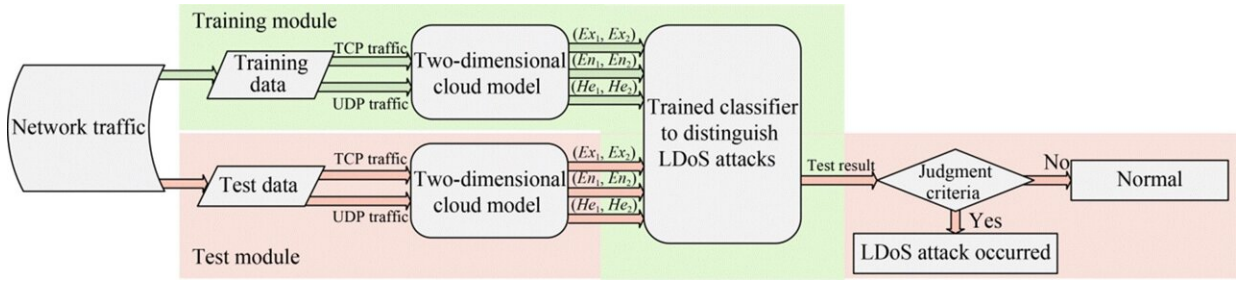
An approach for detecting LDoS attacks based on cloud model

June 2 2022



The processing flow of LDoS detection. Credit: Higher Education Press Limited Company

Cybersecurity has always been a focus of Internet research. An LDoS attack is an intelligent type of DoS attack, which reduces the quality of network service by periodically sending high-speed but short-pulse attack traffic. The existing LDoS attack detection methods generally have the problems of high FPR and FNR.

To solve the problems, a research team led by Wei Shi published their new research on 02 April 2022 in *Frontiers of Computer Science*.

The team proposed a cloud model-based LDoS attack detection method using a classifier based on SVM to train and classify the feature parameters. The detection method is verified and tested in the NS2 simulation platform and test-bed network environment. Compared with

the existing research results, the proposed method requires fewer samples, and it has lower FPR and FNR.

In the research, they analyze the abnormal changes in network traffic caused by the LDoS attack and use the cloud model to compare the difference between the normal state of the network and the state of the LDoS attack. In order to more accurately judge whether the network is under LDoS attack, they use the cloud model to obtain the feature parameters in two states, and then use the Support Vector Machine (SVM)-based LDoS attack detection classifier to train and classify the obtained feature parameters, detecting whether there is an LDoS attack on the network.

Firstly, the cloud model is used to analyze network traffic. The reverse cloud generation algorithm analyzes the network traffic in the bottleneck link to obtain feature values of the cloud model, and analyzes the changes of the feature values under the LDoS attack, then uses the SVM with "small sample" learning ability to establish LDoS attack detection classifier to judge whether the LDoS attack is occurring. The experimental data shows that compared with the existing research methods, the proposed method requires fewer data samples and has the characteristics of a high Accuracy, low FNR, and low FPR value.

More information: Wei Shi et al, An approach for detecting LDoS attack based on cloud model, *Frontiers of Computer Science* (2022). DOI: 10.1007/s11704-022-0486-1

Provided by Higher Education Press