فهرست مطالب

عنوان **شماره صفحه**

فهرست اشکال

عنوان **شماره صفحه**

فهرست جداول

عنوان **شماره صفحه**

فصل ۱ : مقدمه

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم و همچنین فن‌آوری ساخت مدارات مجتمع در اندازه‌های کوچک از یک سو و توسعه فناوری ارتباطات بی‌سیم از سوی دیگر توانایی طراحی و ساخت سنسورهای گوناگونی را داده است که با توان مصرف پایین و اندازه کوچک، از قیمت مناسب وکاربرد های گوناگونیبرخوردار هستند.این سنسورهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی (بر اساس نوع سنسور)، پردازش و ارسال آن اطلاعات را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های سنسوری بی‌سیم[1] شده‌اند.

شبکه‌های سنسور بی‌سیم شامل صدها یا هزاران گره‌ی سنسور هستند که قابلیت‌های حس کردن داده، برقراری ارتباط و محاسبات را دارند. هر گره توانایی حس کردن عناصر محیط خودش را دارد، محاسبات ساده ای را انجام می‌دهد و بهطور مستقیم یا از طریق گره‌های مجاور خود، با ایستگاه پایه ارتباط برقرار می‌کند و از این طریق داده-های جمع‌آوری شده را در اختیار آن قرار می‌دهد.

شبکه‌های سنسوری، شبکه‌های توزیع شده‌ای هستند که سنسورها در آن مجهز به پردازشگر، حافظه و ارتباطات بی‌سیم برد کوتاه می‌باشند. تفاوتآن‌ها با سایر ارتباطات در محدودیت‌های مصرف انرژی، پهنای باند و ازدیاد گره‌های سنسوری است و معمولاً در مناطقی که دسترسی، آسان یا لازم نباشد کاربرد دارد. وجوه مختلف این شبکه‌ها، از قبیل مسیریابی داده به مقصد، مصرف بهینه انرژی و طول عمر شبکه، در مقالات مختلف مورد بررسی قرار گرفته-است. امروزه در بسیاری از ساختمان‌ها و محیط‌های گسترده، مجموعه‌ای از گره‌های سنسوری که وظیفه جمع‌آوری، پردازش و انتقال داده‌ها را به عهده دارند وجود دارد، که این سنسورها با همدیگر تشکیل یک شبکه سنسوری را می‌دهند. این شبکه‌ها برای برنامه‌های کاربردی، نظامی و پزشکی، کشاورزی و... موثر هستند. بعضی موارد استفاده از

[1]Wireless Sensor Networks

این سنسورها عبارتست از: کنترل ربات، هدایت اتوماتیک، ردیابی هدف، گزارش وضعیت آب و هـوایی، محاسـبات توزیع شده، امنیت مکان‌های حساس ومهم مثل موزه‌ها، جبهه جنگ و... .

در اکثر کاربردهای مذکور، امنیت بسیار حائز اهمیت می‌باشد، زیرا به دلیل ساختار ساده، این شبکه‌ها به راحتـی مورد حمله قرار می‌گیرند؛ لذا باید پروتکل‌های موجود برای این شبکه‌ها را با استفاده از روش‌هایی مانند رمزنگـاری، امن نمود.

در این پایان‌نامه ابتدا در فصول یک و دو بـه توضـیح شـبکه‌هـای سنسـوری بـی‌سـیم، تاریخچـه، کاربردهـا و محدودیت‌های این شبکه‌ها پرداخته شده است. سپس در فصل سه با بیان پشته پروتکلی و اهمیت مسیریابی در ایـن شبکه‌ها، انواع پروتکل‌هایمسیریابیشبکه‌هایسنسوریبی‌سیممعرفی گردیده‌اند. در فصل چهار حملات روی مسیریابی به طور کامل توضیح داده شده است و در فصل پنج، پروتکل مسیریابی سلسله مراتبی LEACH را به همراه شبیه‌سازی بررسی می‌شود و در انتهای این فصل آسیب‌های امنیتی این پروتکل بیان خواهد شد. در فصـل شـش توضـیح کامـل پروتکل‌های مسیریابی امن مبتنی بر LEACH آورده شده است و سپس در فصل هفـت تحلیـل ایـن پروتکـل‌هـا از لحاظ امنیت و کارایی در شبکه بررسی می‌شوند. در انتها در فصل هشت جمع‌بندی، نتیجه‌گیری و پیشـنهادات آورده شده‌اند.

