Nome: Davi Jorge Leite Santos - Matricula: 614017

A DDoS Attack Detection System: Applying A Hybrid Genetic Algorithm to Optimal Feature Subset Selection

Abid Saber, Moncef Abbas, Belkacem Fergani

A ARQUITETURA DO DDOS HÍBRIDO SISTEMA DE DETECÇÃO

“Then, these will be used for two purposes at once, reducing the size of the dataset by removing additional information including (noisy, redundant, anomalies, outliers...) and selecting the features related to the clues in order to be able to build a traffic model in a supervised way based on the decision trees.” PAG 3

“2) Protection against DDoS attacks: As seen in the section above, DDoS attacks [7] have several types of attacks. One of the solutions available to virtually all network administrators is to create a route to a black hole and direct malicious traffic to that route. We can also limit the number of requests that a server will accept over a certain period. As a third solution, we cite the Web Application Firewall (WAF), which can act as a reverse proxy, protecting the targeted server against certain types of malicious traffic. By filtering requests based on a series of rules used to identify DDoS tools. Therefore, these rules can be defined according to a deep analysis of network traffic flow. On the other hand, the main difficulty in mitigating a DDoS attack is to detect it, and this is due to the differentiation of attack (malicious) traffic from normal (legitime) traffic. This data flow is defended by a large number of Features that characterize internet traffic.” PAG 3 e 4

“1) 1) Choice of fitness function: The definition of the fitness function is very important because the quality of each chromosome is evaluated by the latter, we have chosen the classification rate (Detection Rate, equation 4), because it gives a global overview of the state of the network traffic. The goal of our hybrid genetic algorithm GA-TS is to maximize this function, to do this we will use decision tree C4.5 [14] as a supervised learning algorithm to calculate the fitness value for each generation.” PAG 5

“Indeed, the approach proposed in this paper could reduce the number of these features to more than 78% of the total number of features, this procedure of automatically selecting the features of the network traffic can reduce the cost of computation and training time, which ultimately leads to the improvement of the detection rate of DDoS attack detection.” PAG 6