ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

An Efficient Way of Denial of Service Attack Detection Based on Triangle Map Generation

Shanofer. S

Master of Engineering, Department of Computer Science and Engineering, Veerammal Engineering College, Dindigul

Abstract: **A Denial - of - Service attack (DoS) is when someone tries to stop someone else from viewing parts of the internet. To avoid this problem earlier 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.. Neuro - fuzzy sytems is proposed as subsystems of the ensemble. Sugeno type Neuro - Fuzzy Inference System has been chosen as a base classifier for our research. Single classifier makes error on different training samples. So, by creating the classifiers and combining their outputs, the total amount of error can be reduced and the detection accuracy can be increased. The proposed Adaptive Neuro -Fuzzy Inference based system will be able to detect an intrusion behavior of the networks. The experiments and the evaluations of the proposed method were performed. The results show that our system outperforms two other previously developed states- of- the-art approaches in terms of detection accuracy.**

Keywords: **Denial of service, Multivariate correlation analysis.**

I. INTRODUCTION

DENIAL-OF-SERVICE (DoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. DoS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. The victim can be forced out of service from a few minutes to even several days. This causes serious damages to the services running on the victim. Therefore, effective detection of DoS attacks is essential to the protection of online services. Work on DoS attack detection mainly focuses on the development of network-based detection mechanisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. These mechanisms release the protected online servers from monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network-based detection systems are less complicated than that of host-based detection systems. 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. Research community, therefore, started to explore a way to achieve novelty-tolerant detection systems and developed a more advanced concept, namely, anomaly based detection. Owing to the principle of detection, which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities. Moreover, it is not constrained by the expertise in network security, due to the fact that the profiles of legitimate behaviors are developed based on techniques, such as data mining machine learning and statistical analysis. However, these proposed systems commonly suffer from high false-positive rates because the correlations between features/attributes are intrinsically neglected or the techniques do not manage to fully exploit these correlations To deal with the above problems, an approach based on triangle area was presented in to generate better discriminative features.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

However, this approach has dependence on prior knowledge of malicious behaviors. More recently, Jamdagni et al. developed a refined geometrical structure-based analysis technique, where Mahalanobis distance (MD) was used to extract the correlations between the selected packet payload features. This approach also successfully avoids the above problems, but it works with network packet payloads. In Tan et al. proposed a more sophisticated non payload-based DoS detection approach using multivariate correlation analysis (MCA. In addition to the work shown in we present the following contributions 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. Our proposed DoS detection system is evaluated using KDD Cup 99 data set and outperforms the state-of-the art systems.

1.1 Need:

In software project issues are delay of packet transmitting and computational complexity. 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

1.2 Objective:

Estimation based on software experts comments: it shows the rational and mental process of effort estimation and is often based of prior experiences in developing and managing similar projects. Algorithmic estimation: this kind of estimation is used in estimation and production of projects which obviously shows the relationship between the efforts of one or several project properties using linear equations. These techniques have been the most prevalent ones in SCE so far.

II. ARCHITECTURES

A. EXISTING ARCHITECTURE:

Interconnected systems, such as Web servers, database servers, and cloud computing servers and so on, 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 system, they presented 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. The MCA-based DoS attack detection system employs the principle of anomaly based detection in attack recognition. This makes the 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 this 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.

DISADVANTAGES:

- Labor intensive task and requires expertise in the targeted detection algorithm. It cannot distinguish both known and unknown DoS attacks from legitimate network traffic