فصل ۲ : شبکه‌های سنسوری بی‌سیم

۲-۱- تاریخچه شبکه‌های سنسوری

تاریخچه این شبکه‌ها از اوایل دهه ۸۰ شروع می‌شود که در قالب سه نسل می‌باشد که به اختصار توضیح می‌دهیم.[۱]

- کاربرد شبکه‌های سنسوری در آمریکا در زمان جنگ سرد جهت نظارت زیر دریایی بوده است که هنوز از سنسورهای آن جهت مانیتور کردن ارتعاشات در زیر اقیانوس‌ها استفاده می‌شود.
- مرحله تحقیقات شبکه‌های سنسوری در دهه ۱۹۸۰ با عنوان DSN[1] شروع شد.
- گسترش یافتن کاربردهای نظامی در دهه ۱۹۸۰ و ۱۹۹۰ که نسل اول محصولات تجاری نامیده شد.
- مرحله تحقیقات در زمینه شبکه‌های سنسوری بی‌سیم از اواخر دهه ۱۹۹۰ که نسل دوم نامیده شد.در این زمان با به وجود آمدن تکنولوژی‌های MEMS[2] و NEMS[3]ابعاد سنسورها بسیار کاهش یافت. همچنین با پیشرفت تکنولوژی بی‌سیم و ایجاد استانداردهایی از جمله IEEE80.11 a/b/g وسیستم‌های بی‌سیم مانند Bluetooth ، ZigBee و Wimaxشبکه‌های سنسوری در قالببی‌سیم کاربرد پیدا کردند. با به‌وجود آمدن فن‌آوری نانو می‌توان آن را علت ظهور نسل سوم شبکه‌های سنسوری نامید.

در جدول (۲-۱) به مقایسه سه نسل بر اساس چند پارامتر پرداخته شده است:

[1]Distributed Sensor Network
[2]Micro Electronic Mechanical System
[3]Nano Electronic Mechaniccal System

جدول (۲-۱) : مقایسه نسل‌های شبکه‌های سنسوری بی‌سیم

	نسل اول(۱۹۸۰-۱۹۹۰)	نسل دوم (اوایل دهه۲۰۰۰)	نسل سوم(اواخر دهه ۲۰۰۰)
اندازه	کیف دستی یا بزرگ‌تر	اندازه یک کتاب یا کوچک‌تر	خیلی کوچک به اندازه یک شن
وزن	چندین پوند	چند اونس-قابل حمل به راحتی	کمتر از گرم و یا تکنولوژی نانو
منبع تغذیه	باتری‌های بزرگ خط برق	باتری‌های AA	روش نوری و یا با تکنولوژی نانو
طول عمر	چند ساعت تا چند روز یا بیشتر	چند روز تا چند هفته	چند ماه تا چند سال

۲-۲- کاربردهای شبکه‌های سنسوری بی‌سیم

در این بخش مواردی از کاربردهای اصلی شبکه‌های سنسوری بی‌سیم معرفی خواهد شد.[۱]

کاربردهای نظامی:

- آگاهی یافتن از نیروهای دشمن در منطقه
- آگاهی یافتن از تجهیزات نظامی
- نظارت جبهه جنگ
- تشخیص حمله شیمیایی، بیولوژی یا هسته‌ای
- و ...

کاربردهای محیطی:

- بررسی آب‌وهوای منطقه
- تشخیص آتش‌سوزی در جنگل
- تشخیص سیل
- کشاورزی دقیق
- و ...

کاربردهای پزشکی:

- بررسی اطلاعات فیزیولوژیکی بیمار به‌صورت کنترل از راه دور
- پیگیری و آگاهی یافتن از موقعیت پزشکان و بیماران در بیمارستان
- مواظبت از سالخوردگان
- و ...

کاربردهای تجاری:

- کنترل محیطی در صنعت و یا ساختمان‌های اداری
- تشخیص و پیگیری وسایل نقلیه
- نظارت بر حجم ترافیک
- و ...

۲-۳- اصطلاحات در شبکه سنسوری بی‌سیم:

- گره سنسوری[1] : عبارتست از قطعه‌ای که شامل سنسور، پردازنده، فرستنده-گیرنده و باتری می‌باشد.
- ایستگاه پایه[2]: به مکانی گفته می‌شود که داده‌های کل شبکه به آنجا ارسال می‌گردد و کاربر به آن دسترسی دارد. معمولاً در شبکه سنسوری یک ایستگاه پایه وجود دارد و محدودیت‌هایی از قبیل محدودیت انرژی یا پهنای باند ندارد. در بعضی مقالات به ایستگاه پایه، سینک (sink) نیز می‌گویند.

[1] Sensor Node
[2] Base Station (BS)

- بسته[1] : داده اندازه‌گیری شده توسط گره‌ها به همراه اطلاعاتی مانند شناسه گره، که به ایستگاه پایه ارسال می‌شود، بسته نامیده می‌شود

۲-۴- وظایف گره‌ها

گره‌های سنسوری سه وظیفه اصلی را به عهده دارند که عبارتند از :

- حس کردن[2] : شناسایی تغییرات محیط .
- ارتباطات[3] : هدایت کردن اطلاعات از مبدأ به مقصد
- محاسبات [4] : پردازش، فشرده‌سازی و تجمیع داده

۲-۵- محدودیت‌های شبکه‌های سنسوری بی‌سیم

این شبکه‌ها چندین محدودیت دارند که باید به هنگام طراحی هر پروتکل برای آن‌ها مورد توجه قرار بگیرند. بعضی از این محدودیت‌ها عبارتند از :

- منبع انرژی محدود : شبکه‌های سنسوری منبع انرژی محدودی مانند باتری، دارند بنابراین حفظ انرژی در طول ارتباطات لازم و ضروری است.
- محاسبه محدود : گره‌های سنسوری قدرت محاسباتی محدودی دارند به طوری‌که شبکه نمی‌تواند یک پروتکل پیچیده و سطح بالا را اجرا کند.
- ارتباطات : پهنای باند رادیویی گره‌های سنسوری محدود است بنابراین ارتباطات را محدود می‌کند.

۲-۶- معیارهای طراحی

قبل از طراحی شبکه‌های سنسوری بی‌سیم باید معیارهایی در نظر گرفته شود که عبارتند از[۲]:

۲-۶-۱- پویایی شبکه[5]

بسته به کاربرد شبکه‌های سنسوری، شبکه می‌تواند ایستا یا پویا باشد. به طور مثال،در یک برنامه کاربردی شناسایی-ردیابی هدف، واقعه پویا است.در حالی که نظارت جنگل برای جلوگیری از آتش سوزی مثالی از یک واقعه ایستا است.

[1]Packet
[2] Sensing
[3] Communication
[4] Computation
[5] Network Dynamics

۲-۶-۲- گسترش گره[1] در شبکه

در موقعیت‌های قطعی و مشخص سنسورها به طور دستی قرار داده می‌شوند و داده در امتداد مسیرهای از پیش تعیین شده مسیریابی می‌شود. روش دیگر گسترش گره‌های سنسوری،گسترش تصادفی استکه معمولاً توسط بال‌گرد در منطقه پراکنده می‌شوند.

۲-۶-۳- ملاحظات انرژی[2]

مسیری که بسته از آن می‌گذرد بسیار مهم است زیرا اگر از ایستگاه پایه خیلی دور باشد ارسال مستقیم بسته، کار درستی نیست زیرا فرستنده آن توان زیادی مصرف می‌کند؛ لذا باید از روش‌های چندگامه سود جست یعنی ارسال دست به دست بسته از گره مبدأ به سینک توسط دیگر گره‌های شبکه.

۲-۶-۴- روش‌های تحویل داده[3]

با توجه به برنامه کاربردی شبکه سنسور، روش تحویل داده به ایستگاه پایه می‌تواند پیوسته، واقعه گرا، مبنی بر درخواست یا ترکیبی باشد.

۲-۶-۵- تجمیع / ترکیب داده[4]

هنگامی‌که گره‌های سنسوری داده افزونه تولید می‌کنند یا بسته‌هایی که از چندین گره جمع‌آوری شده‌اند، تعداد انتقالات باید کاهش یابد. تجمیع و ترکیب داده‌ها از چندین منبع مختلف با استفاده از توابعی مثل ماکزیمم،مینیمم و متوسط است. این تکنیک می‌تواند برای بدست آوردن کارایی انرژی و بهینه سازی ترافیک در تعدادی از پروتکل-های مسیریابی به کار برده شود.

۲-۶-۶- ناهمگن بودن[5]

در بسیاری ازمطالعات فرض شده که همه گره‌ها همگن هستند. با توجه به نوع برنامه کاربردی گره‌ها می‌توانند نقش‌ها و توانایی‌های مختلف داشته باشند و ناهمگن باشند. به عنوان مثال بعضی از برنامه‌های کاربردی ممکن است نیاز به سناریوهایی برای اندازه‌گیری دما، فشار، رطوبت و ... داشته باشند و همچنین سناریوهایی که تصاویری از محیط را ضبط کنند یا حرکت اشیا را ردیابی کنند و مواردی مشابه این‌ها. تعریف دیگری از ناهمگن بودن، یکسان نبودن سطح انرژی اولیه گره‌ها می‌باشد.

