A System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis

ABSTRACT:

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. 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 dataset, 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:

Generally, network-based detection systems can be classified into two main categories, namely misuse-based detection systems and anomaly-based detection systems. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks. Furthermore, it is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise.

DISADVANTAGES OF EXISTING SYSTEM:

· Most existing IDS are optimized to detect attacks with high accuracy. However, they still have various disadvantages that have been outlined in a number of publications and a lot of work has been done to analyze IDS in order to direct future research.

· Besides others, one drawback is the large amount of alerts produced.

PROPOSED SYSTEM:

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.

The DoS attack detection system presented in this paper employs the principles of MCA and anomaly-based detection. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A triangle area technique is developed to enhance and to speed up the process of MCA. A statistical normalization technique is used to eliminate the bias from the raw data.

ADVANTAGES OF PROPOSED SYSTEM:

ü More detection accuracy

ü Less false alarm

ü Accurate characterization for traffic behaviors and detection of known and unknown attacks respectively

MODULES:

1. Feature Normalization

2. Multivariate Correlation Analysis

3. Decision Making Module

4. Evaluation of Attack detection

MODULES DESCRIPTION:

1. Feature Normalization Module:

In this module, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Monitoring and analyzing at the destination network reduce the overhead of detecting malicious activities by concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

2. Multivariate Correlation Analysis:

In this Multivariate Correlation Analysis, in which the “Triangle Area Map Generation” module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the “Feature Normalization” module in this step. The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.

3. Decision Making Module:

In this module, the anomaly-based detection mechanism is adopted in Decision Making. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detectors and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm. This, however, is a labor-intensive task and requires expertise in the targeted detection algorithm. Specifically, two phases (i.e., the “Training Phase” and the “Test Phase”) are involved in Decision Making. The “Normal Profile Generation” module is operated in the “Training Phase” to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database. The “Tested Profile Generation” module is used in the “Test Phase” to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the “Attack Detection” module, which compares the individual tested profiles with the respective stored normal profiles. A threshold-based classifier is employed in the “Attack Detection” module to distinguish DoS attacks from legitimate traffic.

4. Evaluation of Attack detection

In Evaluation module we use real time data instead of KDD dataset, where three types of legitimate traffic (TCP, UDP and ICMP traffic) and different types of DoS attacks are available. All of these records are first filtered and then are further grouped into seven clusters according to their types. We show the evaluation results in graph.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

Ø System : Pentium IV 2.4 GHz.

Ø Hard Disk : 40 GB.

Ø Floppy Drive : 1.44 Mb.

Ø Monitor : 15 VGA Colour.

Ø Mouse : Logitech.

Ø Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

Ø Operating system : Windows XP/7.

Ø Coding Language : C#.net

Ø Tool : Visual Studio 2010

Ø Database : SQL SERVER 2008