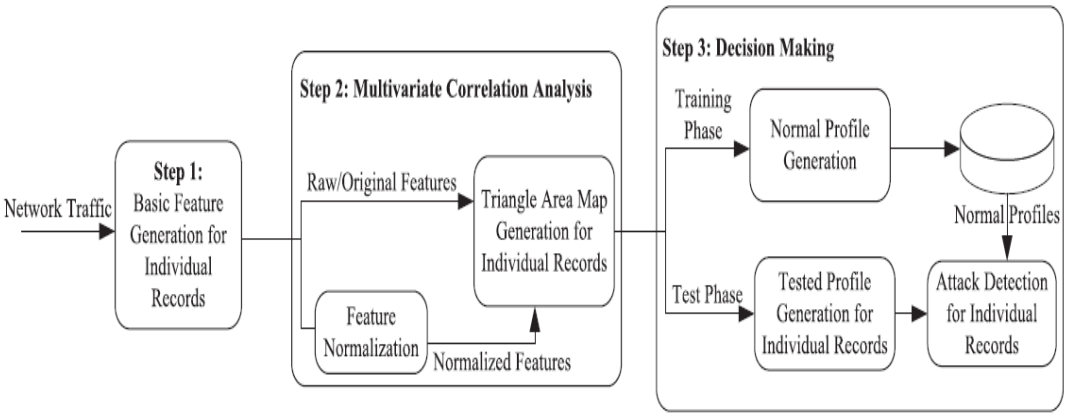


Fig.1.Denial of service attack detection system

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

B. PROPOSED ARCHITECTURE:

A DoS attack is the most prevalent threat, viz., traffic in communication resources in order to make the service unavailable for legitimate users, since a decade and continues to be threatening. Denials-of- Service (DoS) attacks cause serious impact on these computing systems. Neuro-fuzzy systems were proposed as subsystems of the ensemble. Sugeno type Neuro - Fuzzy Inference System has been chosen as a base classifier for our research. Single classifier makes error on different training samples. So, by creating the classifiers and combining their outputs, the total amount of error can be reduced and the detection accuracy can be increased. The proposed Adaptive Neuro-Fuzzy Inference based system will be able to detect an intrusion behavior of the networks. The experiments and the evaluations of the proposed method were performed with intrusion detection Dataset. The results show that our system outperforms two other previously developed states -of- the- art approaches in terms of detection accuracy.

ADVANTAGES:

- Able to distinguish both known and unknown DoS attacks from legitimate network traffic. Gives high accuracy detection.

