
بسم الله الرحمن الرحيم

سمینار

عنوان

امنیت مسیریابی در شبکه‌های حسگر بی‌سیم

فهرست مطالب

فصل سوم: بررسی پروتکل‌های امنیت مسیریابی

فصل چهارم: نتیجه گیری و پیشنهادات

فهرست اشکال

چکیده

با توجه به پیشرفت روز افزون شبکه‌های حسگر بی‌سیم، بحث و بررسی پروتکل‌ها در این زمینه از اهمیت بالایی برخوردار می‌گردد. یکی از این پروتکل‌ها در شبکه حسگر بی‌سیم، پروتکل مبتنی بر مسیریابی می‌باشد. 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 تدرت محاسباتی گره های حسگر، امنیت در شبکه‌های حسگر با چالشهای متفاوتی نسبت به امنیت در شبکه‌های کامپیوتری سنتی روبرو هستند و فراهم آوردن امنیت مسیریابی در این شبکه‌ها بیش از پیش با مشکل همراه می‌سازد. تا به حال پروتکل‌های مسیریابی زیادی برای این شبکه‌ها اراقه شده است ولی تعداد کمی از آنها به مقوله امنیت پرداخته‌اند. در این سمینار به بررسی جامع در مورد مسیریابی شبکه های حسگر بخصوص پروتکل های امنیت مسیریابی پرداخته شده است.

واژه‌های کلیدی: شبکه حسگر بی‌سیم، مسیریابی، امنیت، پروتکل، حملات، پروتکل، گره.

فصل اول

مقدمه

۱ ـ ۱ ـ مقدمه

یک شبکه حسگر بی‌سیم، از تعداد زیادی گره‌های حسگر تشکیل شده است که در یک محیط به طور گسترده پخش شده و به جمع آوری اطلاعات از محیط می‌پردازند. شبکه‌های حسگر بی‌سیم، شبکه‌هایی هستند که در خیلی از کاربردهای مهم مورد استفاده قرار می‌گیرند و نیاز به پاسخ بلادرنگ و سریع در زمان تعیین شده می‌باشد. حسگرها بایستی بدون دخالت انسان و به صورت خودمحور با یکدیگر هماهنگی‌های لازم را در جهت نیل به هدف انجام دهند. خطر معمول در کلیه شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی موردنظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار مبتنی بر استفاده از سیگنالهای رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واتع 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 معرفی کرده و درصورت تحقق این امر امکان دستیابی به اطلاعات حیاتی، حیله به سرویس دهندگان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیر واتعی و گمراه کننده، سوء استفاده 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 موتعیت 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 یک شبکه حسگر از دیگر موارد تهدیدکننده امنیت در این شبکه‌ها است، حسگرها تغییرات پارامترهای خاص و مقادیر را کنترل می‌کنند و طب تقاضا به ایستگاه پایه گزارش می‌دهند[1]. 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 سیع آسیب‌پذیر هستند، هر حمله کننده میتواند جریان ترافیک را کنترل کند، در عملیات وقفه ایجاد کند و یا بسته‌ها را جعل نیاید. بنابراین اطلاعات اشتباه به ایستگاه ارسال می‌شود. موضوع امنیت در برخی کاربردها بخصوص در کاربردهای نظامی یک موضوع بحرانی است و بخاطر برخی ویژگی شبکه‌های حسگر در مقابل مداخلات آسیب‌پذیرترند. یک مورد بی‌سیم بودن ارتباط شبکه است که کار دشین 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 آسیب پذیر می‌کند. مورد بعدی ویژگی پویایی توپولویی 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 سربار کمتری کار کنند، 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 شده‌اند. 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[2].