Nome: Davi Jorge Leite Santos - Matricula: 614017

MACHINE LEARNING BASED DDOS DETECTION THROUGH NETFLOW ANALYSIS

Jiangpan Hou, Peipei Fu, Zigang Cao, Anlin Xu

Sobre o netflow

“[...] In this section, we are going to describe how features are extracted from the NetFlow data to identify DDos. NetFlow is a network protocol proposed by Cisco Systems for collecting the network traffic. NetFlow, which contain a set of attributes, could be captured and forwarded by routers and switches. In this paper, NetFlow raw attributes we used for extracting features to identify DDos are: the source IP address, the destination IP address, the number of bytes and packets transferred, the start and finish time stamps and the protocol. We give up the port in order to avoid overfit models, because the port is always the strong feature of specific behavior [...]” PAG 2

“[...] Detection of DDos is addressed in most flow based IDS [15]. There are two types of the method for detection of DDos by using NetFlow data: the traditional method and machine learning. [...]” PAG 2

“[...] Patterns-based Features. One typical property of DDos is that attacker circulates thousands of the identical behaviour. Therefore, it means producing the periodic NetFlow data for a time of DDos occurring. However, traffic of benign tends to exhibit much more varied patterns due to the vagaries of human action. In order to catch these exceptions, we define four sequence: Pup, Pdown, Bup, Bdown. Pup and Pdown contained a sequence of number of packets in two directions, which come from NetFlow data in intervals time i = 0, 1, 2. . . Similarly, Bup and Bdown represent feature of bytes sequence. In particular, we extract min, max, mean, 25 quantiles, 50 quantiles, 75 quantiles, standard deviation and transition matrix [12] from four sequence as our feature. [...]” PAG 3

“[...] ". Experiment results show a very admirable classification accuracy, more than 99%, and a low false positive rate, less than 0.5% on data from network of our research lab which contain a mixture of real benign traffic and simulated attacks traffic by the aid of multiple and different DDos tools. Besides, our detector is able to discover the type of attacks that the traditional methods can hardly do, such as slow connection DDos. [...]” PAG 6