مطالعات علوم کاربردی در مهندسی

دوره ۸، شماره ۱، بهار ۱۴۰۱

صفحات ۳۱۸-۲۹۱

Online ISSN: 2476-4507

Print ISSN: 2538-2055

www.irijournals.com

یک روش پیشرفته جهت تشخیص حمله حذف خدمات در شبکه‌های حسگر بی‌سیم

رامین صیادی[۱]، معین رستم نیا[۲]

[۱] هیئت علمی دانشگاه آزاد اسلامی واحد ایلام

[۲] کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد ایلام

چکیده

شبکه‌های حسگر بی‌سیم در معرض حملات زیادی هستند، این حملات ممکن است از چندین منبع مختلف همچون گره‌های مخربی که از تکنیک Flooding شبکه (ارسال حجم عظیم پیام‌ها برای همسایه‌هایش و یا برای ایستگاه پایه۱) استفاده می‌کنند. برای در امان ماندن از این نوع حملات تکنیک‌های بسیاری وجود دارد. که ما در روشمان از تکنیکی استفاده می‌کنیم که گره‌ی کنترلی۲ یا Cnode را برای پوشش‌دهی کل شبکه به منظور تشخیص گره‌های در معرض خطا و توقف فعالیتشان انتخاب کند. در این روش ما از الگوریتم LEACH برای انتخاب گره کنترلی یا سرخوشه۳ استفاده می‌کنیم. در کل روش ما با استفاده از تکنیک های خوشه‌بندی در جهت کشف حملات DoS همچون Jamming وGreedy می‌باشد. و نسبت به روش-های پیشین از دقت بالاتری برخوردار می‌باشد.

واژه‌های کلیدی: خوشه‌بندی، گره کنترلی، حمله حذف خدمات در شبکه‌های حسگر بی‌سیم

[1] Base Station=BS

[2] Controlled node = Cnode

[3] Cluster Head= CH

۱- مقدمه

با گسترش شبکه‌های اینترنتی، از جمله شبکه‌های بی‌سیم وزیرساختهای موجود برای تبادل اطلاعات بین این شبکه‌ها، عامل مهم امنیت و مقابله در برابر حملات در این شبکه‌ها همیشه مورد توجه بوده است[1]. پیشرفت شبکه‌های بیسیم، باعث شده است تا گره‌های حسگر در اندازه‌های کوچکتر و قدرتمندتر ظاهر شده و در مصرف انرژی کاراتر باشند و این باعث می گردد تا کاربردهای شبکه‌های حسگر بیسیم، دائما افزایش یابند. از آنجایی که گره‌های حسگر معمولا به صورت تصادفی در محیط پخش می گردند، این شبکه ها دارای توپولوژی پویا و متغیر می باشند، لذا فعالیت های لایه شبکه و مبحث مسیریابی در این شبکه ها و تامین امنیت آنها، یکی از دغدغه های طراحان و محققان این نوع شبکه ها بوده است. هدف در این لایه اینست که گره ها بتوانند به صورت صحیح و درست، گره‌های همسایه خود را شناخته و با توجه به این شناخت و استفاده از آنها، بتوانند بسته های اطلاعاتی خودرا بدون تغییر و خرابی به گره‌های علاقمند دیگر برسانند[2].

بدون شک زندگی امروز بشر از مقوله ارتباطات تفکیک ناپذیراست. ارتباطات به حدی فاصله های دور را به هم نزدیک کرده است که از دنیای بزرگ مابه نام دهکده جهانی یاد میشود. ارتباطات آنقدر با زندگی روزمره ماعجین شده است که نمی توانیم زندگی بدون آن را حتی تصور کنیم. درحالیکه تاقرنی پیش مبادله خبر به روزها زمان نیاز داشت، اینکار تقریباً آنی انجام میشود. مخابرات، اینترنت، وسائل ارتباط جمعی نمونه هایی از ارتباطات امروز ماهستندکه تبادل و انجام امور روزمره را باسهولت بیشتروهزینه کمتر ممکن ساخته است. از طرف دیگر ارتباطات شبکه ای ونفوذ آن به دوردسترین نقاط جهان باعث شده است زمینه سوء استفاده افراد سودجووشرور هم فراهم شود. درحالیکه هم اکنون انجام معاملات کلان واقتصادی وتبادل اطلاعات حیاتی در کوتاهترین زمان به راحتی وباهزینه ناچیزروی شبکه‌های کامپیوتری و اینترنت قابل انجام است، اما انجام این اموربدون درنظرگرفتن تمام جنبه های امنیتی، ممکن است باعث ضررهای جبران ناپذیری گردد. ازهمین جا لزوم امنیت شبکه وایجاد ارتباطات ایمن احساس می شود. که در این پروژه به بررسی سیستم های تشخیص نفوذ IDS[4] درشبکه‌های سنسور بی‌سیم WSN[5] [3,4,5] با استفاده از تکنیک های خوشه بندی پرداخته شده است.

رشد سریع شبکه‌های کامپیوتر است ، موجب مشکلات زیادی برای کاربران وسازمان ها از لحاظ امنیت سیستم ها خصوصاً در بانکها، سازمانهای مختلف رایانه های شخصی شده است . نفوذ وحمله به رایانه ها با روشهای مختلف خصوصاً در شبکه‌های سنسور بسیار معمول شده وپیگیری این حملات و بررسی و ردیابی این دسترسی های غیرمجازاز اهمیت بالائی برخوردار می باشد. هدف ما در این مقاله ارائه الگوریتمی جدید است که میزان دقت کشف حملات در شبکه را افزایش دهد.

مبانی نظری

حملات در شبکه‌ها

حملات موجود در شبکه‌های محلی بی‌سیم به دو دسته فعال و غیر فعال تقسیم می‌گردند[6, 7,8]. حملات فعال بدین صورت است که نفوذگر به نحوی به منابع اطلاعاتی دست می یابد.ولی محتوای اطلاعات منبع را تغییر نمی دهد، این نوع حملات میتواند به یکی از اشکال شنود یا آنالیز ترافیک باشد. درحملات فعال برخلاف حملات غیرفعال، نفوذگر اطلاعاتی را که از منابع به دست می آورد تغییر می دهد که تبعا انجام این تغییرات مجاز نیست. از آنجایی که در این نوع حملات اطلاعات

[4] Intrusion Detection System
[5] Wireless Sensor Network

تغییر می کنند. شناسایی رخ داد حملات فرآیندی امکان پذیر است. حال ما در این نوع حملات به حملات DOS می-پردازیم[1].

حملات DOS

نوعی از حمله است که هدف آن از کار اندازی سیستم هدف، با استفاده از هدر دادن منابع آن است[9]. طوری که سیستم سرویس دهنده دیگر توانایی پاسخ گویی به کاربران قانونی خود را نداشته باشد DOS برخلاف سایر تهدیدهای امنیتی مثل "دزدی اطلاعات"که در آن هدف به دست آوردن اطلاعات محرمانه است، یا "نفوذ" که در آن هدف دسترسی به یک ماشین خاص است و یا "تغییر دادن اطلاعات"، هدف آن تنها جلوگیری از سرویس دهی عادی به کاربران مجاز سرور به وسیله هدر دادن منابع سیستم است. در واقع اگر ما امنیت را در سه زمینه قابلیت اعتماد۶، یکپارچگی۷و دسترسی۸دسته‌بندی کنیم، حملات DOS گزینه سوم را مورد تهدید قرار می‌دهند[10].

شبکه حسگر بیسیم

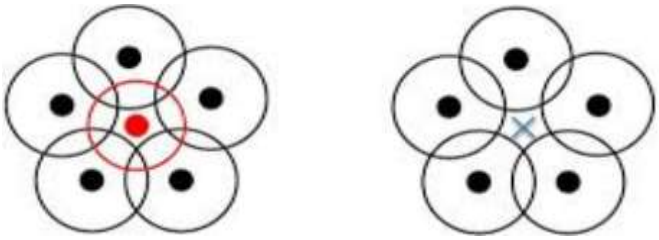
یک شبکه حسگر شامل تعداد زیادی گره‌های حسگر است که در یک محیط بطور گسترده پخش شده و به جمع آوری اطلاعات از محیط می‌پردازند. لزوما مکان قرار گرفتن گره‌های حسگر، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم . پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی‌های خود سازماندهی باشند. هر گره حسگر روی برد خود دارای یک پردازشگر است و به جای فرستادن تمامی‌اطلاعات خام به مرکز یا به گرهی که مسئول پردازش و نتیجه گیری 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 امکانات جدیدی را عرضه می‌کند. در واقع قدرت شبکه‌های بی‌سیم حسگر در توانایی به کارگیری تعداد زیادی گره کوچک است که خود قادرند ترکیب و سازماندهی شوند و در موارد متعددی جون مسیریابی همزمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند.

ویژگی‌های عمومی یک شبکه حسگر

پروتکل‌های شبکه‌ای همتا به همتا یک سرویس ارتباطات مش مانند را جهت انتقال اطلاعات بین هزاران دستگاه کوچک با استفاده از روش چند جهشی ایجاد می‌کنند. معماری انطباق پذیر مش، قابلیت تطبیق با گره‌های جدید جهت پوشش دادن یک ناحیه جغرافیایی بزرگتر را داراست. علاوه بر این، سیستم می‌تواند بطور خودکار از دست دادن یک یا حتی چند گره را جبران کند.بر خلاف شبکه‌های بی‌سیم سنتی، همه گره‌ها در شبکه‌های بی‌سیم حسگر نیازی به برقراری ارتباط مستقیم با نزدیک‌ترین برج کنترل قدرت یا ایستگاه پایه ندارند، بلکه حسگرها به خوشه‌هایی تقسیم می‌شوند که هر خوشه یک سرگروه خوشه موسوم به Parent انتخاب می‌کند. هر حسگر موجود در شبکه دارای یک محدوده حسگری است که به نقاط

[6] confidentiality
[7] integrity
[8] availability

موجود در آن محدوده احاطه کامل دارد. با اینکه توجه زیادی به پوشش کامل منطقه توسط حسگرها می‌شود، احتمال دارد نقاطی تحت پوشش هیچ حسگری قرار نگیرند. این نقاط تحت عنوان حفره‌های پوششی نامیده می‌شوند.



