The Survey on Fuzzy logic: A Soft Computing Approach for Network Security

Mrs. Swetha M S
Assistant Professor
Department of Information Science and Engineering
BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka, India

Miss. Srishti Suman
Student
Department of Information Science and Engineering
BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka, India

Dr. Thungamani M
Assistant Professor
Department of Computer Science and Engineering
COH UHS Campus GKVK Bangalore-560065, Yelahanka, Bangalore -560064, Karnataka, India

Mr. Muneshwara M S
Assistant Professor
Department of Computer Science and Engineering
BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka, India

Abstract

As we know that all the computer networks are very much prone to inside and outside attacks in recent days due to its different types of use in every field. For this aspect, a number of security techniques are applied to reduce the effect of all the possible no attacks in the network. The secure data communication over internet or any other network is under threat of intrusions and misuses all the time. In this case, network security is very important for protecting the intellectual data from attackers in computer network while transmission is being done. So many intrusion detection systems are already proposed to detect the intrusion in the network. We have so many of soft computing techniques one of which is neuro-fuzzy based intrusion detection system. Here we are going to emphasize the proposed neuro-fuzzy based intrusion detection system and discussed their suitability in terms of detection rates and false positives rates towards network security.

Keywords: Fuzzy logic, soft computing, Neuro fuzzy, Intrusion Detection Systems

---

I. INTRODUCTION

The secure data communication over internet or any other network is under threat of intrusions and misuses all the time. As in the increase in so many number of security threats, the Intrusion Detection Systems has evolved as a significant method against these threats. An intrusion is defined as a set of activities, which tries to compromise the integrity, confidentiality or availability of a resource. Intruders are there of two types: external intruders and internal intruders.

- External Intruders: These are the intruders who are illegal users of the machines they attack.
- Internal Intruders: These have authorization to access the system having few limits and expert systems.

Here a variety of range of pre-processing practices are exercised such as data mining, neural networks, Petri-nets, state transition diagrams, genetic algorithms, decision trees and fuzzy based logics. We have different fuzzy methods for intrusion detection system using Fuzzy logic by analysing Fuzzy rule. Here the use of fuzzy if-then rules for intrusion detection. We have a proposed fuzzy logic-based system, which is capable to detect unusual behaviour of the network. The Soft computing techniques are able to construct the modern intelligent systems consisting of neural networks, fuzzy logic, genetic computing and probabilistic reasoning handling the robustness, tractability, low solution cost, uncertainty and partial truth. There are so many soft computing approaches that are also possible i.e. neuro-fuzzy, fuzzy-genetic, neuro-genetic and neuro-fuzzy- genetic. One of the major and most popular approach is in intrusion detection field i.e. neuro-fuzzy because in this approach neural network trains the IDS in various attacks so that IDS gathers the information regarding of traffic patterns, then fuzzy logic generates the rules based on that information about traffic patterns.

As of now, many Artificial Intelligence systems are being used in Intrusion Detection System. Here we will be looking at the most prominent technique- Fuzzy Logic. As attacks on systems may not have a discrete prototype, fuzzy logic is used to detect attack patterns which having a behavioural pattern between regular and abnormal. In addition to this, fuzzy logic also helps to lower the rate of fake positive alarms.

One of the most surface technique logic: Fuzzy logic. It starts and builds on a set of user-supplied human language rules. The fuzzy systems translate these rules into their mathematical equivalents. The outline of fuzzy logic structure is sketched in fig1. All the other supplementary benefits of fuzzy logic include its simplicity and its flexibility. Anything that can be constructed using usual design techniques can also be built with fuzzy logic, and vice-versa. Fuzzy logic is used in intrusion detection and is capable to deal with ambiguity and complexity.

By the help of fuzzy variables or linguistic terms, intrusion detection characteristics can be viewed easily and judgment of normal and abnormal activity in the network are based on its fuzziness nature that can recognize the degree of offensiveness of a node as a substitute of yes or no conditions.

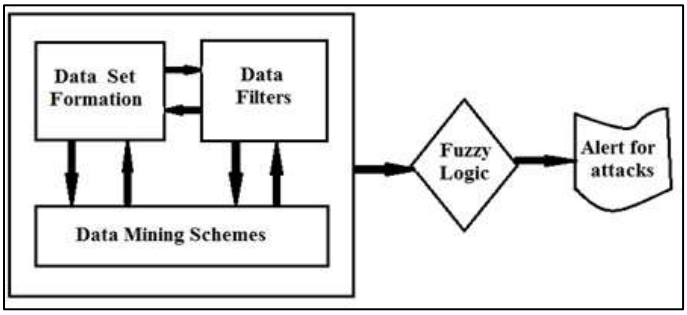

Fig. 1: The outline of Fuzzy logic Structure

The fuzzy logic has been functional in IDS in the past for two key reasons.

