نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

بررسی و مقایسه روش‌های تشخیص و مقابله با حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم

ساجده حرّاز[۱]، علی‌محمّد افشین همّت‌یار[۲]

[۱] کارشناس ارشد، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران
harraz@ce.sharif.edu

[۲] استادیار، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران
hemmatyar@sharif.edu

چکیده

امروزه کاربران شبکه‌های حسگر بی‌سیم علاوه بر غلبه بر چالش‌هایی نظیر محدودیت انرژی، باید با چالش‌های ناشی از حملات مهاجمین به شبکه نیز مقابله کنند. یکی از حملات متداول در شبکه‌های حسگر بی‌سیم، حمله کرم‌چاله است که در آن مهاجمین، یک لینک سریع و با تاخیر کم را بین دو نقطه از شبکه ایجاد می‌کنند. این حمله با توافق دو یا چند گره از شبکه یا با اضافه کردن چندین گره مخرب جدید امکان‌پذیر است. پس از آن‌که لینک ایجاد شد، مهاجم داده‌ها را از یک طرف لینک جمع‌آوری کرده و از طریق لینک سریع ایجاد شده آن‌ها را به سمت دیگر شبکه می‌فرستد. این حمله در جریان انتقال داده‌ها تغییر ایجاد می‌کند و سبب گمراه شدن چاهک می‌شود. حمله کرم‌چاله به سادگی انجام می‌شود و تشخیص آن راحت نیست، چرا که اطلاعات منتقل شده اغلب معتبر هستند. در این مقاله به بررسی روش‌های بکارگرفته شده برای حمله کرم‌چاله می‌پردازیم و روش‌های مختلف مقابله با آن در شبکه‌های حسگر بی‌سیم را بررسی می‌کنیم.

کلمات کلیدی: شبکه‌حسگربی‌سیم، حمله کرم‌چاله، تشخیص نفوذ

۱ مقدمه

شبکه حسگر بی‌سیم متشکل از تعداد زیادی گره‌های حسگر است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. امروزه با توجه به افزایش کاربردهای این شبکه‌ها از جمله کاربردهای محیطی، پزشکی، نظامی، صنعتی و ... نیاز به برقراری امنیت به صورت بهینه و کارا احساس می‌شود. تکنیک‌های امنیتی که در شبکه‌های سنتی قابل استفاده‌اند در شبکه‌های حسگر قابل پیاده‌سازی نخواهند بود. به عنوان مثال در این شبکه‌ها نمی‌توان الگوریتم امضاء دیجیتال را به کار برد زیرا از نظر میزان حافظه و محاسبات، محدودیت وجود دارد. لذا می‌بایست الگوریتم‌هایی را در خصوص مرتفع کردن نیاز امنیتی این شبکه‌ها به کاربرد، که منابع حسگر را کمتر مصرف کنند[1] . اهداف امنیتی شبکه‌های حسگر بی‌سیم عبارتند از:

- محرمانگی داده: محرمانگی داده به مفهوم رمز نمودن داده‌ها جهت غیرقابل درک کردن آن از دید حسگرهای غیرمجاز است، که می‌توان آن را به عنوان اولین نیاز امنیتی شبکه‌های حسگر برشمرد.
- صحت داده: الگوریتم‌های صحت داده در خصوص عدم دستکاری داده در بین راه توسط حسگرهای دیگر ارائه شده‌اند. در ابتدایی‌ترین راهکار می‌توان کد تصدیق پیغام را محاسبه و آن را توسط پیام اصلی ارسال نمود.
- تازگی داده‌ها: امکان ارسال مجدد داده‌های قبلی را از حسگرهای دشمن گرفته و تضمین می‌کنند داده‌هایی که اخیرا توسط گیرنده دریافت شده‌اند، تازه بوده و قدیمی نمی‌باشند.
- مقاومت و ضربه‌پذیری : شبکه‌های حسگر باید در مقابله با حملات بسیاری مقاوم باشند و همچنین اگر حمله‌ای به طور موفقیت‌آمیز صورت گرفت این حمله باید دارای تاثیری محلی باشد و کل شبکه را مختل نکند [2] .

در این مقاله به بررسی و مقایسه روش‌های مختلف مقابله با حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم می‌پردازیم. در ادامه ابتدا به بررسی انواع حملات در لایه شبکه، شبکه‌های حسگر بی‌سیم می‌پردازیم سپس دسته‌بندی از حملات کرم‌چاله بیان خواهیم کرد. بعد از آن به بررسی انواع روش‌های مقابله با این حمله می‌پردازیم و در نهایت روش‌های مقابله بیان شده را مقایسه می‌کنیم.