---

[1] Node Deployment
[2] Energy Considerations
[3] Data Delivery Models
[4] Data Aggregation/Fusion
[5] Node heterogeneity

۲-۶-۷- کیفیت سرویس[1]

در بسیاری از برنامه‌های کاربردی تحویل داده باید در یک پریود خاص زمانی صورت پذیرد. بنابراین تـأخیر در تحویل داده یکی از محدودیت‌های برنامه کاربردی است. در بسیاری از برنامه‌های کاربردی دیگر، حفـظ انـرژی کـه ارتباط مستقیم با طول عمر شبکه دارد، بسیار مورد توجه قرار می‌گیرد. هنگامی‌که انرژی رو بـه اتمـام اسـت ممکـن است شبکه کیفیت را پایین بیاورد و با این کار طول عمر شبکه را افزایش دهـد. پروتکـل‌هـای مسـیریابی بایـد ایـن محدودیت‌ها را در نظر بگیرند.

۲-۶-۸- محدودیت‌های سخت‌افزاری

یک گره سنسور از چهار جز اصلی تشکیل شده است: واحد سنسوری، واحد پردازش، واحد انتقال و واحد توان که ممکن است با توجه به برنامه کاربردی اجزای دیگری از قبیل مولد توان، سیستم موقعیت‌یابی و ...داشته باشد.
واحدسنسوری خود از دو بخش تشکیل شده است : سنسورها و تبدیل کننده آنالوگ به دیجیتال. واحد پردازش از یک پردازنده برای انجام محاسبات تشکیل شده‌است و واحد انتقال،سنسورها را به شبکه متصل می‌کند. مهم‌ترین واحد، واحد توان است که می‌تواند از سلول‌های خورشیدی یا هر منبع دیگری، برای تأمین توان استفاده کند.

۲-۶-۹- امنیت[2]

موضوع امنیت در برخی کاربردها به خصوص در کاربردهای نظامی یک موضوع بحرانی است و به‌دلیل برخی ویژگی‌ها شبکه‌های سنسوری بی‌سیم، این شبکه‌ها در مقابل مداخلات آسیب‌پذیرترند. یک مورد بی‌سیم بودن ارتباط شبکه است که کار دشمن را برای فعالیت‌های ضد امنیتی و مداخلات آسان‌تر می‌کند. مورد دیگر استفاده از یک فرکانس واحد ارتباطی برای کل شبکه است که شبکه را در مقابل استراق سمع آسیب‌پذیر می‌نماید. مورد بعدی ویژگی پویایی توپولوژی است که زمینه را برای پذیرش گره‌های دشمن فراهم می‌آورد. یکی از نقاط ضعف شبکه سنسوری بی‌سیم، کمبود منبع انرژی است و دشمن می‌تواند با قرار دادن یک گره مزاحم که مرتب پیغام‌های بیدار باش به صورت پخش همگانی با انرژی زیاد تولید می‌کند، باعث شود بدون دلیل گره‌های همسایه از حالت خواب خارج شوند که ادامه این روند باعث به هدر رفتن انرژی گره‌ها شده و عمر آن‌ها را کوتاه می‌کند. انواع حملات د فصل چهار توضیح داده خواهد شد.با توجه به محدودیت‌ها باید دنبال راه‌حل‌هایی ساده و کارا مبتنی بر طبیعت شبکه سنسوری بی‌سیم بود. اساساً چالش‌های زیادی در مقابل امنیت شبکه سنسوری وجود دارد و مباحث تحقیقاتی مطرح در این زمینه گسترده و پیچیده است.
البته فاکتورهای دیگری نیز همچون توپولوژی شبکه، پوشش، هزینه تولید و ... در طراحی شبکه‌های سنسوری بی‌سیم وجود دارد[۲].

[1] Quality of Service
[2] Security

فصل ۳ : پروتکل‌های مسیریابی

۳-۱- پشته پروتکلی شبکه‌های سنسوری بی‌سیم

محققان پروتکل‌های جدید زیادی را مخصوص شبکه‌های سنسوری بی‌سیم طراحی کرده‌اند که کمترین مصرف انرژی را دارا باشد. تنوع در کاربردهای این شبکه‌ها و منابع محدود گره‌ها باعث ایجاد مجموعه‌ای بزرگی از پروتکل‌های شبکه شده است که هر کدام مخصوص کاربرد خاصی می‌باشد. در این بخش پشته پروتکلی[1] عمومی در شبکه‌های سنسوری بی‌سیم، که جهت توصیف دستگاه‌های ارتباطی استفاده می‌گردند را توضیح خواهیم داد[۱]. شکل(۳-۱) لایه‌های پشته پروتکلی شبکه‌های سنسوری بی‌سیم را نشان می‌دهد.

