



کد نشست: D3	عنوان نشست: امنیت اطلاعات (۲)
کد مقاله: ۱۲۲	زمان ارائه: چهارشنبه ۱۳ اسفند ۱۳۹۳ ساعت: ۱۴:۵۰ - ۱۴:۳۰

یک الگوریتم دقیق جهت شناسایی حمله تکرار گر در شبکه‌های حسگر بی سیم متحرک به کمک یک گر ناظر

مجتبی جمشیدی^۱، مهدی اثنی عشری^۲، پیمان صیدی^۳، محمد رضا میبیدی^۴

^۱ آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد کرمانشاه، کرمانشاه

jamshidi.mojtaba@gmail.com

^۲ پژوهشکده فناوری اطلاعات، پژوهشگاه فضای مجازی، تهران

esnaashari@itrc.ac.ir

^۳ آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد کرمانشاه، کرمانشاه

peyman_seidi@yahoo.com

^۴ دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران

mmeybodi@aut.ac.ir

چکیده: حمله تکرار گر (یا گرهای کپی) یکی از حمله‌های مشهور و خطرناک علیه شبکه‌های حسگر بی سیم است. در این حمله، دشمن وارد محیط شبکه شده و یک (یا چند) گر نرمال درون شبکه را ضبط می‌نماید. دشمن سپس، تمام توابع، برنامه‌ها و مواد قفل‌گذاری درون حافظه گر ضبط شده را استخراج نموده و چندین گر کپی از آن تولید و در شبکه تزریق می‌کند. این گرهای کپی تحت کنترل دشمن می‌باشند و از آن‌جا که دارای مواد قفل‌گذاری معتبر هستند، لذا به راحتی با دیگر گرهای قانونی شبکه کلید مشترک برپا می‌کنند و به مخابره می‌پردازند. در این مقاله، یک الگوریتم ساده و مقاوم به کمک یک گر ناظر جهت شناسایی گرهای کپی در شبکه‌های حسگر متحرک ارائه می‌گردد. ایده اصلی الگوریتم پیشنهادی، استفاده از اطلاعات همسایگی در طول تحرک گرها در محیط شبکه جهت شناسایی گرهای کپی است. کارایی الگوریتم پیشنهادی از نقطه نظرهای سربار ارتباطات، حافظه و پردازش ارزیابی گردیده و نتایج حاصل با دیگر الگوریتم‌های موجود مقایسه شده است که نتایج این مقایسه، برتری الگوریتم پیشنهادی را می‌رساند. هم‌چنین، الگوریتم پیشنهادی توسط شبیه‌ساز JSIM پیاده‌سازی گردیده و با انجام یک سری آزمایش‌ها مشخص شد الگوریتم پیشنهادی قادر به شناسایی ۱۰۰٪ گرهای کپی است درحالی که احتمال تشخیص غلط آن نزدیک به صفر است.

واژه‌های کلیدی: شبکه‌های حسگر بی سیم، امنیت، گر ناظر، گرهای کپی