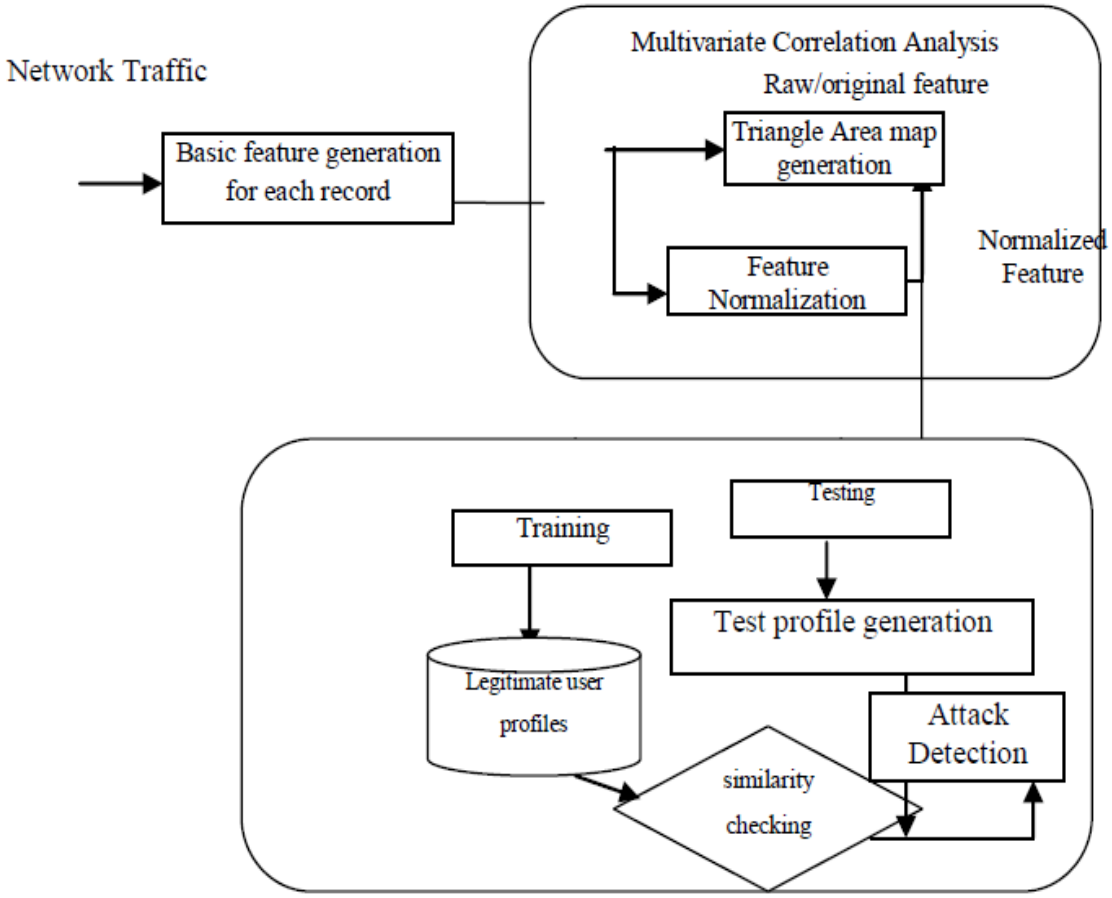


Fig.2.Proposed of Neuro fuzzy inference system

The whole detection process consists of three major steps as shown in Fig. 1. The sample-by-sample detection mechanism is involved in the whole detection phase in step1 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.. Step 2 is 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 (Step 2).. 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.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

Anomaly based detection mechanism overview:

The anomaly based detection mechanism is adopted in decision making.. 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.

Implementation Details:

The system framework and the sample-by-sample detection mechanism are discussed.

- Basic features generation
- Multivariate correlation analysis
- The anomaly based detection mechanism
- Performance comparison

1. Basic features generation:

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:

DoS attack traffic behaves differently from the legitimate network traffic, and the behavior of network traffic is reflected by its statistical properties. To well describe these statistical properties, we present a novel MCA approach in this section. Given an arbitrary data set X = $\{x_1, x_2, \dots x_n\}$ where $x_i = \{f_1^i, f_2^i \dots . f_m^i\} (1 \le i \le n$ represents the i_{th} m-dimensional traffic record. The vector x_i is first projected on the $(j,k)_{th}$ 2D Euclidean subspace $y_{i,j,k} = [\in_j \in_k]^T x_i = [f_j^i f_k^i]^T (1 \le i \le n, 1 \le j \le m, 1 \le k \le m, j \ne k)$. the vectors $\in_j = [e_{j,1}, e_{j,2} \dots e_{j,m}]^T$ have elements with values of zero, except the $(j,j)_{th}$ and $(k,k)_{th}$ elements whose values are ones in $\in_j$ and $\in_k$, respectively. Then, on the Cartesian coordinate system, a triangle $\Delta(f_j^i \, O f_k^i)$ formed by the origin and the projected points of the coordinate (f_j^i , f_k^i). on the j-axis and k-axis is found. Its area $Tr_{j,k}^i$ is defined as

$$Tr_{j,k}^i = \left(\left\| (f_j^i, 0) - (0,0) \right\| \times \left\| (0, f_k^i) - (0,0) \right\| \right) / 2$$ Where and $\ne k$. To make a complete analysis, all possible

permutations of any two distinct features in the vector xi are extracted and the corresponding triangle areas are computed. The values of the elements on the diagonal of the map are set to zeros ($Tr_{j,k}^i = 0$, if j = k) because we only care about the correlation between each pair of distinct features This infers that the values of $Tr_{j,k}^i$ and $Tr_{k,j}^i$ are actually equal.. The lower triangle of the TAM^i is converted into a new correlation vector TAM^i lower denoted as follows:

$$TAM_{lower}^i = [Tr_{2,1}^i \; Tr_{3,1}^i \; \dots \; Tr_{m,1}^i \; Tr_{3,2}^i \; Tr_{4,2}^i \; \dots \; Tr_{m,2}^i \; \dots \; Tr_{m,m-1}^i]^T.$$

