دانشگاه صنعتی اصفهان

دانشکده‌ی مهندسی برق و کامپیوتر

مدیریت کلید در شبکه‌های حسگر بی‌سیم

رساله‌ی دکترای مهندسی برق- کامپیوتر

علی فانیان

استاد راهنما

دکتر مهدی برنجکوب

۱۳۹۰


بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

مدیریت کلید در شبکه‌های حسگر بی‌سیم

رساله دکترای مهندسی برق-کامپیوتر

علی فانیان

استاد راهنما

دکتر مهدی برنجکوب

۱۳۹۰

دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

رساله دکترای مهندسی برق-کامپیوتر آقای علی فانیان

تحت عنوان

مدیریت کلید در شبکه‌های حسگر بی‌سیم

در تاریخ ۱۳۹۰/۱/۲۴ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای رساله	دکتر مهدی برنجکوب
۲- استاد مشاور رساله	دکتر حسین سعیدی
۳- استاد داور	دکتر محمود سلماسی‌زاده
۴- استاد داور	دکتر پژمان خدیوی
۵- استاد داور	دکتر مهران سلیمان فلاح
سرپرست تحصیلات تکمیلی دانشکده	دکتر سید محمود مدرس‌هاشمی

تشکر و قدردانی

می خواهم از خداوند یکتا به خاطر تمامی نعمت هایی که به من ارزانی داشت سپاسگزاری کنم. در اندیشه ام که چگونه! چون نمی توانم. پس پناه می برم به حدیث شریف "من لم یشکر المنعم من المخلوقین لم یشکر الله". پس از استاد راهنمای ارجمندم، جناب آقای دکتر برنجکوب که بار، نمودهای دلسوزانه، در طول دوران تحقیق همراه من بودند قدردانی می کنم. از جناب آقای دکتر سعیدی به خاطر مشاوره های ارزنده شان سپاسگزارم. از اساتید گرانقدر آقایان دکتر محمود سلاسی زاده، دکتر مهران سلیمان فلاح و پژمان خدیوی که زحمت داوری این پایان نامه را پذیرفتند و بار، نمودهای خود به ارتقای آن کمک نمودند، صمیمانه قدردانی می نمایم.

دست ادب بر سینه می گذارم و دستان مادرم، که با صبوری خود به من صبر کردن آموخت و پدرم، که با تلاش خود به من تلاش کردن آموخت می بوسم و از زحمات ایشان سپاسگزارم.

سپاسی صمیمانه از همسرم به خاطر همدلی های خالصانه اش، بی شک تلاش و از خودگذشتگی این عزیز باعث شد تا من با آسودگی خیال به امر تحقیق بپردازم. براستی که همراهی ایشان یکی از بزرگترین مواهب الهی بر من بوده است.

بر خود لازم می دانم که از توجه، راهنمایی، تشویق و همکاری دوستان بسیار ارجمند خود در آزمایشگاه تحقیقاتی رمزنگاری و امنیت سیستم ها سپاسگزاری کنم.

از آقای دکتر سیدی، نماینده ی تحصیلات تکمیلی دانشکده، آقای دکتر مدرس هاشمی سرپرست تحصیلات تکمیلی و سرکار خانم نکویی به خاطر زحمات بی دریغشان تشکر و قدردانی می کنم.