لایه فوقانی(کاربرد)
لایه انتقال
لایه شبکه
لایه پیوند داده
لایه فیزیکی

شکل(۳-۱): پشته پروتکلی

۳-۱-۱- لایه‌های پشته پروتکلی

لایه‌های پشته پروتکلی عبارتند از :

[1]Protocol stack

✓ لایه فیزیکی

دو معیار اساسی و مهم که در این لایه محاسبه می‌گردد، هزینه و توان است. با توجه به آن که در این شبکه‌ها از انتقال کلاسیک رادیویی استفاده می‌شود، لایه فیزیکی وظیفه‌ی عملیات مدولاسیون و ارسال و دریافت اطلاعات در سطح پایین را بر عهده دارد.

✓ لایه پیوند داده(MAC[1])

لایه MAC توابعی دارد که اصلی‌ترینآن‌ها عبارتند از کنترل دسترسی، تخصیص کانال، مدیریت لیست همسایه‌ها و کنترل توان. این لایه می‌تواند برای صرفه‌جویی در توان، گره‌ها را به خواب ببرد. علاوه بر این، لایه MAC لیستی از همسایه‌هایش را نگه می‌دارد و آن‌ها را با توجه به موقعیتشان و انرژی مورد نیاز برای دسترسی به آن‌ها ارزیابی می‌کند. این لیست در لایه شبکه برای تصمیم گیری در مسیریابی بسته‌ها مورد استفاده قرار می‌گیرد. لایه MAC همچنین برای اطمینان از ذخیره توانی، توان را کنترل می‌کند.

✓ لایه فوقانی(کاربرد)

بسته به کاری که شبکه برای آن طراحی شده انواع مختلف نرم‌افزارهای کاربردی می‌توانند روی لایه کاربرد استفاده شوند و خدمات مختلفی را ارائه نمایند. در کاربردهای شبکه، پردازش اطلاعات، تجمع داده و پایگاه داده خارجی در این لایه قرار خواهند داشت.

✓ لایه انتقال

این لایه به صورت مخصوص هنگامی مورد نیاز می‌باشد که قصد ارتباط با شبکه سنسوری از طریق دیگر شبکه‌ها از جمله اینترنت یا هر شبکه خارجی دیگر را داریم.به طور مثال پروتکل TCP در این لایه قرار دارد.

✓ لایه شبکه

لایه شبکه وظیفه مسیریابی و ارسال داده‌های رسیده از لایه انتقال را برعهده دارد. این لایه شامل دو تابع اصلی می‌باشد : آدرس‌دهی گره و مسیریابی[2]. مسیریابی به معنی تعیین مسیر انتقال داده از مبدأ(سنسور) به مقصد (ایستگاه پایه) است که این مسیر باید بهینه بوده و کمترین مصرف انرژی را داشته باشد. دلایل این امر در بخش ۳-۲ توضیح داده خواهد شد.

۳-۲- اهمیت مسیریابی در شبکه‌های سنسوری بی‌سیم

با توجه به تفاوت‌های عمده بین شبکه های سنسوری بی‌سیم با شبکه های امروزی و همچنین شبکه‌هایMANET[3] مسیریابی در این شبکه‌ها توجه بسیاری را به خود جلب کرده است. این تفاوت‌ها به قرار زیر است:

---

[1]Media Access Control
[2] Routing
[3]**M**obile **A**d hoc **NET**work

- امکان ایجاد یک مبنای آدرسدهی کلی در این شبکه‌ها وجود ندارد. بنابراین پروتکل‌هایی مثل پروتکل اینترنت(IP) در این شبکه‌ها کاربرد نخواهد داشت.
- تقریباً در تمامی کاربردهای شبکه‌های سنسوری بی‌سیم نیاز به این امر می‌باشد که داده‌ها از نواحی مختلف به سمت یک ایستگاه پایه‌ی مشخص جریان پیدا کنند (برخلاف شبکه‌های دیگر مخابراتی).
- سنسورهایی که در نزدیکی پدیده مورد نظر برای اندازه‌گیری قرار دارند با احتمال زیاد یک نوع داده تولید می‌کنند، بنابراین تعداد داده‌های تکراری در این شبکه‌ها زیاد است.
- این سنسورها از نظر قدرت در ارسال داده، انرژی، قدرت پردازش اطلاعات و حافظه محدودیت دارند، پس پروتکل‌های مسیریابی باید یک مدیریت بسیار دقیق روی این منابع داشته باشند.

