عنوان مقاله:
مروری بر برررسی عمیق بسته های شبکه با استفاده از عبارت با قاعده در سیستم ها تشخیص نفوذ

محل انتشار:
پنجمین کنفرانس بین المللی تحقیقات نوین پژوهشی در مهندسی و تکنولوژی (سال: 1396)

تعداد صفحات اصل مقاله: 12

نویسندگان:
مجید سعیدی - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر- معماری کامپیوتر دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته کرمان*

حمیدرضا ناجی - *دانشیار گروه مهندسی کامپیوتر دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته کرمان*

خلاصه مقاله:
رشد فوق العاده سریع اینترنت در دهه اخیر و وابستگی فزاینده جامعه به آن و استفاده از خدمات مبتنی به وب همچون بانکداریاینترنتی و دولت الکترونیک باعث بوجود امدن سیل عظیمی از حملات اینترنتی و تهدید جدی برای اطلاعات خصوصی و دولتیشده است. در میان این سالها استفاده از سیستم های تشخیص نفوذ و جلوگیری از نفوذ جایگاه ویژه ای را در بین سیستم هایامنیتی بدست اورده است. بررسی عمیق بسته های شبکه یکی از تکنیک هایی است که بطور عمده در چنین سیستم هایی که نیازبه بررسی محتوای بسته های درون شبکه دارد مرسوم شده است. برنامه هایی چون سیستم های تشخیص نفوذ شبکه ، دیوارهآتش سیستم های توازن بار و همچنین سیستم های محاسبه ترافیک بطور گسترده از روش های بررررسی و تحلیل بسته هایدرون شبکه استفاده می کنند. در این سیستم ها اصلی ترین و بحرانی ترین بخش مربوط به تطبیق الگو است که محتوای هر یکاز بسته ها را با یک پایگاه داده از اطلاعات تطبیق می دهد و سعی در شناسایی بسته هایی که ممکن است ویژگی های مورد نظررا داشته باشند را دارد. در میان عبارات با قاعده یکی از اصلی ترین ابزاری است که به وسیله آن می توان قوانین و ویژگی هایاین پایگاه داده را توصیف کرد. انعطاف پذیری، توان بالا و قدرت بیان این ویژگی ها با استفاده از عبارات با قاعده یکی از اصلیچالش های ممکن را در پیاده سازی آن در سیستم ها و برنامه ی کاربردی اجاد کرده است.در این مقاله در ابتدا سعی در توصیف کلی DPI و همچنین تکنیک های بیان عبارات باقاعده برای توصیف ویژگی های پایگاه داده و بعد از آن سعی در تجزیه وتحلیل و توصیف معایب استفاده از عبارات با قاعده با استفاده از ماشین حالت محدود و معظلگسترش بیش از حد و نامحدود حالت ها و همچنین روش هایی برای دسته بندی و برطرف کردن این مشکلات ارایه شده است ودر نهایت به بررسی روش های پیاده سازی سخت افزاری برای بدست آوردن حداکثر توان پردازشی در شبکه های امروزی با نرخسرعت بالا در لینک های ارتباطی پرداخته ایم.

کلمات کلیدی:
سیستم های تشخیص نفوذ، بررسی عمیق بسته، عبارت باقاعده، ماشین حالت محدود