تقدیم به

همسر

و

فرزند دلبندم علی رضا

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

چکیده

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم، توانایی طراحی و ساخت حسگرهایی با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربری‌های گوناگون را به وجود آورده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی، پردازش اطلاعات و ارسال آن‌ها را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های حسگر بی‌سیم شده‌اند. یک شبکه حسگر متشکل از تعداد زیادی گره حسگر است که در یک محیط به طور گسترده پخش می‌شوند. با توجه به این که ممکن است گره‌های حسگر در محیط‌های عملیاتی ناامن قرار گیرند، مخصوصا در کاربردهای نظامی، امنیت یکی از پارامترهای مهم و ضروری در این شبکه‌ها است. از این رو سرویس‌های امنیتی نظیر احراز اصالت و محرمانگی باید در این شبکه‌ها مورد استفاده قرار گیرند تا بتوان از عملکرد گره‌ها و در نهایت شبکه مطمئن بود. ارائه این سرویس‌ها در سطح شبکه مستلزم وجود یک زیر ساخت امنیتی بین گره‌های شبکه است که به شکل مناسبی کلیدهای مشترکی را برای احراز اصالت و محرمانگی گره‌ها فراهم نماید. چارچوبی که طی آن نیازمندی فوق برآورده می‌شود را مدیریت کلید می‌گویند. در چند سال اخیر روش‌های زیادی برای مدیریت کلید در شبکه‌های حسگر بی‌سیم ارائه شده است. اهم پروتکل‌های ارائه شده مبتنی بر سه روش توزیع کلید تصادفی، Blom و چند جمله‌ای متقارن هستند. برخی از این روش‌ها از همبندی محلی و مقاومت مناسبی در قبال افشای کلید برخوردار هستند اما نیاز به صرف منابع زیادی در گره‌های حسگر دارند به طوری که استفاده از آن‌ها در گره‌های حسگر مقدور نیست. در مقابل، برخی دیگر از این روش‌ها از نظر مصرف منابع مناسب هستند اما با چالش‌های امنیتی و یا کارایی روبرو هستند. در این رساله ابتدا با بررسی و شناخت چالش‌های فراروی شبکه‌های حسگر سعی در طراحی پروتکل‌های مدیریت کلیدی است که قابل به کارگیری در گره‌های حسگر باشند و همچنین کارآمدی و امنیت آن‌ها در سطح قابل قبولی باشد. به این منظور، پس از شناخت مسائل پیرامون مدیریت کلید در شبکه‌های حسگر چارچوبی برای طراحی پروتکل‌های مدیریت کلید جدید ارائه می‌گردد و به دنبال آن چهار پروتکل با نام‌های SKEP، KELR، HKEP و HKey به منظور استفاده در کاربردهای مختلف ارائه می‌گردد. در پروتکل‌های پیشنهادی با استفاده از ساختارهای منظم در گروه‌بندی گره‌ها در شبکه سعی می‌شود دو گره قبل از هر گونه تماس با یکدیگر از امکان تولید کلید مشترک با یکدیگر با خبر باشند. برای ارزیابی کارایی پروتکل‌های پیشنهادی و اهم پروتکل‌های در دسترس پارامترهای مختلفی از قبیل همبندی محلی، حافظه مصرفی، امنیت کلیدهای ارتباطی در مقابل تبانی گره‌های تسخیر شده و انرژی مصرفی از طریق شبیه‌سازی و یا اثبات ریاضی مورد مقایسه قرار می‌گیرند. به منظور مقایسه عادلانه پروتکل‌ها از نظر میزان حافظه و انرژی مصرفی در گره‌ها، شرایط امنیت کامل در نظر گرفته می‌شود. از سوی دیگر برای اینکه بتوان با یک مقایسه اجمالی کارایی پروتکل‌های مختلف را مشاهده نمود، با انتخاب یک گره حسگر معروف مقدار پارامترهای تأثیرگذار در کارایی پروتکل‌های مختلف به طور سرجمع مورد مقایسه قرار می‌گیرند. نتایج بدست آمده نشان دهنده کارایی مناسب پروتکل‌های طراحی شده، به ویژه پروتکل HKey، نسبت به سایر پروتکل‌های موجود است.

کلمات کلیدی : ۱- مدیریت کلید ۲- شبکه‌های حسگر ۳- چند جمله‌ای متقارن ٤- توزیع کلید تصادفی ٥- امنیت کامل

فصل اول

مقدمه

۱-۱ مقدمه

با پیشرفت حاصل شده در دهه اخیر در زمینه شبکه‌های بی‌سیم استفاده از این شبکه‌ها به شدت رو به گسترش است. در این شبکه‌ها عموماً گره‌ها از کانال مشترک برای تبادل اطلاعات استفاده می‌نمایند. این خصوصیت باعث می‌شود تا دسترسی به اطلاعات دیگران به طور غیر مجاز امکان پذیر شده و زمینه بروز حملات مختلف فراهم گردد. از این رو امنیت اطلاعات در شبکه‌های بی‌سیم با چالش‌های جدی مواجه است که نیازمند بررسی و ارائه راه‌کارهایی برای بهبود سطح امنیت در این شبکه‌ها است.

در یک دسته بندی کلی شبکه‌های بی‌سیم را می‌توان به دو دسته شبکه‌های ساختارمند و بدون ساختار تقسیم کرد [۱]. در شبکه‌های ساختارمند به راه‌اندازی ساختار اولیه برای ایجاد شبکه نیاز است. یکی از معروفترین شبکه‌های ساختارمند شبکه‌های سلولی هستند. در شبکه‌های سلولی، محیط تحت پوشش به سلول‌هایی تقسیم‌بندی می‌شود و در هر سلول از یک ایستگاه مرکزی برای برقراری ارتباط کاربران با یکدیگر استفاده می‌گردد. در شبکه‌های بدون ساختار نیازی به ایجاد ساختار از پیش تعیین شده وجود ندارد. شبکه‌های اقتضایی[1] و حسگر نمونه‌هایی از شبکه‌های

