
بسم الله الرحمن الرحيم

دانشکده برق و کامپیوتر

گروه مهندسی کامپیوتر

پایان‌نامه

برای دریافت درجه کارشناسی ارشد در رشته مهندسی کامپیوتر گرایش نرم افزار

عنوان

مسیریابی امن در شبکه‌های حسگر بی‌سیم

استاد راهنما

دکتر مینا زلفی لیقوان

استاد مشاور

دکتر سعید پاشازاده

پژوهشگر

سپیده مرادی

شهریور ۱۳۹۳

تقدیم به:

پدر و مادر عزیزم

تقدیر و تشکر

سپاس خدای را که نور شناختش را به قلب ما تابانید و شکرش را بر وجودمان الهام فرمود. دروازه بی پایان دانش به پروردگاریش را، بر ما گشود و ما را به وادی پر فیض توحید خالصانه اش، راهبری نمود و از هلاکت در ورطه انکار و شک و گمراهی بازمان داشت.

سر تعظیم فرود آورده و بوسه میزنم بر دستان پر خیر و برکت پدر و مادر عزیزم که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از کنار غفلت هایم گذشته اند و در تمامی مراحل زندگی ثانیه به ثانیه لبخندم را، علت و لحظه به لحظه غمم را شریک بودند.

سپاس گزار کسانی هستم که سرآغاز تولد دوباره من هستند. اساتیدی که سپیدی را بر تخته سیاه زندگیم نگاشتند.

به مصداق آیه شریفه " من لم یشکر المخلوق لم یشکر الخالق " بر خود وظیفه می دانم که مراتب سپاس گزاری و قدردانی خود را به محضر اساتید گرانقدرم، سرکار خانم دکتر مینا زلفی لیقوان، که با نکته ها و گفته های فصیح خود، همواره راهنمای بنده در اتمام این پایان نامه بوده اند، تقدیم دارم.

از استاد ارجمندم، جناب آقای دکتر سعید پاشازاده، صمیمانه سپاس گزارم که زحمت مشاوره این پایان نامه را متقبل شدند.

تشکر و سپاس فراوان از استاد مهربانم، سرخانم دکتر فرناز درخشان، که زحمت داوری این پایان نامه را قبول فرمودند.

سپاس بر همدلی و همراهی دوستان عزیزم و همه کسانی که صمیمانه و مشفقانه مرا در به انجام رساندن این مهم یاری نمودند.

نام خانوادگی: مرادی **نام:** سپیده

عنوان پایان نامه: مسیریابی امن در شبکه‌های حسگر بی‌سیم

استادان راهنما: دکتر مینا زلفی لیقوان

استاد مشاور: دکتر سعید پاشازاده

مقطع تحصیلی: کارشناسی ارشد **رشته:** مهندسی کامپیوتر **گرایش:** نرم افزار **دانشگاه:** تبریز

دانشکده: برق و کامپیوتر **تاریخ فارغ التحصیلی:** ۹۳ /۳/۱۹ **تعداد صفحات:** ۸۸

کلید واژه ها: عامل‌های متحرک، مسیریابی، مسیریابی امن، شبکه‌های حسگر بی‌سیم، توزیع شده

