A multi-filter feature selection in detecting distributed denial-of-service attack

ABSTRACT

Distributed Denial of Services (DDoS) has become the most intrusive security threat on the Internet. Flash crowd attack is the most challenging problem among the attacks which targeting the web server during the Flash Events (FEs). It mimics the behaviour of legitimate users and sends high rate malicious traffics toward the server and block the normal users from using the desired services. Thus, making it hard to detect and successfully bypasses the detection mechanism. The key semantic difference between FEs and DDoS is that the former represents legitimate access of the website while the latter does not. However, this does not help in discriminating them automatically. The behavioural differences between the two have to be developed after understanding their individual properties. In this research, a Multi-Filter Feature Selection (M2FS) method is proposed by combining the 3 filter methods which are Information Gain (IG), Gain Ratio (GR) and ReliefF. It consists of 3-stage procedures: feature ranking, feature selection and classification. Subsequently, an experimental evaluation of the proposed Multi-Filter Feature Selection (M2FS) method is performed by using the benchmark dataset, NSL-KDD and employed the J48 classification algorithm. The performance of the proposed M2FS method is evaluated by multi-criteria that take into account which are classification accuracy, True Positive Rate (TPR), False Positive Rate (FPR) and time to build the model. Meanwhile, the performance of effectiveness of the proposed M2FS method is then compared with the existing feature selection methods and also the proposed M2FS with PCA. In addition, the proposed M2FS method is developed through WEKA API with Java Programming language using the IDE of Eclipse Java. The findings show that the proposed M2FS method is effectively reduced the 41 features to 14 features and produced a high accuracy, high TPR, low FPR and shorter time build when compared to other existing feature selection methods.