Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Rule Based Intrusion Detection System to Identify Attacking Behaviour and Severity of Attacks

Bindiya Bansal*
Department of Computer Science & Engineering
Lovely Professional University
Punjab, India

Kulwinder Singh
Department of Computer Science & Engineering
Sri Sai College of Engineering & Technology
Punjab, India

Abstract— As the computer network has an explosive growth from past few years. For this reason it becomes target for intruders. Therefore, security on the network becomes the major key issue. To overcome this issue many network intrusion detection approaches are used. The main goal of intrusion detection system is to identify normal and abnormal behaviour and network traffic. But major problem with these approaches are performance. Performance of intrusion detection system can be achieved by reducing false alarm rates and increasing the detection rates. This paper enhances the intrusion detection system performance by the use of fuzzy rule base. It will also check the severity of attacks. By knowing the levels or severity of attack we can make decisions on it. According to the level of attacks immediate action will be taken by using intrusion preventive system. The work will be continue to take automatic actions according to the behaviour or severity of attacks.

Keywords— intrusion, Security, Network, IDS, Fuzzy Logic, Rule learning.

I. INTRODUCTION

Intrusion detection system aim at detecting attacks against computer networks, computer system and information system. