نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، 15-13 اسفندماه 1392

ارائه یک الگوریتم جهت شناسایی گره‌های سایبیل با استفاده از گره نگهبان و اطلاعات مدل همسایگی گره‌ها درشبکه‌های حسگر متحرک

رضوان الماس شهنی[1]، کریم فائز[2]

[1] دانشکده برق، رایانه و فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد قزوین، قزوین
r.shehni@qiau.ac.ir
[2] دانشکده برق، دانشگاه صنعتی امیرکبیر، تهران
kfaez@aut.ac.ir

چکیده

برقراری امنیت در شبکه‌های حسگراز نیازهای جدی در این شبکه‌هاست.از مسائل مهم در امنیت مقابله با حملات شبکه است.حمله سایبیل یکی از حمله های مهم در شبکه‌های حسگرمی‌باشد که در آن یک گره بدخواه با انتشار چندین شناسه جعلی از خود اقدام به مختل کردن عملیات‌های شبکه از جمله پروتکل‌های مسیریابی،رای‌گیری وتجمیع داده می‌کند.در شبکه‌های متحرک بدلیل ثابت نبودن گره‌ها و به دنبال آن متغییر بودن توپولوژی شبکه، شناسایی این حمله دشوارتر است.در این مقاله ، یک الگوریتم با استفاده از گره‌های نگهبان و اطلاعات مدل همسایگی گره‌ها جهت شناسایی گره‌های سایبیل در شبکه‌های حسگر متحرک ارائه شده است.شبیه سازی این الگوریتم نشان می‌دهد که با افزایش تعداد گره های نگهبان در شبکه این الگوریتم قادر به شناسایی ۱۰۰٪ گره های سایبیل است و این نرخ با افزایش تعداد شناسه‌های سایبیل ویا گره‌های بدخواه کاهش نمی‌یابد.همچنین با انتخاب مناسب تعداد گره‌های نگهبان، میانگین نرخ خطا نیز کمتر از ۲٪می‌شود.

کلمات کلیدی

شبکه‌های حسگر متحرک، امنیت،حمله سایبیل، گره نگهبان.

۱ – مقدمه

شبکه‌های حسگر بی‌سیم امروزه در بسیاری از کاربردها، نظیر نظامی، خدمات شهری، پزشکی، اکتشافات و سیستم‌های تعقیب موجودیت استفاده می‌شود. هر شبکه حسگر از صدها تا هزاران گره حسگر کوچک و ارزان قیمت تشکیل شده است. با توجه به این محدودیت و هم‌چنین، ماهیت انتشار بی‌سیم و پخشی داده‌ها، عملیات معمولاً بدون مراقبت نیاز به برقراری امنیت و مقابله و شناسایی حمله‌ها در این گونه شبکه‌ها بسیار مهم است و مورد توجه بسیاری از محققان قرار گرفته است[1] [2].

یکی از حمله‌های مشهور در شبکه‌های حسگر بی‌سیم، حمله سایبیل[1] است. در این حمله، گره قانونی ضبط شده یا یک گره غیرقانونی درج شده در شبکه توسط دشمن، تحت عنوان "گره بدخواه" چندین شناسه از خود منتشر می‌کند. دشمن این شناسه‌ها را یا به‌طور جعلی می‌سازد و یا از شناسه‌های دیگر گره‌های قانونی در نواحی دیگر شبکه جعل می‌کند. گره بدخواه پس از گسترش در محیط، شناسه‌های سایبیل را از خود منتشر می‌کند که این سبب می‌شود گره بدخواه ترافیک زیادی را به خود جلب کند و می‌تواند پروتکل‌های مسیریابی و عملیاتی نظیر تجمیع داده‌ها، رأی‌گیری، تخصیص منابع را تحت تأثیر قرار دهد[2] [3] [4].

تاکنون الگوریتم‌هایی زیادی نظیر [20-9,15-5] جهت شناسایی گره‌های سایبیل در شبکه‌های حسگر بی‌سیم ثابت توسط محققان مطرح شده است.اکثر این الگوریتم‌ها مبتنی بر تعیین مکان گره‌ها یا مبتنی بر RSSI (مشخصه قدرت سیگنال دریافتی) و یا اطلاعات همسایگی است.در [10,11] الگوریتم‌هایی جهت مقابله با حمله سایبیل در شبکه‌های ad hoc متحرک است. در [12] یک الگوریتم پیچیده و مبتنی بر ایستگاه پایه ودر [13] یک الگوریتم مبتنی بر شناسه گره است و فرآیند تشخیص حمله سایبیل مبتنی بر ثبت‌نام گره در ایستگاه پایه است. این دو الگوریتم به دلیل متکی بودن به ایستگاه پایه، مشکل مقیاس‌پذیری دارند. این روش‌ها در شبکه‌های حسگر متحرک، به دلیل تحرک گره‌های قانونی و بدخواه کارایی چندانی نخواهند داشت. از این‌رو باید الگوریتم‌هایی مطرح کرد که توان