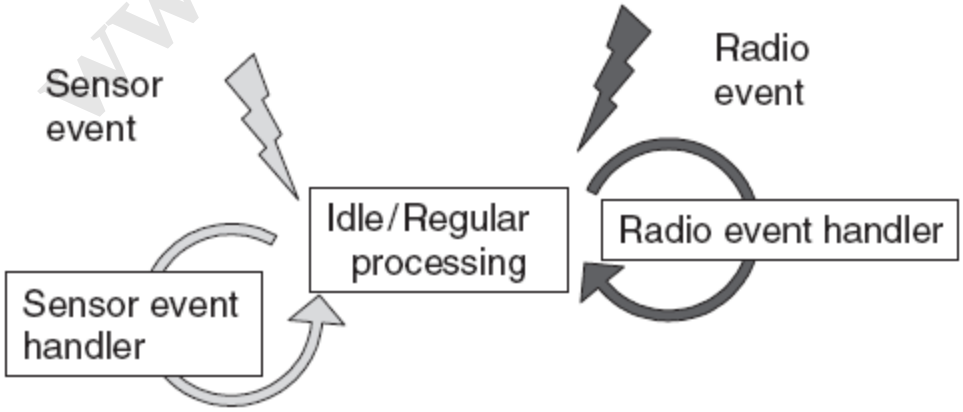
TinyOs اولین سیستم عاملی است که برای شبکه های بی سیم حسگر طراحی شده است. برخلاف بسیاری از سیستم عامل ها، TinyOs به جای مدل چند نخی، بر مبنای مدل برنامه نویسی رویدادگرا طراحی شده است. برنامه های TinyOs، از event handler ها و task ها تشکیل شده است . هنگامیکه یک رویداد خارجی، مانند ورود یک بسته داده یا خواندن داده توسط حسگر رخ می دهد، TinyOs، مدیر رویداد مناسب را برای آن مدیریت آن رویداد فراخوانی می کند. برای نوشتن سیستم عامل TinyOs و برنامه های که در آن

www.markazdanesh.ir

نوشته می شوند، از یک زبان برنامه نویسی خاص به نام nesC استفاده می شود که یک توسعه از زبان برنامه نویسی C است.



شکل ۱.۱۰- دو مدل برنامه نویسی با نقاط ضعف برای شبکه حسگر



شکل ۱.۱۱- مدل برنامه نویسی رویدادگرا

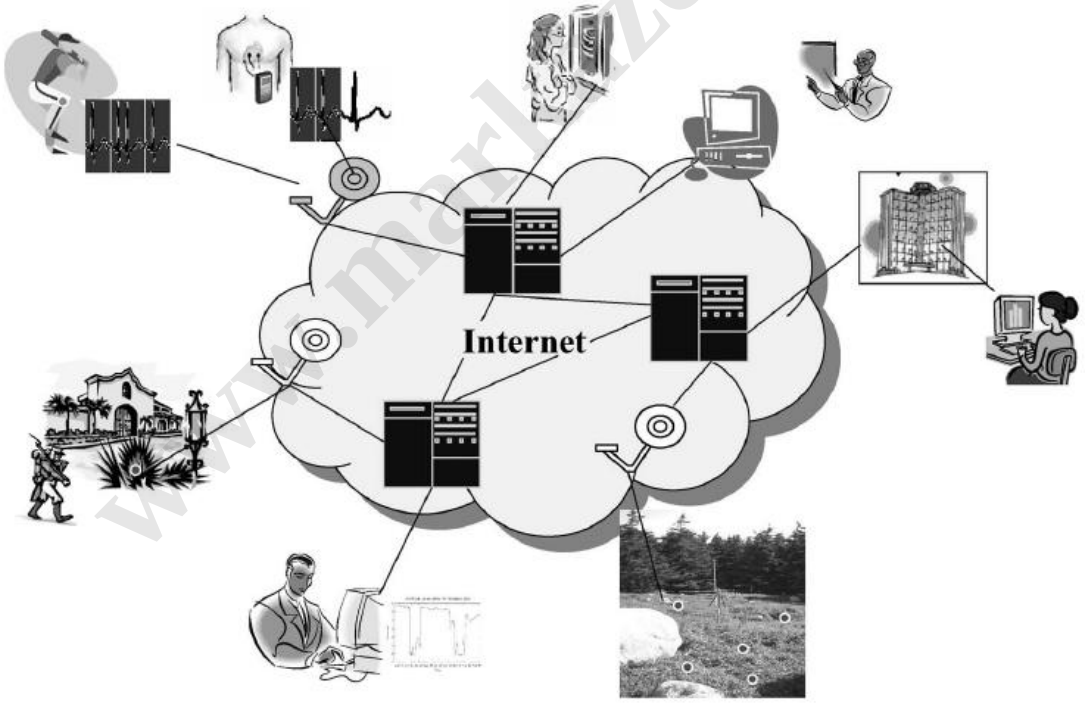
www.markazdanesh.ir

فصل دوم

روشهای جمع اوری اطلاعات در شبکه حسگر بیسیم

۲.۱- مقدمه

شبکه های بی سیم ترکیبی از سنسورهای ثابت و متحرک هستند و سنسورها بسته به ماهیت برنامه ها ی کاربردی استقرار پیدا می کنند. به عنوان مثال در برنامه های ناظر در مدل ad – hoc برای پوشش نواحی خاصی که باید نظارت کنند مستقر می شوند . شبکه ی بی سیم فرصت های جدیدی را در میان طیف وسیعی از تلاشهای آدمی خلق کرده است ، از قبیل : مهندسی ساخت و طراحی سیستم های کنترل و نظارت در محیط ، سیستم های پیگیری حریق در جنگل، مراقبت های پزشکی ، نظارت و نقشه برداری در میدان جنگ، مدیریت حوادث و حفاظت از زیر ساخت های حیاتی، برنامه های مرتبط با جمع آوری اطلاعات و انتشار آنها در شکل ۲.۱ نشان داده شده است.



شکل ۲.۱- برنامه های کاربردی شبکه های بی سیم حسگر

www.markazdanesh.ir

سنسورها اصولاً به منظور دریافت اطلاعات از محیط و در صورت امکان پردازش داده ها قبل از ارسالشان از طریق ایستگاه پایه به سمت چاهک اطلاعاتی و سرانجام برنامه کاربردی، طراحی شده اند . پردازش و ارسال اطلاعات توسط رخداد وقایع خاص، در محیطی که سنسورها در پاسخ به تقاضای برنامه کاربر پیکربندی شده اند انجام می گیرد. در بسیاری از موارد، تجمیع اطلاعات گردآوری شده توسط حس گرهای گوناگون، قبل از ارسالشان به ایستگاه پایه مفید است . تجمیع اطلاعات، تعداد پیغام هایی را که باید منتقل شوند را کاهش می دهد و باعث کاهش انرژی مصرفی در ارتباطات می شود.

۲.۲- انتشار و جمع آوری داده ها

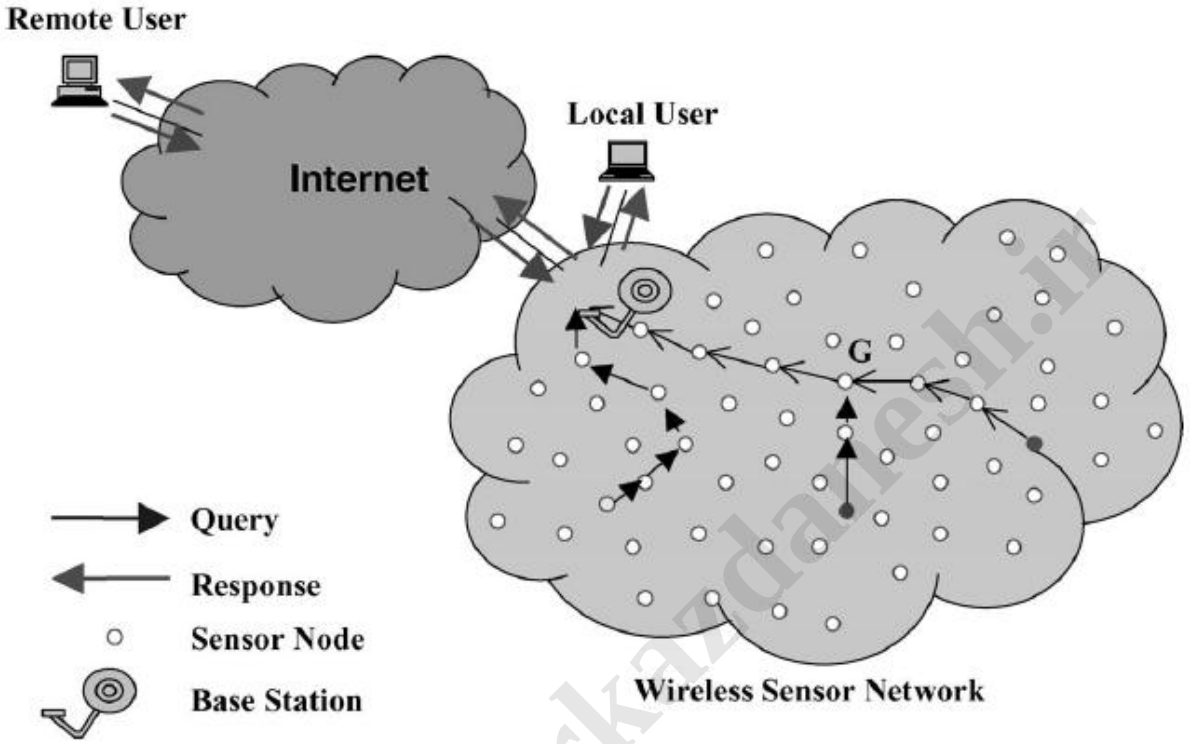
اینکه چگونه داده ها و پرس و جوهای ما بین ایستگاه پایه و چاهک اطلاعاتی یا مکان رخ داد حادثه ای طبیعی، رد و بدل می شود، یکی از ویژگی های مهم شبکه های بی سیم است . یک روند ساده برای انجام این امر، تبادل مستقیم داده ها مابین مرکز و ایستگاه پایه است. روند تک گام گرا، پرهزینه بوده و هرچه گره ها از ایستگاه پایه دورتر باشند، ممکن است که انرژی خود را سریعتر مصرف کنند و بدین ترتیب طول عمر شبکه کاهش یابد. مورد فوق چه در مورد حس گرهای ثابت که ناحیه جغرافیایی بزرگی را پوشش می دهند و چه در مورد گره های متحرک که ممکن است در حین حرکت از ایستگاه پایه دور شوند، مشترک است . برای رفع نواقص بالا، داده ها مابین حس گرها و ایستگاه پایه به صورت انتقال چند گام گرا بر روی یک شعاع محدود ارتباطی ردوبدل می شود.

برای رفع نواقص روند بالا، داده ها بین حس گرها و ایستگاه پایه معمولاً با استفاده از انتقال بسته ها در چندگام بر روی یک شعاع محدود ارتباطاتی. این قبیل روش ها باعث می شود که انرژی زیادی ذخیره شود و کاهش قابل ملاحظه تداخل ارتباطاتی میان سنسورهای رقیب که سعی می کنند به کانال دسترسی پیدا کنند، بخصوص در شبکه هایی که دارای تراکم زیاد هستند.

ارسال اطلاعات میان سنسورهایی که اطلاعات را جمع آوری می کنند و چاهک اطلاعاتی که اطلاعات در آن آماده می شود در شکل ۲.۲ نشان داده شده است.در پاسخ به پرس و جوهای مربوط به چاهک اطلاعاتی یا

www.markazdanesh.ir

هنگام رخ دادن وقایع خاص در داخل ناحیه نظارتی، اطلاعات جمع آوری شده بوسی‌له سنسورها به ایستگاه پایه انتقال داده می شوند با استفاده از مسیرهای چندگامی با توجه به ماهیت برنامه کاربردی، سنسورها می توانند اطلاعات را بر سر راهشان به ایستگاه پایه تجمع کنند .



۲.۲شکل - داده های چندگامه و هدایت پرس و جو

در یک شبکه بی سیم حس گرا، گره های میانی باید در ارسال بسته های داده میان منبع و مقصد شرکت کنند. تعین اینکه کدام گره های میانی بایستی در ارسال داده ها میان منبع و مقصد شرکت کنند وظیفه اصلی الگوریتم های مسیریابی است. در اصل، مسیریابی در شبکه های بزرگ اساساً یک مشکل است، که راه حل بایستی تعادلی را میان نیازمندی های طراحی از قبیل صحت، پایایی، بهینگی با توجه به معیارهای مختلف کارایی برقرار کند. خصوصیات اصلی WSN ، با محدودیت های شدید مربوط به پهنای باند و انرژی ترکیب شده است، تا تعادلی میان نیازهای ترافیکی شبکه را با گسترش طول حیات شبکه برقرار کند.

www.markazdanesh.ir

۲.۳- رقابت بر سر مسیریابی و نتایج طراحی در شبکه های بی سیم حس گر

اگرچه WSN مشترکات زیادی با شبکه های ad – hoc و سیمی دارد ، آنها همچنین تعدادی از ویژگیهای منحصر بفرد را که قسمتی از شبکه های موجودند را نیز ارائه می ده ند، این ویژگیهای جدید و منحصر بفرد موجب تمرکز بر روی مسائل جدید مربوط به مسیریابی شد که فراتر از مسائلی بود که ما در شبکه ای سیمی و ad – hoc با آنها برخورد داشتیم. رقابت مذکور دارای چندین فاکتور است از قبیل: محدودیت های شدید انرژی، توانایی های محدود محاسبا تی و ارتباطاتی، محیط به شدت متغیری که سنسور ما در آن توزیع شده اند، مدل های ترافیک دار، منحصر بفرد و ارزش محدود سرویس به نیازمندیهای برنامه های کاربردی.

۲.۳.۱- ویژگیهای متغیر از لحاظ زمانی و اندازه در شبکه

به علت اینکه تعداد زیادی از برنامه های بستن بر سنسور وجود دارد، تراکم در شبکه های بی سیم حس گر می تواند به طور وسیعی متغیر باشد، در محدود از خیلی کم تا خیلی زیاد . بعلاوه در تعداد زیادی از برنامه های کاربردی سنسورها، تعدادشان به صدها می رسد . که مستقر می شوند در یک ad – hoc و ناحیه ای بدون روش های نظارتی. در این شبکه ها رفتار سنسور متغیر و بسیار تطابق پذیر است آنچنانکه نیاز به خود سازماندهی و نگهداشت انرژی، گره های شبکه را وادار می کند که به طور ثابت سطح برخوردشان را در برابر مسائل تنظیم کنند.

به علاوه، سنسورها ممکن است که رفتارشان را در پاسخ به رویدادهای غیر قابل پیش بینی در شبکه ی بی سیم طوری تنظیم کنند که منجر به تداخل در باندهای فرکانس رادیویی نشود . و افت کارآیی را در پی نداشته باشد.

www.markazdanesh.ir

۲.۳.۲- مدلهای داده ای برنامه های مبتنی بر سنسور

مدل داده تشریح می کند جریانی از اطلاعات بین گره های سنسور و چاهکهای اطلاعات را با این مدلها، به شدت به ماهیت برنامه ی کاربردی در زمینه ی چگونگی برخورد با اطلاعات ؛ مرتبط است.

مدلهای داده ای گوناگونی، پیشنهاد شده است تا نیازهای جمع آوری داده و نیازمندی های تعاملاتی برنامه های گوناگون را برطرف کند. یک رده از برنامه های کاربردی سنسور نیاز به مدلهای جمع آوری داده دارند که؛ برمبنای نمونه برداری دوره ای می باشد یا توسط رویدادهای خاصی رخ می دهند.

نیاز به پشتیبانی مدل های داده ای گوناگون پیچیدگی مسئله طراحی مسیریابی را افزایش می دهد.

به‌ینه سازی پروتکل مسیریابی همراه با تنوع مدل های داده ای و ارائه محصول با بالاترین کارایی و کیفیت به صورت صحیح قابل اعتماد و مسأله مهندسی و طراحی را بسیار پراهمیت کرده است.

۲.۴- استراتژیهای مسیریابی در شبکه های بی سیم

مسئله مسیریابی در شبکه های بی سیم حس گر تبدیل به یک چالش پایاپای میان کارائی و قابلیت پاسخگویی شده است . این معامله پایاپای بایستی تعادل برقرار کند بین نیاز به توانایی های پردازش و ارتباطی محدود در مقابل سربار حاصل از تطابق آنها . در یک WSN سربار اندازه گیری می شود از طریق مقدار استفاده پهنای باشد قدرت مصرفی و نیازهای پردازش بر روی گره های متحرک پیدا کردن یک استراتژی میان نیازهای جدالی فوق بصورت مؤثر پایه مسیریابی رقابتی را تشکیل می دهند . بعلاوه ویژگیهای اصلی شبکه های بی سیم این سؤال را مطرح می کند که آیا پروتکل های مسیریابی موجود برای شبکه های ad – hoc طراحی شده اند موارد فوق را در بر می گیرند.