1) First: A few quantitative parameters that are used in the environment of intrusion detection, e.g., CPU usage time, connection interval, etc, can potentially be viewed as fuzzy variables.
2) Second: The thought of security itself includes some `level of fuzziness. Fuzzy logic is a type of many-valued logic or probabilistic logic, which deals with reasoning that, is approximate rather than fixed and precise.

II. LITERATURE SURVEY

A. Neuro-Fuzzy and Soft Computing—A Computational Approach to Learning and Machine Intelligence

Here first of all it collects in consistent notation at a place. In this paper there are some useful information which control engineers should know beyond the traditional tools of the trade regarding H infinity, robustness, LQG, Lyapunov, and other differential equation/frequency domain-based techniques.

B. Neuro-Fuzzy based Intrusion Detection System for Network Security

This paper has described about the proposed IDS system based on neuro-fuzzy networks. Here in this paper the IDS is trained by the neural network for the attacks .For this, information is gathered by IDS for the traffic patterns and then fuzzy logic is used for generating the rules based on that information about traffic patterns. Here neuro- fuzzy based classifiers is applied in the form of binary and multi classifier .These are also used to classify the normal activity from the abnormal activity in the networks.

C. Intelligent Soft Computing Techniques for Providing Network Security

In this paper, a survey is made based on the soft computing techniques including feature selection and classification algorithms for Intrusion detection. The advantages of soft computing techniques and intelligent agents on feature selection and classification algorithms to perform effective classification were analyzed. The soft computing technique based classification algorithms include Fuzzy classifier, Fuzzy Rough set, Neural Network and neuro-fuzzy classifiers based are discussed in this paper. Comparative analysis is also performed in this paper for the recent classifiers, which are proposed in this direction.

D. Information Security System protection using Soft Computing Techniques

On this paper, we will be able to review the most important factors of smooth computing ways embracing artificial neural network, fuzzy logic, genetic algorithm and probabilistic common sense system. Delicate Computing methods are being greatly employed by the intrusion detection process society given that of their simplification ability is that to help in finding out known and unknown intrusions and the cybercrimes that don't have any previously described guide.

E. A Literature Review on Recent Advances in Neuro-Fuzzy Applications

The paper has presented about applications towards business aiming at employing neuro-fuzzy approach. During 2011 and 2014 the neuro-fuzzy systems designed and developed. Here some wide-spread domains are considered in Prominent applications with the capabilities in respective domains.

III. DEVELOPMENT OF NETWORK SECURITY SYSTEM

Here in designing it involves defining of advanced network security system variables with the collection of data for the network threats and the design of the system with its implementation. These are described below.

A. Structure of Network Security System

1) First step:

Here the first step is the establishment of input and output variables. The studying of the problem domain usually does this task. Here, the key variables are defined.

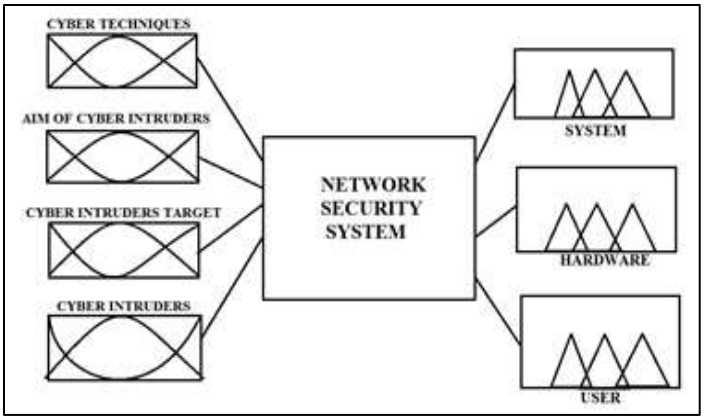

Fig. 2: Structure of Network Security System

B. Collection of the data for the proposed model in Cyber Terrorism

Here the system describes about the various questions communicated by the user. Here the extraction of data, which is being used from a series of questionnaires, gathered from all cyber experts and system administrators. The collected data are related with the topics given below:

1) Denial of Service (Dos):

A denial of service attack is a kind of cyber attack where the perpetrator tries to create a machine or a network ways unavailable in a temporarily or permanently manner to all host which are connected to the internet .It attacks, virus, malware, logic bomb, social engineering, Trojan horse , Out of service, seizing the web page, attacks for protesting, seize critical systems, capture confidential information, system control. This theory does the evaluation about cyber terrorists who generally attacks communications systems, financial centers, power plants, emergency services, transportation, water supply, oil and natural gas distribution stations. On general people are capable of cyber terrorism which includes dedicated special staff, hackers, cyber activists and opponents of the state which are evaluated in the proposed NSS model.

C. Design of the system

All the Advance systems have the forward or backward chaining. In forward chaining systems, it is attempted that we know facts which should be true for establishing new facts whose truth is implied by the antecedent. Backward chaining is just opposite of this. Here, we try of finding up the facts for establishing the truth of some goal state. The emulation of backward chaining by a forward chaining system is possible.

1) Forward Chaining:

As we know that an expert system has rules which is formulated as "if A then B" where,

– A =Set of conditions on data.
– B =Set of instructions to be carried out when the rule is fires.

The examination rules are the rules which is made to see that which all rules are made firable by the data. It means that, A is satisfied, and rules are selected for executing. After this, the execution of rules takes place and the set of instructions B is executed. As we can see that most of rule-based advance systems works in this manner. Here forward chaining is used in the proposed NSS model.

2) Backward Chaining:

As compared to forward chaining, here a different sequence is followed in backward chaining. In backward chaining, the conclusion, which we would like to reach, is specified. That is, specifying B. We find a rule or rules that have the desired consequent, and look at the antecedent A to see what the data must be to satisfy A. After this, it is to find out that how the establishment of data is going to take place and then we look for rules that have those data as a consequent. Work backward from goals is done in backward chaining data, and data to goals is worked in forward chaining. There are three main components according to the theory of expert systems:

1) User interface
2) Decision making interface engine
3) Database(storing up of data and fuzzy rules)

The model that embraces the fuzzy advance system is in this paper. The interaction between the cyber expert and expert system interface can happen in order to ask and read the advice of the proposed model. The cyber terrorist profiles, cyber-attack techniques,

and the cyber data threats are all consisted in an Interface engine. Using Fuzzy module, system administrator (or any user) interacts with NSS. User interface gives command to Inference engine and with the help of database in which rules are deposited it is evaluated.

3) Fuzzy Rule Based Model

In this report the components of a fuzzy rule based inference system and the general architecture for rule-based advance system are shown. Written below are the main modules of a fuzzy rule based system which includes fuzzification - or fuzzifier module, fuzzy rules, inference engine and defuzzifier.

1) Step 1- Fuzzification module:

A grade by fuzzy set is being converted by a crisp input of the domain. A crucial role is played by Constructing a fuzzy logic membership functions for the fuzzy rule based models. Triangular membership function was used in many fuzzy logic based applications. In this study triangular membership functions have been used.

2) Step 2- Defining fuzzy rules:

In the form of IF-THEN statements the Fuzzy rules consist of antecedent and consequent. There are a number of rules, and they make a group, which forms the basis for inference. The following are some fuzzy rules have been taken with the combination of linguistic variable values.

Input and output criteria of the model are:

"cyber techniques(CT)", "aim of cyber intruders-(ACI)", "cyber intruder's target (CIT) "cyber intruders (CI)", "hardware-(H)", "software-(S)" and "user(U)".

3) Step 3-Defuzzification:

By providing the crisp output, it acts like an interface between the fuzzy logic control and the inference system. Centroid, bisector, mean value of maximum values, smallest value of maximum values and largest value of maximum are some of the regular defuzzification methods. The conversion of a fuzzy set to a single crisp value is called defuzzification and reverse process is fuzzification.

4) Fuzzy Rule Generation Algorithm:

It involves three processes:

1) The depiction of the model variables.
2) The production of candidate rules.
3) The choice of the final Rule set.

For the expected cyber threats the system administrators is warned by a fuzzy rule based cyber indicator which is being proposed in this study . It has been found that when applied with in a given cyber threat scenario a system works well. Some warning signals generated by the rules are facilitated here. Here the proposed model goal is not about protecting the system rather than giving some warning signals for any of the expected cyber security.

