Identification of distributed denial of services anomalies by using combination of entropy and sequential probabilities ratio test methods

ABSTRACT

One of the most dangerous kinds of attacks affecting computers is a distributed denial of services (DDoS) attack. The main goal of this attack is to bring the targeted machine down and make their services unavailable to legal users. This can be accomplished mainly by directing many machines to send a very large number of packets toward the specified machine to consume its resources and stop it from working. We implemented a method using Java based on entropy and sequential probabilities ratio test (ESPRT) methods to identify malicious flows and their switch interfaces that aid them in passing through. Entropy (E) is the first technique, and the sequential probabilities ratio test (SPRT) is the second technique. The entropy method alone compares its results with a certain threshold in order to make a decision. The accuracy and F-scores for entropy results thus changed when the threshold values changed. Using both entropy and SPRT removed the uncertainty associated with the entropy threshold. The false positive rate was also reduced when combining both techniques. Entropy-based detection methods divide incoming traffic into groups of traffic that have the same size. The size of these groups is determined by a parameter called window size. The Defense Advanced Research Projects Agency (DARPA) 1998, DARPA2000, and Canadian Institute for Cybersecurity (CIC-DDoS2019) databases were used to evaluate the implementation of this method. The metric of a confusion matrix was used to compare the ESPRT results with the results of other methods. The accuracy and f-scores for the DARPA 1998 dataset were 0.995 and 0.997, respectively, for the ESPRT method when the window size was set at 50 and 75 packets. The detection rate of ESPRT for the same dataset was 0.995 when the window size was set to 10 packets. The average accuracy for the DARPA 2000 dataset for ESPRT was 0.905, and the detection rate was 0.929. Finally, ESPRT was scalable to a multiple domain topology application.

Keyword: Distributed denial of services attack; Entropy; Sequential probability ratio test; Confusion matrix