حفره پوششی استفاده از حسگر اضافی برای حذف حفره پوششی

فاکتورهای طراحی یک شبکه حسگر بی‌سیم

تحمل خرابی از کار افتادن گره‌های حسگر نباید تاثیری روی کارکرد عمومی شبکه داشته باشد .بنابراین تحمل خرابی را «توانایی برقرار نگه داشتن عملیات شبکه علی رغم از کار افتادن برخی از گره‌ها» معرفی می‌کنیم.قابلیت گسترش یک شبکه باید طوری طراحی شود که بتواند چگالی بالای گره‌های حسگر را نیز تحقق بخشد. این چگالی می‌تواند از چند گره تا چند صد گره در یک منطقه تغییر کند.هزینه تولید از آنجایی که شبکه‌های حسگر از تعداد زیادی گره‌های حسگر تشکیل شده‌اند، هزینه یک گره در برآورد کردن هزینه کل شبکه بسیار مهم است.

موانع امنیتی حسگرها در شبکه‌های حسگر

منابع بسیار محدود، فضای ذخیره سازی و حافظه محدود، محدودیت توان، ارتباطات ناامن و غیرمطمئن انتقال ناپایا و غیرمطمئن برخورد تاخیر، عملیات بدون مراقبت پدیدار شدن، حمله‌های فیزیکی، مدیریت از راه دور

نیازمندی‌های امنیتی شبکه‌های حسگر

قابلیت اعتماد داده‌ها، جامعیت داده‌ها، تازگی داده، دسترس پذیری، خودسازماندهی، استقرار امن، استفاده از الگوریتم SeRLoc[9]، احراز هویت سیستمμTESLA

انواع حملات در شبکه‌های حسگر

حملات انکار سرویس، حملهSybil، حملهWormhole، حملهBlack hole/Sinkhole، حملات تحلیل ترافیک، حملات تکرار گره، حملات مخالف محرمانگی پیام، حملات فیزیکی، حمله Hello Flood، حمله بر روی اطلاعات در حال عبور.

[9] Secure Range-In depended Localization

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

حملات انکار سرویس(DoS) :

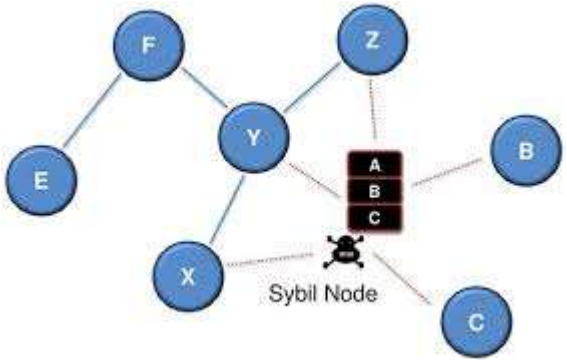
حملات انکار سرویس حملات جدیدی نیستند. در حقیقت، چندین تکنیک استاندارد وجود دارد که از محاسبات قدیمی‌استفاده می‌کنند تا در برابر تعدادی از حملات رایج انکار سرویس مقاوم باشند. هر چند این هنوز به عنوان یک مشکل عمده در جامعه امنیت شبکه محسوب می‌شود.ساده ترین نوع حمله انکار سرویس، برای تخلیه منابع موجود در یک گره ضعیف تلاش می‌کند. دشمن با ارسال بیش از حد بسته‌های غیر ضروری، از دسترسی کاربران مشروع شبکه به سرویس‌های دسترسی و یا منابعی که مستحق آنها هستند جلوگیری می‌کند. حملاتDoS ، تنها به معنی تلاش دشمن برای خرابکاری، مختل کردن کار و یا تخریب شبکه نمی‌باشد، بلکه منظور هر حادثه‌ای است که باعث نقصان ظرفیت حافظه در تامین یک سرویس می‌شود.

حملات DoS و روش های مقابله با آنها در لایه های مختلف شبکه:

حملات انکار سرویس(DoS) یک حمله استاندارد در شبکه‌های بی‌سیم حسگر، ایجاد پارازیت در یک گره یا گروهی از گره‌ها می‌باشد. در پخش پارازیت، حمله کننده سیگنال رادیویی را انتقال می‌دهد که با فرکانس‌های رادیویی مورد استفاده در شبکه‌های حسگر، تداخل پیدا می‌کنند.پارازیت در یک شبکه به دو صورت وارد می‌گردد: پارازیت ثابت و پارازیت پراکنده.در پارازیت ثابت یک پارازیت کامل را به شبکه یکپارچه وارد می‌آورد و هیچ پیامی‌نمی‌تواند ارسال و یا دریافت شود. اگر پخش پارازیت به صورت پراکنده باشد، گره‌ها می‌توانند به صورت دوره‌ای پیام‌ها را مبادله کنند، نه به صورت ثابت.

حملهSybil :

حمله sybilبه عنوان"یک وسیله بد اندیش که بطور نامشروع و نادرست چندین شناسه می‌گیرد"تعریف می‌گردد. این حمله قادر است تا افزونگی مکانیزم سیستم ذخیره سازی توزیع شده را در شبکه‌های نظیر به نظیر شکست دهد. علاوه بر سیستم‌های ذخیره سازی توزیع شده، حمله sybil در برابر الگوریتم‌های مسیر یابی، تراکم داده، رای گیری، تخصیص عادلانه منبع و کشف بی انضباطی تراشه‌ها موثر است.برای مثال در طرح رای‌گیری در شبکه‌های حسگر، حملات sybil باید از چندین شناسه بهره بگیرند تا رای‌های اضافی را تولید کنند. بطور مشابه، در حمله کردن به پروتکل‌های مسیریابی، حمله sybil بر یک گره بداندیش تکیه می‌کند تا شناسه چندین گره را بکار برد. بنابراین از طریق یک گره منفرد بداندیش چندین مسیر را مسیریابی می‌کند.



اساسا هر شبکه نقطه به نقطه، مخصوصا شبکهad hoc ، در مقابل حمله Sybil آسیب پذیر هستند. در بسیاری از موارد، حسگرها در شبکه‌های بی‌سیم حسگر ممکن است برای انجام یک وظیفه به همکاری با یکدیگر نیاز داشته باشند. بنابراین آنها

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

می‌توانند از توزیع زیر وظایف و افزونگی اطلاعات استفاده کنند. در چنین موقعیتی یک گره می‌تواند با استفاده از هویت سایر گره‌های مشروع وانمود کند که بیش از یک گره است و هویت چند گره را جعل می‌کند.حمله Sybil را به عنوان یک ابزار بدخواه نادرست تعریف می‌شود که به صورت هویت‌های دوگانه عمل می‌کند. ما هویت‌های اضافی یک ابزار بدخواه را گره Sybilمی‌نامیم.

دفاع در مقابل حمله Sybil :

برای دفاع در مقابل حمله Sybil ، ما باید اینکه هویت هر گره تنها هویت ارائه شده توسط یک گره فیزیکی مترادف است را قانونی کنیم. دو راه برای معتبر کردن یک هویت وجود دارد: راه اول «تایید مستقیم» است که در آن یک گره مستقیما بررسی می‌کند که ایا هویت گره دیگر معتبر است یا خیر؟ نوع دوم »تایید غیر مستقیم» است که در آن گره‌هایی که هم اکنون محقق شده اند، اجازه ضمانت یا تکذیب سایر گره‌ها را دارند.

حملات تحلیل ترافیک:

یک حمله کننده تنها به نیاز دارد که نظارت کدامیک از گره‌ها در حال ارسال بسته هستند و گره‌هایی که بسته‌های بیشتری را ارسال می‌کنند را دنبال می‌کند.در زمان حمله، دشمن رخدادهایی را تولید می‌کند و نگاه می‌کند کدام گره آن بسته را ارسال می‌کند. برای ایجاد یک رخداد، دشمن به سادگی یک رخداد فیزیکی را که توسط حسگرها در ناحیه نظارت می‌شود تولید می‌کند، مانند روشن کردن یک چراغ.

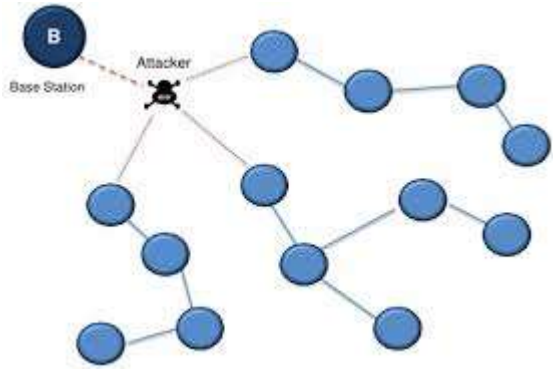
حملات انعکاس گره:

به صورت ادراکی، حمله انعکاس گره خیلی ساده است. حمله کننده سعی می‌کند تا یک گره را با کپی کردن شناسه گره یک گره حسگر موجود، به شبکه حسگر اضافه کند.گره‌ای که به این طریق تکرار می‌گردد به شدت کارایی شبکه حسگر را می‌تواند مختل کند، به این صورت که بسته‌ها خراب می‌شوند و یا اینکه به نادرستی مسیریابی می‌گردند.اگر یک حمله کننده دسترسی فیزیکی به کل شبکه پیدا کند، می‌تواند کلیدهای رمزنگاری شده را در حسگرهای تکرار شده کپی کند و هم چنین می‌تواند گره‌های تکراری را به نقاط راهبردی در شبکه اضافه کند.با اضافه کردن گره‌های تکراری در نقاط خاص شبکه، حمله کننده به آسانی قطعات خاص شبکه را دستکاری می‌کند، شاید با قطع کردن همه جهته آن.

حمله black hole/sink hole :

در این حمله یک گره بداندیش به عنوان یک حفره سیاه حمله می‌کند تا تمام ترافیک شبکه حسگر را جذب کند. به خصوص در یک پروتکل مبتنی بر جریان، حمله کننده به درخواست‌های روی مسیر گوش می‌دهد. سپس به گره‌های هدف پاسخ می‌دهد که این دربرگیرنده کیفیت بالا و یا بهترین مسیر به سمت ایستگاه پایه می‌باشد.تنها یکبار گره بداندیش قادر است تا خود را بین گره‌های که باهم ارتباط دارند، مثل گره حسگر و چاهک، جای دهد و هر کاری با بسته‌های در حال عبور بین آنها انجام دهد.

