نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
9th SASTech Symposium on Advances in & Science Technology (2014)
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

ارزیابی و بررسی روش‌های مقابله با حمله سیاه‌چاله بر روی پروتکل مسیریابی AODV

سینا شهابی رابری، مهدیه قزوینی

۱- دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد بافت

۲- عضو هیئت‌علمی بخش مهندسی کامپیوتر دانشگاه شهید باهنر کرمان

دانشگاه آزاد اسلامی، واحد بافت، باشگاه پژوهشگران جوان و نخبگان، بافت، ایران

آدرس پست الکترونیکی نویسنده رابط mghazvini@uk.ac.ir

نام ارائه‌دهنده: سینا شهابی

خلاصه

شبکه‌های موردی به شبکه‌هایی اطلاق می‌شود که در آن‌ها هیچ زیرساخت از پیش تعیین‌شده‌ای وجود ندارد و به علت عدم مدیریت متمرکز، گره‌ها مدام در حال تغییر توپولوژی شبکه هستند. گره‌ها برای ارسال بسته‌های داده به یکدیگر باهم همکاری می‌کنند و جهت یافتن یک مسیر به مقصد از پروتکل‌های مسیریابی استفاده می‌کنند. با توجه به آسیب‌پذیری امنیتی پروتکل‌های مسیریابی، امنیت باید به‌عنوان یک نکته اصلی و حیاتی در طراحی الگوریتم‌های جدید در نظر گرفته شود. هدف این مقاله معرفی و بررسی روش‌های مقابله با حمله سیاه‌چاله است که تمامی این روش‌ها تلاش می‌کنند سطح قابل قبولی از امنیت را برای شبکه‌های موردی در مقابل این حمله فراهم کنند. با توجه به ضعف شبکه‌های موردی در مقابل حملات سیاه‌چاله، تمرکز اصلی ما در این مقاله بر این است که به بررسی و تحلیل راهکارهای جدید و موجود در این زمینه بپردازیم و آن‌ها را مورد ارزیابی قرار دهیم.

کلمات کلیدی: امنیت، پروتکل مسیریابی AODV، حمله سیاه‌چاله، شبکه‌های موردی.

۱. مقدمه

اغلب شبکه‌های بی‌سیم به‌صورت باساختار[1] پیاده‌سازی می‌شوند. معماری معمول در شبکه‌های بی‌سیم بر مبنای استفاده از نقطه مرکزی[2] است، با نصب یک نقطه مرکزی، عملاً مرزهای یک سلول مشخص می‌شود. گستره‌ای که یک نقطه مرکزی پوشش می‌دهد را BSS[3] می‌نامند. مجموعه‌ی تمامی

[1] Infrastructure
[2] Access Point
[3] Basic Service Set