با توجه به اختلافات ذکرشده، تعداد زیادی الگوریتم جدید برای حل مشکل مسیریابی در شبکه‌های سنسوری بی‌سیم، پیشنهاد شده است. در طراحی این مکانیزم‌های مسیریابی، علاوه بر مشخصات خاص سنسورها برای آن شبکه، کاربرد شبکه و همچنین نیازمندی‌های ساختار آن نیز در نظر گرفته شده‌اند. تقریباً تمامی پروتکل‌های مسیریابی برای این شبکه‌ها را می‌توان در گروه‌های زیرتقسیم بندی کرد.

۳-۳- انواع پروتکل‌های مسیریابی شبکه‌های سنسوری بی‌سیم

پروتکل‌های مسیریابی بر اساس ساختار شبکه در سه دسته زیر جای دارند[۳] :

۱. مسیریابی شبکه‌های مسطح[۱]
۲. مسیریابی مبتنی بر موقعیت[۲]
۳. مسیریابی شبکه‌های سلسله مراتبی[۳]

۳-۳-۱- مسیریابی شبکه‌های مسطح یا مسیریابی داده مرکزی[٤]

پروتکل‌های این روش به گونه‌ای ست که تمامی گره‌های شبکه مانند هم رفتار می‌کنند و به طور عمده، نحوه ارسال داده آن‌ها، سیل آسا می‌باشد. از جمله اشکالات این روش، روی هم افتادگی بسته‌های مشابه، مصرف انرژی به مقدار زیاد و عدم توجه به منابع انرژی است. برخی از پروتکل‌های مسیریابی مسطح مهم عبارتند از DD، SPINs، Rumor Routing، SER و... .

[1]Flat-based routing
[2]Location-based routing
[3]Hierarchical-based routing
[4] Data centering routing

۳-۳-۲- مسیریابی مبتنی بر موقعیت

پروتکل‌های مبتنی بر موقعیت با استفاده از موقعیت جغرافیایی گره‌ها به مسیریابی بسته می‌پردازد. در این پروتکل‌ها برای محاسبه موقعیت از قطعه سخت‌افزاری GPS استفاده می‌شود، اما به دلیل بالا بردن هزینه شبکه روش مطلوبی نیست. روش دیگر برای محاسبه موقعیت، تخمین موقعیت گره می‌باشد. برخی از پروتکل‌های مسیریابی مبتنی بر موقعیت مهم عبارتند از MECN، GAF، GEAR و... .

۳-۳-۳- مسیریابی شبکه‌های سلسله مراتبی یا مسیریابی مبتنی بر خوشه[1]

در این روش، گره‌های شبکه دسته‌بندی می‌شوند. مجموعه‌ی گره‌هایی را که در یک دسته قرار دارند، خوشه یا کلاستر می‌گویند. در هر خوشه، یک گره وظیفه تجمیع داده‌های دریافتی توسط اعضای خوشه و ارسال آن به ایستگاه پایه را دارد که به آن، سرخوشه یا کلاستر هد می‌گویند. بنابراین در مصرف انرژی صرفه‌جویی می‌شود. برخی از پروتکل‌های مسیریابی مبتنی بر سرخوشه مهم عبارتند از LEACH، PEGASIS، SPAN، SHRP و ... .

در این میان، پروتکل LEACH به عنوان عمومی‌ترین پروتکل مسیریابی معرفی شده است که از مسیریابی مبتنی بر خوشه استفاده می‌کند. در این پروتکل برای کاهش مصرف انرژی و کاهش یکنواخت انرژی کل گره‌ها، در هر دور خوشه‌ها عوض می‌شوند و گره‌های دیگر امکان سرخوشه شدن برای خوشه‌ای جدید را بدست می‌آورند.

پروتکل‌های مذکور دارای امنیت کافی نمی‌باشند. در طی دهه اخیر روش‌های بسیار زیادی برای امن نمودن این پروتکل‌ها یا طراحی یک پروتکل امن ارائه شده است؛ لذا قبل از معرفی این پروتکل‌ها، ابتدا حملات موجود روی لایه شبکه معرفی شده و سپس اهداف امنیت و روش‌های امن کردن مطرح خواهد شد.

[1] Cluster-based routing

فصل ۴ : حملات روی مسیریابی شبکه‌های سنسوری بی‌سیم

حملات روی مسیریابی از لحاظ قرار گیری حمله کننده در شبکه به دو دسته تقسیم می‌شود[٤] :

- ✓ **حملات خارجی**[1] : در این حملات، مزاحم، خارج از شبکه قرار دارد و قابلیت دسترسی به گره‌های شبکه را ندارد. اما با وارد کردن گره‌ای در داخل شبکه قابلیت اجرای انواع حملات که در بخش بعد توضیح داده می‌شود را بدست می‌آورد. این نوع حملات در طبقهگره یا موت[2] می‌باشد یعنی نیاز به صرف هزینه زیاد نیست و با گره‌های عادی شبکه سنسوری بی‌سیم حمله اجرا می‌شود.
- ✓ **حملات داخلی**[3] : در این حملات، نفوذگر قابلیت دزدیدن اطلاعات گره موجود در شبکه را دارد که اصطلاحاً به این گره، گره در خطر افتاده می‌گویند. در این نوع حمله، فرض بر آن است که نفوذگر به تمامی اطلاعات موجود در حافظه گره از جمله کلیدهای رمزنگاری، داده و... دسترسی پیدا می‌کند. این نوع حملات در طبقهلپ‌تاپ[4] می‌باشد. یعنی برای دستیابی به گره هزینه زیادی لازم است و نیاز به محاسبات قوی در حد یک لپ‌تاپ است.

انواع حملات روی مسیریابی شبکه‌های سنسوری بی‌سیم عبارتست از :

۴-۱- اطلاعات مسیریابی بازیابی شده، دستکاری شده و جعل شده[5]

بیشترین حمله‌ای که علیه پروتکل‌های مسیریابی می‌شود، هدف قرار دادن اطلاعات مبادله شده بین گره‌های شبکه می‌باشد. با این حمله، نفوذگر قادر خواهد بود با ایجاد حلقه‌های مسیریابی، جذب یا رد ترافیک شبکه، کاهش یا افزایش مسیرها، ایجاد پیام‌های نادرست و افزایش زمان تأخیر انتها به انتها، امنیت شبکه را به خطر بیندازد[٤].

[1] Outdsider attack
[2] Mote class
[3] Insider attack
[4] Laptop class
[5] Spoofed, altered, or replayed routing information

در شبکه‌های سنسوری هر گره مانند یک مسیریاب عمل می‌کند؛ لذا نفوذگر می‌تواند بر روی اطلاعات مسیریابی به طور مستقیم تأثیر بگذارد[۵].

همان‌طور که مطرح شد، یکی از مضرات این حمله ایجاد چرخه مسیریابی می‌باشد به طوری که پیام در یک چرخه می‌افتد و ممکن است هیچ وقت به مقصد نرسد[۷].

۴-۲- حمله تکرار بسته

در این حمله، نفوذگر بسته‌ای را که از گره‌ای دریافت کرده دوباره می‌فرستد(تکرار می‌کند). این بسته می‌تواند به کل شبکه سرازیر شود یا به مجموعه‌ای خاص از گره‌های شبکه فرستاده شود. با افزایش این بسته‌های تکراری در شبکه، هم پهنای باند و هم توان گره‌ها به طور بیهوده‌ای مصرف می‌شود[۸].

۴-۳- حمله ارسال انتخابی[1]

در شبکه‌های سنسوری چندگامه، بسته‌ها توسط گره‌ها تا ایستگاه پایه صادقانه ارسال می‌گردد به عبارت دیگر هر گره وظیفه دریافت بسته و ارسال آن به گره همسایه خود را دارد بی آنکه تغییری در آن دهد یا آن را نفرستد.

در حمله ارسال انتخابی با قرار گرفتن نفوذگر در یکی از گره‌های مجاز شبکه، مانند یک گره قانونی در شبکه بسته‌ای را دریافت می‌کند اما آن را نمی‌فرستد و آن را از بین می‌برد. اگر نفوذگر تمامی بسته‌هایی را که دریافت می‌کند نفرستد به مانند یک حفره سیاه رفتار می‌کند؛ اما این حمله مناسب نیست زیرا گره همسایه فرض می‌کند آن گره خراب شده لذا مسیر ارسال داده را عوض می‌کند. بنابراین برای عدم تشخیص یا جلوگیری از سوء ظن شبکه، نفوذگر برخی بسته‌ها را به طور انتخابی ارسال می‌کند(یا خود بسته یا آن را اصلاح می‌کند بعد می‌فرستد).

این حمله زمانی موثر است که در مسیر جریان داده قرار گیرد تا هم بتواند به داده‌ها دست یابد هم در آن‌ها تغییر ایجاد کند[٤].