IV. CONCLUSION

Here we have outlined a fuzzy logic structure to translate the fuzzy systems to their mathematical equivalents. We have done so many of literature survey on our topic of neuro fuzzy logic architecture for network security. Here a cyber indicator based on fuzzy rule is proposed which warns system administrators for expected cyber threats. Here we can see that a system is working well when it is applied with any cyber threat scenario. The fuzzy rules are used for generating the warning signals, which is being facilitated here. The proposed model's goal is to aim at warning the system administrator for expected cyber threats. In this paper, a network security system based on fuzzy rule was presented. The superiority in the areas of development flexibility and quick response for cyber threats is shown in this proposed model. The system administrators can use the model for determining the nature of cyber threat triggered by cyber terrorists. For a more secured knowledge environment it can also be used by commercial firms or government institutions.

REFERENCES

[1] Lotfi A. Zadeh (1994), "Fuzzy Logic, Neural Networks and Soft Computing", Communication of the ACM, 37(3), pp77-84.
[2] Er. Srinivas Mishra, Dr. Sateesh Kumar Pradhan and Dr. Subhendu Kumar Rath," Network intrusion detection system using fuzzy logic : a soft computing technique" International Journal of Computer Engineering and Applications, Volume XII, Issue IV, April 18 ,ISSN 2321-3469.
[3] J. S. R. Jang,C. T. Sun, and E. Mizutani "Neuro-Fuzzy and Soft Computing—A Computational Approach to Learning and Machine Intelligence (IEEE transaction paper)" IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 42, NO. 10, OCTOBER 1997.
[4] S. M. Bridges, and R. B.Vaughn, "Fuzzy Data Mining And Genetic Algorithms Applied to Intrusion Detection", In Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, 2000, pp.16-19.
[5] J.T. Yao, S.L. Zhao, and L.V. Saxton, "A Study On Fuzzy Intrusion Detection", In Proceedings of the Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, SPIE, Vol. 5812, Orlando, Florida, USA, 2005, pp. 23-30.
[6] S. Mukkamala, G. Janoski, A. Sung, "Intrusion detection: support vector Machines and neural networks." In: Proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE), St.Louis, MO, 2002, pp. 1702-1707.
[7] Y. Yu, and H. Hao, "An Ensemble Approach to Intrusion Detection Based on Improved Multi-Objective Genetic Algorithm", Journal of Software, Vol.18, No.6, pp.1369-1378, June 2007.
[8] J. Cannady, "Artificial Neural Networks for Misuse Detection", in Proceedings of the '98 National Information System Security Conference (NISSC'98), 1998, pp. 443-456.

[9] J. Gomez, D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," Proceeding Of 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point NY, June 2001 .
[10] Copeland JA, Garcia RC, "Real-time anomaly detection using soft computing techniques", In IEEE Southeast Conference, 2001.
[11] M. S. Abade, J. Habibi, C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm," Journal Of Network and Computer Applications, August 2005.
[12] Jill Rowland, Mason Rice, Sujeet Shenoi "The anatomy of a cyber-power" international journal of critical infrastructure protection of Elsevier January 2014.
[13] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, S. Shenoi, "Security strategies for SCADA networks," in: Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, Mar. 19-21, 2007.
[14] S.M.Furnel and M.J.Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?", Computers & Security, vol.18, pp.28-34,1999.
[15] L. Pietre-Cambacedes, T. Kropp, J.Weiss, and R. Pellizzonni, "Cybersecurity standards for the electric power industry-A survival kit," in CIGRÉ Paris Session, 2008, D2-217.
[16] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan, "e-Risk management with insurance: a framework using copula aided Bayesian belief networks" Presented at the Hawaii International Conference on system sciences, Hawaii, USA, 2006.
[17] Vikas Kumar, MS Swetha, MS Muneshwara, S Prakash, "Cloud computing: towards case study of data security mechanism," vol-2 issue-4 page no-1-8 2011.
[18] MS Muneshwara, MS Swetha, M Thungamani, GN Anil, "Digital genomics to build a smart franchise in real time applications," IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT),IEEE page no 1-4 2017.
[19] MS Muneshwara, A Lokesh, MS Swetha, M Thungamani, "Ultrasonic and image mapped path finder for the blind people in the real time system," IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) IEEE, page no 964-969 2017
[20] Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber-Espionage Campaign," Washington Post, February 10, 2013.