چکیده

شبکه حسگر بی‌سیم یک نوع از شبکه‌های بی‌سیم موردی و ترکیبی از حسگرهای کوچک است که به صورت انبوه در محیط پخش شده‌اند. گره‌های حسگر اساسا منابع و قدرت محدودی دارند. در تعدادی از کاربردهای این شبکه‌ها، تضمین امنیت یک مسئله حیاتی است. همچنین پروتکل‌های مسیریابی طراحی شده بیشتر بر روی قدرت گره‌ها تمرکز می‌کنند و کمتر جنبه امنیت را درنظر گرفته‌اند. از این‌رو اغلب الگوریتم‌های مسیریابی توسعه یافته برای این شبکه‌ها در برابر حملات آسیب‌پذیر هستند. نیازمندی‌های امنیتی شبکه‌های حسگر بی‌سیم شامل احراز هویت، صحت، تازگی اطلاعات و محرمانگی است. در سال‌های اخیر عامل‌های متحرک برای پخش موثر داده‌ها در شبکه‌های حسگر پیشنهاد شدند و تعدادی از محققین این عامل‌ها را به عنوان یک نمونه جدید و هوشمند برای اهداف توزیع شده و فائق آمدن بر محدودیت‌های شبکه‌های حسگر مورد استفاده قرار می‌دهند. ما در این پژوهش تعدادی از پروتکل‌های مسیریابی که بر مسیریابی امن تاکید دارند را مورد بررسی قرار می‌دهیم و سپس یک روش توزیع شده بر روی پروتکل مسیریابی AODV، جهت مقابله با حملات خارجی و تعدای از حملات داخلی(Sybil و Clone) موثر بر مسیریابی با استفاده از تکنولوژی عامل‌های متحرک در شبکه‌های حسگر بی‌سیم متحرک ارائه می‌دهیم. روش ارائه شده یک راه‌کار توزیع شده است و احراز هویت در شبکه را با رمزنگاری متقارن انجام می‌دهد. آنالیز و نتایج شبیه‌سازی، موثر بودن و کارآمدی روش ارائه شده را نشان می‌دهد. این روش تعداد بسته‌های از دست رفته در شبکه را کاهش و باعث افزایش عملکرد شبکه نسبت به الگوریتم‌های ارائه شده قبلی و پروتکل AODV می‌شود.

فهرست مطالب

عنوان **شماره صفحه**

فهرست شکل‌ها

عنوان **شماره صفحه**

فهرست جدول‌ها

عنوان **شماره صفحه**

فصل اول

کلیات تحقیق

۱-۱- مقدمه

امروزه زندگی بدون ارتباطات بی‌سیم قابل تصور نیست. پیشرفت تکنولوژی CMOS و ایجاد مدارهای کوچک و کوچکتر باعث شـده اسـت تا استفاده از مدارهای بی‌سیم در اغلب وسایل الکترونیکی امروز، ممکن شـود. این پیشـرفت همچنین باعث توسـعه ریزحسـگرها شده است. این ریزحسگرها توانایی انجام حس‌های بی‌شمار در کارهایی مانند شناسایی صدا برای حس‌کردن زلزله را دارا می‌باشند. همچنین جمع‌آوری اطلاعات در مناطق دور افتاده و مکان‌هایی که برای اکتشـافات انسـانی مناسـب نیسـتند را فراهم کرده‌اند. اتومبیل‌ها می‌توانند از ریزحسگرهای بی‌سیم برای کنترل وضعیت موتور، فشار تایرها، تراز روغن و غیره... استفاده‌کنند. خطوط مونتاژ می توانند از این حسـگرها برای کنترل فرایند مراحل تولید اسـتفاده کنند. در موقعیت‌های راهبردی ریزحسـگرها می توانند توسـط هواپیما بر روی خطوط دشـمن ریخته شوند و سپس برای ردگیری هدف (مانند ماشـین یا انسـان) استفاده شوند. شبکه‌های سنتی ارتباط بین انسان‌ها و پایگاه‌های اطلاعاتی را فراهم می‌کنند. درحالی که شبکه حس/کار مستقیما با جهان فیزیکی در ارتباط است و با استفاده از حسگرها محیط فیزیکی را مشـاهده کرده و براساس مشاهدات خود تصمیم‌گیری و عملیات مناسب را انجام می‌دهند. نام شـبکه حس/کار بی‌سـیم یک نام عمومی اسـت و برای کاربردهای مختلف طراحی می‌شـود. برخلاف شبکه‌های سنتی که همه منظوره‌اند شبکه‌های حس/کار تک منظوره هستند.