For the aforementioned data set X, its geometrical multivariate correlations can be represented by $X_{TAM_{lower}} = \{TAM_{lower}^1, TAM_{lower}^2, \dots . TAM_{lower}^i, \dots, TAM_{lower}^n\}$. When putting into practice, the computation of the $Tr_{j,k}^i$ defined and it can be simplified because the value of the $Tr_{j,k}^i$ is eventually equal to half of the multiplication of the absolute values of f_{ij} and f_{ik}. Therefore, the transformation can be eliminated, and (10) can be replaced by $Tr_{j,k}^i =$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

$(|f_j^i| \times |f_k^i|)/2$. First, it does not require the knowledge of historic traffic in performing analysis. Second, unlike the Covariance matrix approaches proposed in [12] which is vulnerable to linear change of all features,. Third, it provides characterization for individual network traffic records rather than model network traffic behavior of a group of network traffic records.

3. The anomaly based detection mechanism:

A threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. A low-quality normal profile causes an inaccurate characterization to legitimate network traffic. First apply the proposed triangle-area-based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

3.1 Normal Profile Generation:

Set of legitimate training traffic records

$X^{normal} = \{x_1^{normal}, x_2^{normal}, \dots, x_g^{normal}\}$.

The triangle-area based MCA approach is applied to analyze the records. The generated lower triangles of the TAMs of the set of g legitimate training traffic records are denoted by $X_{TAM_{lower}}^{normal} = \{TAM_{lower}^{normal,1}, TAM_{lower}^{normal,2}, \dots . TAM_{lower}^{normal,g}\}$.

Mahalanobis distance is adopted to measure the dissimilarity between traffic records.. traffic records ($TAM_{lower}^{normal,i}$) and the expectation ($\overline{TAM_{lower}^{normal}}$) of the g legitimate training traffic records.

$$Cov = \begin{bmatrix} \sigma(Tr_{2,1}^{normal}, Tr_{2,1}^{normal}) & \cdots & \sigma(Tr_{2,1}^{normal}, Tr_{m,m-1}^{normal}) \\ \sigma(Tr_{3,1}^{normal}, Tr_{2,1}^{normal}) & \cdots & \sigma(Tr_{3,1}^{normal}, Tr_{m,m-1}^{normal}) \\ \vdots & \ddots & \vdots \\ \sigma(Tr_{m,m-1}^{normal}, Tr_{2,1}^{normal}) & \cdots & \sigma(Tr_{m,m-1}^{normal}, Tr_{m,m-1}^{normal}) \end{bmatrix}$$

The covariance between two elements in the lower triangle of a normal TAM is defined given below equation.

$$MD^{normal,i} = \sqrt{\frac{(TAM_{lower}^{normal,i} - \overline{TAM_{lower}^{normal}})^T (TAM_{lower}^{normal,i} - \overline{TAM_{lower}^{normal}})}{Cov}}$$

$$MD^{observed} = \sqrt{\frac{(TAM_{lower}^{observed} - \overline{TAM_{lower}^{normal}})^T (TAM_{lower}^{observed} - \overline{TAM_{lower}^{normal}})}{Cov}}$$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1039-1045), Month: April - June 2015, Available at: www.researchpublish.com

3.2 Threshold Selection:

The threshold given used to differentiate attack traffic from the legitimate one

$$Threshold = \mu + \sigma * \alpha.$$

This means that detection decision can be made with a certain level of confidence varying from 68 to 99.7 percent in Algorithm for normal profile generation based on triangle-area based MCA. association with the selection of different values of . Threshold, it will be considered as an attack.