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱



حملات مخالف محرمانگی پیام:

دشمن می‌تواند حتی از داده‌های بی ضرر برای استنتاج اطلاعات حساس استفاده کند، اگر آنها بدانند چگونه چند منبع حسگر را بهم مرتبط کنند.مشکل اصلی محرمانگی فقط این نیست که گره‌های حسگر قادر باشند که اطلاعات را جمع آوری کنند. در حقیقت بیشتر اطلاعات جمع‌آوری شده از شبکه حسگر از طریق کاوش و جستجوی محوطه کاری بدست می‌آید.شبکه‌های حسگر مسئله محرمانگی را وخیم‌تر می‌کنند، به این دلیل که آنها حجم وسیعی از اطلاعات را به آسانی در دسترس دستیابی از راه دور قرار می‌دهند. از این رو، دشمنان نیازی ندارند که بطور فیزیکی جستجو را انجام دهند، آنها می‌توانند اطلاعات را با یک ریسک پایین و با یک نام مستعار جمع آوری کند.دستیابی از راه دور به دشمن تنها اجازه می‌دهد که تا چندین مکان را با هم نظارت کند.

انواع حملات مخالف محرمانگی پیام :نظارت کردن و استراق سمع این واضح ترین حمله به محرمانگی به شمار می‌آید .با گوش دادن به داده، دشمن به آسانی می‌تواند به محتویات ارتباط پی ببرد.تحلیل ترافیکتحلیل ترافیک به نوعی با مانیتور کردن و استراق سمع ترکیب شده است. افزایش تعداد بسته‌های منتقل شده بین گره‌های معین، می‌تواند اعلام کند که فعالیت یک حسگر خاص ثبت می‌شودمخفی کاریحمله کنندگان می‌توانند گره‌هایشان را به یک شبکه حسگر اضافه کنند و یا اینکه آنها را در شبکه پنهان کنند. سپس می‌توانند به شکل گره‌های معمولی در آیند و بسته‌ها را جذب کنند و به غلط بسته‌ها را مسیریابی کنند.

حملات فیزیکی:

شبکه‌های حسگر در محیط‌هایی راه اندازی می‌شوند و عمل می‌کنند که دشمنان به راحتی می‌توانند به آن وارد شوند.وقتی حسگرها با این محیط که دارای طبیعت توزیع شده و بدون مراقبت هستندپیوند برقرار می‌کنند، به شدت در معرض حملات فیزیکی قرار می‌گیرند و به علت خرابی گره‌های فیزیکی مورد تهدید قرار می‌گیرند. بر خلاف تعداد زیادی از حملات که قبلا ذکر شد، حملات فیزیکی بطور دائم حسگرها را خراب می‌کنند و این تلفات غیر قابل برگشت است.

حمله hello flood :

این حمله از بسته‌های Hello به عنوان یک سلاح برای قانع کردن حسگرها در شبکه‌های بی‌سیم استفاده می‌کنند. در این نوع حمله، حمله کننده با یک موج رادیویی بالا از محدوده منتقل می‌شود و بسته‌های Hello را به تعدادی از گره‌های حسگر که در ناحیه وسیعی از محدوده شبکه بی‌سیم حسگر پخش شده‌اند، ارسال می‌کند. بدین ترتیب، حسگرها متقاعد می‌شوند که

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

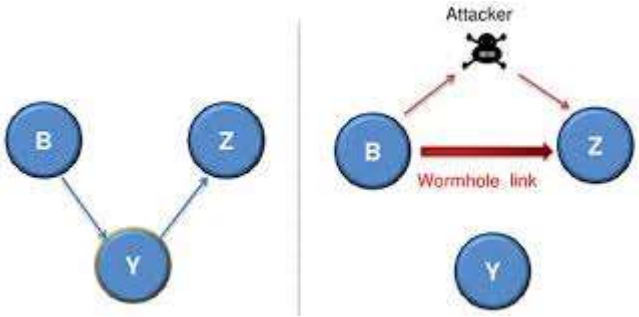
دشمن همسایه آنهاست.در نتیجه در زمان ارسال اطلاعات به ایستگاه پایه، گره‌های ضعیف سعی می‌کنند تا با حمله کننده کار کنند، به این دلیل که حمله کننده را همسایه خود می‌دانند و سرانجام توسط مهاجم از بین می‌روند.

حمله بر روی اطلاعات در حال عبور:

در یک شبکه حسگر، حسگرها تغییرات پارامترهای خاص و مقادیر را کنترل می‌کنند و طبق تقاضا به چاهک گزارش می‌دهند. در زمان ارسال گزارش ممکن است که اطلاعات در راه عبور تغییر کنند، مجدداً پخش شوند و یا ناپدید گردند.از آنجایی که ارتباطات بی‌سیم در مقابل استراق سمع آسیب پذیر هستند، هر حمله کننده می‌تواند جریان ترافیک را کنترل کند، در عملیات وقفه ایجاد کند و یا بسته‌ها را جعل کند. بنابراین، اطلاعات اشتباه به ایستگاه و چاهک ارسال می‌شود.به دلیل اینکه گره‌های حسگر معمولا دارای برد کوتاهی برای انتقال و منابع محدودی دارند، حمله کننده‌ای با قدرت پردازش بالا و برد ارتباطی بیشتر می‌تواند بطور همزمان برای تغییر اطلاعات واقعی در طول انتقال، به چندین حسگر حمله کند.

حمله wormhole :

حمله wormhole ، یک حمله بحرانی است به نحوی که حمله کننده بسته‌ها را در مکانی از شبکه ضبط می‌کند و از طریق یک تونل آنها را به مکان دیگری می‌برد .تونل سازی و یا ارسال مجدد بیت‌ها می‌تواند بصورت انتخابی انجام شود.این حمله یک تهدید مهم برای شبکه‌های بی‌سیم حسگر محسوب می‌شود، چون این حمله نیازی به سازش با حسگرها در شبکه ندارد و می‌تواند در زمانیکه حسگرها شروع به کشف اطلاعات همسایه می‌کنند انجام گیرد.



کشف :wormhole حملات wormhole ، بر روی شبکه‌های ad hoc متحرک ، توسط Dahill ، Hass و Hu کشف شد. برای دفاع در مقابل این حمله، تلاش‌هایی بر روی تکنیک‌های پردازش سیگنال انجام گرفته است.اگر بیت‌های داده‌ای با استفاده از روش‌های مدوله مخصوص ارسال شوند، تنها گره‌های همسایه شناخته می‌شوند و این گره‌ها در برابر wormholeمقاوم هستند. روش دیگر RF watermarking می‌باشد که به روشی مشابه کار می‌کند. هر دوی این روش‌ها به علت دشواری تصرف کردن الگوهای سیگنالی، از wormhole جلوگیری می‌کنند. بکارگیری آنتن‌های جهت دار، توسط گره‌های متحرک می‌تواند امنیت را بهبود دهد.گره‌های همسایه دستوالعملِ سیگنالهای دریافتی از یکدیگر و شواهد مشترک را زمانی که ارتباط همسایگان تایید شده باشد، بررسی می‌کنند.

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

اقدامات تدافعی در شبکه‌های حسگر بی‌سیم

تشکیل کلید رمزنگاری نامتقارن ؛ دفی-هلمن، رمزنگاری متقارن؛DES,3DES,RC5,AES طرح کلید پیش توزیع شده ، تکنیک بهره برداری از کلیدهای چندگانه، پروتکلLEAP طرح تشکیل کلید مرکب، رمزنگاری منحنی بیضوی Elliptic Curve Cryptography(ECC)، رمزنگاری کلید عمومیRSAوECC

اهداف تحقیق

ارائه یک روش جدید جهت شناسایی تشخیص نفوذ در شبکه‌های سنسور بی‌سیم

سؤالات تحقیق

۱.راهکارهای ارائه روشهای پیشنهادی بهینه تشخیص نفوذ در شبکه‌های سنسور کدام است؟

۲.آیا استفاده از تکنیک‌های خوشه‌بندی در سیستم‌های تشخیص نفوذ می تواند مفید واقع شود؟

فرضیه‌های تحقیق

- با بهره‌گیری از روشهای آماری می توان تشخیص نفوذ را در مراحل آغازین حمله شناسایی کرد.

پیشینه پژوهش

در منبع [16] به بررسی و مقایسه دو رویکرد امنیتی در برابر حملات DOS پرداخته شده، که هرکدام را با مقایسه و بررسی مورد بحث قرار داده‌اند و نقاط قوت و ضعف هر کدام را در برابر حملات نسبت به دیگری ذکر نمودند. در این مقاله دو رویکرد امنیتی شبکه‌های Ad hoc مورد بررسی قرار گرفت.

در مقاله‌ای با عنوان" کشف حملات DOS در شبکه‌های حسگر بیسیم مبتنی بر تکنیک خوشه بندی" آنها یک راه حل حفظ انرژی را برای کشفِ گره‌های در معرض خطا[10] در شبکه‌های حسگر بیسیم ارائه دادند. روش پیشنهادی شان مبتنی بر تکنیک خوشه بندی سلسله مراتبی بود که گره‌های کنترل کننده (که ترافیک درونِ یک خوشه را نظارت می کنند و هشدار ها را به سر خوشه ها ارسال میکنند) انتخاب میکرد[17].

روش شناسی پژوهش

ابزار اصلی گردآوری اطلاعات در بخش اصلی پایان نامه شامل بانک اطلاعاتی، اینترنت، کتابخانه‌ها و مقالات می‌باشد.روش گردآوری اطلاعات به صورت کتابخانه ای است. داده‌های این پژوهش با استفاده از مقالات منتشر شده در مجلات و کنفرانس‌های علمی معتبر و بانک‌های اطلاعاتی و شبکه‌های مخابرانی، پایگاه داده انتشارات معتبر علمی دنیا همچون Springer، Elsevier، IEEE و .... گردآوری می‌شود.

[10] Compromised nodes

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

روش‌ها، ابزار تجزیه و تحلیل داده‌ها

تجزیه و تحلیل کمی: این شیوه که به روش تجزیه و تحلیل آماری نیز شهرت دارد در مورد اطلاعات و داده‌های کمی به کار می‌رود.

تجزیه و تحلیل کیفی: چون برخی از اطلاعات به صورت کمی نمی‌باشند و جنبه آماری ندارند، مبنا و معیار دیگری غیر از روش‌های آماری باید برای تجزیه و تحلیل آنها بکار رود. این مبنا و معیار در تجزیه و تحلیل‌های کیفی مشخصا عقل، منطق، تفکر و استدلال است.