تکنیک‌ها و شـیوه‌های مورد استفاده در چنین شبکه‌ها وابستگی شدیدی به ماهیت کاربرد شبکه دارد. ساختار توپولوژی شبکه، شرایط جوی و محیطی، محدودیت‌ها و غیره... عوامل موثری در پارامترهای کارایی و هزینه شـبکه می‌باشند. لذا امروزه در سرتاسر دانشگاه‌های معتبر و مراکز تحقیقاتی کامپیوتری، الکترونیکی و بخصوص مخابراتی، شبکه‌های حسگر بی‌سیم یک زمینه تحقیقاتی بسیار جذاب و پرطرفدار محسوب می‌شود. هدف اصـلی تمامی این تلاش‌ها و ارائه راه‌کارها، داشتن سیستمی با شیوه‌های کنترلی ساده، آسان و با هزینه پائین اسـت که در نهایت با پاسـخگویی به نیازمندی‌های ما بتواند در مقابل محدودیت‌ها (پهنای باند، انرژی،

دخالت‌های محیطی، محوشدگی[1] و ...) ایستادگی کند و شرایط کلی را طبق تمایلات ما فراهم سازد.

از آنجا که عمل مسیریابی در شبکه‌های حسگر بر عهده خود گره‌های شرکت کننده در شبکه است، امنیت مسیریابی در این شبکه بیش از دیگر شبکه‌ها خود را نشان می‌دهد، از طرفی به خاطر محدودیت‌های ذاتی منابع و قدرت محاسباتی گره‌های حسگر، امنیت در شبکه‌های حسگر با چالش‌های متفاوتی نسبت به امنیت در شبکه‌های کامپیوتری سنتی روبرو هستند و فراهم آوردن امنیت اطلاعات در این شبکه‌ها بیش از پیش با مشکل همراه می‌سازد. تا به حال پروتکل‌های مسیریابی زیادی برای این شبکه‌ها ارائه شده است ولی تعداد کمی از آن‌ها به مقوله امنیت پرداخته‌اند.

۱-۲-بیان مسئله

خطر معمول در کلیه شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی موردنظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار مبتنی براستفاده از سیگنال‌های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از شبکه معرفی‌کرده و درصورت تحقق این امر امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهندگان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیر واقعی و گمراه‌کننده، سوءاستفاده از پهنای باند موثر شبکه و دیگر فعالیت‌های مخرب وجوددارد. در شبکه‌های حسگر بی‌سیم پروتکل‌های بسیاری به موضوع مسیریابی پرداخته‌اند. این پروتکل‌ها می‌توانند از دید ساختار شبکه به دسته‌های: مسیریابی تخت، سلسله مراتبی و مبتنی بر مکان تقسیم شوند. در مدل تخت همه گره‌ها نقش یا کار مساوی دارند اما در سلسله مراتبی گره‌ها نقش مختلفی بازی می‌کنند و در مدل مبتنی بر مکان نیز از موقعیت گره‌های سنسور برای مسیردهی داده در شبکه استفاده می‌شود. یک حمله استاندارد در شبکه‌های حسگر بی‌سیم، ایجاد پارازیت در یک گره یا گروهی از گره‌ها است. حمله بر روی اطلاعات در حال عبور در

[1] Fading

یک شبکه حسگر از دیگر موارد تهدیدکننده امنیت در این شبکه‌ها است، حسگرها تغییرات پارامترهای خاص و مقادیر را کنترل می‌کنند و طبق تقاضا به ایستگاه‌پایه[1] گزارش می‌دهند. در زمان ارسال گزارش ممکن است که اطلاعات در راه عبور تغییر کنند، مجدداً پخش شوند و یا ناپدیدگردند. از آنجایی که ارتباطات بی‌سیم در مقابل استراق سمع آسیب‌پذیر هستند، هر حمله‌کننده می‌تواند جریان ترافیک را کنترل کند، در عملیات وقفه ایجاد کند و یا بسته‌ها را جعل نماید. بنابراین اطلاعات اشتباه به ایستگاه ارسال می‌شود.