Require: Observed traffic record $x^{observed}$, normal profile $Pro : (N(\mu, \sigma^2), \overline{TAM_{lower}^{normal}}, Cov)$ and parameter α

1: Generate $TAM_{lower}^{observed}$ for the observed traffic record $x^{observed}$
2: $MD^{observed} \leftarrow MD(TAM_{lower}^{observed}, \overline{TAM_{lower}^{normal}})$
3: **if** $(\mu - \sigma * \alpha) \leq MD^{observed} \leq (\mu + \sigma * \alpha)$ **then**
4: **return** Normal
5: **else**
6: **return** Attack
7: **end if**

3.3 Attack Detection:

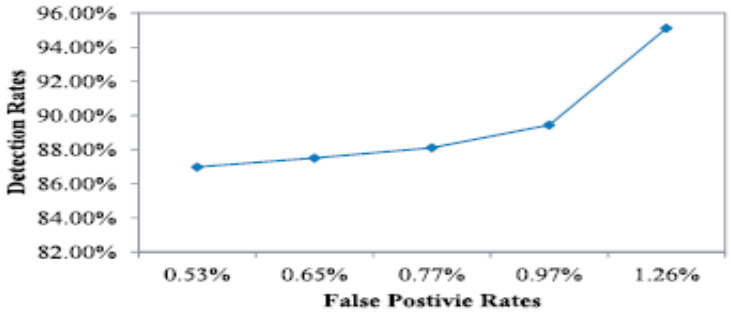
Then, the MD between the TAM observed lower and the TAM normal lower stored in the respective regenerated normal profile Pro is computed using (15).

4. Multivariate Correlation Analysis and Detection:

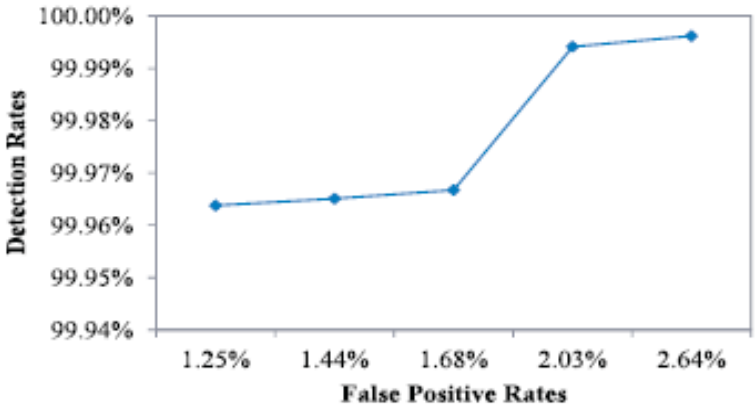
It is measured by the square root of determination, including nonlinear prediction which the predicted values have not been derived from a model-fitting procedure are exactly correct and a value of zero indicating that no linear combination of the independent variables is a better predictor than is the fixed mean of the dependent variable.

5. Performance comparison:

Two state-of-the-art detection approaches, namely, triangle area-based nearest neighbors approach and Euclidean distance map-based approach are selected to compare with our proposed detection system the our proposed MCA-based detection system (95.20 percent for the original data and 99.95 percent for the normalized data) clearly outperforms the triangle area based nearest neighbors approach (92.15 percent). In addition, our proposed detection system cooperating with normalized data (99.95 percent) shows a marginal advantage over the approach based on Euclidean distance map (99.87 percent).



ROC curve for analyzing original data



ROC curve for analyzing Normalized data

III. CONCLUSIONS AND FUTUTRE WORK

My work is about MCA-based DoS attack detection system in which triangle-area-based MCA technique and the anomaly-based detection technique is used. The technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and gives more accurate characterization for network traffic behaviors.Ttriangle area map generation technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. Evaluation has been conducted using KDD Cup 99 dataset it contains the traffic record. Accurate detection in the fixed threshold value the neuro-fuzzy systems were proposed as subsystems of the ensemble. Sugeno type Neuro-Fuzzy Inference System has been chosen as a base and by using this classifier the system gives high accuracy detection and low computational overload has been obtained.

IV. FUTURE WORK

To be part of the future work, use SVM based anomaly detection to improve the detection accuracy.

REFERENCES

[1] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, pp. 2435-2463, 1999.

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, pp. 18-28, 2009.

[3] D.E. Denning, "An Intrusion-Detection Model," IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.

[4] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion Detection Using Fuzzy Association Rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB Using SVM," Computer Comm., vol. 31, no. 17, pp. 4212-4219, 2008.

[7] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," IEEE Trans. Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.