Analysis of Fuzzy Inference System for Intrusion detection

L.Gnanaprasanambikai [1]
Asst. Prof. Department of Information Technology,
Nehru Arts and Science College, Coimbatore.
gnanaambikai@gmail.com

K.Pargunarajan [2]
Asst.Prof. Department of ECE,
Amrita Vishwa Vidhyapeedham,
pargunarajank@gmail.com

M.Sheela new sheeba [3]
Asst. Prof. Department of IT,
Nehru Arts and Science College
Sheela79.rincy@gmail.com

Abstract:

Security is important in computer networks, Intrusion detection system monitors network or system activities for malicious activities or policy violations and produces reports to a management station. There are various approaches being utilized for intrusion detection, Fuzzy logic is one Artificial Intelligence approach, for effective rule generation in intrusion detection. This paper focuses on study of fuzzy logic and fuzzy inference systems for intrusion detection. The paper proposed the necessary steps of fuzzy inference systems for fuzzy rule.

Keyword: *Intrusion Detection, Fuzzy, Fuzzy logic, Fuzzy inference System, Fuzzy rule, Fuzzy toolbox, Fuzzy inference system types.*

Introduction:

Due to the enormous growth of the usage of computers, computer networks and its applications, the security concern has become very crucial. Though there are a number of ways to provide security such as cryptography, anti-virus, malwares, spywares, etc., it is not possible to provide complete secure systems. So there should be a second line of defence, IDS has emerged as one of the significant field of security in today's world to detect attacks. An intrusion detection systems watches networked devices and searches for anomalous or malicious behaviours in the patterns of activity in the audit stream.[1].

There are various methodology and approaches have been developed and deployed for IDS implementation such as ANN, Data mining, Fuzzy logic etc. Fuzzy logic is very appropriate focusing on intrusion detection. One reason is that usually there is no clear boundary between normal and anomaly events. The use of fuzziness of fuzzy logic helps to smooth the abrupt separation of normality and abnormality. Another reason is that it can defined clearly when to raise an alarm that is fuzzy. At what degree of intrusion we should raise an alarm is often depends on

different situations. [3]. This paper analysis fuzzy logic and fuzzy inference systems for intrusion detection.

2. Fuzzy Logic and Fuzzy inference Systems

Fuzzy logic was introduced by Dr. Lofti Zadeh of UC/Berkeley in the 1960's as a means to model the uncertainty of natural language. Fuzzy logic is based on building a set of human language rules as specified by the user. The fuzzy systems convert these rules into their mathematical equivalents and thus simplifying the job of the computer and the system designer. The obtained results are much more accurate and it represents the way that systems behave in the real world. Fuzzy logic has also included the benefit of its simplicity and flexibility. Fuzzy logic can handle the problems with inaccurate and incomplete data and it can also model nonlinear functions of arbitrary complexity [3].

Fuzzy inference is the process of formulating the mapping from a given input to an output using fuzzy logic. The mapping then provides a basis from which decisions can be made, or patterns discerned. The process of fuzzy inference involves all of the pieces that are described in the previous sections: membership functions, fuzzy logic operators, and if-then rules. There are two types of fuzzy inference systems that can be implemented in the Fuzzy Logic Toolbox: Mamdani-type and Sugeno-type.[5]

A) Mamdani fuzzy inference system

Mamdani's fuzzy inference method is the most commonly seen fuzzy methodology. Mamdani's method was among the first control systems built using fuzzy set theory.Mamdani-type inference,as defined for the toolbox, expects the output membership functions to be fuzzy sets .After aggregation, Mamdani method, uses centroid for defuzzification which is a two dimensional function.[3]

B) Sugeno Fuzzy inference system

Sugeno Fuzzy inference system was introduced in 1985.Sugeno output membership function are either linear or constant. Rather than integrating across the two-dimensional function to find the centroid, Sugeno-type systems uses the weighted average of a few data points.[5]

3. Fuzzy inference System Processing Steps

In the Fuzzy Logic Toolbox, there are five parts of the fuzzy inference process: fuzzification of the input variables, application of the fuzzy operator (AND or OR) in the antecedent, implication from the antecedent to the consequent, aggregation of the consequents across the rules, and defuzzification.[5]

Step 1: Fuzzify inputs

The first step is to take the inputs and determine the degree to which they belong to each of the appropriate fuzzy sets via membership functions. In the Fuzzy Logic Toolbox, the input is always a crisp numerical value limited to the universe of discourse of the input variable (in this case the interval between 0and 10) and the output is a fuzzy degree of membership in the qualifying linguistic set (always the interval between 0 and 1). Fuzzification of the input amounts to either a table lookup or a function evaluation.[5]