موضوع امنیت در برخی کاربردها بخصوص درکاربردهای نظامی یک موضوع بحرانی است و بخاطر برخی ویژگی شبکه‌های حسگر 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 می‌کند. مورد بعدی ویژگی پویایی توپولوژی است که زمینه را برای پذیرش گره‌های دشمن فراهم می‌کند. اینکه پروتکل مربوط به مسیردهی کنترل ترافیک و لایه کنترل دسترسی شبکه سعی دارند با هزینه و سربارکمتری کارکنند، مشکلات امنیتی بوجود می‌آورد. مثلا برای شبکه‌های حسگر در مقیاس‌های بزرگ برای کاهش تاخیر بسته‌هایی که در مسیر طولانی در شبکه حرکت می‌کنند، یک راه حل خوب این است که اولویت مسیردهی به بسته‌های عبوری داده شود. این روش باعث می‌شود حمله‌های سیلی موثرتر باشد. یکی از نقاط ضعف این شبکه‌ها کمبود منبع انرژی است و دشمن می‌تواند با قرار دادن یک گره مزاحم که مرتب پیغام‌های بیدار باش بصورت پخش همگانی که با انرژی زیاد تولید می‌کند و باعث می‌شود بدون دلیل گره‌های همسایه از حالت خواب خارج شوند. ادامه این روند باعث هدر رفتن انرژی گره‌ها شده و عمر آن‌ها را کوتاه می‌کند. با توجه به این محدودیت‌ها باید دنبال راه حل‌های ساده و کارا مبتنی بر طبیعت شبکه حسگر بود.

[1] Base Station

۱-۳- انگیزه و کاربرد امنیت در شبکه‌ها

امنیت یک موضوع حیاتی در شبکه‌های حسگر بی‌سیم[1] است. چرا که حسگرها، حامل اطلاعات مهمی برای کنترل کاربردهای مختلف مثل کنترل محیط یا آتش سوزی و غیره هستند. در این شبکه ها به دلیل ارتباطات ناامن و وجود یک کانال ارتباطی مشترک بین گره‌ها، مهاجم نسبت به شبکه‌های سیمی راحتر می‌تواند داده‌ها را کنترل و دستکاری کند. دو ویژگی سادگی و محدودیت منابع در شبکه‌های حسگر بی‌سیم آن ها را به شدت در برابر انواع حملات آسیب پذیر می کند. این حملات مانند استراق سمع در شبکه، تزریق بیت در کانال های ارتباطی، پخش مجدد بسته های اطلاعاتی و موارد دیگر می تواند در زمان انتقال امواج رادیویی رخ دهد.

برقراری امنیت در یک شبکه حسگر بی سیم نیاز به ایجاد شبکه های پشتیبانی شده از تمام خواص امنیتی اعم از محرمانگی، صداقت، صحت و قابلیت فراهم نمودن دسترسی در شبکه را دارد، مهاجمان شبکه ممکن است چندگره مخرب را به عنوان گره های مجاز در شبکه به منظور انتقال اطلاعات جایگزین نمایند و با این عمل مقدمات حمله به این سیستم را فراهم کنند. همچنین در برخی از موارد گره‌های مخرب ممکن است از طریق برقراری ارتباطی با کیفیت بالا حملات خود را ایجاد نمایند. در بسیاری از مواقع گره های حسگر شاید در برابر مداخله‌ها مقاوم نباشند و در صورتی که دشمن یک گره را کشف رمز نماید، قادر به استخراج تمام موارد کلیدی، داده‌ها و کدهای ذخیره شده در خصوص آن گره‌ها است. اگر چه ممکن است مقاومت در برابر بروز این حملات در برخی از شبکه‌ها مناسب باشد. ولیکن نمی‌توان آن را به عنوان یک راه حل عمومی دانست. بنابراین اگر یک مهاجم بتواند به این اطلاعات حساس دست پیدا کند، به راحتی می‌تواند در روند شبکه اختلال ایجاد کند و گاهی باعث تخریب داده‌های جمع‌آوری شده می‌شود. این ممکن است مسبب صدمات جبران ناپذیری در کنترل کاربرد مورد نظر باشد.