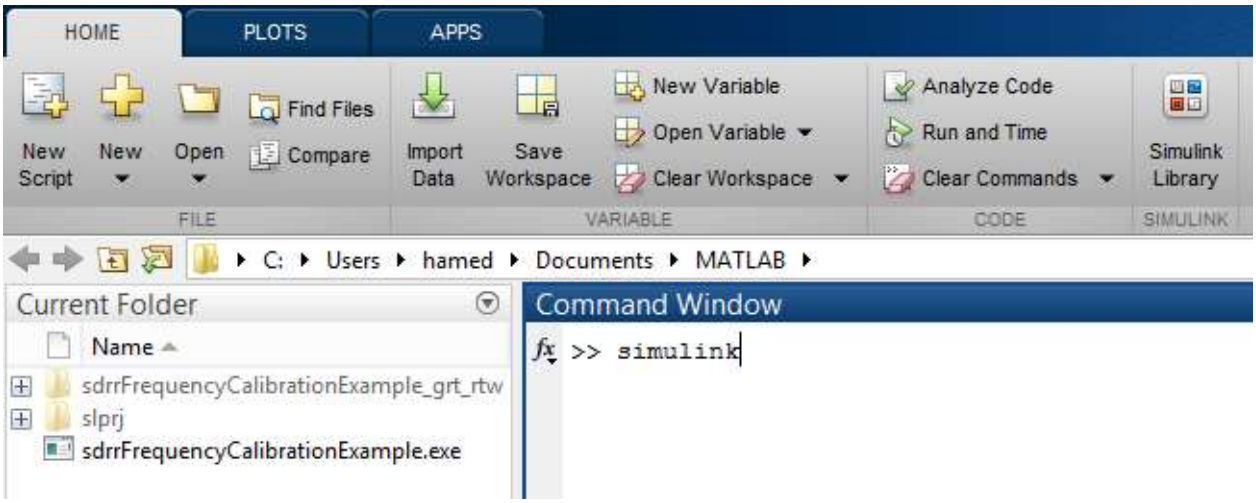
یکی از مراحل اساسی در پژوهش اندازه‌گیری است اندازه‌گیری روشی است که از طریق آن به یک صفت یا یک ویژگی، با توجه به ملاک مشخص، عددی نسبت داده می شود. به عبارت دیگر، اندازه‌گیری عبارت است از تبدیل کیفی به کمی، با توجه به ملاک معین اندازه‌گیری را می‌توان به روشی اطلاق کرد که از طریق آن عددی براساس یک قانون جایگزین یک صفت می‌شود. پژوهشگر کار خود را با متغیر آغاز می‌کند و سپس برای بیان متغیر به صورت عدد از قوانینی و مقیاس‌های مختلفی استفاده می‌کند. ماهیت روش اندازه‌گیری و اعدادی که از طریق اعمال روش‌های اندازه‌گیری حاصل می شوند، تعیین می‌کنند که برای تفسیر آنها باید از چه روش آماری استفاده کرد.

مبانی و توضیحات اولیه روش پیاده سازی

سیمولینک

سیمولینک قسمتی از نرم افزار MATLAB بوده و یک ابزار برنامه سازی قدرتمند برای مدلسازی و تحلیل سیستم های دینامیکی است .این مجموعه از سیستم های خطی، غیرخطی، زمان پیوسته، زمان نمونه و ترکیبی پشتیبانی می کند .با استفاده از سیمولینک می توان رفتار یک سیستم را بدون نیاز به ساختن آن تحلیل نمود .در نتیجه یک مهندس با استفاده از سیمولینک می تواند علاوه بر صرفه جویی در هزینه و زمان به بررسی تاثیر اغتشاشات یا سایر عوامل ورودی بر عملکرد یک سیستم بپردازد .همچنین شبیه سازی سیستم ها این توانایی را در اختیار می گذارد تا عکس العمل یک سیستم در صورت تغییر پارامترهای ورودی آن به خوبی شناخته شود .سیمولینک به صورت یک کتابخانه در نرم افزار MATLAB عرضه شده است که شبیه سازی توسط بلوک های این کتابخانه به صورت دیاگرام های بلوکی انجام می‌شود. و نحوه ورود به این بخش با دستور Simulink امکان پذیر میباشد شکل ۱).

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱



شکل ۱: ورود به بخش simulink

برخی از بلوکهای سیمولینک:

- بلوک مقدار ثابت(Constant)
- بلوک سیگنال ژنراتور(Signal Generator)
- بلوک شیب(Ramp)
- بلوک موج سینوسی(Sine Wave)
- بلوک پله(Step)
- بلوک Chrisp Signal
- بلوک Pulse Generator
- بلوک رشته تکرار(Repeating Sequence)
- بلوک ساعت (Clock)
- بلوک ساعت دیجیتال(Digital Clock)
- بلوکForm File

بلوک مقدار ثابت(Constant)

بلوک Constant برای تولید یک سیگنال ثابت به کار می رود. مقدار خروجی بلوک Constant در وسط بلوک نشان داده شده است و مقدار پیش فرض این بلوک ۱ است. برای تغییر این مقدار می توانید روی بلوک دبل کلیک کنید و در قسمت Value Constantهر مقدار ثابت دلخواهی انتخاب کنید.

بلوک سیگنال ژنراتور(Signal Generator)

بلوک Signal Generator یکی از بلوک های مهم در قسمت منابع است که می توان به وسیله آن توابع مختلفی را ایجاد کرد .این بلوک می تواند شکل موج های متفاوتی مانند سینوسی، مربعی و دندانه اره ای به علاوه سیگنال تصادفی تولید کند .

یک بلوک Signal Generator به داخل پنجره مدل وارد کنید. به صورت پیش فرض سیگنال ژنراتور یک موج سینوسی با دامنه ۱ و فرکانس ۱ هرتز تولید می کند .برای تغییر این پارامترها روی بلوک Signal Generator دبل کلیک کنید تا پنجره مربوط به ویرایش پارامتر ها ظاهر شود .همانطور که در شکل می بینید شما می توانید مقدار دامنه و فرکانس سیگنال خود را عوض کرده همچنین قادر به تغییر نوع سیگنال نیز هستید .برای تغییر نوع سیگنال قسمت مربوطه را کلیک کنید تا نوع سیگنال های انتخابی ظاهر شود و سپس با انتخاب هر کدام از این شکل موج ها سیگنال مربوطه قابل نمایش است.

بلوک شیب(Ramp)

بلوک شیب، سیگنالی را تولید می کند که در ابتدا ثابت بوده و در یک زمان مشخص به طور ثابت افزایش (یا کاهش) می یابد . شیب، زمان شروع و خروجی مقدار خروجی نیز می تواند مشخص شده باشد.

موج سینوسی(Sine Wave)

بلوک موج سینوسی یک سیگنال سینوسی تولید می کند .دامنه ، فرکانس و فاز (برخلاف Signal Generator) سیگنال می تواند مشخص شده باشد. یک پارامترچهارم به عنوان زمان نمونه (Sample time) نیز وجود دارد که می تواند برای تولید موج سینوسی در حالت زمان گسسته استفاده شود.

بلوک پله(Step)

بلوک یک تابع پله تولید می کند .مقادیر اولیه و نهایی دلخواه برای تولید سیگنال پله مطلوب می تواند انتخاب شود.

بلوکChirp Signal

بلوک Chirp Signal یک سیگنال سینوسی تولید می کند که بالای یک محدوده فرکانس را اسکن می کند. فرکانس های اولیه و نهایی به علاوه زمان اسکن کردن می تواند تعیین شده باشد .دامنه این سیگنال همیشه یک است و این سیگنال بعد از هر اسکن فرکانسی مجدد تکرار می شود.

بلوک Pulse Generator

بلوک Pulse Generator یک قطار پالس از سیکل کاری متفاوت تولید می کند. این سیگنال بین صفر و مقدار شروع اولین مقدار تعیین شده در یک زمان مشخص سوئیچ می کند. دوره (Period) سیکل کاری (Duty Cycle) ، دامنه (Amplitude)و زمان شروع (Start Time) می تواند مشخص شده باشد.

بلوک رشته تکرار(Repeating Sequence)

مجموعه قراردادی یا اختیاری از نقاط t,y می تواند به صورت مشخص شده باشد. این نقاط به عنوان یک بردار ویژه از مقادیر زمانی و یک بردار ویژه مطابق با مقادیر خروجی آن زمان ها وارد می شوند .خروجی به صورت خطی، بین مقادیر زمانی مشخص درون یابی می شوند، در آخرین مقدار زمانی، خروجی احتمالا با یک انتقال ناپیوسته فورا شروع به زیاد شدن می کند.

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

بلوک ساعت (Clock)

بلوک Clock یک سیگنال معادل با زمان اجرای شبیه سازی تولید می کند .این عمل زمانی اهمیت دارد که خروجی شبیه سازی به محیط متلب انتقال داده می شود اما در مراحل زمانی مناسبی اتفاق نمی افتد. خروجی Clock زمان هایی را که خروجی های سیگنال دیگر اتفاق می افتند منعکس می کند.

بلوک ساعت دیجیتال(Digital Clock)

این بلوک یک سیگنال زمانی متناوب اکید در یک فاصله نمونه برداری مشخص تولید می کند.

بلوکForm File

خروجی این بلوک یک سیگنال گرفته از فایل mat . مشخص است .به طور مثال یک ماتریس ذخیره شده در محیط MATLABبه صورت فایل mat تبدیل به سیگنالی می شود که ردیف اول ماتریس، مقادیر زمانی را مشخص می کند .این بلوک مشابه بلوک Repeating Sequence است.

تجزیه و تحلیل داده ها:

ما راه حلی را مبتنی بر انتخاب گره های کنترلی برای پوشش بهتر در کل شبکه به منظور تشخیص تعداد ماکزیمم گره های در معرض خطا در جهت بلاک کردن فعالیتشان مد نظر قرار می‌دهیم. در این بخش ما به طور جالبی با روشی جدید از الگوریتم LEACH برای انتخاب سرخوشه (که به عنوان گره کنترلی Cnode در نظر گفته می‌شود) استفاده می‌کنیم. در ابتدا، ما عملیات پایه الگوریتم LEACH را ارائه دادیم سپس روش پیشنهادی مان را برای انتخاب گره کنترلی با استفاده از الگوریتم LEACH توسعه دادیم و باروش های تصادفی و بِن اوتمان[۱۶] مقایسه نمودیم. بطور حتم LEACH یکی از آسانترین الگوریتم ها برای پارتیشن بندی شبکه می‌باشد و به نوعی یک خوشه‌بندی دینامیکی و الگوریتم مسیریابی می‌باشد. مجموعه گره‌ها را به چندین زیر مجموعه تقسیم میکند. هرکدام از انها شامل یک سرخوشه می‌باشد. این سرخوشه تنها گره‌ی پر مصرف[11]است که با BS عمل تبادل را انجام می‌دهد.

- با استفاده از تابع زیر کار خوشه‌بندی را انجام دادیم

```
function [delay,S,CH]=clustring(S,nodes,network,r)
global p
delay=0;
[S,CH]=head_election_phase(r,p,S);
if CH(1)~=-1
[S,delay]=advertisement(S,nodes,network,delay);
[S,delay]=cluster_setup(S,nodes,delay);
[S,delay]=aggrigate_in_CH(S,nodes,delay);
```

[11] cost-expensive

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

```
end
end
function [S,delay]=aggrigate_in_CH(S,nodes,delay)
global data_packet
for i=1:1:nodes
if strcmp(S(i).type,'cluster')
S(i).E=S(i).E-energyreceive_CH(data_packet*S(i).members);
elseif strcmp(S(i).type,'normal')
S(i).E=S(i).E-energysend(data_packet,S(i).dist_CH);
delay=caldelay(S(i).dist_CH,data_packet)+delay;
end
end
end
function [S,delay]=cluster_setup(S,nodes,delay)
global control_packet
for i=1:1:nodes
if strcmp(S(i).type,'normal')
mindist=1000;
candidateCH=nodes+1;
for j=1:1:nodes
if strcmp(S(j).type,'cluster')
dist=distancee(S(i),S(j));
if dist<mindist
mindist=dist;
candidateCH=j;
end
end
end
S(i).CH=candidateCH;
S(i).dist_CH=mindist;
% final setup
S(i).E=S(i).E-energysend(control_packet,mindist);
delay=caldelay(mindist,control_packet)+delay;
S(candidateCH).E=S(candidateCH).E-energyreceive(control_packet);
%plot([S(i).xd S(candidateCH).xd],[S(i).yd S(candidateCH).yd])
end
end
for i=1:1:nodes
S(i).members=1;
if strcmp(S(i).type,'cluster')
for j=1:1:nodes
if strcmp(S(j).type,'normal')
```

```
if S(j).CH==i
S(i).members=S(i).members+1;
end
end
end
end
end
end
function [S,delay]=advertisement(S,nodes,network,delay)
global control_packet
advertisementdist=sqrt(network^2 + network^2)/2;
for i=1:1:nodes
if strcmp(S(i).type,'cluster')
S(i).E=S(i).E-energysend(control_packet,advertisementdist);
delay=caldelay(advertisementdist,control_packet)+delay;
for j=1:1:nodes
if distancee(S(i),S(j))<advertisementdist
S(j).E=S(j).E-energyreceive(control_packet);
end
end
end
end
end
```

در اینجا به طور کامل پردازش LEACH بیان شده است. P برابر است با درصد میانگین خوشه‌هایی که ما میخواهیم در لحظه t از شبکه مان بگیریم. LEACH مرکب از چرخه هایی است که از rounds $\frac{1}{p}$ ایجاد شده است. هر راند r بصورت زیر سازماندهی شده است:

۱) هر گره i آستانه $T(i)$ را محاسبه می‌کند.

اگر i هنوز خوشه نشده است.

$$T(i)=\begin{cases}\frac{P}{1-P.(r \bmod \frac{1}{p})} \\ 0\end{cases}$$

اگر i هم اکنون خوشه است.

هر گره عدد شبه تصادفی $0 < x_i <$ را انتخاب می‌کند.

۱. اگر $x_i < T(i)$ سپس i خودش را به عنوان CH برای راند جاری طراحی(آماده) می‌کند. $T(i)$ به گونه ای که همه گره‌ها یکبار در هر چرخه‌ی راند $\frac{1}{p}$ سرخوشه شده باشند، محاسبه می‌شوند: که داریم $T(i) = 1$ در زمانی که $r = \frac{1}{p}$ – 1.

۲)سرخوشه‌ی خودساخته (آماده شده) دیگر گره‌ها را از طریق ارسال پیام با توان انتقالِ مشابه با استفاده از دسترسی چندگانه حسگر حسی حامل MAC[۱۲] مطلع مینماید.

۳)دیگر گره ها اتصال به خوشه ی مرتبط با CHی که سیگنالی با توان بالا را دریافت میکند را انتخاب میکنند.

۴)CHها یک لیست تبادل[۱۳] (TDMA) را برای گره‌هایی که به خوشه‌هایشان متصل شدند را کامپایل میکند. آنها به گره‌ها هشدار میدهند که چه زمانی ارسال داده‌ها به CHشان انتظار میرود.

۵) CH ها منتظر نتایج میمانند. گره‌های نورمال از محیطشان پیمایش (اندازه‌گیری) میشوند و داده‌هایشان را ارسال میکنند. زمانی که نوبت ارسالشان نرسیده است در حالت sleep میمانند تا انرژِی‌شان ذخیره شود. برخورد (تصادم)های بین ارسال ها و دریافت‌های گره ها از خوشه‌های مختلف به میمنت استفاده از CDMA کم و محدود هستند.

۶)CHها داده های دریافتی را تجمیع و یا احتمالا فشرده میکند و آنها را در یک تبادل منفرد به BS ارسال میکنند. این تبادل ممکن است بصورت مستقیم باشد و یا اگر متکی بر دیگر CHها باشد، بصورت Multi-hopped باشد.

۷)مراحل ۵ و ۶ تا زمانی که راند به پایان برسد ادامه می‌یابد.

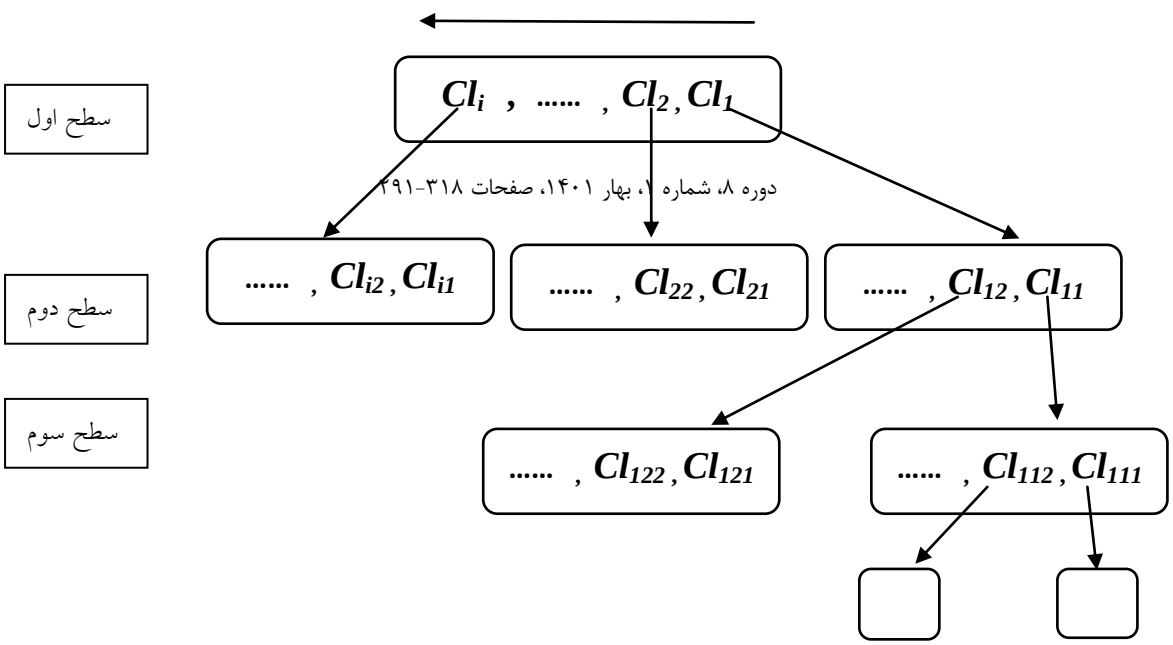
این احتمال وجود دارد که با اضافه کردن انرژی باقیمانده گره ها به عنوان یک پارامتر مکمل برای محاسبه آستانه $T(i)$ ، LEACH توسعه یابد[۲۰]. باید توجه داشت که هر گره میتواند تصمیم بگیرد که خودش را برای CH شدن آماده (سازماندهی) کند یا خیر. و تصمیم آن گره ربطی به رفتار گره‌هایی که آنرا احاطه کرده‌اند ندارد. براین اساس، احتمالا برای یک راند داده شده تعدادی از CH ها که بسیار متفاوت از درصدِ انتخابی هستند را داریم. همچنین، تمام CH ها ممکن است در یک منطقه مشابه (جدا از مناطق غیر پوششی که پوشش داده نشده‌اند) در شبکه قرار گرفته باشند. در این مورد ما فقط میتوانیم امیدوار باشیم پارتیشن‌بندی مجدد فضایی در طول راند بعدی ممکن است بهتر باشد.

LEACH بازگشتی

زمانی که الگوریتم LEACH برای تعیین اولین مجموعه از خوشه‌ها بکار گرفته شده، هیچ چیز برای ما مانع از بکارگیری مجدد آن بر روی خوشه نشد. این روشی است که ما k-clustersمان را بدست می‌آوریم: ما به تعداد k times، الگوریتم بازگشتی را الگوریتم k-LEACHنامگذاری کردیم. در عمل، ما بنا به دلایل زیر k را مساوی ۲ قرار دادیم:

- بخاطر ذخیره انرژی بیشتر نسبت به کاری که با 1-LEACH انجام میدهیم.
- بخاطر داشتن یک پارتیشن‌بندی خوب از شبکه (به منظور انتخاب گره‌های کنترلی در هر 2-clusters) برای ماکزیمم‌سازی محدوده پوششی و احتمال کشف گره‌های در معرض خطا

[12] Carrier Sense Multiple Access (CSMA) MAC
[13] Transmission order



دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

شکل۲: اجرای LEACH در چندین مرحله

مثال

شبکه حسگر که ترکیبی از گره های با Id ها ۱ تا ۱۰۰ می‌باشد سپس ما LEACH را اجرا می‌کنیم و نتایج آن ۱۰ خوشه توزیع شده (شکل۴-۲) به صورت زیر است:

1-LEACH(۱

Cl_1=این خوشه تشکیل شده از گره های ۴۴ و ۵۰ می‌باشد و سرخوشه آن گره شماره ۱۸ می‌باشد.

Cl_2=این خوشه تشکیل شده از گره های ۵، ۹، ۱۴، ۱۷، ۲۲، ۴۳، ۵۶، ۶۰، ۶۵، ۶۷، ۷۴، ۷۶، ۷۷، ۸۵، ۸۶، ۸۷، ۸۸، ۹۴، ۹۵، ۹۹میباشد و سرخوشه آن گره شماره ۲۱ می‌باشد.

