



بخشی از ترجمه مقاله

عنوان فارسی مقاله :

تشخیص حملات DdoS با استفاده از ماتریس ترافیک پراکنده شونده
و میانگین متحرک وزندار

عنوان انگلیسی مقاله :

Detecting DDoS Attacks Using Dispersible Traffic
Matrix and Weighted Moving Average



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

4 Conclusion

In this paper, we have presented an efficient approach to detect DDoS attacks using traffic matrix and WMA. Considering the previous detection approach, there is commonly tradeoff between attack efficiency and cost [4]. Increasing the attack detection rate requires the increase of false alarm rate or increment of computational overheads or memory overheads. While detecting attacks as soon as possible is very important for preparing defense measures in DDoS attacks, most of the previous researches have been focused on the traffic generated by compromised host to extract detection parameters. However, our proposed detection model using traffic matrix can detect fast and decrease the false alarm through WMA. It is also efficient in terms of the cost. The contributions of our approach are (i) the network traffic analysis using traffic matrix can visualize the network traffic streams (ii) the traffic pattern analysis algorithm through the variance of traffic matrix is very efficient in terms of the cost (iii) fast detection of DDoS attack, so we can handle the DDoS attack proactively (iv) detection accuracy, speed and false alarm rate which have been validated through several experiments on DARPA 2000 dataset and real data in our testbed network environment.

4. نتیجه گیری

در این مقاله، یک شیوه کارآمد برای تشخیص حملات DDoS با استفاده از ماتریس ترافیک و WMA معرفی کرده ایم. با در نظر گرفتن شیوه تشخیص قبلی، بین کارایی حمله و هزینه ها، معمولاً رابطه جانشینی وجود دارد. افزایش نرخ تشخیص حمله مستلزم افزایش نرخ آلام کاذب یا افزایش سربارهای محاسباتی یا سربارهای حافظه می باشد. در حالیکه تشخیص زودهنگام حملات نقش بسیار مهمی در تهیه معیارهای دفاعی در حملات DDoS ایفا می کند، اما اکثر تحقیقات قبل، بر ترافیک تولید شده توسط میزبان به خطر افتاده برای استخراج پارامترهای تشخیص تمرکز کرده است. اما، مدل تشخیص پیشنهادی، با استفاده از ماتریس ترافیک و از طریق WMA می تواند آلام کاذب را به سرعت تشخیص و کاهش دهد. آن از لحاظ هزینه نیز کارآمد می باشد. کارهای شیوه پیشنهادی به شرح ذیل می باشد: (1) تجزیه و تحلیل ترافیک شبکه با استفاده از ماتریس شبکه قادر به تجسم جریانات ترافیک شبکه می باشد (2) الگوریتم تجزیه و تحلیل الگوی ترافیک از طریق واریانس ماتریس ترافیک از لحاظ هزینه بسیار کارآمد می باشد (3) تشخیص سریع حمله DDoS، بنابراین می توانیم به شکلی پویا با حمله DDoS سرو کار داشته باشیم، (4) صحت تشخیص، سرعت و نرخ آلام کاذب که از طریق آزمایشات گوناگون روی مجموعه داده DARPA 2000 و داده های واقعی در محیط شبکه بستر تست، اعتباریابی (اعتبارگذاری) شده اند.

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.

برای جستجوی جدیدترین مقالات ترجمه شده، [اینجا](#) کلیک نمایید.