شبکه‌های حسگر بی‌سیم کاربردهای مختلفی در زمینه‌های مهمی دارند. شبکه‌های حسگر همچنین برای

[1] Wirless Sensor Network(WSN)

نظارت و مطالعه پدیده‌های طبیعی که ذاتا مانع از حضورانسان هستند، مانند طوفان و آتش سوزی جنگل‌ها می‌توانند مورد استفاده قرارگیرند. از کاربردهای عمومی مانند ارتباط وسایل نقلیه ازکاربردهای نظامی مانند ارتش، ردگیری اشیاء و ارتباط ناوکان جنگی، بهداشت مانند کنترل علائم حیاتی، محیط مانند آنالیز زیستگاه‌های طبیعی، مصارف صنعتی از جمله عیب‌یابی خط تولید، سرگرمی و بازی‌های مجازی و در مواردی در زندگی دیجیتالی به طور مثال ردگیری مکان پارک ماشین است. در همه این کاربردها در صورت دستکاری در اطلاعات و یا نفوذ عوامل مزاحم با اهداف مختلف باعث ایجاد مشکلاتی در روند شبکه‌ها یا به سرقت برده شدن اطلاعات محرمانه خواهد شد.

۱-۴-چالش‌ها

در ادامه تعدادی از موانع و چالش‌های پیاده سازی مکانیزم‌های امنیتی رایج برای شبکه‌های حسگر بیان شده است[۱]

حافظه و فضای ذخیره سازی محدود: هر حسگر دستگاه بسیار کوچکی است که مقدار کمی حافظه و فضای ذخیره‌سازی برای کد دارد.

محدودیت توان: فرض بر این است که بعد از استقرار شبکه حسگر، گره‌های شبکه به راحتی نمی‌توانند جایگذاری گردند یا آنکه شارژ شوند.

انتقال نامطمئن: به خاطر مسیریابی بر پایه بسته‌ها در شبکه‌های حسگر بی‌سیم ارتباطات بدون اتصال می‌باشند.

برخورد: اگر بسته ها در وسط راه خویش به هم برخورد نمایند عمل انتقال با شکست مواجه خواهد شد در شبکه‌هایی با چگالی بالا این امر می‌تواند به یک مشکل جدی تبدیل شود.

تاخیر: مسیریابی چندگامی ازدحام شبکه و پردازش گره‌ها می تواند به تاخیرهای زیادی منجر گردد، که ممکن است باعث عدم دست‌یابی به همگام سازی در شبکه‌های حسگر بی‌سیم گردد.

حملات تصاحب گره: حسگرها می‌توانند در محیط‌های قابل دسترس برای دشمن مستقر گردد.

۱-۵- نوآوری

در این پایان‌نامه از عامل‌های متحرک[1] به عنوان قطعه کد و نمونه‌های هوشمند و خود کنترل، برای مسیریابی امن در شبکه‌های حسگر استفاده شده است. عامل‌های متحرک علاوه‌بر انتقال داده‌ها، می‌توانند محاسبات و وظایفی را نیز در شبکه انجام دهند و به جای انتقال داده‌ها از کانال‌های ارتباطی نا امن به سمت ایستگاه‌پایه، برنامه‌هایی اجرایی به سمت داده‌های جمع‌آوری شده برده شود. این کار باعث کاهش هزینه‌های ارتباطی خواهد شد، بنابراین برای کاربردهایی که کمبود پهنای باند دارند مانند شبکه‌های حسگر بی‌سیم بسیار مناسب هستند، عامل‌های متحرک بیشتر در محیط های توزیع شده[2] کاربرد دارند.