....

Cl_{10}= این خوشه تشکیل شده از گره های ۲، ۸، ۱۵، ۱۶، ۲۰، ۲۵، ۲۸، ۳۸، ۵۵، ۶۳، ۷۰، ۸۲، ۹۰، ۹۱، ۹۸ می‌باشد و سرخوشه آن گره شماره ۱۰۰ می‌باشد.

2-LEACH(۲

در زمان دوم اجرای LEACH بر روی خوشه Cl_2، که زیر شبکه ای از ۲۰ گره می‌باشد، نتیجه اش دو زیر خوشه جدید می‌باشد (شکل۴-۳)، این زیر خوشه ها عبارتند از Cl_{21} با ۸ گره که سرخوشه اش گره۶۰ می‌باشد و Cl_{22} با ۷ گره که سرخوشه‌اش گره ۶۵ می‌باشد، نتایج به دست آمده در زیر نوشته شده است:

Cl_{21} در این سطح برابر با گره های ۵، ۱۷، ۴۳، ۷۴، ۷۶، ۸۵، ۸۶، ۸۷ و ۶۰ می‌باشد که گره آخر سرخوشه است.

Cl_{22} در این سطح برابر با گره های ۹، ۲۲، ۶۷، ۸۸، ۹۴، ۹۵، ۹۹ و ۶۵ می‌باشد که گره آخر سرخوشه است.

در انتها خوشه Cl_2 با دو زیر خوشه Cl_{21} و Cl_{22} تشکیل یافته است و بقیه گره‌ها، گره‌ی ۲۱ به عنوان سرخوشه دارند.

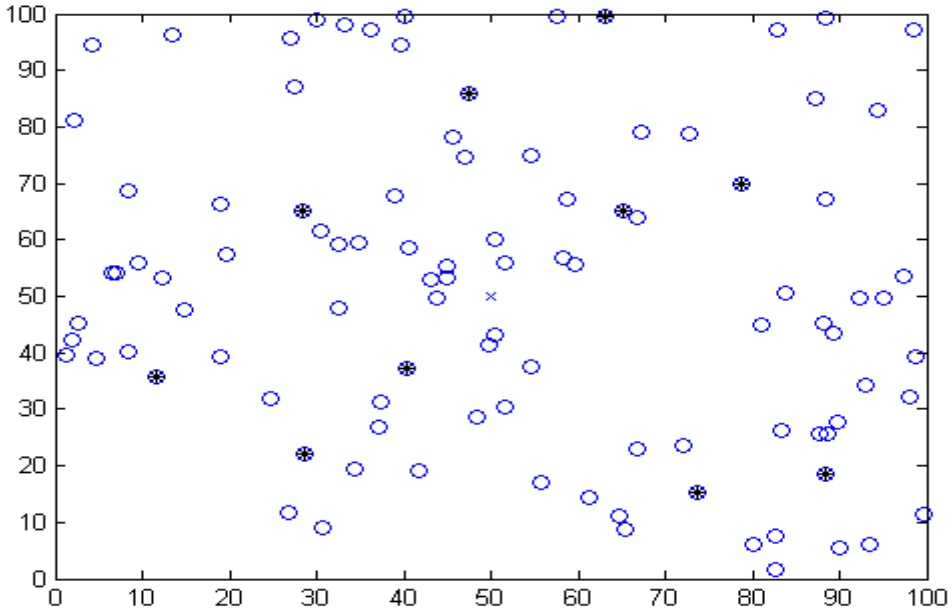
3-LEACH(۳

و به همان شیوه LEACH برای سومین بار برای خوشه Cl_{21} و Cl_{22} اجرا میگردد. که نتایج ان در زیر نوشته شده است:

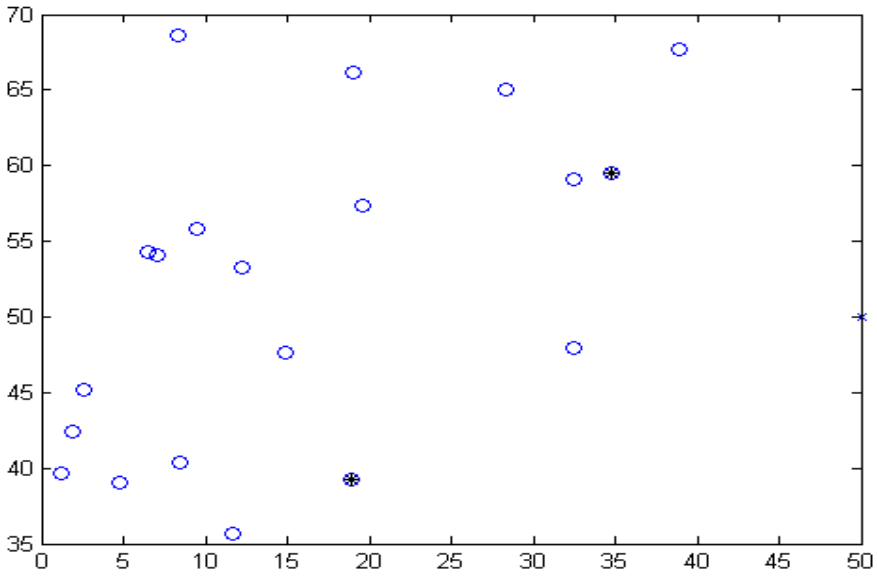
Cl_{21} در این سطح برابر با گره های ۴۳، ۷۴، ۷۶، ۸۷ و ۱۷ است که گره آخر سرخوشه می‌باشد.

Cl_{221} در این سطح برابر با گره های ۹، ۶۷، ۸۸، ۹۴، ۹۵، ۹۹ و۲۲ است که گره آخر سرخوشه می‌باشد.

ما میدانیم که خوشه Cl_{21} با یک زیر خوشه Cl_{211} تشکیل شده است و بقیه گره‌ها گره ۶۰ را به عنوان سرخوشه دارند.



شکل۳: اجرای LEACH برای بار اول



شکل۴: اجرای LEACH برای Cl2-بار دوم

به منظور نشان دادن مزیت راه حل پیشنهادی ما شبیه سازی ها را در متلب انجام دادیم. در این شبیه سازی ها در ابتدا ۱۰۰ گره را بصورت تصادفی که در یک محدوده با ابعاد۱۰۰ mدر ۱۰۰m توزیع شده اند را تولید نمودیم.

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

بنابراین موقعیت هرگره بصورت تصادفی بین ۰ تا ۱۰۰ بر روی هر محور (افقی و عمودی) انتخاب میشود. سینک در میان محدوده (فیلد) شبیه سازی شده قرار داده شده است. سپس الگوریتم LEACH را با نرخ مطلوب سر خوشه ۱۰ و راند برابر با ۱۰ مورد استفاده قرار میدهیم.

بعد از اجرا ما 1-cluster را با k گره (که$K > 2$) به دست می]وریم. آن خوشه‌ها خودشان با در نظر گرفتن مختصات هر کدام از گره‌هایشان (با روش مشابه) با استفاده از LEACH در زمان دوم تقسیم شده‌اند. زیر مجموعه صادر شده از تقسیم هر l-cluster، li-cluster خوانده میشود. علاوه بر این، هر CH که در این مرحله انتخاب میشود به عنوان گره کنترلی Cnode برای هر Cluster Cl_i در نظر گرفته میشود. ما این فرایند را چندین بار تا زمانی که clusters Cl_i ها در سطح جاری مشابه خوشه های سطح قبلی (با در نظر گرفتن تعداد گره های هر خوشه) باشند تکرار می‌کنیم (شکل ۴-۱). در این مرحله الگوریتم به همگرایی میرسد. حداقل ما برای هر خوشه، فاصله بین هر سر خوشه (node) و گره‌های همسایه‌اش را محاسبه مینمائیم. نتیجه این میشود که: Cl_i-cluster با گره های k_j برای هرخوشه تشکیل میشود. مرحله دوم شامل انتخاب عدد تصادفی Cnode با در نظر گرفتن ماتریس مختصات گره های استفاده شده در LEACH می‌باشد. ما بطور تصادفی تعداد Cl_i cluster را با Cnodeهای k_j برابر با تعداد Cnode بدست آمده از اجرای چندین باره LEACH انتخاب کردیم. ما گره‌های k_j را برای هر Cnode به منظور ساخت زیر مجموعه‌های هم ارز (متعادل) با خوشه های به دست آمده در مرحله اول، را پیوند (جفت) دادیم. ما گره‌هایی که کمترین فاصله را با گره کنترلی پیوندی دارد، انتخاب می‌کنیم. برای انتخاب سرخوشه از کد زیر استفاده می‌کنیم:

```
%% head election phase
function [S,CH]=head_election_phase(r,p,S)
global nodes
global sink
CH(1)=-1;
threshold=p/(1-p*(mod(r,1/p )));
w=0;
for i=1:1:nodes
random=rand(1,1);
if random<threshold && S(i).Head_in_round <= r-1/p && ~strcmp(S(i).type,'dead')
w=w+1;
S(i).type='cluster';
CH(w)=i;
S(i).dist_to_BS=distancee(S(i),sink);
S(i).Head_in_round=r;
end
end
end
```

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

نتیجه این است که: S_i به عنوان زیر مجموعه مرکب با گره‌های k قرار دارد. در آخر با توجه به زیر مجموعه‌های S_i که تعداد یکسانی گره دارند، ما برای هرخوشه Cl_i که در مرحله اول به دست آمده‌اند، هرS_i زیر مجموعه که از مرحله دوم به دست امده-اند، فاصله بین گره‌ها و گره‌های کنترلی متناظرشان عمل مقایسه را انجام میدهیم.

الف) نتیجه روش ما به شرح زیر است:

بعد از شبیه‌سازی روش مان در متلب به نتایج زیر دست یافتیم:

۵ خوشه که هر کدام از انها از ۶ گره تشکیل شده اند.

۳ خوشه که هرکدام از آنها از ۴ گره تشکیل شده اند.

۴ خوشه که هر کدام از انها از ۳ گره تشکیل شده اند.

۵ خوشه که هر کدام از آنها از ۲ گره تشکیل شده اند.

سرخوشه هر کدام از خوشه ها به عنوان گره های کنترلی در نظر گرفته شده است. این شبیه سازی۱۷ گره کنترلی توزیع شده را طبق جدول ۴-۲ نشان میدهد.

ب) نتیجه برای روش تصادفی

در این روش ما بطور تصادفی ۱۷ گره کنترلی[۱۰۰ ..... ۱] را انتخاب می‌کنیم. نتیجه این است که:

Cnode ID =[۳ ،۸ ،۱۳ ،۱۵ ،۲۰ ،۲۹ ،۳۷ ،۵۰ ،۵۴ ،۵۹ ،۶۶ ،۸۳ ،۹۰ ،۹۳ ،۹۶ ،۹۸]

ما زیر مجموعه S_i را برای هر گره کنترلی (ID) بر اساس نتیجه حاصل در شبیه سازی مان و با در نظر گرفتن فاصله مینیمم بین هر گره کنترلی و نزدیکترین گره های همسایه اش (جدول ۴-۱) تشکیل دادیم. بر اساس این شرط ما هجده Batch از زیر مجموعه ها را که ترکیبی از شش، چهار، سه و دو گره میباشند را همانند زیر میسازیم:

۵ زیر مجموعه هر کدام تشکیل شده از ۶ گره

۳ زیر مجموعه هر کدام تشکیل شده از ۴ گره

۴ زیر مجموعه هر کدام تشکیل شده از ۳ گره

۵ زیر مجموعه هر کدام تشکیل شده از ۲ گره

سپس ما فاصله میانگین بین هر گره کنترلی و گره‌های تشکیل شده در این زیر مجموعه را محاسبه می‌کنیم.

دوره ۸، شماره ۱، بهار ۱۴۰۱، صفحات ۳۱۸-۲۹۱

جدول ۱: نتیجه اجرای روش تصادفی

زیر مجموعه	مجموعه گره ها	گره کنترلی	میانگین فاصله
S_1	۱۴، ۳۱، ۵۱، ۶۱، ۷۵، ۲۲	۳	۸,۵۸۴
S_2	۲۲، ۱۶، ۲۵، ۲۸، ۶۳، ۸۲	۸	۱۲,۴۷۹
S_3	۷، ۳۰، ۷۱، ۷۲، ۸۰، ۸	۱۳	۱۴,۰۹۲
S_4	۲، ۶۲، ۶۸، ۷۰، ۹۱، ۱۰۰	۱۵	۱۰,۷۹۱
S_5	۲۳، ۳۴، ۳۵، ۳۸، ۴۹، ۵۸	۲۰	۲۵,۶۲۰
S_6	۶، ۵۶، ۶۴، ۷۹	۲۹	۱۳,۲۱۵
S_7	۱۰، ۴۲، ۶۷، ۸۹	۳۳	۲۵,۶۴۲
S_8	۴، ۹، ۳۶، ۹۹	۳۷	۳۲,۷۳۵
S_9	۱۸، ۴۴، ۵۷	۵۰	۶,۴۴۹
S_{10}	۴۵، ۵۳، ۷۸	۵۴	۹,۳۶۳
S_{11}	۱۹، ۴۷، ۹۲	۵۹	۱۹,۳۴۹
S_{12}	۲۱، ۲۲، ۷۷	۶۶	۲۸,۳۹۸
S_{13}	۲۴، ۴۰	۸۳	۴۷,۱۲۶
S_{14}	۴۱، ۴۸	۹۰	۳۱,۳۸۸
S_{15}	۶۹، ۸۶	۹۳	۱۲,۶۴۹
S_{16}	۳۹، ۵۲	۹۶	۸,۳۴۳
S_{17}	۲۶، ۱۱	۹۸	۵۴,۹۰۳

جدول ۲: نتیجه اجرای روش بِن اوتمان در سه سطح

Cl_i	Cl_{ij}	Cl_{ijk}	مجموعه گره ها	گره کنترلی	میانگین فاصله
Cl_1			۵۰,۴۴	۱۸	۱۰,۱۳۵
Cl_2	Cl_{21}	Cl_{211}	۸۷ ،۷۶ ،۷۴ ،۴۳	۱۷	۵,۵۷۸
			۸۶ ،۵	۶۰	۱۳,۴۰۰
	Cl_{22}	Cl_{221}	۹۹ ،۹۵ ،۹۴ ،۸۸ ،۶۷ ،۹	۲۲	۱۲,۱۴۵
			۷۷ ،۵۶ ،۱۴	۲۱	۶,۱۹۲
Cl_3	Cl_{31}	Cl_{311}	۷۳ ،۶۴ ،۵۸ ،۴۲ ،۳۴ ،۲۷	۴۱	۱۹,۷۵۵
			۴۹ ،۴۰ ،۱۰ ،۳	۲۴	۸,۴۷۲
Cl_4	Cl_{41}		۷۲ ،۲۹	۷۹	۸,۵۸۰
			۸۱ ،۶۱ ،۵۱	۳۱	۷,۱۱۰
Cl_5	Cl_{51}		۹۷ ،۵۹	۲۳	۱۵,۹۳۹
Cl_6	Cl_{61}	Cl_{611}	۸۹ ،۸۳ ،۷۱ ،۳۳ ،۳۰ ،۷	۸۰	۱۲,۷۱۱
	Cl_{62}		۸۴ ،۳۶ ،۴	۶۶	۲۲,۴۴۴
Cl_7	Cl_{71}		۷۸ ،۴۷ ،۴۵ ،۳۲ ،۲۶ ،۱۲	۵۷	۱۶,۰۱۸
Cl_8	Cl_{81}		۱۹ ،۱۱	۹۲	۱۰,۴۰۳
Cl_9	Cl_{91}		۶۸ ،۵۲ ،۳۹	۶۲	۷,۰۰۷
Cl_{10}	Cl_{101}	Cl_{1011}	۹۸ ،۹۱ ،۳۸ ،۱۶	۱۵	۱۳,۳۱۳
	Cl_{102}	Cl_{1021}	۹۰ ،۶۳ ،۵۵ ،۲۵ ،۲۰ ،۸	۲۸	۱۰,۵۱۸

جدول ۳: نتیجه اجرای روش مان در سه سطح

Cl_i	Cl_{ij}	Cl_{ijk}	مجموعه گره ها	گره کنترلی	میانگین فاصله
Cl_1			۵۲,۴۵	۲۰	۹,۱۲۰
Cl_2	Cl_{21}	Cl_{211}	۹۱ ،۷۹ ،۷۶ ،۴۴	۱۹	۴,۳۲۱
			۸۸ ،۶	۵۵	۱۲,۴۰۸
	Cl_{22}	Cl_{221}	۹۹ ،۱۰۰ ،۹۸ ،۹۱ ،۶۸ ،۱۰	۳۵	۱۱,۹۸
			۸۰ ،۵۸ ،۱۵	۲۷	۶,۴۵۰
Cl_3	Cl_{31}	Cl_{311}	۷۳ ،۶۴ ،۶۲ ،۴۳ ،۳۶ ،۲۸	۴۲	۱۹,۴۵۵
			۴۹ ،۴۳ ،۱۲ ،۴	۱۸	۷,۱۲۲
Cl_4	Cl_{41}		۷۴ ،۳۰	۸۷	۸,۱۲۰
			۸۴ ،۶۳ ،۵۲	۳۴	۶,۱۱۰
Cl_5	Cl_{51}		۹۹ ،۶۰	۲۳	۱۵,۹۳۹
Cl_6	Cl_{61}	Cl_{611}	۸۹ ،۸۳ ،۷۱ ،۳۶ ،۳۲ ،۸	۸۷	۱۱,۶۱۱
	Cl_{62}		۸۴ ،۳۸ ،۵	۶۶	۲۱,۴۴۰
Cl_7	Cl_{71}		۷۸ ،۴۷ ،۴۵ ،۳۵ ،۲۸ ،۱۳	۷۸	۱۴,۰۱۸
Cl_8	Cl_{81}		۲۱ ،۱۲	۹۲	۱۰,۴۰۳
Cl_9	Cl_{91}		۶۸ ،۵۴ ،۴۰	۶۲	۶,۱۰۷
Cl_{10}	Cl_{101}	Cl_{1011}	۹۸ ،۹۱ ،۴۰ ،۱۷	۱۵	۱۲,۳۳۰
	Cl_{102}	Cl_{1021}	۹۰ ،۶۳ ،۵۵ ،۲۸ ،۲۲ ،۹	۳	۹,۴۴۰

در جدول، ما سه خوشه را که هر کدام ترکیبی از چهار گره می‌باشد را در نظر گرفتیم و فاصله میانگینِ روش تصادفی و روش خودمان را محاسبه می‌کنیم. طبق روش ما Cnode با ID۱۷ گره‌های کنترلی [۴۴، ۷۶، ۷۹، ۹۱] و فاصله میانگین بین این گره کنترلی و همسایه‌هایش برابر با ۴,۳۲۱ می‌باشد.

بر خلاف آن، در روش تصادفی و روش بِن اوتمان[۱۶] ما میدانیم که گره کنترلی با۲۹ ID گره‌های کنترلی [۵، ۵۶، ۴، ۷۹] با فاصله میانگینی برابر با ۱۳,۲۱۵ و با۳۲ ID گره‌های کنترلی[۴۳، ۷۴، ۷۶، ۸۷] با فاصله میانگینی برابر با ۵,۵۷۸ قرار دارد.

برای تمامی خوشه‌های ارائه شده در این جدول، فاصله میانگین آخرین ستون با فرمول $\frac{\sum d_{avg}}{3}$ محاسبه میگردد.

ما تشخیص دادیم که فاصله میانگین حاصل شده از روشمان، بطور چشمگیری کمتر از روش تصادفی و بن اوتمان می باشد. در حقیقت، در جدول ما چهار خوشه را که هر کدام با سه گره تشکیل شده است در نظر میگیریم. همانند جدول ۴-۳، ما فاصله میانگین را برای هر دو روش محاسبه می‌نمائیم. ما همچنین میتوانیم متذکر شویم که فاصله میانگین با استفاده از روش ما

همچنان بهترین رابطه/نزدیکی را با روش تصادفی و بِن اوتمان دارا می‌باشد. سرانجام، در جدول ما همچنین پنج خوشه را که هر کدام از دو گره تشکیل شده را در نظر گرفتیم. همانند قبل، ما فاصله میانگین را برای دو روش به کار میبریم. ما تاکید می‌کنیم که روش‌مان بهترین نتیجه را نسبت به روش تصادفی و بِن اوتمان ارائه میدهد.

جدول ۴: فاصله بین گره کنترلی و چهار گره با سه خوشه

روش	Cl_1	Cl_2	Cl_3	میانگین فاصله
تصادفی	۱۳,۲۱۵	۲۵,۶۴۲	۳۲,۷۳۵	۱۱,۹۳۲
روش بِن اوتمان	۵,۵۷۸	۸,۴۷۲	۱۳,۳۱۳	۴,۵۶۰
روش ما	۴,۳۲۸	۷,۱۲۲	۱۲,۳۳۰	۴,۱۰

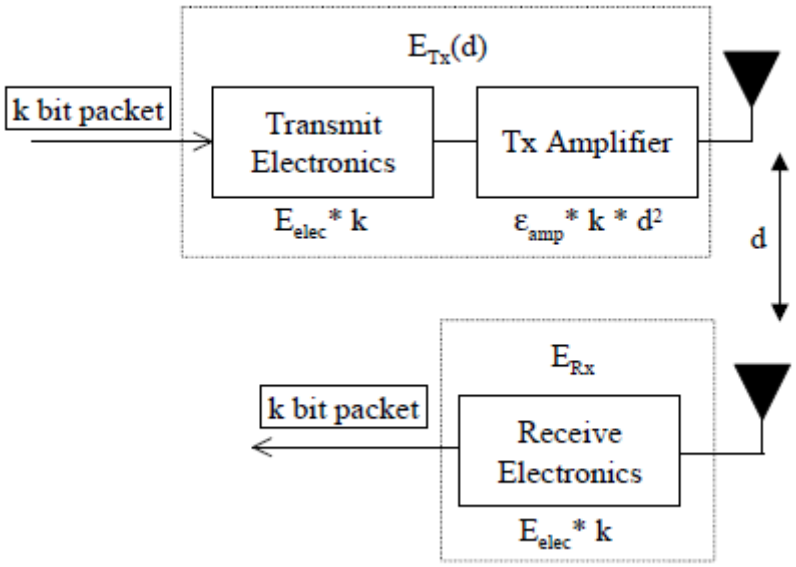
جدول ۵: فاصله بین گره کنترلی و سه گره با چهار خوشه

روش	Cl_1	Cl_2	Cl_3	Cl_4	میانگین فاصله
تصادفی	۶,۴۴۹	۹,۳۶۳	۱۹,۳۴۹	۲۸,۳۹۸	۱۱,۹۳۲
روش بِن اوتمان	۶,۱۹۲	۷,۰۰۷	۸,۵۸۰	۲۲,۴۴۴	۴,۵۶۰
روش ما	۶,۴۵۰	۶,۱۰۷	۸,۱۲۰	۲۱,۴۴۰	۴,۱۰

جدول ۶: فاصله بین گره کنترلی و دو گره با پنج خوشه

روش	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5	میانگین فاصله
تصادفی	۴۷,۱۲۶	۳۱,۳۸۸	۱۲,۶۴۹	۸,۳۴۳	۵۴,۹۰۳	۲۷,۰۷۵
روش بِن اوتمان	۸,۵۸۰	۱۰,۱۳۵	۱۰,۴۰۳	۱۳,۴۰۰	۱۵,۹۳۹	۱۰,۷۱۴
روش ما	۸,۱۲۰	۹,۱۲۰	۱۰,۴۰۳	۱۲,۴۰۸	۱۵,۹۳۹	۹,۱۴۳

در حال حاضر، مدل رادیویی اتلاف انرژی در [۱۸] مصرف انرژی در شبکه را متناسب با مربع فاصله در نظر میگیرد. در واقع، اگر فاصله افزایش یابد، هزینه انرژی بالا میرود. از اینرو، ما معیار را برای ارزیابی روش خود مورد استفاده قرار میدهیم. در این مدل رادیویی میزان مصرف انرژی ارسال بسته‌ای از بیت‌ها به تعداد K را نشان میدهد. در این مدل برای ارسال داده بعد از گره‌ی فرستنده یک تقویت کننده[۱۴]قرار داده شده است تا داده‌ها یا پاکت‌ها با نهایت توان ارسال شوند.



شکل۵: مدل رادیویی میزان مصرف انرژی در زمان ارسال و دریافت داده ها در گره ها[۱۸]

با جمع بستن انرژی ارسال از سوی گره و انرژی مصرفی توسط تقویت کننده مجموع میزان اتلاف انرژی به دست می‌آید. که طبق فرمول زیر داریم[۱۸]:

$$E_{elec} * \mathrm{k} + \varepsilon_{amp} * k * d^2$$

[14] Amplifier

و همچنین فرمول میزان مصرف انرژی در زمان دریافت داده در گره ها از رابطه زیر به دست می‌آید:

$E_{elec} * k$

```
%% energy consumption for sending packet to dist
function [con]=energysend(Packet,dist)
global Eelec
global Emp
global Efs
global d0
if dist<d0
con=Packet*Eelec+Packet*Efs*dist^2;
else
con=Packet*Eelec+Packet*Emp*dist^4;
end
end
```

بنابراین، ما مربع میانگین فاصله بین Cnode ها و گره های همسایه شان را در تمام شبکه با استفاده از فرمول زیر محاسبه می‌کنیم.

$$\text{فاصله میانگین} = \frac{\sum d_{avg}^2}{N}$$

d_{avg} فاصله میانگین در هر خوشه را نمایش میدهد و N تعداد خوشه های تولید شده است. در شبیه سازی ما برابر با ۱۷ می‌باشد. جدول نشان میدهد که در روش ما، فاصله مربع میانگین ما (۱۳۸,۲۴۷) بطور چشمگیری در مقایسه با روش تصادفی (۶۳۹,۵۴۳) و روش بِن اوتمان (۱۵۹,۲۰۹) کم می‌باشد. ما نتیجه گرفتیم که استفاده از روش ما بهره‌وری اقتصادی انرژی را تضمین میکند. بنابراین، عمر شبکه را طولانی میکند.

جدول۷: میانگین فاصله بین گره‌کنترلی و بقیه گره‌ها در سراسر شبکه

روشها	میانگینِ مسافت‌های مربع
روش تصادفی	۶۳۹,۰۴۳
روش بِن اوتمان	۱۵۹,۲۰۹
روش ما	۱۳۸,۲۴۷

بحث و نتیجه گیری

در این مقاله ما روش جدید راه حل امنیتی مبتنی بر خوشه‌بندی را برای شبکه‌های حسگر بیسیم ارائه دادیم. این روش شامل انتخاب گره‌های کنترلی به منظور ارتقا تصمیمِ حملاتِ DoS همچون Jamming و Greedy می‌باشد. ای روش مبتنی بر رویکرد LEACH است. این روش برای ساخت خوشه‌ها استفاده میشود. و بعد از آن ما مجددا آنرا بصورت بازگشتی به منظور انتخاب یک سرخوشه با گره‌هایی نه چندان دور به کار گرفتیم. گره انتخاب شده CH با هدف نظارت بر رفتار گره‌های اطرافش به کار گرفته شده است. نتایج شبیه سازی نشان میدهد که رویکرد ما در مقایسه با روش تصادفی بهتر است. در کارهای بعدی ما، ابتدا مطالعه مقایسه‌ای را بین نتایج به دست آمده از شبیه‌سازی روش پیشنهادی در این پروژه و دیگر روشهای خوشه‌بندی به عهده میگیریم. بعد از آن روش مان را با در نظر گرفتن دیگر پارامترهای عملکردی (تاخیر، توان عملیاتی و ...) را برای انتخاب درصد گره‌های در معرض خطا در جهت حمایت از شبکه‌های حسگر بیسیم ارتقا خواهیم داد.

منابع

[1] . حامد یار احمدی، مجتبی رشیدی ()، بررسی ومقایسه روش تشخیص نفوذ با روشهای مسیریابی امن برای مقابله با حملات DOS.

[2]. مسعود پورزحمتکش، علی پورزحمتکش، مینا فتحی (۱۳۹۱)، بررسی حملات لایه شبکه در شبکه‌های حسگر بیسیم، دومین کنفرانس ملی مهندسی نرم افزار.

[3] JunWu,1 Song Liu,1 Zhenyu Zhou,1 and Ming Zhan2 , Toward Intelligent Intrusion Prediction for Wireless Sensor Networks Using Three-Layer Brain-Like Learning Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012.

[4] Andreas A. Strikos, A full approach for Intrusion Detection in Wireless Sensor Networks, School of Information and Communication Technology KTH, Stockholm, Sweden 16453, March 1, 2007.

[5] Eui-Nam Huh and Tran Hong Hai, Lightweight Intrusion Detection for Wireless Sensor Networks, Kyung Hee University Republic of Korea 2011.

[6] Stamouli ,Ioanna.(2003); "Real-time Intrusion Detection for Ad hoc Networks",University of Dublin.

[7] Jhaveri, R.H. , Patel, S.J. , Jinwala, D.C. (2012);" DoS Attacks in Mobile Ad Hoc Networks: A Survey", Advanced Computing & Communication Technologies (ACCT), Second International Conference on,Pages 535 – 541.

[8] Lauf , Adrian P., Peters, Richard A., Robinson , William H.(2010);" A Distributed Intrusion Detection System for Resource-Constrained Devices in Ad Hoc Networks",Elsevier Journal of Ad Hoc Networks,Volume 8,Pages 253-266.

[9] Boorks,RR.,Carl,G.,Kesidis,G.,Rais,S.(2006);"Denial of Service Attack Detection Techniques",in Internet Computing, IEEE,Pages 82-89

[10] Mou Cheng, Chen., Kung, H.T., Koan-Sin Tan.(2002);" Use of Spectral Analysis in Defense Against Dos Attacks", Global Telecommunications Conference, GLOBECOM '02. IEEE, Volume 3,Pages 2143-2148.

[11] Jhaveri, R.H. , Patel, S.J. , Jinwala, D.C. (2012);" DoS Attacks in Mobile Ad Hoc Networks: A Survey", Advanced Computing & Communication Technologies (ACCT), Second International Conference on,Pages 535 – 541.

[12] S.A.Joshi, Varsha S.Pimprale .Network Intrusion Detection System (NIDS) based on Data Mining, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013.

[13] Julian May, Analysis of the NIDS Wave 1 Dataset, School of Development Studies University of Kwa-Zulu Natal, July 2009.

[14] Suman Rani, Vikram Singh, SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Network Invironment, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 1, 2010.

[15]. پایان نامه مروری بر داده کاوی و بررسی شبکه‌های عصبی در چند زمینه مختلف – فردین نوروزی و عارف طائفی همراه.

[16]. حامد یار احمدی، مجتبی رشیدی ()، بررسی ومقایسه روش تشخیص نفوذ با روشهای مسیریابی امن برای مقابله با حملات DOS.

[17]. D. Mansouri, L. Mokdad, Jalel Ben-othman, M. Ioualalen (2013), Detecting DoS attacks in WSN based on Clustering Technique.