الگوریتم های مسیریابی در شبکه های ad – hoc دسته بندی می شوند با توجه به روشی که از طریق آن اطلاعات دریافت می شوند و روشی که در آن از این اطلاعات برای محاسبه مسیرها استفاده می شود

www.markazdanesh.ir

سه استراتژی متفاوت می توان در نظر گرفت، proactive ، reactive ، hybrid استراتژی روش proactive متکی بر انتشار متناوب اطلاعات مربوط به مسیریابی به صورتیکه اطلاعات مربوط به جداول مسیریابی به صورت سازگار و درست نگهداری شوند . ساختار شبکه می تواند مسطح یا سلسله مراتبی باشد . این استراتژیهای مسیریابی proactive مسطح پتانسیل محاسبه مسیرهای بهینه را دارا می باشند . سربار مورد نیاز برای محاسبه این مسیرها ممکن است مانعی باشد برسر راه الگوریتم در یک محیط به شدت متغیر . مسیریاب سلسله مراتبی برای شبکه های بزرگ و ad – hoc مناسب تر است . استراتژیهای مسیریابی reactive مسیرهایی را به یک مجموعه محدودی از مقصدها ایجاد می کند . این استراتژی ها اطلاعات عمومی را در ارتباط با کل گره های شبکه نگهداری نمی کنند . آنها بایستی همچنین متکی باشند به یک جست و جوی مسیر پر یا برای برقراری ارتباط میان مبداء و مقصد . این معمولاً شامل یک پرس و جوی اکتشاف مسیر به صورت سیل آسا با گرفتن جواب لز طریق مسیر برگشت. استراتژی مسیریابی reactive در روشی که فرآیند پردازش سیل را برای کاهش سربار اطلاعاتی کنترل می کند و روشی که از طریق آن مسیرها محاسبه و در صورت خطا دوباره محاسبه می شوند متفا وت است. استراتژیهای hybrid متکی بر ساختار شبکه های امروزی برای دستیابی به پایایی و قابلیت گسترش در شبکه های بزرگ می باشد. در این استراتژیها شبکه به خوشه های دو به دو مجاور سازماندهی می شوند . ساختار خوشه ای می تواند استفاده شود برای محدود کردن دامنه مسیریابی الگوریتم reaction برای تغییر در محیط شبکه، استراتژی مسیریابی ترکیبی می تواند به صورتی استفاده شود که دو گره مجاور یکی از الگوریتم مسیریابی proactive استفاده کند و یکی هم از الگوریتم مسیریابی reactive . چالش اصلی بر سر کاهش سربار مورد نیاز در نگهداری خوشه ها. خلاصه الگوریتم های مسیریابی در شبکه های ad – hoc تمایل به شرکت در محیط های بسیار پویا ندارند. سربار پروتکل مسیریابی معمولاً با افزایش اندازه شبکه مقدار پویایی بودنش افزایش می یابد

یک سربار زیاد معمولاً می تواند کل منابع شبکه را مختل کند . بعلاوه پروتکل مسیریابی قدیمی بر روی شبکه های بزرگ نیازمند هماهنگ سازی بین شبکه ای به صورت اساسی و در برخی موارد الگوریتم سیل آسا برای حفظ پایایی، صحت اطلاعات که برای دستیابی به مسیریابی صحیح و بهینه لازم است می باشد .

www.markazdanesh.ir

استفاده از این پروتکل ها سربار پروتکل مسیریابی و زمان همگرایی را افزایش می دهد . در نتیجه اگر آنها خیلی خوب برای کار در محیط منطبق می شوند . اما کارایی این تکینک ها یا نیازهای مسیریابی در شبکه های بی سیم در تضاد است. استراتژیهای جدید مسیریابی مورد نیاز در شبکه های بی سیم قادر به مدیریت کارا برای ایجاد تعادل بین بهینگی و کارایی می باشند.

۲.۵- تکنیک های مسیریابی WSN

طراحی پروتکل های مسیریابی برای WSN باید با در نظر گرفتن محدودیت های منابع و انرژی در گره های شبکه و احتمال کم شدن بسته ها و امکان تأخیر آنها انجام شود.

برای برطرف کردن این نیازمندیها، چندین استراتژی مسیریابی برای شبکه های بی سیم حس گر پیشنهاد شده است. یک رده از پروتکل های مسیریابی دارای ساختاری مسطح هستند که در آن همه گره ها همسان در نظر گرفته می شوند . یک شبکه با ساختار مسطح دارای مزایای زیادی می باشد، هم انند سربار کم ، پتانسیل بالقوه برای ردیابی مسیرهای چندگانه میان گره های ارتباطاتی در هنگام وقوع خطا برای بالا بردن قابلیت تحمل پذیری در برابر خطا.

دومین رده از پروتکل های مسیریابی ساختاری را بر مبنای دستیابی به کارایی بالا، پایایی و قابلیت گسترش ایجاد می کنند در این رده گره های شبکه به صورت خوشه هایی سازماندهی می شوند که در آنها یک گره با انرژی باقیمانده بالاتر به عنوان سر خوشه در نظر گرفته می شود . سر خوشه مسئول هماهنگی فعالیت های داخل خوشه و ارسال اطلاعات میان خوشه ها می باشد. خوشه سازی به صورت بالقوه انرژی مصرفی را کاهش می دهد و طول عمر شبکه را افزایش.

سومین رده از پروتکل های مسیریابی از روش داده گرا برای پخش داده استفاده می کند . این روش از نامگذاری مبتنی بر صفت استفاده می کند که به موجب آن گره های شبکه به جای جست و جو در میان گره های سنسور مجاز او افرادی در میان صفات جست و جو می کنند.

این نوع انتشار انتساب وظایف به سنسورها و تشریح پرس و جو ها بر مبنای صفات می باشد. استراتژی های متفاوت می توانند در ارتباطات استفاده شوند از قبیل پخش همگانی، پخش گروهی بر مبنای صفات، پخش جهانی و هر نوع پخش دیگر.

رده چهارم پروتکل های مسیریابی از مختصات برای آدرس دهی سنسورها استفاده می کنند . مسیریابی مبتنی بر مختصات در برنامه های کاربردی، جائیکه موقعیت گره داخل ناحیه جغرافیایی شبکه مرتبط با پرس و جوی انتشاری بوسیله گره مبداء می باشد مفید است. این قبیل پرس و جوها ممکن است در نواحی خاصی از شبکه در مجاورت نقطه خاصی در محیط شبکه معمولاً کاربرد دارد

۲.۶- انتشار مستقیم

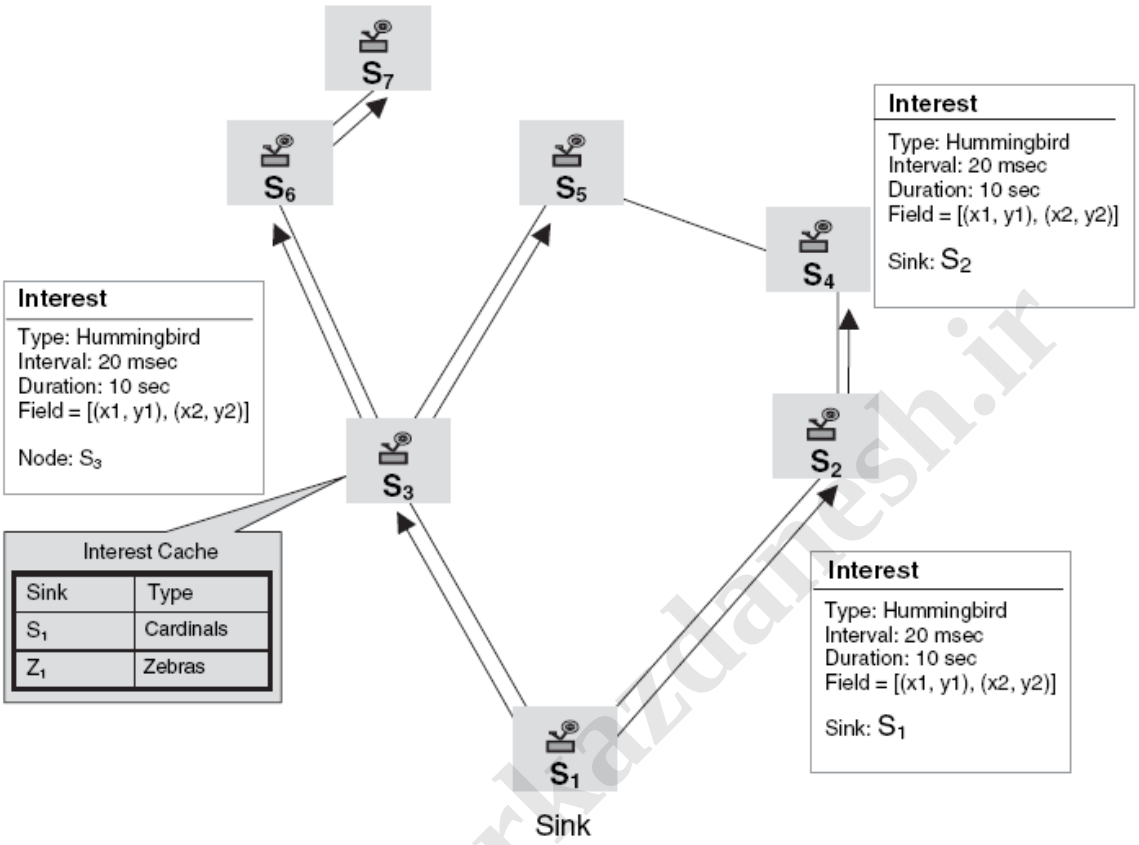
انتشار مستقیم یک پروتکل مسیریابی مبتنی بر داده در WSN می باشد. هدف اصلی این پروتکل ذخیره انرژی به موجب بالا بردن طول عمر شبکه می باشد. برای دستیابی به این هدف انتشار مستقیم از ارتباطات بین گره ها را به صورت محلی بین گره های همسایه در می آورد

با استفاده از این روش، انتشار مستقیم می تواند زیر مجموعه ای از مسی رهای بهینه را کشف کند . این ویژگی منحصر بفرد همراه با توانایی تجمع اطلاعات منجر به کاهش زیاد انرژی مصرفی می شود

عناصر اصلی این پروتکل interest ، بخش داده ، gradient ها و عنصر تقویت یک interest می تواند به عنوان یک پرس و جو در نظر گرفته شود شکل ۲.۱۴ مثالی را از یک interest از نوع hummingbirds با استفاده از یک مجموع از جفت های مقدار ـ صفت نشان می دهد. چاهک اطلاعاتی یک پیغام interest را به هر همسایه ارسال می کند. این پیغام سبکه حسگر پخش می شود . به عنوان یک interest برای داده های نامگذاری شده. همه ی گره های حس‌گر یک Interest cache دارند. هر مدخل این cache مربوط به یک interest متفاوت است و شامل چندین فیلد است. از جمله فیلد مهر زمان ، چندین فیلد gradient برای هر همسایه و یک فیلد طول . فیلد مهر زمان شامل مهر زمان آخرین interest دریافت شده است . هر فیلد gradient هم شامل جهت و نرخ داده ارسالی است.

www.markazdanesh.ir

مقدار نرخ داده از طریق صفت intervac بدست می آید. فیلد طول عمر تقریبی interest را نشان می دهد و از طریق فیلد مهر زمان بدست می آید. شکل ۲.۳ مثالی از روش فوق است.



شکل ۲.۳- پخش interest

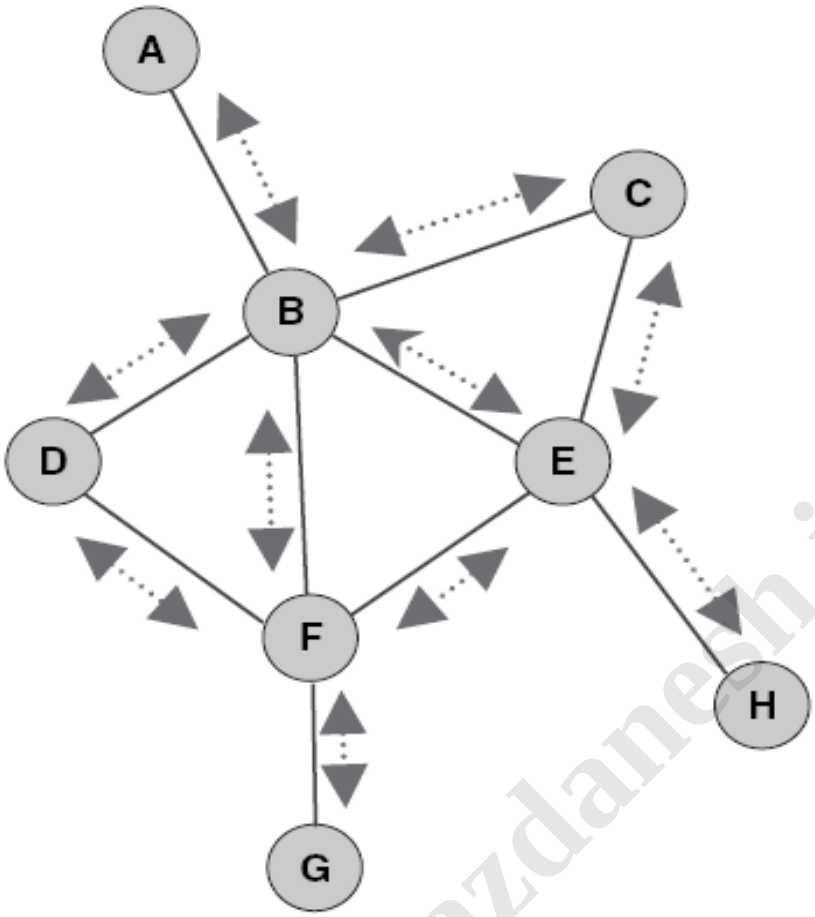
۲.۷- سیل آسا و انواع آن

تکنیک سیل آسا یک گزینه رایج و مورد استفاده برای اکتشاف مسیر و انتشار اطلاعات در شبکه های سیمی و بی سیم ad – hoc می باشد. استراتژی مسیریابی ساده است در ضمن متکی به هزینه و پیچیدگی الگوریتم های اکتشاف مسیر نیست. این تکنیک از روش reactive استفاده می کند که به موجب آن هر گره همزمان با دریافت یک بسته داده یا کنترلی، آن بسته را به همه همسایه هایش ارسال می دارد

www.markazdanesh.ir

بعد از انتقال یک بسته همه مسیرهای ممکن را طی می کند برخلاف شبکه ای که از نظر ارتباطی قطع است. بسته سرانجام به مقصدش می رسد . بعلاوه همچنانکه توپولوژی شبکه تغییری کند بسته اطلاعاتی مسیر های جدید را کشف می کند . شکل ۲.۴ مفهوم تکنیک سیل آسا را در شبکه های اطلاعاتی ـ ارتباطاتی نشان می دهد. آنچنانکه شکل نشان می دهد تکنیک سیل آسا در ساده ترین حالت ممکن است منجر به تکرار و تکثیر نا محدود بسته ها در شبکه بشوند برای جلوگیری از گردش نامحدود یک بسته در شبکه یک فیلد به نام شمارنده گام معمولاً در سرآیند بسته قرار داده می شود . این فیلد با اندازه قطر شبکه پر می شود. در حالیکه بسته در طول شبکه در حرکت است این فیلد در عبور از هر گره یک واحد کاهش می یابد.هنگامیکه به صفر برسد بسته دور انداخته می شود . ممکن است کار دیگر نیز برای اصلاح مشکل فوق الذکر انجام شود. آن هم توسط فیلدی به نام طول عمر که زمان طول عمر مجاز برای یک بسته را در داخل یک شبکه نگاه می دارد . با انقضاء زمان مورد نظر بسته به جلوتر هدایت نمی شود . این استراتژی حداقل نیازمند یک تاریخچه در ارتباط با بار ترافیک جاری می باشد . با وجود سادگی قاعده فوق نسبت به هزینه کم قابلیت نگهداری تکنیک سیل آسا حاوی چندین عیب هنگام استفاده در شبکه های بی سیم می باشد.

