An Approach for Detecting LDoS Attack based on Cloud Model

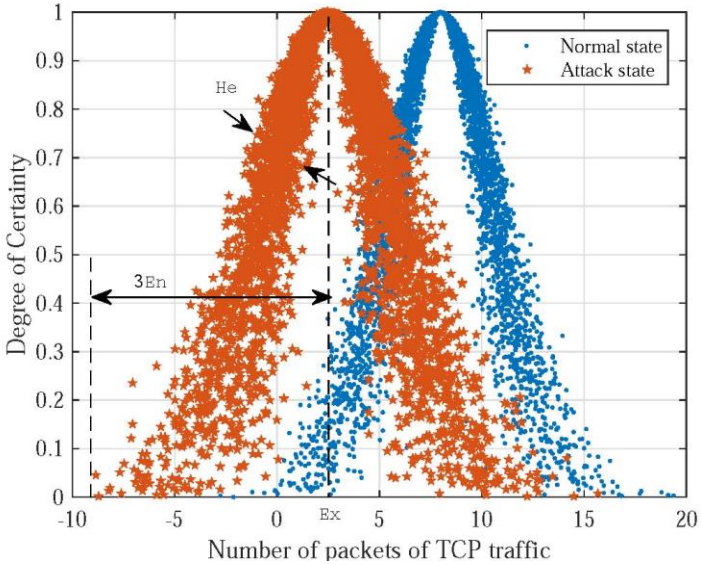
Wei SHI, Dan TANG, Sijia ZHAN, Zheng QIN, Xiyin WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-022-0486-1

Problems & Ideas

- Problems of Looking for more effective way to detect LDoS attacks:
  - Network traffic is usually uncertain and random in a realistic network environment. Traditional quantitative algorithms are prone to bias in network traffic assessment inaccuracy;
  - the existing LDoS attack detection methods generally have the problems of high FPR and FNR.
- Ideas: We use cloud models based on fuzzy theory and probability theory to simulate network traffic from different states, thereby efficiently distinguish them.

— cloud model theory can more objectively reflect the randomness, ambiguity, and unpredictability of network traffic, complete the conversion of fuzzy concepts to specific values and present them as cloud images, which makes expression more intuitive and specific.



The qualitative concept of the cloud can be represented by the three numerical characteristics of E_x, E_n, and H_e as a whole. E_X is the point that best represents the qualitative. E_n is a measure of cloud uncertainty. H_e is the entropy of entropy. As can be seen from the above figure, the values of E_x, E_n, and H_e of the normal state and attack state have a large difference.

Main Contributions

- Contributions:
  - The cloud model-based LDoS attack detection method is proposed due to the advantage of the cloud model, which can avoid the modeling error caused by network traffic randomness;
  - The method use the SVM with “small sample” learning ability to establish LDoS attack detection classifier to judge whether the LDoS attack occurs;
  - Compared with the existing research methods, the proposed method requires fewer sample data and has the characteristics of a high *Accuracy*, low *FNR*, and low *FPR* value

Table 8 Detection performance of different environments

Methods \ Performance	Accuracy	FPR	FNR
Network Multifractal [18]	91%	10%	9%
Kalman Filtering [31]	89.6%	12.6%	10.4%
Our method	96.5%	5.8%	0%

As can be seen from the above table, the *Accuracy* value of this article is 96.5%, higher than the other two methods, the *FPR* is 5.8%, *FNR* is 0%, lower than the other two methods.