

CLAIMS

1. A method of detecting a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack, comprising:

acquiring traffic data of a preset service in a preset time period, wherein the traffic data is correspondence data between an overall traffic of the service and time;

acquiring an overall traffic threshold data of the service corresponding to different time intervals calculated according to historical traffic data of the service; wherein the larger the historical traffic data of the time interval, the larger corresponding overall traffic threshold data of the service;

determining the time interval corresponding to the acquired traffic data, and finding the overall traffic threshold corresponding to the time interval according to the determined time interval; and

comparing the traffic data with the found overall traffic threshold, and performing an attack detection to the service when a duration for which the traffic data keeps exceeding the overall traffic threshold exceeds a preset value; wherein the method further comprises

collecting correspondence relation data of historical traffic value of the service and the time;

setting adjacent historical traffic rate values with a difference therebetween being less than a preset value as interval traffic values in the same time interval; and

calculating an average traffic value of the interval traffic values, and determining the overall traffic threshold of the time interval according to the average traffic value.

2. The method according to claim 1, wherein the overall traffic threshold data of the service corresponding to different time intervals is acquired by calculation according to the historical traffic data of the service and computing resource data allocated for the service, wherein the larger the historical traffic data of the service, the larger the computing resource data allocated for the service, and the larger the acquired overall

traffic threshold data of the service.

3. The method according to claim 1, wherein the performing an attack detection to the service comprises:

locating abnormal time information when attack traffic occurs;

acquiring module traffic data of each service module contained in the service corresponding to the abnormal time information; and

comparing the acquired module traffic data with module traffic threshold calculated in advance corresponding to the abnormal time information, and determining a service module identifier that exceeds the module flow threshold;

wherein the module traffic threshold corresponding to the abnormal time information is calculated according to the historical traffic data of each service module.

4. The method according to claim 2, wherein after the acquiring an overall traffic threshold data of the service corresponding to different time intervals calculated according to historical traffic data of the service; wherein the larger the historical traffic data of the time interval, the larger corresponding overall traffic threshold data of the service, the method further comprises:

acquiring the computing resource data allocated for the service, and determining a maximum traffic threshold according to the computing resource data; and

adjusting the overall traffic threshold data of the service corresponding to the different time intervals according to the determined maximum traffic threshold.

5. The method according to claim 1, further comprising:

acquiring attribute information of a newly added service module when monitoring that the newly added service module is provided in the service, wherein the attribute information comprises type information and duration information;

acquiring newly added traffic threshold data configured for the newly added service module according to the type information; and
adjusting the overall traffic threshold of the time interval corresponding to the duration information according to the newly added traffic threshold data.

6. A device of detecting a DoS/DDoS attack, comprising:

a traffic acquiring module configured to acquire traffic data of a preset service in a preset time period, wherein the traffic data is correspondence data between an overall traffic of the service and a time;

a multiple traffic threshold acquiring module configured to acquire an overall traffic threshold data of the service corresponding to different time intervals calculated according to historical traffic data of the service; wherein the larger the historical traffic data of the time interval, the larger corresponding overall traffic threshold data of the service;

a threshold comparing and determining module configured to determine the time interval corresponding to the acquired traffic data, and finding the overall traffic threshold corresponding to the time interval according to the determined time interval; and

an attack traffic detecting module configured to compare the traffic data with the found overall traffic threshold, and performing an attack detection to the service when a duration for which the traffic data keeps exceeding the overall traffic threshold exceeds a preset value; wherein the device further comprises

a historical traffic collecting module configured to collect correspondence relation data of historical traffic value of the service and the time;

a time interval dividing module configured to set adjacent historical traffic rate values with a difference therebetween being less than a preset value as interval traffic values in the same time interval; and

an interval threshold calculating module configured to calculate an average traffic

value of the interval traffic value, and determining the overall traffic threshold of the time interval according to the average traffic value.

7. The device according to claim 6, wherein the overall traffic threshold data of the service corresponding to different time intervals is acquired by calculation according to the historical traffic data of the service and the computing resource data allocated for the service, wherein the larger the historical traffic data of the service, the larger the computing resource data allocated for the service, and the larger the acquired overall traffic threshold data of the service.