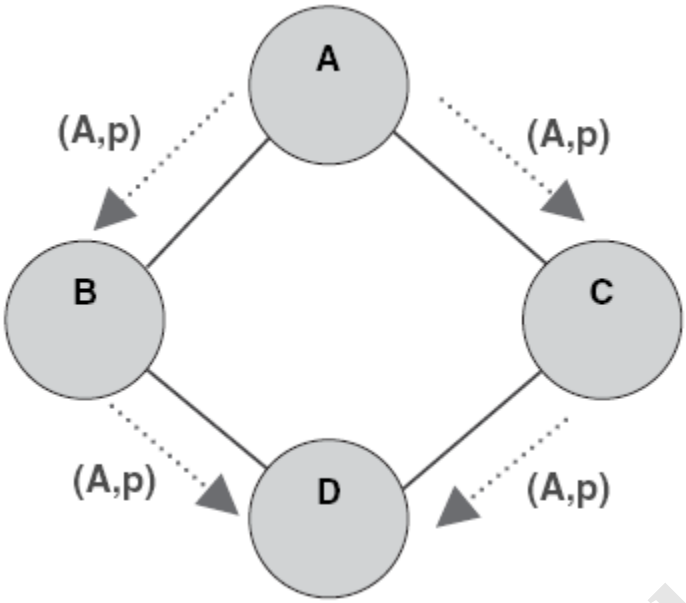
www.markazdanesh.ir



شکل ۲.۴- Flooding در شبکه های ارتباطی داده

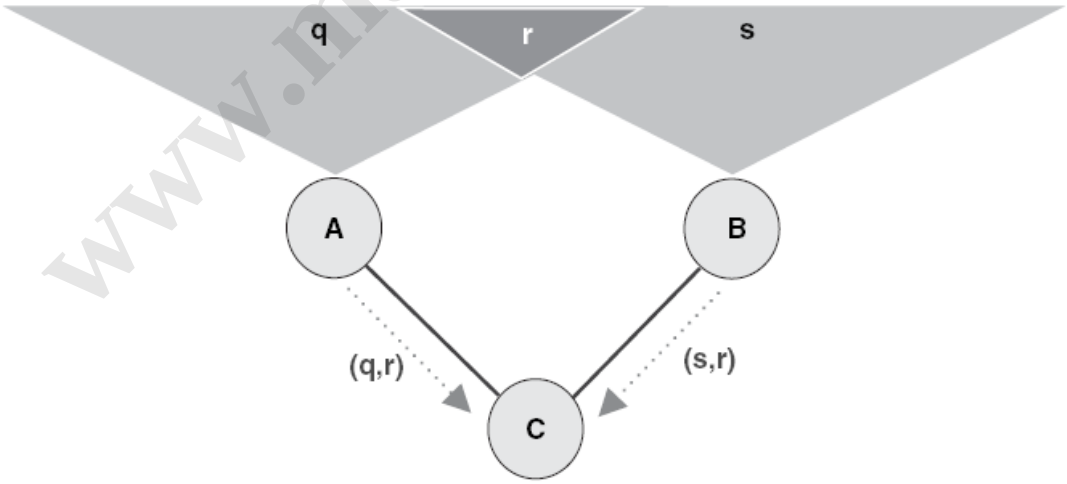
اولین مانع بر سر راه این تکنیک ایجاد ترافیک بالایی است می کند. آنچنانکه در شکل ۲.۵ نشان می دهد. این اثر نامطلوب بر اثر تکرار و تکثیر بسته های داده و کنترلی که به صورت تکراری به یک گره ارسال می شود ایجاد می شود.

www.markazdanesh.ir



شکل ۲.۵- مسئله Implosion ترافیک در پروتکل های سیل آسا

دومین مانع بر سر راهش مسئله همپوشانی است که در شکل ۲.۶ نشان داده شده است. مسئله همپوشانی هنگامی رخ می دهد که دو گره ناحیه یکسانی را هنگام ارسال بسته ها آن هم حاوی اطلاعات یکسان به یک گره پوشش می دهند.



شکل ۲.۶- مسئله رویهم افتادگی ترافیک در پروتکل سیل آسا

www.markazdanesh.ir

سومین مانع lesource blindess می باشد. ساده ترین تکنیک که سیل آسا باشد محدودیت های مربوط به انرژی را اصلاً رعایت نمی کند در نتیجه انرژی موجود ممکن است سریعاً تخلیه شده و طول عمر شبکه به طور ملاحظه ای کاهش یابد.

برای برطرف کردن این نواقص در الگوریتم سیل آسا، یک روش م شتق شده از آن به نام gossiping معرض شد. همانند الگوریتم سیل آسا، gossiping از یک قانون ساده انتقال استفاده می کند . و همچنین نیازی به الگوریتم پیچیده اکتشاف ندارد . برخلاف الگوریتم سیل آسا، که یک بسته داده به همه همسایه ها پخش عمومی می شود در gossiping یک بسته تنها به یک گره که تصادفاً انتخاب می شوند ارسال می شود

هنگامیکه بسته دریافت شد، همسایه به طور تصادفی یکی از همسایه های خودش را انتخاب می کند و بسته را به همسایه انتخاب شده ارسال می کند. این فرآیند ادامه می یابد تا زمانیکه بسته به مقصد برسد یا منقضی شود. در این روش تعداد بسته هایی که هرگره می فرستد، محدود است . بسته ممکن است با تأخیر زیاد به مقصد برسد که به دلیل ماهیت تصادفی روش فوق می باشد

۲.۸-روش شایعه پراکنی

هر گاه داده در روش همه پخشی کلاس یک، به یک گره با مرتبه بالا برسد ، کپی ه ای بیشتری از داده شروع به پراکنده شدن در داخل شبکه می کنند تا وقتی که این کپی ها در اثر تصادم به انتها برسند در صورتی که روش شا یعه پراکنی جلوی چنین تصادم هایی را می گیرد چون در این روش تنها یک کپی از داده در هر گره ا یجاد می شود و هر چه تعداد کپی های ایجاد شده کمتر باشد احتمال تصادم این کپی ها کمتر می شود.

در حالی که روش شایعه پراکنی اطلاعات را به کند ی در شبکه پراکنده می کند، سرعت مصرف انرژی آهسته ای هم دارد.

LEACH -۲.۹

LEACH از خوشه بندی برای انتشار موثر و کارایی پرس و جو ها و جمع آوری داده های خوانده شده توسط تمام گره های شبکه استفاده می کند. LEACH فرض می کند که هر گره می تواند بطور مستقیم

www.markazdanesh.ir

با ایستگاه پایه ارتباط برقرا کند . اگر چه، ارتباط مستقیم با ایستگاه (انتقال تک گام) عملی است که به شدت توان هر گره را مصرف می کند و به عنوان یک کار کم بازده در شبکه های حسگر در نظر گرفته می شود. LEACH گره ها را در خوشه های سازماندهی می کند و یک گره را به عنوان سر خوشه در نظر می گیرد.

گره ها در ابتدا داده های را که از محیط دریافت کرده اند را به سر خوشه شان ارسال می کنند، و سر خوشه تمام داده های فرزندانش را برای ارسال به ایستگاه پایه تجمع یا فشرده می کند . اگر سر خوشه به صورت ایستا انتخاب شود، روشن و آشکار است که انرژس آن گره به سرعت تخلیه می شود و آن گره از بین خواهد رفت. LEACH بطور دوره ای یک گره را به عنوان، سر خوشه انتخاب می کند تا مصرف انرژی به صورت یکنواخت در شبکه انجام شود.

حملات: از آنجائیکه انتخاب یک سر خوشه از طریق دریافت یک سیگنال قوی صورت می گیرد، یک نفوذگر از رده-alptop می تواند کل شبکه را به وسیله استفاده از حملات HELLO flood که یک پیام را به کل گره های موجود در شبکه ارسال می کند، غیر فعال کند. بعد از دریافت این پیام، هر گره در شبکه ناگریز نفوذگر رابه عنوان سر خوشه خود انتخاب خواهد کرد . بعد از این عمل نفوذگر می تواند از حمله ارسال انتخابی استفاده کند، و فقط داده های خاص را ارسال کند، و با اینکار باعث غیر فعال شدن باقی شبکه شود.

www.markazdanesh.ir

۲.۱۰ Energy conserving topology maintenance

شبکه های بی سیم حسگر ممکن است در ناحیه های که به سختی قابل دسترسی هستند توسعه پیدا کند و مدت زیادی را بدون سرپرست و ناظر اجراء شوند . یکی از مشکلاتی که در ا ین موارد رخ می دهد، مسئله جایگزینی گره های است که انرژی باترهای خود را مصرف کردند و عملا از کار افتادند . اما روش های برای غلبه بر این مشکل وجود دارد، یک روش می تواند بدین صورت باشد که در ابتدا گره های بیشتری را نسبت

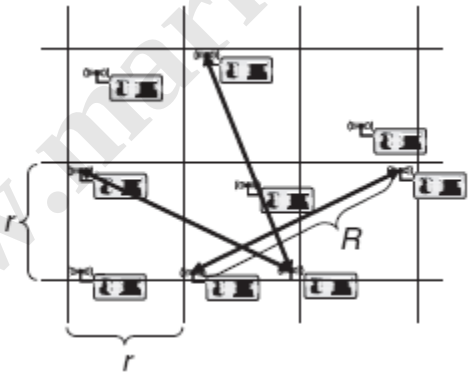
به آنچه نیاز داریم، در منطقه توزیع کنیم و به روشی از گره ها استفاده کنیم که طول عمر شبکه را افزایش دهد. SPAN و GAF دو روشی هستند که می توانند در بکارگیری انتخاب گره های که باید فعال باشنداستفاده شود تا سطح قبولی از درستی مسیریابی به دست آید.

GAF –۲.۱۰.۱

GAF گره ها را بر طبق مکان جغرافیایی و محدوده رادیویی در یک "مربع توری" مجازی قرار می دهد. هر جفت از گره ها در مجاور مربع توری قادر به ارتباط هستند گره ها در یکی از سه حالت زیر قرار دارند:

۱. حالت فعال: در این حالت گره ها در عمل مسیریابی شرکت می کنند.
۲. حالت اکتشاف: در این حالت گره ها در شبکه جستج و می کنند تا بفهمند که در شبکه به آنها نیازی هست یا نه؟
۳. حالت خواب: در این حالت، رادیوی گره ها خاموش می باشد.

گره نسبت به وضعیت فعلی و طول حیاتشان رده بندی می شوند، پیام های اکتشافی برای مبادله اطلاعات وضعیت و رده بندی گره ها در یک "مربع توری" استفاده می شود.



شکل ۲.۷- GAF

حملات: گره ها در حالت فعال یا اکتشاف، یک پیام اکتشافی را از یک گره با رتبه بالا دریافت می کنند، که آنها را به حالت خواب انتقال می دهد. گره ها بعد از چند دور زمانی از حالت خواب بیرون می آیند

www.markazdanesh.ir

و به حالت اکتشاف وارد می شوند. یک نفوذگر می تواند به سادگی کل شبکه را به این صورت غیر فعال کند که به صورت متناوب پیام های اکتشافی با رده بالا را پخش عمومی کند . نفوذگر سپس می تواند یک حمله ارسال انتخابی را ایجاد کند، یا انتخاب کند که پیام ورودی بطور کامل نادیده گرفته شوند . برای یک نفوذگر از رده- laptop با یک فرستنده قوی نیز امکان غیر فعال کردن شبکه وجو دارد . با استفاده از حملات Sybil و HELLO flood، مربع های توری دیگر را از مربعی که در آن قرار دارد را با ارسال پیام اکتشافی، به حالت خواب ببرد.

SPAN – ۲.۱۰.۲

در SPAN، گره ها تصمیم می گیرند که آیا در حالت خواب بمانند یا به یک ستون فقرات از هماهنگ کننده ها متصل شوند که تلاش می کنند درستی مسیریابی را حفظ کنند . هماهنگ کننده ها بطور پیوسته بیدار می ماند در حالیکه گره های دیگر به مد "ذخیره توان" می روند و به طور متناوب پیام های HELLO را ارسال و دریافت می کنند تا تشخیص بدهند که آیا بابد به یک هماهنگ کننده تبدیل شوند یا نه؟ در یک پیام HELOO، یک گره وضعیت جاری خود را اعلام می کنند (هماهنگ کننده هست یا نه).

یک گره در صورتی شرایط تبدیل شدن به یک هاهنگ کننده را دارد که، دو تا از همسایه هایش نتوانند بطور مستقیم یا از طریق یک یا دو هماهنگ کننده به همدیگر دسترسی پیدا کنند . به منظور جلوگیری از ازدحام پیام های پخش عمومی، اگر چندین گره کشف کنند که نیاز است به یک هماهنگ کننده تبدیل شوند، هر گره اعلان خودش را تا یک مدت زمان که بصورت تصا دفی در نظر گرفته می شود، به تاخیر می اندازد. زمان انتظار تصادفی، یک تابع از سودمندی و انرژی باقی مانده است. یک گره با سودمندی زیاد و انرژی زیاد به احتمال زیاد، مدت زمان انتظار کمی را محاسبه می کند. بعد از مدتی گره های هماهنگ کننده، از این کار دست خواهند کشید که این کار به دو دلیل صورت می گیرد:

۱. نیازمندیهای را که برای این کار نیاز است را نمی توانند تامین کنند.

www.markazdanesh.ir

۲. اگر یک هماهنگ کننده، متوجه شود که همسایه های آن می توانند توسط هماهنگ کننده های دیگر با هم ارتباط برقرار کنند.

سپس گره، خواسته خود را برای برکناری از هماهنگ کنندکی اعلان می کند، اما برای یک مدت کوتاه بسته ها را ارسال می کند تا زمانیکه یک هماهنگ کننده جدید انتخاب شود.

حملات: یک نفوذگر از رده-laptop ممکن است تلاش کند تا مسیریابی در شبکه را بوسیله جلوگیری از تبدیل گره ها به هماهنگ کننده ها در شبکه مختل کند . یک حمله ممکن است کل مسیریابی در شبکه را با کارهای زیر مختل کند:

در ابتدا، نفوذگر ناحیه مورد نظر را به چند ناحیه با سایزهای معقول تقسیم می کند. برای هر ناحیه C_i، نفوذگر یک هماهنگ کننده ID_i، انتخاب می کند . نفوذگر n پیام HELLO با قدرت انتقال کافی را ارسال می کند، تا بوسیله همه گره ها در شبکه دریافت شود و به آنها اعلان کند که ID_i (i=1 to n) یک تنظیم کننده و همسایه های زیر را دارد:

$$\{C_{i1},C_{i2}m, \dots ,C_{ik}, ID_1, ID_2, \dots,ID_n \}$$

$C_{i1},C_{i2}m, \dots ,C_{ik}$، گره های در ناحیه C_i هستند، هر گره در ناحیه C_i اعتقاده دارد که:

۱. $ID_1, ID_2, \dots,ID_n$ به عنوان همسایه هایشان هستند.

آن گره می تواند به هر کدام از همسایه هایش چه مجاز و غیر مجاز از طریق ID_i دسترسی داشته باشند، هر هماهنگ کننده جعلی باید $ID_1, ID_2, \dots,ID_n$ را باید به عنوان همسایه هایش معرفی کند، در غیر این صورت یک گره واقعی تبدیل به هماهنگ کننده می شود و اتصال بین آنها از طریق این گره انجام می گیرد، نفوذگر می تواند به طور کارا کل شبکه را غیر فعال کند، زیرا هیچ گره واقعی در مسیریابی شرکت نمی کند .

www.markazdanesh.ir

۲.۱۱ - پروتکل های ساختار درختی مبتنی بر هسته ی توزیع شده

چالش در پروتکل های ساختار درختی مبتنی بر هسته در پیدا کردن گره هسته ای قرار دارد . زمانیکه این گره انتخاب شد، پروتکل مربوطه با گره هسته ای به عنوان منبع عمل می کند . بررسی چنین پروتکل هایی و مقایسه عملکرد را می توان در منبع پیدا کرد . نمونه های بیشتر در منابع هستند. فرض کنید که سینکهای متعددی در شبکه وجود دارند که باید اطلاعات را در ساختار درختی مبتنی بر هسته توزیع کنند. ابتدا باید نقطه ی اولیه آنرا پیدا کرد. برای انجام این کار، هرسینک دارای پیامهائی است که وجود آنرا نشان می دهد و هر گره در شبکه این نوع تبلیغات را جمع آوری می کند و در امتداد با شناسه ی سینک قرار می دهد. در واقع شبکه های بی سیم دارای اختلاف در مصرف کلی نیرو بین دو منبع بر روی این درخت می باشند، بعلاوه، ساختاری برای هر ساختار درختی SBT مجموع نیروی این ساختار درختی را از منبع دلخواهی S را در 2H(|V|-1) را جمع آوری می کند. که H(۰) تابع هارمونیک است.

۲.۱۲ - پروتکل های مبتنی بر مش : برای فائق آمدن به چهارچوب میزان منابع و مسائل حجیم پروتکل های مربوطه، ساختاری با حالت قابلیت ارتباطی لازم است که منابع مخالف را به مقاصدشان مربتط سازد. اولین پروپوزال در این روند CAMP است و مش یک زیرگراف گراف اصلی باید کل منابع مقصد ها را در اختیار داشته باشد و حداقل یک مسیر را از هر منبع به مقصد دیگر اختصاص دهد . منابع مربوط به این پروتکل ها بیشتر دارای یک تاریخچه هستندکه ۲/ (۱+۴) بار بزرگتر از پروتکل هایی قبلی است که $F \leq ۲$ در رابطه گره است و برای گره هایی که در الگوی آن قرار دارند تعبیه شده است. بنابراین کاربرد این پروتکل ها باعث می شود تا TTPP را ایجاد کنیم.

