عنوان مقاله:

شناسایی حملات مخرب از نوع DDOS به مراکز داده با استفاده ازالگوریتم ژنتیک و گراف پوشای کمینه (نمونه برداری از مرکز داده کاملاً مجازی)

محل انتشار:

سومین همایش بین المللی مهندسی فناوری اطلاعات، کامپیوتر و مخابرات ایران (سال: 1399)

تعداد صفحات اصل مقاله: 16

نویسنده:

جواد غفاری - *دانشگاه آزاد اسلامی، واحد یادگار امام خمینی (ره) شهرری، باشگاه پژوهشگران جوان و نخبگان، شهرری، ایران*

خلاصه مقاله:

با رشد روزافزون صنعت نرم افزار و تکنولوژی وب نیاز به مراکز داده قوی برای رفع نیازکاربران بیش ازپیش احساس می شود. باپیشرفت همزمان فناوی زیرساخت وارتباطات شبکه پیچیده تر و تولید اطلاعات بیشترمی گردد.دراین مورد پژوهشگران این حوزه هرروزبه دنبال روش های نوین جهت تسهیل ارتباطات و تعریف سیاست های پویا جهت کنترل اطلاعات و جلوگیری از نفوذ خرابکاران شبکه و متعادل بودن مرکزداده به تکاپو واداشته است. ما دراین مقاله علمی پژوهشی سعی داریم با استفاده ازنمونه برداری ازترافیک لحظه ای شبکه (که البته در این مقاله ما ازسرور مرکز داده مجازی استفاده کرده ایم) به وسیله ی نرم افزار wireshark نسخه ی 3,4,1 حملات از نوع DDOS را درپیکره و Backbone شبکه (خصوصاً لایه سوم شبکه) با استفاده ازالگوریتم ژنتیک و الگوریتم گراف پوشای کمینه تشخیص و برای شناسایی منطقه بحرانی حمله با استفاده از دانش برنامه نویسی پایتون در نرم افزار Anaconda نسخه ی 3 و ماشین مجازی jupyter به کاوش می پردازیم. هدف ما دراین مقاله شناسایی هدفمند ترافیک و بار شبکه درلحظه می باشد و ترافیک غیرمتعارف نشانی از غیرعادی بودن رفتار خدمات گیرنده های(کلاینت ها)شبکه می باشد که شناسایی رفتار ترافیک شبکه در کوتاهترین زمان و شناسایی آدرس مبدا ارسال اطلاعات در شبکه و محتوای ارسالی از چالش های مهم الگوریتم های استفاده شده در طول زمان می باشد. توجه به این نکته که تشخیص اشتباه منجر به ازبین رفتن اطلاعات مفید در شبکه و سردرگمی نودهای حامل می گردد.

کلمات کلیدی:

هوش مصنوعی، الگوریتم ژنتیک ، مرکز داده، ترافیک، DDOS، امنیت شبکه، مسیریابی، الگوریتم کراسکال، گراف