گنگره بین المللی علوم و مهندسی
آلمان – هامبورگ
اسفند ماه ۱۳۹۶

بررسی روشی جهت تشخیص و جلوگیری از حمله ی سیاه چاله در شبکه های Ad-Hoc بی سیم سیار

سید حامد حسینیان[۱*]، محمد مهدی شیرمحمدی[۲]

[۱،۲] دانشگاه آزاد اسلامی ، واحد همدان ، گروه کامپیوتر ، همدان ، ایران

[1]hamed.hoseyniyan@gmail.com
[2]mmshirmohammadi@iauh.ac.ir

چکیده

شبکه های Ad-Hoc در حال رواج یافتن هستند. به دلیل ماهیت این نوع از شبکه ها، به شدت در معرض حملات قراردارند. حمله سیاه چاله یکی از مهمترین نوع حملات محتمل در این نوع از شبکه ها می باشد. در این مقاله یکی از روش های مقابله با این نوع حمله مورد بررسی قرار گرفته است. این روش توسط پاسخ های مسیر که از سمت گره میانی، با توجه به یک اطمینان که از سمت گره مقصد صورت میگیرد، تصمیم گیری میکند. اگر گره منبع بر روی پاسخ های مسیر پیام تصدیقی که توسط یک گره میانی در حال ارسال است، از گره مقصد در طی یک زمان مشخص، دریافت کرد گره منبع تصمیم می گیرد که مسیر مطمئن است و گره میانی مخرب نمی باشد. در همین حال یک شمارنده برای شمارش تعداد دفعاتی که هر گره میانی چه تعداد پاسخ مسیر اشتباه معرفی کرده است، تنظیم می شود. هر گره که یک پاسخ مسیر اشتباه پیشنهاد کند در یک لیست سیاه ثبت می شود. همچنین روند پردازش برای همه همسایگان با یک واسط فاصله از گره مشکوک چک می شود و اگر در طی فرآیند کشف مسیر یک پاسخ مسیر اشتباه پیشنهاد بدهند سابقه ی این گره ها در لیست سیاه ثبت و جمع آوری می شوند. زمانی که شمارنده برای هر گره از حد تعیین شده اش تجاوز کند، یک زنجیره از گره های مشکوک به عنوان سیاه چاله معرفی خواهند شد و یک پیام هشدار برای همه ی گره ها در سطح شبکه برای از بین بردن این گره های مخرب از جدول مسیریابی شان ارسال می شود.

واژه های کلیدی : شبکه های Ad-Hoc سیار،پروتکل های مسیر یابی، DSR و حمله سیاه چاله

۱- مقدمه

شبکه های ad-Hoc سیار بی سیم ، یک مجموعه از کاربران(گره های) سیار خودمختار است، که با یکدیگر بدون هیچ گونه زیرساختار ویژه ای ارتباط برقرار می کنند. از انجا که موقعیت گره ها در هر زمان در حال تغییر است ، موقعیت مکانی شبکه نیز بدون پیش بینی در حال تغییر است. هر گره به محض اینکه در شبکه مکان یابی میشود به مجموعه ی گره ها اضافه میشود. هر گره در این شبکه میتواند آزادانه به شبکه اضافه شود و عملیات هدایت و مسیر یابی بسته های داده رو انجام دهد. از این رو شبکه های ادهاک یک گستره وسیعی از کاربردها در زمینه های دفاعی ، در نواحی میدان جنگ، فراهم سازی کلاس های مجازی پایگاه داده بیمارستان در زمان یک وضعیت اورژانسی و مکان های تاریخی شامل مکان هایی که ایجاد زیرساخت در ان مناطق مشکل می باشد، می شود . هدف امنیتی در شبکه های ادهاک فراهم کردن محرمانگی، یکپارچگی، در دسترس بودن و احراز هویت می باشد. به طورکل شبکه های ادهاک از فقدان امنیت فیزیکی به دلیل ماهیت ساختارغیر قابل پیش بینی و نامنظم آن آسیب پذیر است به نحوی که شناسایی مهاجمان در مقایسه با شبکه های سیمی متناظر با این شبکه بسیار دشوار می باشد. به عنوان مثال احتمال استراق سمع یا جعل هویت مربوط به گره های مخرب در این شبکه ها بسیار زیاد