آنتن های مستقیم برای انتشار می تواند ظرفیت بیشتری برای انقال شبکه داشته باشد، برای مثال، پروتکل های BIP/MIP دارای مزیت چنین آنتنی هایی هستند و برای انتقال پیام به گره های مجاور بکار برده می شوند. این روند باعث پیشرفتهای قابل ملاحظه ی در دوره عمر شبکه می شود . رابطه ای نسبت با کنترل توپولوژی نیز دارای اختلاف اساسی در ماهیت مبتنی بر منبع پروتکل های انتشار است، در صورتیکه

www.markazdanesh.ir

پروتکل های کنترل- توپولوژی سعی دارند تا شبکه را در کل بهینه سازند. راه حل های بهینه شده ای برای برنامه ریزی خطی نیز در شبکه ها دیده شده است و سه مشکل برنامه ریزی خطی برای بدست آوردن مشکل انتشار وجود دارد. راه حل مورد نظر برای این موضوع ر ا می توان به عنوان چارچوبی برای الگوریتم های عملکردی در نظر گرفت. راه حل بهینه شده برای شبکه های درختی نیز در روش جمع آوری و توزیع اطلاعات در یک شبکه ی دارای ساختار درختی تعبیه شده است.

زمان مورد نظر برای تکمیل انتشار چند منظوره نیز برای مشکل برخی از رونده ا بسیار ضروری است . جایگزینی اطلاعات نیز در تقریبهای ساختار درختی توسط بیشتر محققان بررسی شده است.

۲.۱۳ - مسیریابی جغرافیایی

پروتکل های روتینگ جغرافیائی دو کاربرد دارند:

۱- کاربردهایی برای تمامی منظور، مکانهای فیزیکی را باید در روند کار مطرح ساخت برای مثال، هر گره در هر منطقه ی مزبور می تواند یک نقطه ای را در بر گیرد

۲- زمانیکه وضعیت یک منبع و مقصد به عنوان وضعیتهای گره های واسطه شناخته شده باشند، این اطلاعات را می توان برای کمک در پروسه ی روتینگ بکار برد . برای انجام چنین کاری، گروه مقصد باید از لحاظ جغرافیایی شناسایی شده باشد که ما آنرا سرویس مکان می گوییم . فرمت این روند در پروتکل های روتینگ ساده است که مکانهای فیزیکی اطلاعات دقیقی را به گروه های مجاور با فوروارد کردن یک پاکت به آنرا، انتقال می دهد.

اولین جنبه ی مهم انتقال اطلاعات به گره های مورد دلخوه در یک منطقه مزبور است که ما آنرا انتشار و توزیع جغرافیایی می گوییم . اولین جنبه را روتینگ مبتنی بر وضعیت می گوییم که در تلفیق با سرویس نکات بکار برده می شود اولین بار روتینگ کارتزین نام داشت . در شبکه های سنسور بی سیم، معمولاً جوانب انشار یا توزیع جغرافیایی بسیار مهم است . چنین این گره ها قابل مبادله هستند و توسط جوانب

خارجی شناسایی می شوند. و در وضعیت خاص آنها، سرویس مکان معمولاً لازم نیست . بنابراین، این فصل تمرکز بر روی جوانب انتشار یا توزیع جغرافیایی است.

۲.۱۴ – استراتژیهای مسیریابی

هدف مسیریابی جغرافیایی استفاده از اطلاعات محلی برای پیدا کردن مسیر می باشد. برای دستیابی به این هدف بسته اطلاعاتی به گره های در داخل ناحیه هدایت فرستاده می شود . در این الگو ، فقط گره هایی که داخل ناحیه هدایت هستند اجازه ارسال بسته را دارند . ناحیه هدایت می تواند به صورت ایستاء توسط گره منبع تعریف شود یا توسط گره های میانی جهت حذف گره های که باعث انحراف در مسیر بهینه می باشند انجام گیرد. کارایی استراتژی فوق وابسته به روشی است که از طریق آن ناحیه هدایت تعریف می شود و همچنین ارتباط گره های ناحیه فوق نیز وابسته است.

استراتژی دوم مسیریابی بر اساس موقعیت می باشد که نیاز است گره ها اطلاعات محلی همسایه هایشان را داشته باشند در اینجا یک مکانیزم مسیریابی حریصانه استفاده می شود که به موجب آن هر گره بسته ای را به نزدیکترین همسایه اش می فرستد . چندین معیار برای تعیین مفهوم نزدیکی وجود دارد از جمله فاصله اقلید حس، فاصله خط مستقیم از گره جاری تا مقصد و میزان انحراف از خط مستقیم به سمت مقصد

پروتکل های مسیریابی مبتنی بر موقعیت، پتانسیل بالقوه در کاهش سربار و انرژی مصرفی دارند. کارایی این الگو وابسته به تراکم شبکه، محل دقیق گره ها و مهم تر از همه قانون هدایت استفاده شده برای جلو بردن ترافیک به سمت مقصد است.

۲.۱۵ – اصول روتینگ مبتنی بر وضعیت

- برخی از استراتژیهای فورواردینگ ساده:

* فوروارد در داخل:

فرض کنید که یک گره بخواهد پاکت اطلاعاتی را به گره دیگر ارسال کند و هر گره در شبکه وضعیت خودش را بشناسد. در یک حالت فوروارد ینگ پاکت مزبور به پاکت مجاور فوروارد می شود که نزدیک به مقصد قرار دارد.

D-1+(i-1)/N, i=1, …, N

و پهنای 1/N که D=|ST| و فاصله ی بین گره های T,S است و دامنه ی رادیوئی تا ۱ حالت نرمال دارد. حالا بیائید Ai را تقاطع این آنولی با دامنه ی رادیوئی را در نظر بگیریم بعد از اینکه S پاکت اش را ارسال کرد، گره ها در A برای فوروارد ینگ آماده می شوند. اگر یک گره پاکت را ارسال کند، مشکل فوروارد‌ینگ حل می شود . اگر گره های متعددی تلاش به فوروارد‌ینگ بکنند، نوسان نیز با استف اده از الگوریتم رزولاسیون حل می شود و اگر گره ها پاسخ نشان ندهند، گره های به A باید پاکت را فوروارد کنند . اگر گرهی در AN وجود نداشته باشد، گره S به سادگلی مدتی منتظر می ماند تا انتقال مجدداً انجام شود . در این حالت، N بزرگتر تقریب بهتری از لحاظ جغرافیایی م ی باشد یعنی، نزدیک ترین گره است و از طرفی دیگر پتانسیل فوروارد‌ینگ را نیز افزایش می دهد . این روند را می توان با GAF نیز مقایسه کرد. GERAF مشابه به مورد قبلی در بخش های است و به کل گره های حاصل از روتینگ نیازی ندارد . وضعیتهای همان روتینگ جغرافیائی یا GEM نیز در پروسه شبکه سازی بسیار مهم است . کاربرد ویژگیهای روتینگ جغرافیایی همان اطلاعات وضعیتی کمی بحث بر انگیز است.

این روش دارای دو بخش است : روتینگی که در سیستم هماهنگ کننده یا مختصات قطبی استفاده می کند و با توجه به شعاع و زاویه ی حاصل از یک مرکز عمل می کن د و ساختار توزیع شده چنین مختصات قطبی مجازی به مختصات فیزیک بستگی ندارد . اگر یک گره وضعیت خود را بشناسد، دامنه هایی به آن اختصاص می دهد یعنی Vi باید به دامنه ی زاویه اختصاص می یابد.

www.markazdanesh.ir

$$[\alpha + (\beta - \alpha)(S_1 + ... + S_{i-1}) / (S_1 + ... + S_n)$$
$$\alpha + (\beta - \alpha)(S_1 + ... + S_i) / (S_1 + ... + S_n)]$$

محققان نیز در این باره نشان داده اند که میزان د قت برای سیستم مختصات مجازی کافی نیست . در عوض روشی را مبتنی بر شمارش hop مطرح کردند که بدون اطلاعات مکان فیزیکی که می کند . تعیین اطلاعات زاویه ای با استفاده از شمارش های hop نیز به خوبی کار انجام می دهد. دو گره را انتخاب کنید و یک ریشه ی منبع به آن اضافه کنید، سه گره باید جدا از یکدیگر و غیر خطی باشند برای هر گره در شبکه یک شمارش hop از کوتاه ترین مسیر بین هر یک از این سه گره را انتخاب و تعیین کنید. بعلاوه، هر گره در شبکه باید فواصل خودش را بشناسد . تا کنون این روش به روش DV-Hop مشابهت دارد. با استفاده از اطلاعات زاویه ای حاصل از این وضعیتها، مرکزیت باید در وضعیت متوسط کل گره ها تعیین شود.

بنابراین، محاسبات در یک ساختار درختی به همراه مختصات مجازی با وضعیت توپولوژیی شبکه اختصاص می یابد . این ساختار درختی در گراف اصلی احاطه شده است و نام آن برای این روند GEM نامیده شده است. در کل این روش، بسیار قابل ملاحظه است و منجر شده است تا روتینگ و ذخیره مرکزیت دیتا تحقیق و پیاده سازی شود.

۲.۱۶ – انتشار توزیع جغرافیایی: ارسال اطلاعات یا دیتا به زیر مجموعه ای از گره ها که در منطقه ی نشان داده شده قرار دارند را انتشار جغرافیائی می گویند. مشابه به همین مورد، اطلاعات وضعیتی منطقه ای تعبیه شده است و گره های واسطه ای را می توان جهت افزایش باز دهی به آن اختصاص داد . مکانهای مبتنی بر انتشار یا توزیع نیز ساده ترین روش جهت انتشار یا توزیع جغرافیائی است و در هر صورت به منطقه ی جغرافیائی بستگی دارد.

البته مناطق پویا و استاتیک نیز می تواند هم منبع و هم منطقه ی مقصد را تحت پوشش قرار دهد . مناطق سازگار نیز دارای گره هایی می باشند که در مناطق استاتیک شامل می شوند و البته یک مسیر فرعی نیز به عنوان گره واسطه در روند فورواردینگ دخیل خواهد شد.

www.markazdanesh.ir

نگاهی دیگر

هدف اصلی مسیریابی جغرافیایی استفاده از اطلاعات محلی برای پیدا کردن مسیر بهینه به سمت مقصد است. این مسیریابی مفید است جائیکه تجمع اطلاعات یک تکنیک مفید در کاهش تعداد ارسالات به سمت ایستگاه پایه با حذف بسته های تکراری از منابع مختلف می باشد . نیاز به تجمع اطلاعات در کاهش انرژی مصرفی ، مدل ارتباطاتی را در شبکه های حسگر از الگوی آدرس گرای سنتی به الگوی داده گرا انتقال می دهد جائیکه محتوای داده در تشخیص گرهی که داده را جمع آوری می کند مهم تر است

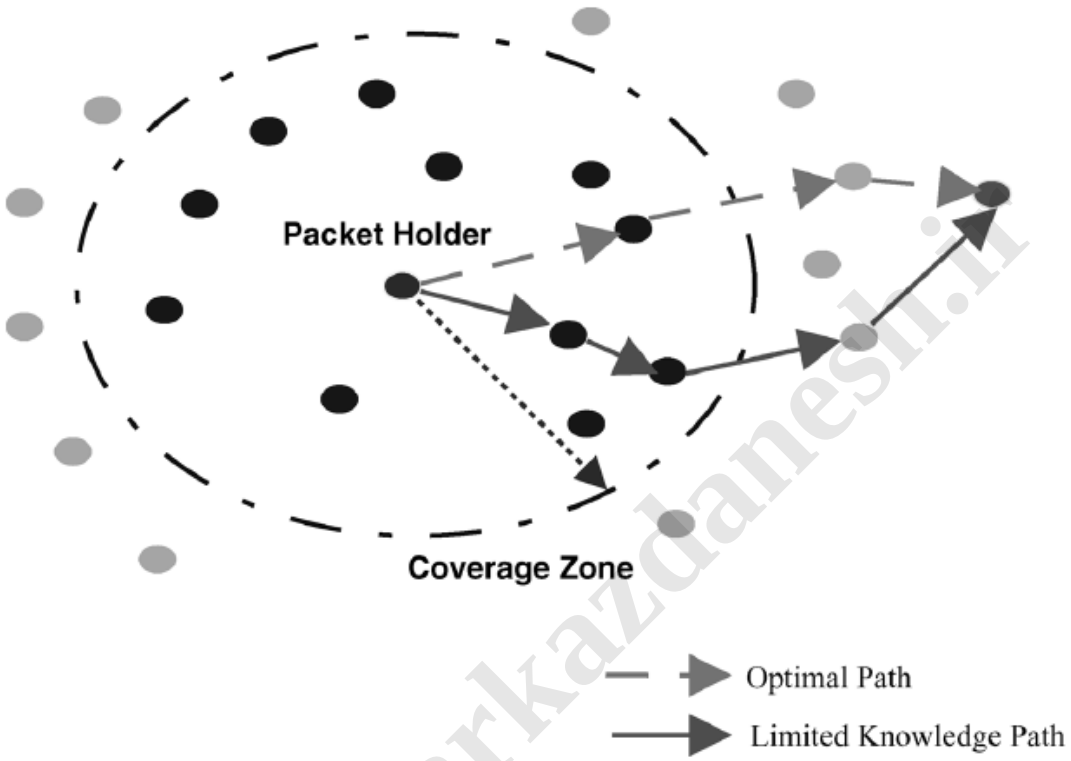
ماهیت حسگرهایی که اطلاعات را جمع آوری و منتشر می کنند ب ه اندازه محتوای داده مهم نیست .روش های مسیریابی قدیمی که عموماً برای تعیین مسیر بین دو نقطه آدرس دهی شده طراحی شده بودند . پرس و جوی چند بعدی مناسب نیستند. مسیریابی جغرافیایی اطلاعات محلی مورد نیاز برای رسیدن به هر مقصد را بسته بندی می کنند . بعلاوه مسیریابی جغرافیایی در برنامه های داده گرا کمترین سربار اطلاعاتی و محاسباتی را دارد.

۲.۱۷ - روش های هدایت

یک جنبه مهم در مورد مسیریابی جغرافیایی ، قاعده استفاده شده برای هدایت ترافیک داده به سمت مقصد است در مسیریابی مبتنی بر موقعیت، هر گره در مورد پیدا کردن گره بعدی بر اساس موقعیت خودش و همسایه هایش و موقعیت مقصد تصمیم می گیرد . کیفیت تصمیم گیری به طور واضح وابسته به مقدار آگاهی هر گره از توپولوژی عمومی است. دانش محلی از توپولوژی ممکن است منجر به پیدا کردن مسیرهای نیمه بهینه همانند شکل ۲.۸ بشود. پیدا کردن مسیر بهینه نیازمند داشتن دانش کلی یا عمومی در مورد توپولوژی می باشد که سربار آن از پیش در شبکه های حس گر پیش بینی شده است . طرح مسیریابی حریصانه یکی از نزدیکترین همسایگان را به مقصد انتخاب می کند، در شکل ۲.۹ ، گره فعلی MH ، گره GRS را به عنوان گره بعدی انتخاب می کند . باید بدانیم که طرح فوق از میان مجموعه ای از گره های نزدیک به مقصد یکی را انتخاب می کند، اگر این مجموعه خالی باشد، طرح فوق با شکست روبرو می شود .

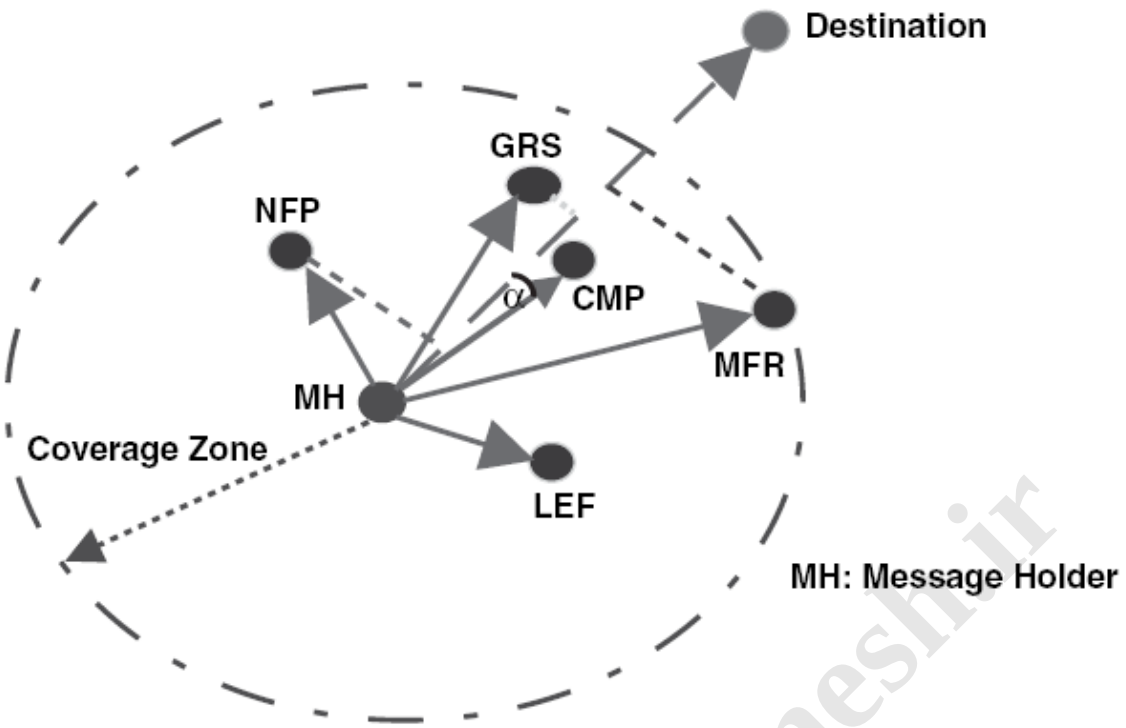
www.markazdanesh.ir

در استراتژی (MFR) ، (R محدوده انتقال را مشخص می کند) یک گره بسته خود را به جلوترین همسایه اش در جهت مقصد می فرستد . در این روش گره بعدی، بعد از MH ، MFR است. این روش حریصانه نزدیک بین است و لزوما مسیر بهینه را پیدا نمی کند. به شکل (۲.۲۲) مراجعه شود.



