عنوان مقاله:
ارتقا حریم خصوصی ترافیک شبکه در برابر حمله ی دسته بندی به کمک یادگیری خصمانه

محل انتشار:
هفدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1399)

تعداد صفحات اصل مقاله: 8

نویسندگان:
محمدرضا کریمی - *فارغ التحصیل کارشناسی ارشد، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، آزمایشگاه امنیت داده و شبکه*

رسول جلیلی - *دانشیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف*

خلاصه مقاله:
در چند سال اخیر بطور گسترده از معماری های مختلف شبکه های عصبی عمیق در ادبیات پژوهش های دسته بندی ترافیک و انگشت نگاریوب سایت استفاده شده است. دسته بندی هاییاد شده بر روی ویژگی های آماری ترافیک مانند طول بسته ها و فاصله ی زمانی بین بسته هاصورت می پذیرد. ارتقا حریم خصوصی ترافیک شبکه در برابر حملات دسته بندی با الگوریتم هاییصورت می پذیرد که ترکیبی از افزایش طول(لایه گذاری) و شکستن بسته ها و اضافه کردن تاخیر در ارسال بسته را انجام می دهند. در این پژوهش به جای طراحی چنین الگوریتم هایی،با استفاده از روش های سنجش و ارزیابی مقاومت شبکه های عصبی موسوم به الگوریتم های تولید نمونه ی خصمانه با اعمال حداقل سربار اقدام به لایه گذاری بسته های جریان ترافیک شده است. یک دسته بند شبکه ی عصبی عمیق همگشتی را قبل و بعد از اعمال دفاع بر روی ترافیک، به کمک پنج الگوریتم تولید نمونه ی خصمانه، کارلینی-ونگر، جِی.اس.ام.ای، اف.جی.اس.ام، دیپ فول و پریشیدگی سراسری، ارزیابی می کنیم. هر یکاز الگوریتم ها با اضافه کردن میزان سربار متفاوت، از دقت و مثبت کاذب دسته بندی شبکه عصبی یاد شده می کاهند.

کلمات کلیدی:
دسته بندی ترافیک، مبهم نگاری ترافیک، یادگیری عمیق، یادگیری ماشین، شبکه ی عصبی، شبکه ی عصبی همگشتی

لینک ثابت مقاله در پایگاه سیویلیکا: