System for denial of service attack detection based on multivariate correlation analysis

Abstract:
In this paper, we present a dos attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based dos attack detection system employs the principle of anomaly based detection in attack recognition. This makes our solution capable of detecting known and unknown dos attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 data set, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.

Existing System:
Interconnected systems, such as webservers, database servers etc are now under threats from network attackers. As one of the most common and aggressive means Denial of Service attacks cause serious impact on these computing systems.

Disadvantages
This makes our solution capable of detecting known and unknown dos attacks effectively by learning the patterns of legitimate network traffic only.
Proposed System:

We present a dos attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic features. Our MCA based DOS attack detection system employs the principle of anomaly based detection in attack recognition. This makes our solution capable of detecting known and unknown dos attacks effectively by learning the patterns of legitimate network traffic only.

Advantages:

The results show that our system outperforms two other previously developed state of the art approaches in terms of detection accuracy.

System Architecture:
System Requirements:

Hardware Requirements:

System : Pentium IV 2.4 GHz.
Hard Disk : 40 GB.
Floppy Drive : 1.44 Mb.
Monitor : 15 VGA Colour.
Mouse : Logitech.
Ram : 512 Mb.

Software Requirements:

Operating system : Windows 7.
Coding Language : C#.net, Asp.net
IDE : VisualStudio 2010