شکل ۲.۸- تصمیم ارسال محلی شده و سراسری

www.markazdanesh.ir



شکل ۲.۹- ستراتژی ارسال مسیریابی جغرافیایی

ادامه :

در پایان فرآیند انتخاب عنصر سرخوشه هر گره ای که به عنوان سرخوشه انتخاب می شود نقش جدیدش را به سایر گره های شبکه اعلام میکند با اعلام این خبر سایر گره ها نیز به خوشه وصل می شوند در هر خوشه عنصر سرخوشه زمان بندی مبتنی بر TDMLایجاد ودر خوشه پخش می کند که حاوی بازه های زمانیی اختصاص داده شده به هر عضو خوشه می باشد . هر عنصر سرخوشه از تکنیک CDMAنیز بهره می گیرد با تکمیل فاز بر پاسازی فاز steady _ stateشروع می شود در این فاز گره ها در بزه های زمانی اختصاص داده شده اطلاعات را جمع آوری و به گره سرخوشه ارسال می کنند . در ضمن جمع آوری اطلاعات به صورت متناوب می باشد نتایج اخیر شبیه سازیها حاکی از این است روش leach انرژی مصرفی قابل ملاحظه ای را ذخیره می کند . در ضمن طول دوره steady _ state در کاهش انرژی مصرفی موثر است . کوتاه بودن دوره

www.markazdanesh.ir

steady _ state سر بار پروتکل را افزایش می دهد در حالیکه طولانی بودن انرژی مصرفی را افزایش میدهد .

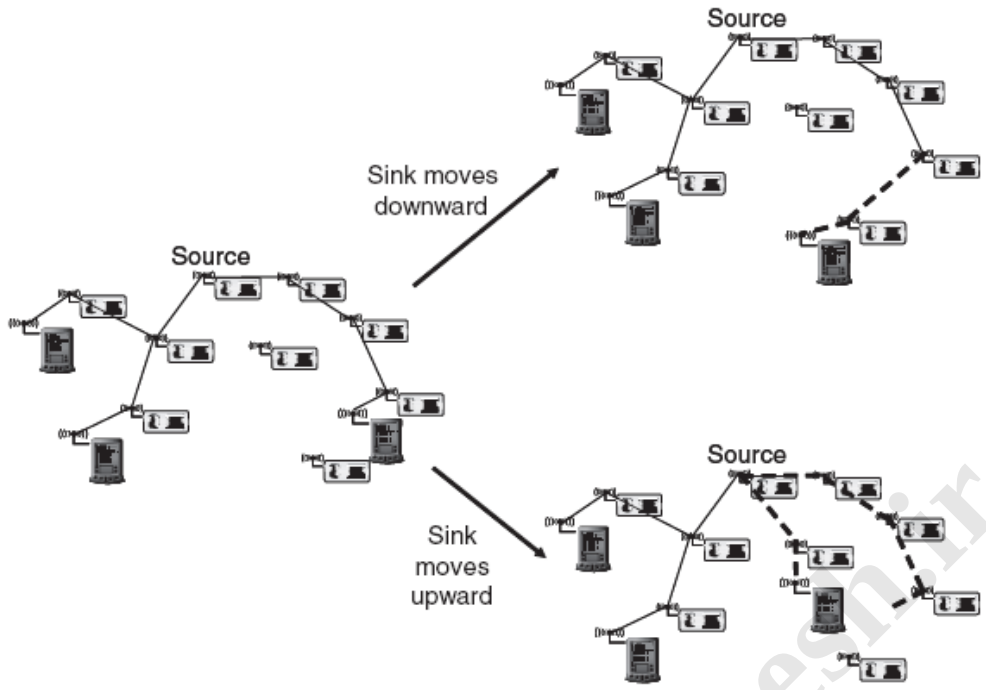
۲.۱۸ - گره های سیار

همانطورکه قبلا بحث شد منابع مهمی از سیار بودن در WSN وجود دارد: سیار بودن گره های سنسور، سیار بودن سینکهای دیتا و سیار بودن مورد مشاهده شده . کل این سه نوع سیار بودن داری میزان بزرگ یا کوچک بودن می باشد که توسط مکانیسم های بحث شده به اجرا در می آید . بعلاوه کنترل این سیار بودن تمرکز اصلی تحقیق در شبکه می باشد.

۲.۱۸.۱- سینکهای سیار

اولین مورد با نیازهای خاص این است که سینکهای سیار در شبکه سازی از یک منبع دیتا استفاده می کند که اطلاعات را نسبت به نزدیک ترین نقطه توزیع می کند . انتخاب دیگر بر مبنای ساختار درختی چند توزیعی تعبیه شده است. سینک سیار خودش دارای گره سنسور است و به عنوان پروکسی در این ساختار درختی عمل می کند . زمانی که این ساختار درختی ایجاد شده این سینک در اطراف پروکسی خود به گردش در می آید و پروکسی جدیدی را اختصاص می دهد در این مورد دو گزینه وجود دارد : سینک به طرف گره پروکسی قبلی حرکت می کند که در سا ختار درختی زیاد به طول نمی انجامد . در این مورد پروکسی جدید به ساختار درختی ملحق می شود و مورد قبلی از این گره جدا می شود در دومین مورد پروکسی قدیمی هنوز قابل قبول است ولی ارتباط بین پروکسی قبلی و گره سنسور به سینک سیار در نزدیک ترین حالت قرار داد و پروکسی قدیمی از آن برای پربار کردن دیتا به سینک استفاده می کند . این دو مورد در شکل ۲.۱۰ نشان داده شده است بالاخره اینکه طراحی SINA نیز این مشکل را دارد. و هدف این است تا مکان سینک سیار را با یک گره در شبکه آپ دیت بکند که مسئولیت ردیف ها را به عهده دارند و این سینک سیال به دور از این مکان حرکت می کند.

www.markazdanesh.ir



شکل ۲.۱۰- تعدادی چاهک سیار که به یک درخت multicast وصل شده است

۲.۱۸.۲- کلکتورهای دیتای سیار

گاهی اوقات انتقال سینکهای دیتا مطلوب نمی باشد ولی ارتباط نیز شاید مفید واقع نشود و مفهوم شبکه های لن قابل اجرا باشد. یک MULE ابزار سیاری است که مجهز به پایانه های رادیویی است که می توان با گره های سنسور ارتباط برقرار کند و بین گره های سنسور به حرکت در می آورد و دیتای آنها را جمع آوری و بافر می کند نمونه هایی برای MULE ها را می توان در رباط ها مشاهده کرد . MULE یک واسته مستقل بین الگوی حرکت MULEها است که می توان گره های سنسور را بررسی و ضریب جمع آوری دیتا را برآور کند. و فضای بافر در سنسور ها و MULE ها وسرعت ارتباط بین MULE و سنسور منجر به وقفه در ضریب تحویل اطلاعات در سینک اطلاعاتی می شود. محققان مدعی شده اند که چنین MULE ها دارای بازدهی انرژی بیشتری نسبت به سایر دستگاه های ارتباطی هستند و می توانند دوره عمر شبکه را بدون امپدینگ جمع آوری اطلاعات افزایش دهد.

www.markazdanesh.ir

۲.۱۸.۳- نواحی سیار

نواحی مقصد توزیع جغرافیایی حالت استاتیک تلقی شده است. برای برخی کاربردها مانند ردیابی موارد سیار این روند می تواند در تعیین یک منطقه مقصد که مقصدش تغییر می کند، موثر واقع بشود . برای چنین منطقه حرکتی یا سیار دیتا باید در زمان T به کل گره ها توسط منقطه مقصد در زمان T تحت پوشش قرار گیرد. این روش سرویس دهی را توزیع سیار می گویند . و این پروتکل می تواند دیتا را در زمان مناسب با گره ها تحویل دهد روش اصلی نیز انتقال اطلاعات به منطقه هدایت است که با حرکت منطقه مقصد شروع می شود.

www.markazdanesh.ir

مسیر یابی امن در شبکه های بی سیم سنسور: حملات و اقدامات متقابل

۳.۱ - مقدمه

تمرکز ما در این قمست از پروژه بر روی امنیت مسیریابی در شبکه های بی سیم حسگر است. طرح های پیشنهادی فعلی برای الگوریتم های مسریابی در شبکه های سنسور حسگر بر ویژگیهای محدود و خاص از گره ها و کاربردهای خاصی از طبیعت این شبکه ها تمرکز کرده اند . اما امنیت را که یکی از اساس ترین نکات در طراحی شبکه ها است به طور جدی در نظر نگرفته ا ند. به همین جهت ما احساس کردیم که امنیت به عنوان یک نکته اصلی باید در الگوریتمهای موجود بررسی و تحلیل شود و در طراحی الگوریتم های جدید باید از ابتدا به عنوان یک نکته حیاتی در نظر گرفته شود . زمانیکه در محیط موجود امکان ارتباطات بی سیم نا امن وجود دارد و گره ها توانایی های محدودی دارند و امکانات تهدیدات داخلی و خارجی وجود دارد و یک نفوذگر می تواند با استفاده از یک سیستم کامپیوتری با توانایی زیاد به شبکه نفوذ کند، طراحی یک پروتکل مسیریابی حیاتی و ضروری است.

یکی از ویژگیهای که طراحی یک پروتکل مسیریابی امن را پیچیده می کند، تراکم در درون شبکه است . در شبکه های مرسوم، یک پروتکل مسیریابی امن فقط نیاز دارد تا در دسترس بودن پیام ها را تضمین کند . تمامیت، صحت و محرمانگی پیام ها در لایه های بالاتر و بوسیله یک مکانسیم امنیتی انتها به انتها مانند SSL یا SSH تامین می شوند . امنیت انتها به انتها در شبکه های مرسوم امکان پذیر است زیرا برای مسیریاب های میانی ضروری نیست تا به متن پیام ها دسترسی داشته باشند. اگر چه، در شبکه های حسگر، پردازش درون شبکه ای، توسعه مکانسیم های امنیت انتها به انتها را به خاطر اینکه گره های میانی نیاز دارند تا به طور مستقیم به محتوای پیام ها دسترسی داشته باشند، مشکل تر می سازد . مکانسیم های امیتی لایه پیوند می تواند کمک کند تا تعدادی از آسیب پدیرها آشکار شوند، اما آن کافی نیست : ما حال نیاز به تعدادی از پروتکل های مسیریابی نیاز داریم، و آنها باید با در نظر گرفتن این نکات طراحی شوند.

۳.۱.۱ –ادعاهای ما

www.markazdanesh.ir

ما انواع حملات مهم در برابر همه پروتکل های مسیریابی مهم در شبکه های بی سیم حسگر را معرفی خواهیم کرد. بخاطر اینکه این پروتکل ها بدون در نظر گرفتن امنیت به عنوان یکی از اهداف اصلی طراحی شده است، تعجب آور نخواهد بود که اکثر آنها از لحاظ امنیتی دارای مشکلات زیاد و اساسی باشند . اگر چه ضوروی هست تا این مشکلات اصلاح شوند، اما بسیار بعید است که بتوانیم بعد از طراحی یک پروتکل مسیریابی بدون در نظر گرفتن امنیت و فقط با ترکیب مکانسیم های امنیتی با این پروتکل ها بتوانیم به یک پروتکل مسیریابی کاملا امن دسترسی پیدا کنیم . هدف و توصیه اصلی ما این است که تمام الگوریتم ها و پروتکل های مسیریابی باید با در نظر گرفتن امنیت به عنوان یکی از مهمترین نکات طراحی و توسعه پیدا کند. و این تنها راه حل موثر برای مسیریابی امن در شبکه های بی سیم حسگر است.

ما پنج ادعا اصلی داریم.

- ما انواع تهدیدات و اهداف امنیتی را برای مسیریابی امن در شبکه های بی سیم حسگر معرفی می کنیم.
- ما دو کلاس جدید از حملات که اخیرا به این نوع شبکه ها شده است اما مستند نشده است را معرفی می کنیم، حملات sinkhole و HELLO flood ها
- ما نشان می دهیم که چگونه حملاتی که در شبکه های ad-hoc و نظیر به نظیر اتفاق افتاده است می تواند با کمی تغییر به عنوان حملات قوی در شبکه های بی سیم حسگر نیز رخ دهند
- ما آنالیز امنیتی را برای همه پروتکل های مهم و اساسی مسیریابی را بتفصیل ارائه خواهیم داد . ما شرح خواهیم داد حملات عملی مهم در این نوع شبکه ها را و دلایلی را که باعث می شود این پروتکل ها با شکست روبرو شوند.
- ما بر روی اقدامات متقابل و نکاتی که باید برای طراحی یک پروتکل مسیریابی امن در نظر گرفته شود، بحث خواهیم کرد.

www.markazdanesh.ir

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sink-holes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGA-SIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes
Energy conserving topol-ogy maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

شکل ۳.۱- خلاصه ای از حملات بر علیه پروتکل های مسیریابی پیشنهاد شده

۳.۲ - پیش زمینه

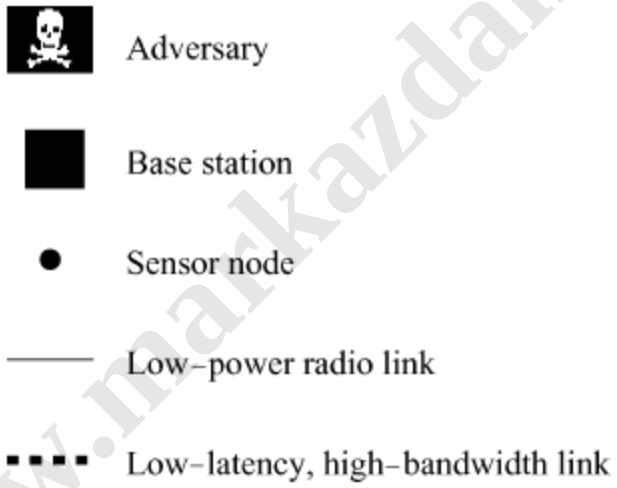
ما از واژه شبکه حسگر برای اشاره به سیستم های ناهمگن که ترکیبی از حسگرهای کوچک و محرک های با عناصر محاسباتی همه منظوره استفاده خواهیم کرد . شبکه های حسگر ممکن است شامل صدها یا هزاران گره ارزان قیمت و با مصرف انرژی کم می باشد، اما امکان دارد که این گره ها از لحاظ مکانی سیار یا ثابت باشند، اما در اغلب موارد گره ها در مکان های ثابتی قرار می گیرند. ما نیز در این فصل فرضی می کنیم که گره ها در مکان ثابتی قرار گرفته اند و موقعیت مکانی آنها در طول حیاتشان تغییر نخواهد کرد

ما در این فصل فرضی می کنیم که از پلات فرم Berkeley TinyOS sensor استفاده می کنیم. بخاطر اینکه این محیط اسا با هر محیطی که ما قبلا با آن برخورد داشتیم فرق می کند

یک مثال نمونه Mica mote هست، یک واحد حسگر /محرک کوچک با یک CPU، منبع تغذیه، رادیو و عناصر مختلف دریافت کننده مختلف.