[1] ad-hoc network

بدون ساختار هستند که به شدت مورد توجه قرار گرفته‌اند. این شبکه‌ها با اجتماع تعدادی گره بی‌سیم با هزینه کم راه‌اندازی می‌شوند [۲، ۳، ۴]. این ویژگی باعث شده است که این شبکه‌ها در حوزه‌های مختلف به ویژه دفاعی، زیست محیطی و علمی کاربردهای زیادی پیدا کنند [۵، ۶، ۷]. با توجه به آنکه شبکه‌های حسگر در آینده در کاربردهای مختلف مورد استفاده قرار می‌گیرند، در این رساله مباحث پیرامون مدیریت کلید در این شبکه‌ها مورد تحقیق و بررسی قرار خواهد گرفت. شبکه‌های حسگر بر اساس نوع سخت‌افزار مورد استفاده به دو دسته همگن[۱] و ناهمگن[۲] تقسیم‌بندی می‌شوند [۸]. در شبکه‌های که از حسگرهای همگن استفاده می‌شود قابلیت سخت‌افزار گره‌ها شبیه بهم است. اما در گره‌های ناهمگن سخت‌افزار گره‌ها مشابه نیستند و دارای قابلیت‌های مختلف می‌باشند. در یک دسته بندی دیگر که بر اساس نقش گره‌های حسگر در شبکه انجام می‌شوند، شبکه‌های حسگر به دو دسته مسطح[۳] و سلسه مراتبی[۴] تقسیم‌بندی می‌شوند [۹، ۱۰، ۱۱]. در شبکه‌های حسگر مسطح نقش گره‌های حسگر در شبکه مشابه هستند اما در شبکه‌های سلسه مراتبی گره‌ها با توجه به قابلیت‌ها و امکاناتشان وظایف و نقشهای متفاوتی دارند. در این رساله شبکه‌های حسگر مسطح مورد توجه و تحقیق قرار گرفته‌اند. از این رو در ادامه منظور از شبکه‌های حسگر، شبکه‌های حسگر مسطح است.

در این فصل ابتدا شبکه‌های حسگر معرفی خواهد شد و پس از آن مؤلفه‌های امنیتی و مکانیزم‌های امنیتی مورد نیاز مرور خواهد شد. در پایان فصل نیز ساختار ادامه گزارش خواهد آمد.

۱-۲ شبکه‌های حسگر بی‌سیم

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم، توانایی طراحی و ساخت حسگرهایی با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربردهای گوناگون را به وجود آورده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی (بر اساس نوع حسگر)، پردازش اطلاعات و ارسال آن‌ها را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های بی‌سیم حسگر شده‌اند. شبکه‌های حسگر در واقع زیر مجموعه‌ای از شبکه‌های اقتضایی محسوب می‌شوند که در آن‌ها توان پردازشی و رادیویی گره‌های حسگر بسیار پایین می‌باشد [۱۲].

---

[1] homogeneous
[2] heterogeneous
[3] flat
[4] hierarchical

یک شبکه حسگر متشکل از تعداد زیادی گره‌های حسگر است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. لزوماً مکان قرار گرفتن گره‌های حسگر، از قبل‌تعیین‌شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آن‌ها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم. این بدان معنی است که پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی‌های خودسازماندهی باشند [۱۳].

هر گره حسگر بر روی سخت‌افزار خود دارای یک پردازشگر می‌باشد و به جای فرستادن تمامی اطلاعات خام به مرکز یا به گره دیگر که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را بر روی اطلاعات انجام می‌دهد و سپس نتایج و یا در صورت لزوم داده‌ها را ارسال می‌کند. از طرف دیگر ممکن است یک گره حسگر به صورت کارانداز[1] عمل کند و یک عمل خاصی مانند قطع و وصل یک کلید را انجام دهد. بنابراین تبادل اطلاعات در شبکه‌های حسگر /کارانداز به صورت دوطرفه صورت می‌گیرد.

