چهارمین کنفرانس بین المللی
مطالعات نوین درعلوم کامپیوتر و فناوری اطلاعات
4th International Conference
On New studies Of Computer And IT
مشهد
۰۵ اسفند ماه ۱۳۹۶
FEBRUARY 24 ,2018

استراتژی نوین تشخیص نفوذ مبتنی بر الگوی ترافیک در شبکه های نرم افزارمحور

مهسا سیدابراهیمی[۱]، کامبیز مجیدزاده[۲]

۱-کارشناسی ارشد نرم افزار، گروه کامپیوتر، واحد ارومیه، دانشگاه ازاد اسلامی، ارومیه، ایران،

۲-استادیار، گروه کامپیوتر، واحد ارومیه، دانشگاه ازاد اسلامی، ارومیه، ایران،

چکیده

یکی از مسائل مهم در محیط های ابری، امنیت و حریم خصوصی می‌باشد و از انجایی که سیستم تشخیص نفوذ بخش مهمی از سیستم‌های دفاعی در شبکه‌های کامپیوتری است، به همین منظور برای شناسایی ترافیک و حملات مشکوک در شبکه کارایی دارد. ظرفیت سیستم تشخیص نفوذ که از مقدار ترافیکی که در شبکه های بزرگ مورد وارسی قرار می گیرد کمتر می‌باشد. در این مقاله، یک رویکرد جدید نسبت به نمونه برداری ترافیک برای شبکه‌های مبتنی بر نرم افزار پیشنهاد می‌شود که از ترافیک و حملات در شبکه بر اساس الگوریتم بهینه‌تری با استفاده از شبکه های نرم افزار محور نمونه برداری می کند، این در حالی است که تمرکز بیشتر روی ترافیک مشکوک با تخمین نرخ تصمیم‌گیری نمونه برداری برای هر سوییچ را خواهد داشت. اگر تعداد زیادی قوانین فرستادن برای مسیرهای پشتیبان استفاده شود باعث می‌شود جریان‌ها در تعویض‌ها یا تغییرها پشت سرهم خارج شوند. برای اینکه نیازمندی‌های پهنای باند یک جریان تضمین گردد. به محض یک خطای ارتباطی، ملاحظه و نگهداری پهنای باند نیز به یک مسیر پشتیبان نیاز است.

مقایسه‌ی روش پیشنهادی در مقایسه با روش‌های موجود دقت بیشتر و عملکرد بهتر در شبکه‌های بزرگ مقیاس را به همراه دارد

واژگان کلیدی: امنیت، شبکه نرم‌افزار محور، تشخیص وکشف نفوذ، نرم افزار تعریف شده