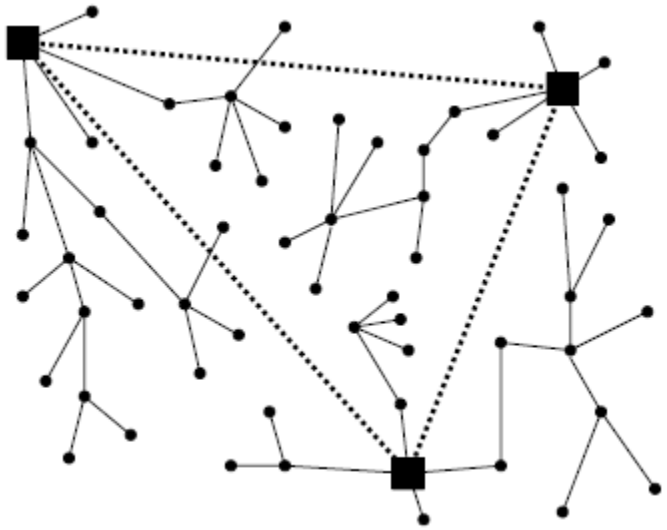
www.markazdanesh.ir

شبکه های حسگر بی سیم اغلب یک یا تعدادی نقطه کنترلی متمرکز دارند که ایستگاه پایه نامیده می شود. یک ایستگاه پایه به طور مهمول یک دروازه به شبکه های دیگر، یک پردازشگر داده قوی یا مرکز ذخیر ه سازی، یا یک نفطه دسترسی برای رابط انسانی است. آنها می توانند به عنوان یک اتصال رابط استفاده شوند، تا اطلاعات کنترلی را در شبکه پخش کند، یا داده ها را از آن استخراج کند در بعضی از کارهای قبلی روی پروتکل های مسیریابی شبکه های بی سیم، از واژه Sink معادل با ایستگاه پایه استفاده شده است . ایستگاه پایه بطور معمول بسیار قوی تر از گره های دیگر شبکه است، آنها ممکن است یک پردازنده قوی یک ایستگاه کاری یا laptop، حافظه، منبع تغذیه AC و پهنای یاند زیاد ارتباطاتی باشند. اگر چه حسگرها مجبور هستند، اگر چه حسگرها مجبور هستند انرژی کم، پهنای باند کم و رادیو در دامن ه پایین را مصرف کنند. شکل ۳.۲ و۳.۳ یک معماری نمونه را برای شبکه های حسگر نشان می دهد.



۳.۲- علائم شبکه حسگر

www.markazdanesh.ir



شکل ۳.۳- یک معماری نمونه برای شبکه های حسگر

یک ایستگاه پایه ممکن است درخواست یک رشته از داده ها را به صورت پیوسته بکند . به طور مثال یک حسگر در هر ثانیه اطلاعات را از گره ها می خواند تا بتواند به یک پرس و جوی خاص جواب بدهد . ما به یک چنین رشته ای، با جریان داده اشاره خواهیم کرد . و گره های را که آنها ا رسال می کنند را به عنوان منبع اشاره خواهیم کرد.

به منظور ذخیره انرژی در شبکه های حسگر تعداد کل پیام های که باید ارسال را شوند کاهش دهیم، این کار می تواند بدین صورت انجام گیرد که پیام های ارسال شده از منابع مختلف با هم در یک نقطه به نام نقاط تجمع، تجمع شون‌د. یک نقطه تجمع، یک گره معمولی در شبکه است . نقاط تجمع ضرورتا، ایستا نیستند و این نقاط می توانند برای هر پرسجو یا رویداد، بصورت پویا انتخاب شود . آن ممکن است که هر گره در شبکه به عنوان یک نقطه تجمع عمل کند.

مدیریت انرژی در شبکه های حسگر بحرانی هست . یک ذره م یکا دانشگاه برکلی با انرژی کامل می تواند فقط برای دو هفته استفاده شود. بنابراین اگر ما بخواهیم شبکه های حسگر برای سال ها استفاده شود، آنها در حدود ۱۰٪ از چرخه وظایف را مشغول بکار باشند، به طور مشابه، از آنجائیکه مصرف انرژی در حالت

www.markazdanesh.ir

انتقال داده ها یا استراق سمع ۳ برابر زیادتر از زمانیکه است، در حالت خواب است. آن بحرانی هست تا زمان عمده ای را در حالت خواب نگه داریم.

روشن است که ما باید اغلب داشته ها و فر ضیات قبلی را درباره امنیت شبکه دور بیاندازیم . شبکه های حسگر، تفاوت های مهمی نسبت به سیستم های توزیع شده دیگر دارند. طبیعت کمیود منابع در شبکه های حسگر، یک چالش مهم برای امنیت این شبکه ها ایجاد می کند . این وسایل قدرت محاسباتی خیلی کم دارند: رمزگذاری کلید عمومی پر هزینه است و به همین جهت برای این نوع شبکه ها غیر مفید است . و حتی کلید متقارن سریع تر و ارزان تر نیز باید با احتیاط استفاده شود . همچنین پهنای باند نیز به شدت مهم هست: هر بیت که انتقال داده می شود، انرژی معادل اجرای ۸۰۰ تا ۱۰۰۰ دستور را مصرف می کند/ توان، انرژی از همه منابع مهم تر و مقدارش کم تر است . هر میلی آمپر که از انرژیگره حسگر مصرف می شود، آن گره حس‌گر یک گام به مرگ خود نزدیگتر می شود . به عنوان یک نتیجه، تقریبا هر جنبه ای از شبکه های حسگر را باید با در نظر گرفتن مسئله انرژی طراحی کرد.

۳.۳ - شبکه های حسگر در مقابل شبکه های بی سیم ad-hoc

شبکه های بی سیم حسگر شباهت های زیادی با شبکه های بی سیم ad-hoc دارند. متد ارتباطی برجسته هر دوشبکه، شبکه سازی چند گام است. اما تفاوت های مهمی و مختلفی بین هر دو گره وجود دارد . شبکه های ad-hoc معمولا مسیریابی بین هر جفت از گره ها را پشتبانی می کند، در حالیکه شبکه های حسگر یک الگوی ارتباطی خیلی خاص دارند . عمده ترافیک در شبکه های حسگر می توانند در سه دسته تقسیم بندی شوند.

۱) چند به یک: چندین گره حسگر داده های دریافت و حس شده از محیط را به یک ایستگاه پایه یا نقطه تجمع در شبکه ارسال می کند.

۲) یک به چند: یک گره خاص (معمولا ایستگاه پایه) یک پرس و جو یا اطلاعات کنترلی را به گره های مخ‌تلف ارسال می کند.

www.markazdanesh.ir

۳) ارتباطات محلی: گره های همسایه پیام های متمرکز شده را ارسال می کنند تا همدیگر را کسف کنند و با همدیگر هماهنگ شوند.

گره ها در شبکه های ad-hoc به طور منابع محدودی دارند، اما همانطوریکه در قسمت ۲ دیدیم، گره های خسگر خیلی منابع خیلی محدودتر دارند، و همه منابع دارای محدودیت هستند و همه انرژی بیشتر از همه منابع دیگر محدود تر هستند.

گره ها در شبکه بی سیم حسگر اغلب ارتباطات قابل اعتمادتر نسبت به شبکه های ah-hoc ارائه می دهند. گره های همسایه در اغلب شبکه های حسگر گواه رویدادهای محیطی مشابه یا مرتبطی هستند. اگر هر گره یک بسته، به ایستگاه پایه در پاسخ ارسال کند . انرژی بسیار و پهنای باند زیادی مصرف می کند، با حذف افزونگی این پیام ها، ترافیک کاهش می یابد و انرژی ذخیره می شود.

۳.۴ - بیان مشکل

قبل ار اینکه بطور جدی وارد بحث پروتکل های مسیریابی شویم، در ابتدا بهتر است که بیان دقیقی از مسئله امنیت در مسیریابی شبکه های بی سیم داشته باشیم . در بخش زیر ما فرضیات خودمان را درباره اصول شبکه، مدل های پیشنهادی برای رده های مختلفی از نفوذگر ها به صورت خلاصه بیان می کنیم . و اهداف امنیتی را در سری بیان حواهیم کرد.

۳.۴.۱ -فرضیات شبکه

بخاطر اینکه شبکه های حسگر از ارتباطات بی سیم استفاده می کنند، ما باید فرض کنیم که پیوندهای رادیویی امن نیستند. پس نفوذگرها می توانند روی ارسالات رادیویی ما استراق سمع کنند .و سپس بسته های را که استراق سمع کردند را تغییر دهند و سپس روی کانل مجددا ارسال کنند . ما فرضی می کنیم، اگر مدافع بتواند گره های حسگر زیادی را در محیط توزیع کند، پس نفوذگر احتمالا قادر خواهد بود که تعدادی از گره های غیر قانونی و غیر مجاز را با قابلیت های سخت افزاری مشابه توزیع کند.

www.markazdanesh.ir

ما تصور می کنیم که نفوذگر ممکن است بیش از یک گره را کنترل کند، و گره های غیر مجاز ممکن است برنامه ریزی کنند تا به سیستم حمله کنند . همچنین، در بعضی از موارد گره های غیر مجاز ممکن است پیوندهای ارتباطی با کیفیت بالا را برای هماهنگ سازی گره ها استفاده کنند.

لایه های فیزیکی و MAC مستعد حملات مستقم هستند. نفوذگرها می توانند پیوندهای رادیویی را بوسیله انتقال بدون توقف شلوغ کنند . یا تلاش می کند با استفاده از مسئله "ترمینال های پنهان" باعث ایجاد برخورد در شبکه شود. با یک پروتکل MAC که از فریم های CTS/RTS استفاده می کند، نفوذگر می تواند به طور متناوب فریم های CTS را با یک فیلد "مدت" طولانی را ارسال کند، و باعث می شود که گره های دیگر نتوانند بطور موثر از کانال استفاده کنند . علاوه بر اینها، پروتکل های MAC از backoff تصادفی استفاده می کنند. که این پروتکل هر مستعد نفوذ وحمله می کند . اگر گره های شبکه مدیریت بی نظمی ضعیفی داشته باشند یا از الگوریتم تولید اعداد تصادفی مشخص و آشکار شده استفاده کنند، نفوذگرها قادر خواهند با استفاده از این ضعف ها، رمانهای backoff را بیش بینی کنند و می توانند باعث ایجاد زمانهای backoff طولانی یا ایجاد برحورد شوند.

حملات لایه MAC می تواند بوسیله استفاده از تعداد پروتکل های مدیریت خوب بی نظمی و یک الگوریتم رمز گذاری شده برای تولید اعداد تصادفی دفع شود . آن برای نفوذگران امکانپذیر است که از ضعف های موجود در لایه های مختلف استفاده کنند، و حملاتی را بر طبق اهدافشان و با ستفاده از این ضعف ها تداراک ببینند.

۳.۴.۲ -انواع تهدیدات

یک تمایز مهم بین نفوذگر های رده- mota و رده-laptop این است که نفوذگر های رده- mota به تعدادی گره، با قابلیت های مشابه حسگرهای مجاز در شبکه دسترسی دارد. اما یک نفوذگر از رده- laptop به یک سیستم قویتر مانند یک laptop یا یک سیستم مشابه آت دسترسی دارد. در حالت دوم، گره های غیر مجاز

www.markazdanesh.ir

برتریهای را نسبت به گره های مجاز دارند . برای نمونه آنها ممکن است یک باتری با توان زیاد، یک CPU قوی تر، یک فرستنده قوی و یک آنتن حساس داشته باشند.

یک نفوذگر از رده- laptop می تواند با توجه به تجهیزاتی که در اختیار دارد می تواند کارهای بیشتر را نسبت به زمانیکه فقط به چند گره ساده دسترسی دارد، انجام دهد . یک حسگر معمولی ممکن فقط قادر باشد در پیوندهای رادیویی که در مجاورتش قرار دارد، ایجاد پارازیت کند. در حالیکه یک نفوذگر از رده دوم، ممکن است در کل شبکه ایجاد پارازیت کند . یک نفوذگر از رده- laptop امکان دارد از کل شبکه استراق سمع کند، در صورتیکه یک گره معمولی فقط به محدوده کوچکی از شبکه دسترسی دارد . همچنین نفوذگرهای از رده- laptop ممکن است دارای پهنای باند زیاد و کانال های ارتباطی با تاخیر کم باشند در حالیکه گره های معمولی به این قابلیت ها دسترسی ندارند.

تفاوت دوم که می توان قائل شد، تفاوت بین نفوذگرهای داخلی و خارجی است . ما تا اینجا فقط درباره نفوذگرهای خارجی بحث کردیم، که این نفوذگره دسترسی خاص به شبکه ندارند . در مقابل یک نفوذگر داخلی، جزء معتبر ی از شبکه است که به بی راه می رود. حملات داخلی ممکن است بر اثر اجرای دستورات یک گره غیر مجاز ایجاد شود. و یا امکان دارد توسط نفوذگرانی که عناصر کلیدی، کد و داده یک گره مجاز را دزده اند ایجاد شود.

۳.۴.۳ اهداف امنیت

در یک دنیا ایده ال، ما مایل هستیم که محرمانگی، جامعیت، صحت و قابلیت دسترسی پیام ها در مقابل نفوذگران تضمین شود. هر گیرنده مطلوب باید همه پیام های را که برای او ارسال شده اند را دریافت کند و قادر باشد که درستی آنها را بررسی کند و فرستنده پیام را مشخص کند . نفوذگرها نباید قادر باشند تا محتوای پیام را حدس بزنند، حتی اگر، آنها در مسیریابی آن پیام شرکت کرده باشند

اگر چه این سوال باقی می ماند که آیا پروتکل های مسیریابی مسئولیت این کارها را به عهده دارند، یا بهتر اسن که این کارها بر عهده لایه های پایین تر باشد. در شبکه های اولیه و مرسوم، هدف اولیه و اصلی امنیت

www.markazdanesh.ir

در یک پروتکل مسیریابی تحویل قابل اطمینان پیام ها هست. حفاظت در برابر عدم پذیرش سرویس، صحت پیام، جامعیت و محرمانگی معمولا بوسیله یک مکانسیم انتها به انتها مانند SSH یا SSL بدست می آید.

اما موارد بالا درباره شبکه های حسگر بی سیم صادق نیست. در بسیاری از موارد، الگو ترافیک در این شبکه ها چند به یک است، گره های حسگر زیادی نیاز دارند تا داده های خوانده شده یا رویداده های شبکه را به ایستگاه پایه ارسال کنند. همانطوریکه در قسمت ۳ بحث شد، پردازش های داخل شبکه همانند تجمع داده ها، فشرده سازی داده ها یا ... نیاز دارند تا این عملیات را به گونه ای انجام دهند که انرژی را به شیوه کارآمدی مصرف کنند.

در حضور نفوذگرهای خارجی، مکانیزم های امنیتی لایه پیوند می توانند جامعیت، صحت و محرمانگی پیام ها را تضمین کنند بخاطر اینکه می تواند دسترسی خارجی به شبکه را نادیده بگیرد . اگر چه، ما هنوز باید برای قابلیت دسترسی پیام ها روی پروتکل های مسیریابی تکیه کنیم.

در حضور نفوذگر های داخلی، کارایی مکانیزم های امنیتی لایه پیوند به شدت کاهش می یابد. طبق تعریف، یک نفوذگر داخلی کسی یا چیزی است که به شبکه دسترسی مجاز دارد . امنیت لایه پیوند می تواند از دخالت گره های غیر مجاز بین پیام های ارسال شده جلوگیری کند، اما چنین گرهی دسترسی کاملی به پیام های خواهد داشت، که در طول مسیریابی از آن عبور خواهند کرد، و می توانند این پیام ه ا را تغییر، حذف، یا استراق سمع کند.

در نهایت، از دیدگاه ما، حفاظت در برابر تکرار بسته های داده نباید به عنوان یک هدف امنیتی در یک پروتکل مسیریابی امن در نظر گرفته شود . این وظیفه بهتر است توسط مکانیزم های امنیتی که در لایه کاربرد طراحی می شود، دفع شود . زیرا فقط برنامه کاربردی می تواند بطور کامل و صحیح این بسته ها را تشخیص دهد.

www.markazdanesh.ir

۳.۵ - حملات روی مسیریابی شبکه های حسگر

بسیاری از پروتکل های مسیریابی شبکه های حسگر خیلی ساده هستند، و به همین دلیل در اغلب موارد آنها مستعد حمله هستند. اغلب حملات بر علیه لایه شبکه به یکی از دلایل زیر رخ می دهد:

- استراق سمع، تغییر و تکرار اطلاعات مسیر یابی
- ارسال انتخابی
- حملات Sybil
- Wormhole ها
- حملات HELLO flood

در توضیحات زیر، به تفاوت بین حملاتی که سعی می کنند به طور مستقیم داده های کاربران را تغییر دهند و حملاتی که سعی می کنند تاثیرات اساس بر روی توپولوژی مسیریابی بگذارند توجه کنید.

۳.۵.۱- استراق سمع، تغییر، یا تکرار اطلاعات مسیریابی

رایجترین حمله مستقیم بر علیه یک پروتکل مسیریابی، هدف قرار دادن اطلاعات مسیریابی است که بین گره ها مبادله می شود. بوسیله استراق سمع، تغییر، یا تکرار اطلاع ات مسیریابی، نفوذگران می توانند حلقه های مسیریابی، ایجاد پیام های خطای اشتباه، تقسیم بندی شبکه، افزایش تاخیر انتها به انتها، افزایش یا کوتاه کردن مسیرهای منبع و ....