Step 2: Apply Fuzzy Operator

Once the inputs have been fuzzified, we know the degree to which each part of the antecedent has been satisfied for each rule. If the antecedent of a given rule has more than one part, the fuzzy operator is applied to obtain one number that represents the result of the antecedent for that rule. This number will then be applied to the output function. The input to the fuzzy operator is two or more membership values from fuzzified input variables. The output is a single truth value. In the Fuzzy Logic Toolbox, two built-in AND methods are supported: min (minimum) and prod (product). Two built-in OR methods are also supported : max (maximum), and the probabilistic OR (probor). [5]

Step 3: Apply Implication Method

Before applying the implication method, we must take care of the rule's weight. Every rule has a weight (a number between 0 and 1), which is applied to the number given by the antecedent. Once proper weighting has been assigned to each rule, the implication method is implemented. A consequent is a fuzzy set represented by a membership function, which weights appropriately the linguistic characteristics that are attributed to it. The consequent is reshaped using a function associated with the antecedent (a single number). The input for the implication process is a single number given by the antecedent, and the output is a fuzzy set. Implication is implemented for each rule. Two built-in methods are supported, and they are the same functions that are used by the AND method: min (minimum), which truncates the output fuzzy set, and prod (product), which scales the output fuzzy set.[5].

Step 4: Aggregate All Outputs

Since decisions are based on the testing of all of the rules in an FIS, the rules must be combined in some manner in order to make a decision. Aggregation is the process by which the fuzzy sets that represent the outputs of each rule are combined into a single fuzzy set. The input of the aggregation process is the list of

truncated output functions returned by the implication process for each rule. The output of the aggregation process is one fuzzy set for each output variable.[5]

Step 5: Defuzzify

The input for the defuzzification process is a fuzzy set (the aggregate output fuzzy set) and the output is a single number. The aggregate of a fuzzy set encompasses a range of output values, and so must be defuzzified in order to resolve a single output value from the set.[5]

4. IDS using Fuzzy inference Systems

For intrusion detection, a wide variety of techniques have been applied specifically, datamining techniques, artificial intelligence technique and Soft computing techniques. Researchers are focussing on fuzzy rule learning for effective intrusion detection. Fuzzy logic is appropriate for the intrusion detection problem for two major reasons. First, many quantitative features are involved in intrusion detection. The second motivation for using fuzzy logic to address the intrusion detection problem is that security itself includes fuzziness.[6]. From above study of fuzzy logic and intrusion detection, we analyzed that for an intrusion detection system, the fuzzy inference system (mamdani method or sugeno method), aggregation and defuzzification steps are not necessary. In order to evaluate all the fuzzy rules, and to take a decision, the aggregation and defuzzification is used.

5. Conclusion and Future Work

In this paper, we analysed and studied the fuzzy inference system processing steps and reason for fuzzy logic in intrusion detection. We conclude the necessary steps of fuzzy inference systems for intrusion detection. In future, we implement these fuzzy rules for effective intrusion detection. We will use intrusion detection datasets and fuzzy logic applied on these datasets, for effective fuzzy rule generation.

References

[1]ANVBS.Harikishan, P.Srinivasulu, “Intrusion Detection System Using Fuzzy Inference System”, International Journal of Computer & Organization Trends – Volume 3 Issue 8 – Sep 2013, ISSN: 2249-2593, page 345-352.

[2] S. Revathi, Dr. A. Malathi, “Network Intrusion Detection Based On Fuzzy Logic”, International Journal of Computer Application Issue 4, Volume 1 (February 2014), ISSN: 2250-1797, page 143- 149

[3] Harjinder Kaur, Nivit Gill, “Performance Comparison of Host based and Network based Anomaly Detection using Fuzzy Genetic Approach”,

International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 8–August 2013,page 2740-2746

[4] Macdonald Mukosera, Thabiso Peter Mpofu, Budwell Masaiti, "Analysis of NSL-KDD Dataset for Fuzzy Based Intrusion Detection System", International Journal of Science and Research (IJSR), Volume 3 Issue 6, June 2014.

[5]http://home.agh.edu.pl/~mrzyglod/iw/iw_pliki/MatlabFuzzyLogicToolboxUser'SGuide.pdf.

[6]http://csrc.nist.gov/nissc/2000/proceedings/papers/005.pdf.

[7] Emma Ireland, "Intrusion Detection with Genetic Algorithms and Fuzzy Logic", UMM CSci Senior Seminar Conference, December 2013.

[8] Dipali Kharche, Prof. Rahul Patil, "Use of Genetic Algorithm with Fuzzy Class Association Rule Mining for Intrusion Detection", International Journal of Computer Science and Information Technologies, Vol. 5(6), 2014.

[9]K.G. Srinivasa and N.Pramod, "gNIDS: rule-based network intrusion detection systems using genetic algorithms", International Journal of Intelligent Systems Technologies and Applications, vol 11, Nos 3/4, pp 252-266, 2012.

[10] Amin Einipour, "Intelligent Intrusion Detection in Computer Networks Using Fuzzy Systems", Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Volume 12 Issue 11 Version 1.0 Year 2012.