



## بخشی از ترجمه مقاله

عنوان فارسی مقاله :

تشخیص حملات DDoS با استفاده از ماتریس ترافیک بهینه سازی شده

عنوان انگلیسی مقاله :

Detection of DDoS attacks using optimized traffic matrix



### توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.



## بخشی از ترجمه مقاله

### 5. Conclusions

In this paper, we have proposed a novel detection model to detect DDoS attacks using the dispersibility of the inbound packets' source IP addresses. We have employed an enhanced traffic matrix based approach and optimized parameters through the Genetic Algorithm (GA). We showed that our proposed approach satisfies the major requirements of the detection approach such as low processing overheads, short detection delay, and high detection rates. Furthermore, our model can be used in a real-time network environment and it can be implemented easily. Constructing a traffic matrix requires only two fields of IP header such as arrival time of packet and source IP address. A simple reformed hash function was also adopted to locate packets to the traffic matrix and avoid hash collisions. A variable window based on the number of incoming packets makes our model effective in terms of the detection delay and reduces computational overheads comparable to our previous approach. Our detection model can also maximize the detection rates by optimizing detection parameters through GA according to corresponding network environments.

### 5. نتایج

در این مقاله، مدل تشخیص جدیدی برای تشخیص حملات DDoS با استفاده از قابلیت پراکندگی آدرس های IP مبدا بسته های ورودی پیشنهاد کرده ایم. در اینجا از یک شیوه مبتنی بر ماتریس ترافیک بهبود یافته و پارامترهای بهینه سازی شده از طریق الگوریتم ژنتیک (GA) استفاده کرده ایم. نشان دادیم شیوه پیشنهادی به نیازمندیهای اصلی شیوه تشخیص، نظیر سربار پردازش پائین، تاخیر در تشخیص کوتاه، و نرخ تشخیص بالا دست می یابد. به علاوه، از مدل پیشنهادی می توان در محیط شبکه بلادرنگ استفاده و به راحتی آن را پیاده نمود. ساخت ماتریس ترافیک تنها نیازمند دو فیلد از هدر یا عنوان IP نظیر زمان ورود بسته و آدرس IP مبدا می باشد. از تابع هش اصلاح شده ساده نیز برای استقرار بسته ها در ماتریس ترافیک و اجتناب از برخوردهای هش استفاده گردید. پنجره متغیر براساس تعداد بسته های ورودی، مدل پیشنهادی را از لحاظ تاخیر در تشخیص موثر جلوه داده و سربارهای محاسباتی را در مقایسه با شیوه قبل، کاهش می دهد. مدل تشخیص پیشنهادی با بهینه سازی پارامترهای تشخیص از طریق GA طبق محیط های شبکه متناظر، نیز می تواند نرخ تشخیص را به حداکثر برساند.

### توجه!

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت

ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.

همچنین برای جستجوی ترجمه مقالات جدید [اینجا](#) کلیک نمایید.