۴-۴- حملات حفره سینک[2]

در شبکه‌های سنسوری، تمامی بسته به ایستگاه پایه ارسال می‌شود؛ لذا در صورتی که نفوذگر بتواند ترافیک شبکه را به سمت خودش جذب کند، قابلیت اجرای دیگر حملات را خواهد داشت. در این حمله، نفوذگر با قرار گرفتن در منطقه‌ای خاص کل ترافیک آن منطقه از شبکه را جذب می‌کند تا اول از او عبور کنند. اگر نفودگر نزدیکایستگاه پایه باشد، کل ترافیک شبکه از او عبور خواهد کرد لذا می‌تواند دیگر حملات مانند ارسال انتخابی را روی بسته‌ها قبل از ارسال به ایستگاه پایه اجرا نماید.

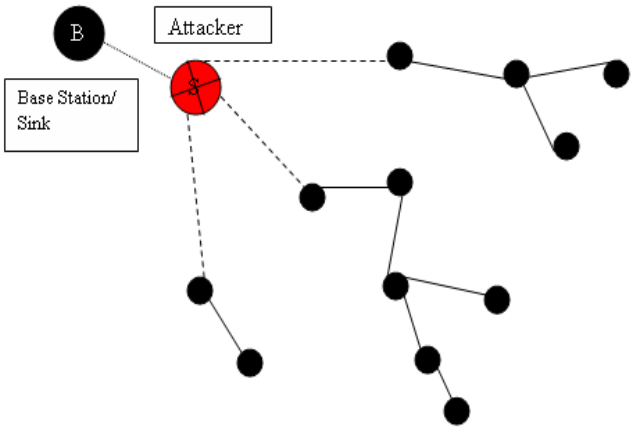
این حمله به نحوی است که نفوذگر با تبلیغ در شبکه (تبلیغ یک مسیر با کیفیت بالا یا کوتاه‌ترین مسیر به ایستگاه پایه)، توجه گره‌های همسایه را به خود جذب می‌کند. با جذب گره‌های همسایه، دیگر گره‌ها نیز او را به

[1]Select Forwarding
[2]Sinkhole

عنوان بهترین مسیر به دیگر گره‌ها اعلام می‌کنند. به دلیل اینکه گره دستکاری شده بتواند بهترین مسیر یا بـا کیفیـت-ترین مسیر را تبلیغ کند باید دارای توانایی‌های بیشتری نسبت به گره‌های شبکه باشد(طبقه لـپ‌تـاپ). نفـوذگر بایـد قابلیت تبلیغ این ویژگی‌ها را داشته باشد و الزامی ندارد مسیری وجود داشته باشد و می‌تواند غیـر واقعـی یـا واقعـی باشد.

بعد از اجرای این حمله می‌توان حمله ارسال انتخابی (عدم ارسال یـا تغییـر در بسـته‌هـا) را بـه راحتـی اعمـال کرد[٤].

این حمله روی پروتکل‌های مبتنی بر سیل گونه (شکل(٤-١)) بیشتر اعمال می‌شود[٥].



شکل(٤-١): حمله حفره سینک/حفره سیاه[٥]

در اکثر مقالات حفره سینک و حفره سیاه را یک تعریف در نظر گرفته‌انـد. امـا در مقالـه [٨] ایـن دو را از هـم متمایز کرده است.

٤-٤-١- حمله حفره سیاه

در این نوع حمله تمامی ترافیک شبکه به این حفره جذب می‌شود و دیگـر ارسـال نمـی‌گردنـد. بنـابراین تـوان عملیاتی[1] (نسبت کل تعداد بسته‌های دریافتی در ایستگاه پایه به طول‌عمر شبکه) گره‌ها به طور چشـمگیری کـاهش می‌یابد، مخصوصاً در گره‌هایی که همسایه حفره‌اند. اگر این حفره نزدیک ایستگاه پایه باشد، ارتباط شبکه با ایسـتگاه پایه کاملاً قطع می‌گردد اما اگر حفره در گوشه یا لبه شبکه واقع باشد، احتمالاً تعداد کمی گـره بـرای مخـابره از ایـن حفره استفاده می‌کنند؛ لذا ضرر خیلی محدود می‌شود[٨].

٤-٤-٢- حمله حفره سینک

این حمله نسبت به حمله حفره سیاه، پیچیده‌تر است. در این حمله، نفوذگر با تبلیغ مسیر کیفیت بالا بـه جـذب ترافیک شبکه می‌پردازد سپس می‌تواند حملات استراق سمع، ارسال انتخابی، حفره سیاه و... را اعمال کند[٨].

[1]throughput