نقاط ضعف امنیتی در شبکه های حسگر بیسیم

ناهید ابراهیمی

۱- ارشد مخابرات-دانشگاه صنعتی شیراز.ebrahimi.cm.en.el@gmail.com

چکیده

شبکه های بیسیم یکی از شاخه های علم مخابرات در عصر حاضر هستند که اثرات آن در زندگی روزمره به وضوح دیده می شود. در نوع خاص از این شبکه ها، مجموعه ای از حسگرها برای جمع آوری اطلاعات در یک محیط بیسیم با یکدیگر مرتبط هستند و به نام شبکه های حسگر بیسیم شناخته می شوند. از آنجایی که امنیت و حفاظت حریم شخصی در بسیاری از کاربردهای پیشنهادی مربوط به شبکه های حسگر بیسیم بسیار با اهمیت هستند شبکه های حسگر بیسیم معمولاً برای جمع آوری رکوردها از محیط غیر ایمن تنظیم می شوند. تقریباً تمامی پروتکل های امنیتی WSN بر این تاکید دارند که یک مهاجم میتواند به طور کلی یک گره حسگر را با روش دسترسی فیزیکی مستقیم کنترل نماید. ظهور شبکه های حسگر به عنوان یکی از تکنولوژیهای عمده در آینده، چالشهای مختلفی را برای محققان در پی داشته است. شبکه های حسگر بیسیم از تعداد زیادی گره حسگر کوچک که جداگانه اجرا می شوند و در موارد مختلف بدون دسترسی به منابع تجدیدپذیر انرژی تشکیل شده است. علاوه بر این امنیت بحث اساسی در پذیرش و بکارگیری شبکه های حسگر برای کاربردهای مختلف است؛ همچنین چالش های مختلفی در شبکه های حسگر نیز وجود دارد. در این مقاله امنیت شبکه های حسگر بیسیم مورد بررسی قرار خواهد گرفت.

کلمات کلیدی: شبکه های حسگر بیسم،امنیت شبکه حسگر،ضعف شبکه.

۱. مقدمه

این 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. یک حمله استاندارد در شبکه‌های حسگر بی‌سیم، ایجاد پارازیت در یک گره یا گروهی از گره‌ها می باشد. حمله بر روی اطلاعات در حال عبور در یک شبکه حسگر از دیگر موارد تهدید کننده امنیت در این شبکه ها است، حسگرها تغییرات پارامترهای