سومین کنفرانس فناوری اطلاعات و دانش
۶ تا ۸ آذرماه ۱۳۸۶

سامانه تشخیص نفوذ برای مقابله با حمله DoS از طریق تقاضای زیاد مسیریابی

محمود صالح اصفهانی، مهرداد ابوعلی

دانشگاه امام حسین (ع)، دانشکده برق و فناوری اطلاعات و ارتباطات

aboali@kavatelecom.com , msaleh@ihu.ac.ir

چکیده - در سال های اخیر تکنولوژی بی سیم به طور چشم گیری مورد توجه قرار گرفته است. این توجه موجب بوجود آمدن زمینه های فعالیت جدیدی در عرصه شبکه های کامپیوتری گردیده است. یکی از این زمینه های کاری، شبکه های بی سیم *Ad hoc* می باشد که گره های شبکه برای برقراری ارتباطات از هیچگونه زیرساختی استفاده نمی کنند. در حقیقت طبیعت شبکه های *Ad hoc*، تغییرات توپولوژیکی مداوم و عدم وابستگی گره ها به یک واحد مرکزی می باشد. به دلیل طبیعت متغیر ارتباطات بین گره ها و همچنین مشکلات امنیتی ذاتی شبکه های بی سیم، برقرای امنیت در اینگونه شبکه ها کار بسیار مشکلی می باشد.

در این مقاله، یک سامانه تشخیص نفوذ جدید برای تشخیص حملات فعال علیه مسیریابی در شبکه های *Ad hoc* ارائه می گردد. این سامانه پس از تشخیص حمله با اتخاذ تدابیری، اثر حمله را به حداقل رسانده و عملکرد شبکه را در حد قابل قبولی نگه خواهد داشت. حسن عملکرد این سامانه تشخیص نفوذ، مقابله آنی آن با گره های حمله کننده و خنثی کردن حمله آن ها می باشد. سامانه تشخیص نفوذ پیشنهادی، منجر به تغیر پروتکل مسیریابی نخواهد گردید بلکه به عنوان یک واسط بین ترافیک شبکه و پروتکل مسیریابی قرار می گیرد. ما در نهایت کار خود را با استفاده از نرم افزار قدرتمند *OPNET* شبیه سازی می کنیم. نتایج شبیه سازی بیانگره عملکرد موثر روش ما می باشد.

کلید واژه- تشخیص نفوذ، *IDS* ، اقتضایی، *Adhoc*

۱- مقدمه

شبکه‌های بی‌سیم Ad hoc اغلب در مکانهایی استفاده می شود که زیر ساخت مناسبی برای شبکه کابلی یا سلولی در آنجا وجود نداشته باشد. یکی از ویژگی های مهم شبکه های Ad hoc اینست که گره های شبکه بدون نیاز به هرگونه زیر ساخت قبلی شبکه با هم ارتباط برقرار می کنند[۳]. شبکه های بی سیم Ad hoc در حقیقت مجموعه ای از گره های بی سیم می باشند که قادرند بسرعت یک شبکه چند پرشی رادیویی را بدون نیاز به زیر ساخت خاص یا مدیریت مرکزی تشکیل دهند [۴].

از سوی دیگر بر قراری امنیت در شبکه های Ad hoc بخاطر طبیعت متغیر و توپولوژی کاملاً غیر متمرکز آن، مزید بر آسیب پذیری ها و محدودیت های شبکه های بی سیم گردیده است. یکی از مشخصه های شبکه های بی سیم Ad hoc این است که همه گره ها باید در امر مسیریابی شرکت داده شوند [۱، ۵، ۶]. از این رو روش های مسیریابی سنتی در این شبکه ها قابل استفاده نیست. شبکه های بی سیم به مراتب از امنیت کمتری در مقایسه با شبکه های سیمی برخوردارند. زیرا در شبکه های بی سیم Ad hoc، از آنجا که اطلاعات در هوا پخش می شود هر گره سومی نیز می تواند آن اطلاعات را شنود کرده و یا حتی به شبکه بپیوندد. در حقیقت در اینگونه شبکه ها تشخیص گره های بدخواه بسیار مشکل می گردد. بنابراین شبکه های