A Brief Study of Fuzzy Evaluation Method for Intrusion Detection System

Tushi Kumar
Research Scholar, I.T., B.R.A.Bihar University, Muzaffarpur
D.K.Singh
Associate Professor, Univ. Dept. of Mathematics, B.R.A.Bihar University, Muzaffarpur

Abstract

This paper demonstrates the use of fuzzy mathematics for selection of the best algorithm for the implementation of intrusion detection system. All the steps required for this evaluation have been explained in this paper. The importance of this evaluation method from the point of view of Internet has also been discussed in this paper.

Introduction

The fuzzy theory is suitable for use in intrusion detection because it can easily combine input data from various sources. Since many types of intrusions cannot be clearly defined, the advance warnings that they trigger are usually vague too.

Fuzzy mathematics is used for describing, researching, and managing the mathematical relationships found in things with fuzzy characteristics. A comprehensive fuzzy evaluation is an important application of fuzzy mathematics. When the circumstances involve very complex factors, it can be used for selecting the best program for execution or making a choice after ranking the system detection results after the evaluation.

Steps of Fuzzy Evaluation Method

The main steps of the fuzzy evaluation method are as follows:

(i) determine the factors and comments sets for evaluation, and then establish the fuzzy sets of the various factors (membership function);

(ii) establish the fuzzy relationship between the evaluation factors and the comments, and then determine the weight that the respective factors.

(iii) derive a conclusion on the basis of calculations using a specific operand. Flexibility in the handling of attacks and the use of reasonable judgment are required for identifying a strict boundary between the normal and the abnormal.

We have used the fuzzy sets technique in this study. The fuzzy sets of basic variables are represented by the following quintuple:

Fuzzysets ::= (Object, Attribute, FC, Domain, ML) ....(1)

Here, Object refers to the item being described; Attribute, a particular property of the object; FC, the fuzzy concept; Domain, the location of the attribute; and ML, the membership list.

Fuzzy Evaluation Method in Details

The procedure for conducting a fuzzy evaluation is as follows:

Step 1:

Determine the factors and comments sets for evaluation, and then establish the fuzzy sets of the various factors. Internet access can be described using various characteristics such as the duration of the connection, communication volume, source and destination addresses, and types of service (i.e., the target port number). A compilation of these characteristics is known as the factors set. The evaluation vector is the bituple E = (U, W), where U denotes the factors set U = {u_1, u_2,...u_n} and W represents the weight vector. Every component of W corresponds to the degree of importance of a factor during evaluation and can be represented as follows: W = ò$_u$ w/u. Corresponding to the factors set is the comments set, which refers to the set of linguistic variables of the condition "degree of abnormality." The method of describing each factor is consistent. Therefore, the density distribution function of these factors can be treated as their membership function. During this step, the task is to calculate the density distribution function of each factor using the existing data.

Step 2:

Evaluate the fuzzy relation between the factors and comments sets, and then determine the weight to be ascribed to the various factors during evaluation. This is the most important step in intrusion detection based on fuzzy evaluation. The detection model can be established once the fuzzy relation between the two sets has been determined. The fuzzy relation between the factors ui and comments indicates the degree of membership that the respective factors have with the various degrees of abnormality. The determination of the fuzzy relation between the factors u_i and comments e_j is based on ¦$_i$(u_i), which is the density distribution function of u_i. If the comments set is {e_1, e_2,....e_m} then the density distribution function of u_i will be mapped onto m number of fuzzy relations.

In order to determine the weight of each factor, it is necessary to assess and rank the importance of all the factors. In this study, a judgment matrix established through the expert evaluation method (EEM) was used. The EEM is an important fuzzy mathematics tool used for creating fuzzy sets, fuzzy relations, and other mathematical models. It relies mainly on the experience of experts in the related fields. The sequence to establish a judgment matrix using EEM is as follows.

(i) Invite number of experts to establish a comparative judgment matrix A_1, A_2,.....A_n for a particular type of intrusion, on the basis of their own experiences and the concept of fuzzy relations.

(ii) Set up a group of weights W_1, W_2,....W_n , W_1+ W_2+....+ W_n= 1 in accordance with the authority ranking of the experts, where W_i represents the authority ranking of expert number i, i Î 1, 2, ...n.

(iii) Represent the final judgment matrix as $A = W_1 x A_1 + ... + W_n x A_n$.

Step 3:

The conclusion from the evaluation and calculations carried out using a particular operand is derived as follows:

(i) Use the comments set to assess each eigenvalue that was determined by the aforementioned fuzzy relations, and then compose the evaluation matrix.

(ii) Carry out a compositional operation of the fuzzy matrix using the weight vector of the factors list and the evaluation matrix, thereby deriving a comprehensive evaluation vector.

(iii) Determine the comments for this particular set of eigenvalues on the basis of the principle of the maximum degree of membership.

Fuzzy Evaluation Method Role in IDS

Internet and data fraud has become one of the most challenging cybernetic acts that security officers around the world try to combat. The more critical and confidential the data is the more appealing it is for attackers. The impact of a successful attack on an institution can have disastrous consequences such as privacy breach, data loss, or service interruption. Researchers around the word constantly develop and improve NIDS that are meant to combat such threats. For a NIDS to function properly all of its building blocks and processing components need to be properly designed. The feature selection stage is one of the first steps that need to be addressed. The main focus of this work is on mining the most useful network features for attack detection. In order to do this, we proposed a network feature classification, feature evaluation procedure that helps to identify the most useful features that can be extracted from network packets.

Conclusion

Finally, the proposed feature evaluation method is applied on all the features, tunings, and datasets to produce the final results. The procedure uses mathematical, statistical and fuzzy logic techniques to rank the participation of individual features into the detection process. The implementation can be done by the use of any modern programming languages that provide the facility of implementation of object oriented concepts.

REFERENCES

1. J. A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, 2002.

2. P. Gupta and N. McKeown, “Algorithms for packet classification,” IEEE Network, vol. 15, no. 2, pp. 24–32, 2001.

3. J. Moscola, J. Lockwood, R. P. Loui, and M. Pachos, “Implementation of a content-scanning module for an Internet firewall,” in Proceedings of the 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM '03), pp. 31–38, 2003.

4. J. F. Maddox and M. Arlington, “Intrusion detection system,” U.S. Patent No. 4, 772, 875. 20 Sep. 1988.