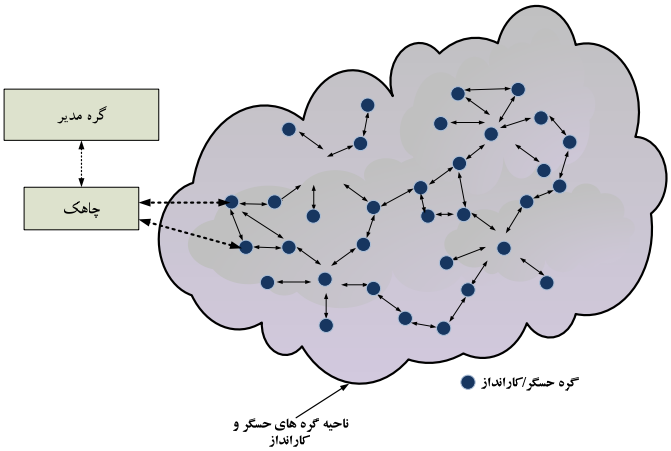
با اینکه هر حسگر به تنهایی توانایی ناچیزی دارد، ترکیب صدها حسگر کوچک امکانات جدیدی را برای کل شبکه عرضه می‌کند. در واقع قدرت شبکه‌های بی‌سیم حسگر در توانایی به‌کارگیری تعداد زیادی گره کوچک است که قادرند به شکل خودکار سازماندهی شوند و در موارد متعددی چون مسیریابی هم‌زمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند.

در ابتدای راه اندازی شبکه حسگر، گره‌های حسگر به صورت نامنظم در یک منطقه پراکنده می‌شوند. هر کدام از این گره‌های پخش‌شده دارای توانایی جمع‌کردن اطلاعات و ارسال آن‌ها به پایانه‌ای موسوم به چاهک[2] هستند. این اطلاعات از یک مسیر چند گامی[3] که زیرساخت مشخصی ندارد (همانند شبکه اقتضایی) به چاهک فرستاده می‌شوند و چاهک می‌تواند توسط ارتباط ماهواره یا اینترنت با گره مدیر ارتباط برقرار کند. از سوی دیگر یک چاهک یا مدیر ممکن است اطلاعات خاصی را برای گره‌های حسگر یا کارانداز ارسال نماید [۱۴].

طراحی یک شبکه حسگر تحت تأثیر عوامل متعددی می‌باشد. این عوامل عبارتند از: تحمل خرابی، قابلیت گسترش، هزینه تولید، محیط کار، توپولوژی شبکه حسگر، محدودیت‌های سخت‌افزاری، محیط انتقال و مصرف توان. در شکل ۱-۱ ساختار کلی شبکه حسگر مشاهده می‌شود.

---

[1] actuator
[2] sink
[3] multi-hop



شکل ۱-۱: ساختار کلی شبکه حسگر

۱-۳ مروری بر مفاهیم کلی امنیت

بدون شک زندگی امروز بشر از مقوله ارتباطات تفکیک ناپذیر است. ارتباطات به حدی فاصله‌های دور را به هم نزدیک کرده است که از دنیای بزرگ ما به نام دهکده جهانی یاد می‌شود. ارتباطات آنقدر با زندگی روزمره ما عجین شده است که نمی‌توانیم حتی زندگی بدون آنرا تصور کنیم. در حالیکه تا قرنی پیش مبادله خبر به روزها زمان نیاز داشت، اینکار اکنون تقریباً آنی انجام می‌شود. مخابرات، اینترنت و وسایل ارتباط جمعی نمونه‌هایی از ارتباطات امروزه ما هستند که تبادل اطلاعات و انجام امور روزمره ما را با سهولت بیشتر و هزینه کمتر ممکن ساخته است.

از طرف دیگر گسترش ارتباطات شبکه‌ای و نفوذ آن به دوردست‌ترین نقاط جهان باعث شده است زمینه سوء استفاده افراد سودجو هم فراهم شود. در حالیکه هم‌اکنون انجام معاملات کلان اقتصادی و تبادل اطلاعات حیاتی در کوتاهترین زمان به راحتی و با هزینه ناچیز روی شبکه‌های کامپیوتری و اینترنت قابل انجام است، اما انجام این امور بدون در نظر گرفتن تمام جنبه‌های امنیتی، ممکن است باعث ضررهای جبران ناپذیری گردد. از همین جا لزوم امنیت شبکه و ایجاد ارتباط امن احساس می‌شود. برای آشنایی دقیق‌تر با ابعاد امنیت، در این بخش مفاهیم کلی امنیت مرور خواهند شد.

۱-۳-۱ مؤلفه‌های امنیتی

برای تبیین مفهوم امنیت باید به مؤلفه‌های برقراری امنیت در شبکه‌های کامپیوتری پرداخت. این مؤلفه‌ها شامل محرمانگی[1]، صحت[2] و دسترس پذیری[1] است [۱۵، ۱۶، ۱۷، ۱۸] که در ادامه معرفی می‌شوند.

[1] confidentiality
[2] integrity