۳.۵.۲- ارسال انتخابی

شبکه های چند گام بر مبنای این فرض کار می کنند که گره های شرکت کننده میانی در مسیریابی، پیام های دریافت شده را به صورت کامل و دست نخورده به گره بعدی ارسال می کنند . در یک حمله ارسال انتخابی، گره های غیر مجاز ممکن است پیام های خاص را به گره بعدی ارسال نکنند و آنها را حذف کنند،

www.markazdanesh.ir

تا مطمئن شوند که این پیام ها در هر صورت اننشار نخ واهند یافت. یک شکل ساده از این حمله بدین صورت است که گزه غیر مجاز بعنوان یک سیاه چال عمل می کند و هر بسته ای را که به آن می رسد به گره بعدی ار سال نمی کند و آنرا حذف می کند. اگر یک نفوذگر از طرف گره های همسایه اش تهدید شود و نتیجه بگیرد که دارد از مسیر حذف می شود، تصمیم می گیرد که یک مسیر دیگر را جستجو کند . یک فرم خیلی زیرگانه از این حمله زمانی هست که یک نفوذگر بطور انتخابی بسته ها را ارسال می کند . یک نفوذگر تمایل دارد که بسته های نشات گرفته از تعداد گره های خاص را حذف یا تغییر دهد و بقیه بسته های را به شکل صحیح ارسال کند و با این کار باعث شود که بدگتنی و سوظن نسبت به کارهای غیر مجازش کاهش یابد.

حملات ارسال انتخابی معمولا زمانی خیلی موثر هستند که نفوذگر دقیقا روی یک مسیر از یک جریان داده قرار می گیرد. اگر چه، آن امکانپذیر است که یک نفوذگر، جریان عبوری از گره های همسایه را استراق سمع کند و با ایجاد پارازیت یا ایجاد تصادف باعث شود که عملی مانند ارسال انتخابی را شبیه سازی کند . بنابراین، ما اعتقاد داریم که یک نفوذگر اقدام به یک حمله ارسال انتخابی بکند یه طور حتم می خواهد و تلاش می کند که بر روی یک مسیری که جریان داده در آن جریان دارد قرار گیرد. در دو قسمت بعدی ما روی حملات sinkhole و Sybil بحث خواهیم کرد، دو مکامسیمی که یک نفوذگر می تواند به طور کارآمد خودش را روی جریان داده ای مورد نظر قرار دهید.

۳.۵.۳- حملات sinkhole

در یک حمله sinkhole، هدف نفوذگر ها تقریبا جذب همه ترافیک توسط یک گره است که از یک ناحیه سر چشمه می گیرند. بخاطر اینکه گره ها در نزدیگی یا روی مسیری قرار دارند که بسته ها از آن عبور می کنند، فرصت های زیادی وجود دارد که داده های برنامه ها در مرض دسترسی باشند. حملات sinkhole می توانند وسیله ای برای حملات دیگر (مانند ارسال انتخابی) با شند.

www.markazdanesh.ir

حملات sinkhole معمولا بوسیله یک گره که با توجه به الگوریتم مسیریابی نسبت به گره های دیگر جذاب تر است صورت می گیرد. برای نمونه، یک نفوذگر می تواند استراق سمع کند یا یک آگهی را برای یک مسیر با کیفیت تا ایستگاه پایه تکرار کند. بعضی از پروتکل ها ممکن است کیفیت یک مسیر را با اطلاعات انتها به انتها که شامل قابلیت اعتماد یا اطلاعات تاخیر است بررسی کنند. در این مورد، یک نفوذگر دسته laptop با یک فرستنده قوی می تواند یک مسیر با کیفیت بالا را ایجاد کند بوسیله ارسال با توان زیاد تا با یک گام به ایستگاه پایه برسد، یا با استفاده از یک حمله wormhole که در بخش زیر بحث می شود.

آن محتمل است که هر گره همسایه نفوذگر برای ارسال بسته هایش به یک ایستگاه پایه از طریق گره نفوذگر عمل کند. به طور موثر و کارا، نفوذگر یک منطقه نفوذ بزرگ ایحاد می کند، که همه ترافیکی را که به سوی ایستگاه پایه از تمام گره های که چندین گام تا گره غیر مجاز در جریان هستند را جذب می کند.

یک انگیزه برای انجام یک حمله sinkhole می تواند یک حمله ارسال انتخابی باشد. چون همه ترافیک مورد نظر از طریق یک گره جریان می یابد، یک نفوذگر می تواند بطور انتخابی بسته های را که از تمامی گره ها در یک منطقه خاص سر چشمه می گیرند را حذف یا دستکاری کنند.

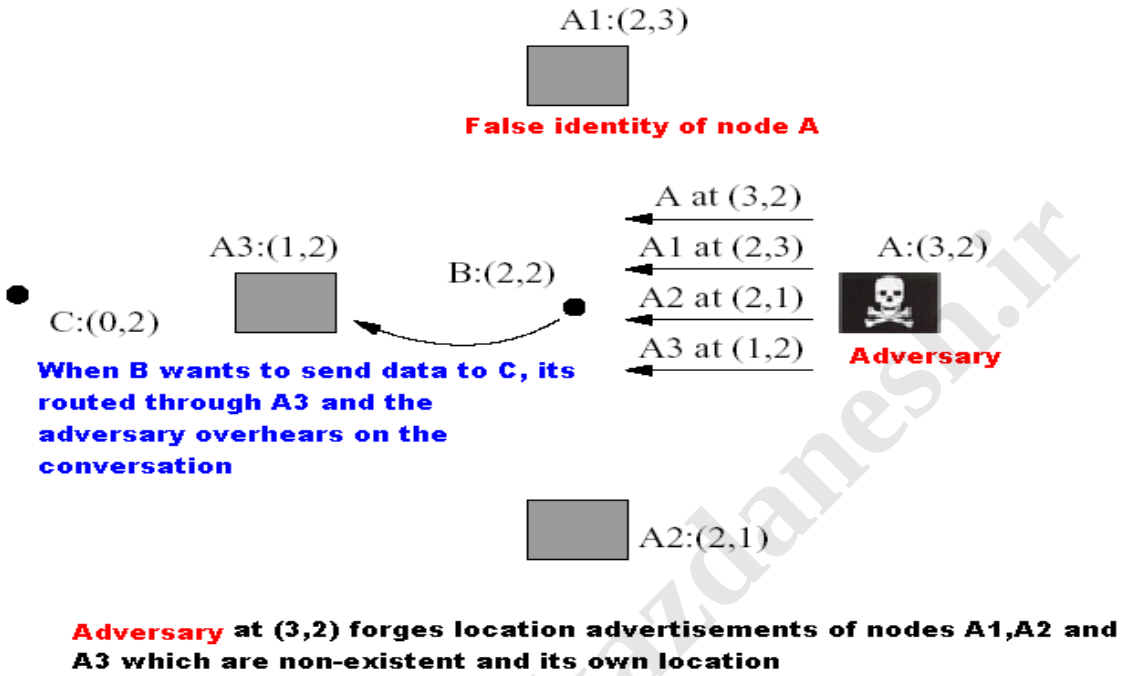
دلیلی که شبکه های بی سیم حسگر مستعد حملات sinkhole هستند به علت الگو های ارتباطی خاص آنها است. از آنجائیکه همه بسته ها مقصد نهایی مشابهی دارند (در شبکه های فقط با یک ایستگاه پایه)، یک گره غیر مجاز فقط نیاز دارد تنها یک مسیر با کیفیت بالا را تا ایستگاه پایه فراهم کند تا بتواند به همه گره ها نفوذ کند.

۳.۵.۴- حمله Sybil

در یک حمله sybil، یک گره منفرد آدرس های شناسایی مختلفی را به دیگر گره ها در شبکه ارائه می دهد. حمله Sybil می تواند سودمندهای از تحمل پذیری خطا مانند ذخیره سازی توزیع شده، انتشار و مسیریابی چند مسیری را کاهش دهد . همچنین حملات Sybil یک تهدید عمده برای پروتکل های مسیریابی جغرافیایی می باشد. مسیریابی مانند مسیریابی جغرافیایی اغلب نیاز دارند گره ها اطلاعات مختصاتی را با

www.markazdanesh.ir

همسایه هایشان مبادله می کنند تا بطور موثری مسیر را بطور جغرافیایی آدرس دهی کنند. یک گره در یک شبکه فقط دارای یک مختصات ثابت است، اما با استفاده از حملات Sybil یگ گره غیر مجاز می تواند در یک لحظه در بیش از یک مکان باشد.



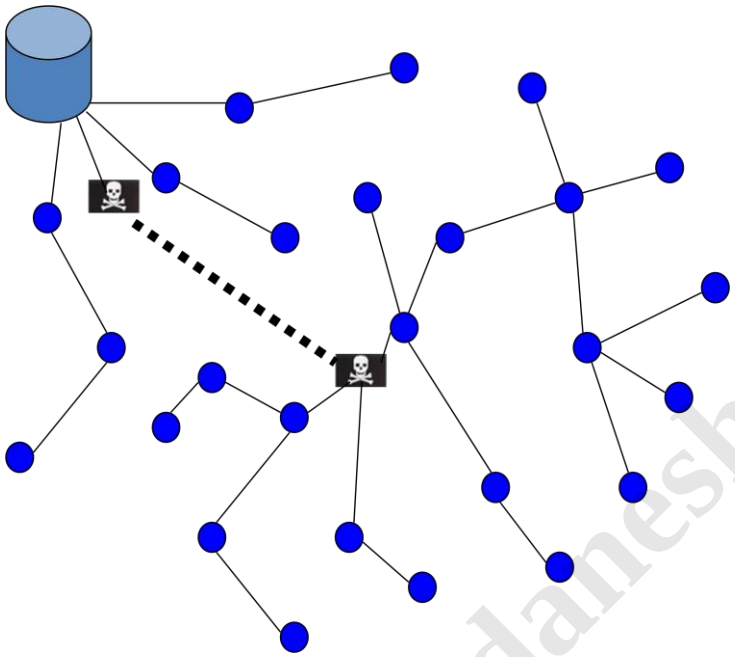
شکل ۳.۴- حمله Sybil

۳.۵.۵- Wormhole ها

در یک حمله wormhole، یک نفوذگر پیام های دریافت شده از یک قسمت از شبکه روی یک لینک با تاخیر کم را تونل می کند و آنها را در قسمت های دیگر تکرار می کند. برای اجرای یک حمله wormhole، یک نفوذگر دو نقطه دور از هم را در شبکه با استفاده از لینگ های ارتباطی کم تاخیر که پیوند wormhole نامیده می شود را به هم متصل می کند. زمانیکه این پیوند ایجاد یکی از گره ها، داده های انتقال داده شده

www.markazdanesh.ir

در آن قسمت را می گیرد و از طریق پیوند wormhole برای گرهی که در قمست دیگر قرار دارد تکرار می کند.



شکل ۳.۵- حمله Wormhole

یک نفوذگر که در نزدیگی ایستگا ه پایه قرار دارد ممکن است قادر باشد که کل مسیریابی را بوسیله ایجاد یک wormhole در مکان خوب مختل کند. یک نفوذگر می تواند به طور معمول گره های را که چندین گام از ایستگاه پایه فاصله دارند را متقاعد کنند که با استفاده از wormhole تنها یگ گام یا دوگام با ایستگـاه پایه دارند. از آنجائیکه نفوذگر با استفاده از پیوند wormhole یک مسیر با کیفیت تا ایستگاه پایه ایجاد می کند، همه ترافیک در آن ناحیه از طریق این پیوند جریان می یابد و به همین می تواند یک حمله sinkhole ایجاد کند. در شکل بالا یک نمونه از wormhole که بکار می رود تا یک sinkhole ایجاد کند.

حملات wormhole احتمال دارد که همراه با ارسال انتخابی یا استراق سمع به کار برود. تشخیص این حمله هنگامیکه در ترکیب با حمله Sybil به کار می رود بسیار مشکل است.

www.markazdanesh.ir

۳.۵.۶- حمله HELLOflood

ما یک حمله جدید بر علیه شبکه های حسگر معرفی می کنیم : HELLOflood. در بسیاری از پروتکل ها، گره ها نیاز دارند تا بسته های HELLO را پخش عمومی کند تا وجود خود را به گره های دیگر اعلام کند، و یک گره که چنین بسته ای را دریافت می کند تصور می کند که در محدوده رادیو یی گره فرستنده است. این تصور می تواند اشتباه باشد، یک نفوذگر از رده- laptop اطلاعات مسیریابی یا دیگر را با توان ارسالی زیاد پخش عمومی می کند و می تواند هر گره را در شبکه متقاعد کند که نفوذگر همسایه آن است

برای مثال، یک نفوذگر اعلان یک مسیر با کیفیت با لا را به ایستگاه پایه به همه گره های موجود در شبکه می کند و می تواند باعث شود که تعد زیادی از گره ها از این مسیر استفاده کنند، اما آن دسته از گره ها در فاصله خیلی دروی از نفوذگر قرار دارند بسته هایشان را از یک مسیر دیگر ارسال می کنند

یک نفوذگر ضرورتا نیاز نداردبه منظور استفاد از حمله HELLOflood قادر باشد ایجاد ترافیک مجاز کند . او به سادگی می تواند بسته های سر بار را با توان زیاد پخش عمومی مجدد کند تا بوسیله هر گره در شبکه در یافت شود.

توجه: "سیل آسا" معمولا برای انتشار یک پیام که قرار هست توسط همه گره ه ا در یک توپولوژی چند گام دریافت شود استفاده می شود. در حالیکه در حمله HELLOflood از یک پخش عمومی یک گام بر انتقال یک پیام به تعداد زیادی از گیرنده ها استفاده می شود.

www.markazdanesh.ir

Acknowledgement spoofing –۳.۵.۷

الگوریتم های مسیریابی مختلف روی دانش صریح یا ضمنی بر روی لایه پیوند کار می کنند . به علت ذات رسانه پخش عمومی، یک نفوذگر می تواند اطلاعات لایه پیوند را استراق سمع کند تا از آن برای آدرس دهی بسته های سر بار به مقصد گره های همسایه استفاده کند.

اهدفی که در این حمله مد نظر است عبارتند از اینکه یک فرستنده یک پیوند ضعیف را پیوند قوی تصور کند یا یک گره غیر فعال را فعال فرض کند و یا بطور برعکس. در این صورت بسته های که به یک گره غیر فعال ارسال می شوند، از بین می روند و کم می شوند . از این روش نیز می توا ن برای ارسال انتخابی نیز استفاده کرد، بدین صورتیکه بسته های که از گره های خاص ارسال می شوند از طریق یک گره غیر فعال انتقال داده شوند که با این کار باعث حذف بسته خواهد شد.

۳.۶- حملات روی پروتکل های خاص شبکه های بی سیم حسگر

همه پروتکل های مسیریابی شبکه های حسگر به شدت مستعد حمله و نفوذ هستند . نفوذ گران می توانند جریان ترافیک را جذب یا دفع کنند، تاخیر را افزایش دهند، یا با کارهای کوچکی مانند ارسال یک بسته باعث غیر فعال شدن کل شبکه شوند. در این قسمت، ما پروتکل های مسیریابی شبکه های حسگر را معرفی خواهیم کرد و بر روی حملات مربوط به هر پرتوکل تمر کز خواهیم کرد.

۳.۷ – ارسال با حداقل هزینه

ارسال با حداقل هزینه، یک الگوریتم کارا برای ازسال بسته ها از گره های حسگر به ایستگاه پایه با ویژگهای مفید است. ویژگیهای مفیدی مانند اینکه این گره ها نیاز ندارند تا مسیر دقیق اطلا عات را نگهداری کنند. آن بوسیله ساختن یک فیلد هزینه، کار می کند . هرینه ایستگاه پایه برابر صفر است . و گره های دیگر حداقلی هزینه ای را که نیاز دارند، تا به ایستگاه پایه برسند، را نگهداری می کنند . هزینه می تواند مواردی مانند، تعداد گام ها، انرژی، تاخیر و ... باشند.

در ابندا هزینه هر گره به غیر از ایستگاه پایه را بی نهایت در نظر گرفته می شود . مقدار هزینه بوسیله امواج رادیویی که به صورت سیل آسا از طرف ایستگاه پایه ارسال می شود، ساخته می شود . این امواج، هزینه

ایستگاه پایه را که صفر است اعلان می کنند و آنرا از طریق شبکه پخش می کنند. به محضی اینکه گره N، یک اعلان را از گره M دریافت می کند، گره Nمی داند که هزینه آن از طریق گره M برابر است با: $C_M + L_{N,M}$. سپس گره N هزینه فعلی خود را C_N را با $C_M + L_{N,M}$ مقایسه می کند. اگر مقدار جدید از مقدار قبلی کوچکتر باشد، آنگاه گره N مقدار قبلی را با مقدار جدید جایگزین می کند و مقدار هزینه جدید خود را توسط یک پیام پخش عمومی دیگر به گره های دیگر اعلان می کند تا دیگر گره ها در صورت نیاز هزینه خود را بروز رسانی کنند.

حملات:

ارسال با حداقل هزینه بشدت مستعد حملات sinkhole است. یک نفوذگر از رده-mote می تواند یک حمله sinkhole وسیع را توسط اعلان یک هزینه صفر از هر جای از شبکه ایجاد کند. بهینه سازی که در بالا شرح داده شد ممکن باعث سردرگمی شدید شود هنگامیکه یک هزینه کمتری را دریافت می کنند نسبت به آنکه قبلا فکر می کرد بهینه است.

با استفاده از یک حمله HELLO flood، یک نفوذگر رده-laptop می تواند کل شبکه را به وسیله ارسال یک پیام با هزینه صفر و به اندازه کافی قدرتمند که بتواند توسط کل گره های شبکه دریافت شود، غیر فعال کند. تصور کنید یک نفوذگر می تواند

یک پیام با مقدار هزینه نزدیگ به میانگین هزینه پیوند بین دو گره همسایه را اعلان کند، آن محتمل است که هزینه همه گره ها در شبکه کاهش خواهد یافت . هنگامیکه یک گره پیام بعدی را به سوی ایستگاه پایه ارسال می کند، یک گره همسایه به یک هزینه نزدیگ به صفر نیاز دارد تا مسئولیت ارسال بسته را برای ایستگاه پایه بر عهده بگیرید. این ممکن می سازد که نفوذگر تنها مقصد همه پیام های باشد.

۳.۸ - اقدامات متقابل

۳.۸.۱- حملات خارجی و عملیات لایه پیوند

www.markazdanesh.ir

عمده حملات خارجی در برابر پروتکل های مسیریابی شبکه های حسگر را می توان با استفاده از رمز گذاری لایه پیوند و استفاده از کلید عمومی مشترک در هم شکست. حملیه Sybil ارتباطی زیادی با این لایه ندارد. زیرا گره ها تمایلی برای دریافت حتی یک شناسه تنها از نفوذگرها ندارند . اکثر حملاتی از نوع sinkhole و ارسال انتخابی امکانپذیر نیست، بخاطر اینکه نفوذگر از اتصال به توپولوژی بازدا شته می شود. صحت لایه پیوند می تواند، تصدیق شود. عمده حملاتی که می تواند از مکانیزم های دفاعی این لایه عبور کند، حملات wormhole و HELLO flood می باشد. اگر چه از اتصال نفوذگر به شبکه جلوگیری می شود، اما هیچ چیزی نمی تواند او را از استفاده از پیوند wromhole باز دارد.

لایه پیوند داده ها هیچ مکانیزم دفاعی در مورد حملات که بر علیه TinyOS beaconing که در قمست ۷.۱ توضیح داده شد، می شود ندارد. اگر یک wormhole ایجاد شود رمز گذازی هیچ ارزشی ندارد، زمانیکه یک نفوذگر همانند یک سیاه چال عمل می کند.

مکانیزم استفاده از کلید عمومی مشترک در لایه پیوند داده در مواردیکه حملات داخلی وجود دارد بی فایده می باشد . نفوذگر ها می توانند از طریق استراق سمع یا ترزیق اطلاعات اشتباه مسیریابی، ایجاد sinkhole،HELLO flood و استفاده از ارسال انتخابی توسط حمله Sybil به شبکه حمله کند.

۳.۸.۲- حمله Sybil

از فعالیت یک گره داخلی و خودی در شبکه نمی توان جلوگیری کرد، اما او فقط باید قادر باشد با استفاده از شناسه گره ها کارهایش را انجام دهد . استفاده از یک کلید عمومی مشترک اجازه می دهد یک گره داخلی خودش را به عنوان هر گره دیگر جا بزند، پس شناسه ها باید بررسی شوند. در موارد معمول و فدیمی، اینکار با استفاده از رمزگذاری کلید عمومی صورت می گیرد. اما تولید و بررسی امضا دبجیتال فراتر از قابلیت های گره های حسگر است.

یک راه حل اینست که هر گره یک کلید متقارن منحصر بفرد با یک ایستگاه پایه قابل اعتماد داشته با شد. دو گره می توانند سپس از Needham–Schroeder استفاده کنندتا هر شناسه دیگر را بررسی کنند و یک

کلید عمومی مشترک ایجاد کنند . یک جفت از همسایه ها می توانند از کلید بدست آمده استفاده کنند تا یک پیوند رمز گذاری شده و تصدیق هویت شده را ایجاد کنند.

بنابراین یک گره محدودیت دارد که فقط با گره های همسایه اش که تصدیق هویت شده اند ارتباط برقرار کند. این صحیح نیست که بگویم گره ها مجاز نیستند تا پیام هایشان را به ایستگاه پایه ارسال کنند، اما آنها محدود هستند با گره های تصدیق هئیت شده ارتباط برقرار کنند و از طریق آنها کار هایشان را انجام دهند. علاوه بر اینها، یک نفوذگر می تواند هنوز از یک wormhole استفاده کند تا پیوندی مصنوعی بین دو گره ایجاد کند، تا آنها را نتقاعد کند که آنها باهم همسایه هستند . اما نفوذگر قادر نخواهد بود استراق سمع کند یا هر ویژگی ارتباطی را بین آنها تغییر دهد.

۳.۸.۳- حملات HELLO flood

ساده ترین دفاع در برابر حمله HELLO flood، بررسی یک پیوند در هر دو سو است قبل از اینکه یک عمل معنا دار روی یک پیام دریافت شده از یک پیوند انجام بدهد. اگرچه، این اقدام متقابل هنگامیکه یک نفوذگر یک گیرنده قوی همانندفرستنده قویش داشته باشد، کارایی خود را از دست می دهد . به این طریق یک نفوذگر می تواند بطور کارا یک wormhole را ایجاد کند. از آنجائیکه پیوند بین این گره ها و نفوذگر دو طرفه است، روش بالا بعید است که قادر باشد یک HELLO flood را تشخیص دهد و در مقابل آن مقاومت کند.

یک راه حل ممکن برای این مسئله می تواند به این صورت باشدکه هر گره، همسایه هایش را با یک پروتکل تصدیق شناسه که از یک ایستگاه پایه امن، تصدیق هویت کند . اگر پروتکل پیام های را در هر دو جهت پیوند بین گره ها بفرستد، HELLO flood هنگامیکه نفوذگر یک فرستنده قوی دارد می تواند دفع شود، بخاطر اینکه پروتکل پیوند را در هر دو جهت بررسی می کند.

www.markazdanesh.ir

۳.۸.۴- حملات wormhole و sinkhole

دفاع در برابر حملات wormhole و sinkhole بسیار سخت است، بخصوص زمانیکه این دو حمله در تر کیب با یکدیگر استفاده شوند. کشف حملات wormhole به سختی می تواند صورت گیرد، زیرا آنها از یک کانال خصوصی و خارج از باند است و برای شبکه حسگر غیر قابل تشخیص است . دفاع در برابرحملات sinkhole زمانی دشوار است که از پروتکل های که از اعلان اطلاعاتی مانند انرژی باقیمانده یا تخمین یک قابلیت اعتماد انتها به انته ا که توسط پروتکل مسیریابی ایجاد می شود، استفاده می کنند، زیرا این اطلاعات به سختی می توانند از نظر صحت و درستی بررسی شوند. مسیر های که تعداد گام را تا ایستگاه پایه به حداقل می رسانند می توانند به سادگی بررسی شوند، اگر چه تعدا گام می تواند به طور کامل توسط یک wormhole، اشتباه محاسبه شود.

یک wormhole هنگامیکه برای ایجاد sinkhole ها یا پیوندهای مصنوعی که ترافیک را جذب می کنند، بسیار کارآمد است . پیوندهای مصنوعی به آسانی در پروتکل های مسیریابی جغرافیایی قابل تشخیص هستند، زیرا گره های همسایه به فاصله بین خودشان بیشتر از محدوده رادیویی توجه دارند.

۳.۸.۵- استفاده از دانش سراسری

یک چالش عمده در شبکه های حسگر بزرگ امن، ذات خود سازمانده و غیر متمرکز آنها است . هنگامیکه اندازه شبکه محدود هست، یا توپولوژی خوش ساخت یا کنترل شده باشد، دانش سراسری می تواند به عنوان یک مکانیزم امنیتی استفاده شود . یک شبکه نسبتا کوچک با تعداد صد گره یا کمتر را تصور کنید. اگر بتوانیم فرض کنیم که هیچ گره غیر مجازی در مرحله توسعه وجود ندارد، و سپس بعد از اینکه توپولوژی اولیه شکل گرفت، هر گره می تواند اطلاعات را به همسایه هایش ارسال کند و مکان جغرافیایی خود را به ایستگاه پایه ارسال می کند. با استفاده از این اطلاعات، ایستگاه پایه می تواند توپولوژی کل شبکه را ترسیم کند. دلیل تغییر توپولوژی به علت تداخلات رادیویی یا خطای گره می باشد، گره ها بصورت دوره ای یا اطلاعات مناسب یک ایستگاه پایه را بروزرسانی می کنند، و باعث می شوند که ایستگاه پایه توپولوژی شبکه را بطور صحیح ترسیم کند. ما بحث کردیم که چرا مسیریابی جغرافیایی می تواند نسبتا در برابر حملات

www.markazdanesh.ir

wormhole، sinkhole و Sybil مقاوم باشد، اما مسئله اصلی باقیمانده این است که اطلاعات مکانی که همسایه ها باید اعلان کنند، باید قابل اعتماد باشد . انتخاب احتمالی یک گام بعدی، از مقاص د قابل قبول مختلف با مسیریابی چند مسیری به چندین ایستگاه پایه می تواند ما را در این حا این مسئله کمک کند

۳.۸.۶- پخش عمومی تصدیق هویت شده و flooding

از آنجائیکه ایستگاه امن و قابل اعتماد هست، خیچ نفوذگر نباید قادر باشد تا پیام های پخش عمومی را که از ایستگاه پایه ارسال می شوند رااستراق سمع کند . این نیاز به رده های از عدم تقارن دارد : بدلیل اینکه از هر گره در شبکه می توان سوء استفاده کرد، هیچ گرهی نباید قادر باشد از ایستگاه پایه استراق سمع کند، با اینحال هر گره باید قادر باشد آنها را بررسی کند. پخش عمومی تصدیق هویت شده برای تعاملات محلی نیز می تواند مفید باشد. بسیاری از پروتکل ها نیاز دارند تا پیام های HELLO را برای همسایه ها یشان پخش عمومی کنند. این پیام باید باید تصدیق هویت شوند و در استراق سمع از آنها غیر ممکن باشد.

μTESLA یک پروتکل برای پخش عمومی تصدیق هو یت شده و کارا و flooding است که فقط از رمزگذاری کلید متقارن استفاده می کند و به حداقل سر بار نیاز دارد

خلاصه اقدامات متقابل

رمزگذاری و تصدیق هویت لایه پیوند، مسیریابی چند مسیر، اعتبار سنجی شناسه، اعتیار سنجی پیوند دو طرفه و پخش همگانی تصدیق هویت شده می تواند پروتکل های مسیریابی را در در برابر بیگانه ها، اطلاعات مسیریابی جعلی، حملات Sybil، HELLO flood ها و استراق سمع اطلاعات محافظت کند و امکان آن وجود دارد که که پروتکل های موجود را به این مکانیزم ها مجهز کنیم

حملات Sinkhole و wormhole چالش های اساسی را برای طراحی پروتکل های مسیریابی مطرح می کنند، و بعید است مکانیزم های دفاعی در مقابل این حملات بعد از اتمام طراحی پروتکل مسیریابی وجود داشته باشد. طراحی پروتکل های برای غلبه بر این دو حمله کار، مشکلی است. اما با پروتکل های مانند مسیریابی جغرافیایی می توان امیدی به غلبه بر این حملات داشت.

www.markazdanesh.ir

نتیجه گیری :

همانگونه که در فصل های قبل ذکر شده ، یکی از مهمترین ماسئل در شبکه های حسگر ، استقاده بهینه از منابع موجود در شبکه است ؛ چون معمولا در چنین شبکه هایی ، با تمام شدن منابع انرژی یک گره ، آن گره از از چرخه کار شبکه حذف می شود و معمولا تعویض کردن منبع انرژی و استفاده مجدد از یک گره ، که منبع انرژی آن به پایان رسیده است ، مقرون به صرفه یا در مواردی مقدور نیست و به جای چنین کاری ، گره های جدیدی در شبکه جایگزین می شود ؛ پس با صرفه جویی در مصرف انرژی د ر هر گره می توان به طور قابل ملاحظه ای هزینه نگهداری شبکه را کاهش داد.

همانطور که می دانیم ، عمده انرژی که یک گره حسگر استفاده می کند، صرف تبادل اطلاعات بین آن گره با سایر گره ها می شود وارتباطات رادیویی بیشترین هزینه انرژی را برای گره ها دربر دارد . بر اساس یک آزمایش بدست آمده ، ثابت شده است که انتقال یک بیت در یک شبکه حسگر در طول صد گره ، تقریبا معادل با ۳۰۰۰ دستورالعمل اجرا شده در هر گره از لحاظ انرژی هزینه دارد . به همین دلیل تاکنون روشهای زیادی در جهت کاهش سربار ترافیکی گره ها ارائه شده است و بر روی م واردی همچون متراکم سازی و فشرده سازی اطلاعات ، رویکردهای زیادی ارائه شده است.

یکی از ساده ترین روشها در انتقال اطلاعات در شبکه های حسگر بیسیم ، روشهای پایه ریزی شده بر اساس روش همه پخشی سیل آسا است که ساده ترین آنها ، خود روش سیل آسا می باشد . روشهای دیگری نیز به منظور بهبود دادن عملکرد روش سیل آسا ارائه شده اند که هر یک ب ه نحوی ، سعی در بر طرف کردن یک یا چند از نقاط ضعف این الگوریتم را دارند . مثلا روش انتشار شایعه پراکن ، به منظور کاهش دادن مشکل تصادم در الگوریتم سیل آسا ، به جای ارسال یک نسخه کپی از داد ه ها یه تمامی همسایگان یک گره ، این کار را تنها برای یک گره همسایه که به صورت تصادفی انتخاب شده انجام می دهد . این روش اگر چه تا حدی مشکل تصادم را برطرف میکند ولی سرعت انتشار را پایین می اورد که ممکن است به میزانی پایین تر از حداقل سرعت قابل قبول برسد . به صورت کلی هر روشی که بر مبنای روش پخش سیل آسا پایه ریزی شده باشد ، با استفاده از انرژی تمامی گره ها ، بزودی منابع تمامی شبکه را مورد مصرف قرار می دهد و بنابراین برای استفاده در شبکه های حسگر بیسیم مناسب نمیباشد .

www.markazdanesh.ir

دسته دیگر از الگوریتمهای مطرح شده سعی برآن دارند که به کمک نامگذاری اطلاعات با استفاده از خصوصیات آنها ، قبل از ارسال اطلاعات ، اطمینان ۱یدا میکنند که گیرنده داده های ارسالی را در اختیار ندارند . دو دسته از روشهای مطرح شده در این زمینه الگوریتم های SPIN و انتشار مستقیم هستند که در الگوریتم SPIN برا ی نامگذاری داده ها از شبه- داده ها استفاده میشود و در الگوریتم انتشار مستقیم ، از زوج های صفت – مقدار جهت نامگذاری داده ها استفاده می شود .

در الگوریتم انتشار مستقیم ، بر خلاف روش SPIN ، داده ها به صورت جهت دار منتشر می شوند و همچنین هر گره به محتویات داده ارسالی دسترسی دارد و می تواند به ترکیب و خلاصه سازی اطلاعات جمع آوری شده به صورت محلی ، از حجم سربار ترافیکی شبکه تا میزان نسبتا بالایی بکاهد . الگوریتم انتشار مستقیم یک روش گیرنده – محور است چون در این روش ابتدا اطلاعات مورد نیاز در قالب یک بسته علاقه من دی در طول سطح شبکه منتشر می شود و گیرنده هایی که داده مورد نظر را در اختیار داشته باشند ، با دریافت مشخصات اطلاعات مورد نیاز ، آنها را از طریق مسیرهایی که از قبل در هنگام ارسال علاقه مندی تشکیل شده است ، ارسال میکنند .

یکی از مواردی که در زمینه بهبود عملکر د الگوریتم های مطرح شده جهت انتشار اطلاعات در شبکه های حسگر می توان در نظر گرفت ، این است که پدیده های مشاهده شده توسط شبکه های حسگر اغلب پدیده های طبیعی هستند که سرعت تغییرات نسبتا کندی دارند . ما می توانیم از این واقعیت برای فشرده سازی موثر اطلاعات استف اده کنیم ؛ به این صورت که جهت کاهش ترافیک بین منبع و گیرنده ها در شبکه می توان داده ها را در نقطه ای نزدیک منابع جمع آوری و خلاصه کرد و سپس نتایج بازه زمانی مشاهد شده را در قالب یک پیغام ، از گره جمع آوری کننده اطلاعات به گیرنده ارسال کرد که این عمل تاثیر قابل توجهی بر کاهش ترافیک عبوری در شبکه خواهد داشت .

www.markazdanesh.ir

منابع :

۱ – نصیری اقبالی ، آرش ، روشهای نشر اطلاعات در شبکه حسگر بیسیم ، سمینار ارشد دانشگاه صنعتی امیر کبیر .

۲ – www.atalebi.com

۳ – www.ccw.ir

۴ – www.forum.wslab.ir

۵ – www.itna.ir

۶ – www.parsbook.org

۷ – www.tebyan.net

۸ – www.wikipedia.com

www.markazdanesh.ir