۱-۶- ساختار پایان نامه

ادامه این نوشتار، مشتمل بر مطالب زیر است:

فصل دوم به مفاهیم اولیه در خصوص شبکه‌های حسگر بی‌سیم، انواع و طبقه‌بندی پروتکل‌های مسیریابی، عامل‌های متحرک، انواع نیازمندی‌های امنیتی پروتکل‌ها و موضوع‌های استفاده شده برای برقراری امنیت و انواع و طبقه‌بندی حملات مختلف در لایه‌های مختلف اختصاص دارد که برای فهم بهتر روش‌های مختلف مسیریابی امن ضروری است. در فصل سوم به روش‌های ارائه شده مسیریابی‌های امن در شبکه‌های حسگر بی‌سیم پرداخته شده است. فصل چهارم به شرح روش پیشنهادی، چگونگی شبیه‌سازی صورت گرفته و نحوه استفاده از عامل های متحرک برای مسیریابی امن و نتایج حاصل از روش پیشنهادی و مقایسه آن با روش‌های قبلی در زمینه مسیریابی و مسیریابی امن اختصاص داده شده است. فصل پنجم نیز جمع‌بندی و نتیجه‌گیری پژوهش انجام شده و پیشنهاداتی برای کارهای آینده در این زمینه پرداخته شده است.

---

[1] Mobile Agents

[2] Distributed

فصل دوم

مفاهیم پایه

۲-۱- مقدمه

امروزه اســتفاده از شبکه‌های حسگر بی‌سیم درحال رشد است و در زمینه‌های مختلف مورد استفاده قرار می‌گیرد. مســیریابی در شبکه‌های حسگر به دلیل ویژگی‌های برجسته این شبکه‌ها بسیار چالش برانگیز است و آن‌ها را از شبکه‌های بی‌سیم موردی[1] از جنبه‌های مختلف جدا می‌کند. از طرفی امنیت نیز برای این شــبکه‌ها به دلیل انتقال اطلاعات حیاتی در بعضی از کاربردهای این شبکه، جایگاه خاصی خواهد داشت. در این فصــل تعدادی مفاهیم پایه در مورد شبکه‌های حسگر، امنیت این شبکه‌ها و مفاهیم پایه در مورد عناصر استفاده شده در این پایان‌نامه را بیان می‌کنیم.

۲-۲- شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر یک نوع از شبکه موردی می‌باشند[۱]. شبکه حسگر شبکه‌ای شامل صدها یا هزاران گره کوچک اســت. در هرگره تعدادی حسگر وجود دارد، گره‌های حسگر نوعا از لحاظ فیزیکی بسیار کوچک هستند و دستگاه‌هایی کم هزینه، مجهز به حسگرهای محیطی و امواج رادیویی برای ارتباطات بی‌سیم است. کاربردهای اصلی شبکه‌های حسگر بی‌سیم حداقل، به تعدادی سطوح امنیتی نیازمند هستند. شبکه حسگر با شــــدت با محیط تعامل دارد و در محیط‌های مورد نظر برای جمع‌آوری و پردازش اطلاعات محیطی پخش می‌شــوند. هر گره به صــورت مســتقل و بدون دخالت انســان کار می‌کند. در اغلب موارد گره حسگر کوچک مجهز به فرســتنده و گیرنده رادیویی، یک آنتن، یک پردازنده و باتری است. این وسیله در محاسبات، میزان ارتباطات بی‌ســیم و حافظه ذاتا محدود است. هدف آن‌ها حس کردن نمونه‌ها در محیط، جمع‌آوری داده‌ها و ارســال اطلاعات به ســمت ایستگاه‌پایه است. حسگرها می‌توانند در دو حالت ثابت یا متحرک باشند، به دلیل عدم دســترسی به حسگرها بعد از پخش آن‌ها در محیط، گره‌ها پس از مصرف انرژی موجود، در عمل بدون استفاده می‌شوند و به اصطلاح می‌میرند. بنابراین مسئله انرژی و بهینه‌سازی آن یکی از چالش‌های موجود در این شــبکه‌ها اســت. حسگرهایی که به دستگاه‌ها وسازه‌ها متصل شده یا در محیط زیست قرارداده می‌شوند،

[1] Ad Hoc