8. The device according to claim 6, wherein the attack traffic detecting module is further configured to locate abnormal time information when attack traffic occurs; acquire module traffic data of each service module contained in the service corresponding to the abnormal time information; and compare the acquired module traffic data with module traffic threshold calculated in advance corresponding to the abnormal time information, and determining a service module identifier that exceeds the module flow threshold; wherein the module traffic threshold corresponding to the abnormal time information is calculated according to the historical traffic data of each service module.

9. The device according to claim 7, further comprising:

a computing resource acquiring module configured to acquire the computing resource data allocated for the service, and determine a maximum traffic threshold according to the computing resource data; and

a traffic threshold adjusting module configured to adjust the overall traffic threshold data of the service corresponding to different intervals according to the determined maximum traffic threshold.

10. The device according to claim 6, further comprising:

a newly added module information acquiring module configured to acquire attribute information of an newly added service module when monitoring that the newly added service module is provided in the service, wherein the attribute information comprises type information and duration information;

a newly added module traffic determining module configured to acquire a newly added traffic threshold data configured for the new service module according to the type information; and

a traffic threshold updating module configured to adjust the overall traffic threshold of the time interval corresponding to the duration information according to the newly added traffic threshold data.

11. A server comprising a processor; and a memory storing instructions, which, when executed by the processor, cause the processor to perform steps comprising:

acquiring traffic data of a preset service in a preset time period, wherein the traffic data is correspondence data between an overall traffic of the service and a time;

acquiring an overall traffic threshold data of the service corresponding to different time intervals calculated according to historical traffic data of the service; wherein the larger the historical traffic data of the time interval, the larger corresponding overall traffic threshold data of the service;

determining the time interval corresponding to the acquired traffic data, and finding the overall traffic threshold corresponding to the time interval according to the determined time interval; and

comparing the traffic data with the found overall traffic threshold, and performing an attack detection to the service when a duration for which the traffic data keeps exceeding the overall traffic threshold exceeds a preset value; wherein the processor further performs the steps of:

collecting correspondence relation data of historical traffic value of the service and the time;

setting adjacent historical traffic rate values with a difference therebetween being less than a preset value as interval traffic values in the same time interval; and

calculating an average traffic value of the interval traffic value, and determining the overall traffic threshold of the time interval according to the average traffic value.

12. The server according to claim 11, wherein the overall traffic threshold data of the service corresponding to different time intervals is acquired by calculation according to the historical traffic data of the service and the computing resource data allocated for the service, wherein the larger the historical traffic data of the service, the larger the computing resource data allocated for the service, and the larger the acquired overall traffic threshold data of the service.

13. The server according to claim 11, wherein the attack detection to the service performed by the processor comprises:

locating abnormal time information when attack traffic occurs;

acquiring module traffic data of each service module contained in the service corresponding to the abnormal time information; and

comparing the acquired module traffic data with module traffic threshold calculated in advance corresponding to the abnormal time information, and determining a service module identifier that exceeds the module flow threshold;

wherein the module traffic threshold corresponding to the abnormal time information is calculated according to the historical traffic data of each service module.

14. The server according to claim 12, wherein after the acquiring an overall traffic threshold data of the service corresponding to different time intervals calculated

according to historical traffic data of the service; wherein the larger the historical traffic data of the time interval, the larger corresponding overall traffic threshold data of the service, the processor further performs the steps of:

acquiring the computing resource data allocated for the service, and determining a maximum traffic threshold according to the computing resource data; and

adjusting the overall traffic threshold data of the service corresponding to different intervals according to the determined maximum traffic threshold.

15. The server according to claim 11, wherein the processor further performs the steps of: acquiring attribute information of a newly added service module when monitoring that the newly added service module is provided in the service, wherein the attribute information comprises type information and duration information;

acquiring a newly added traffic threshold data configured for the new service module according to the type information; and

adjusting the overall traffic threshold of the time interval corresponding to the duration information according to the newly added traffic threshold data.

16. At least one non-transitory computer-readable storage medium storing computer-readable instructions that, when executed by at least one processors, cause the at least one processor to perform the method of detecting a DoS/DDoS attack according to any one of claim 1 to claim 5.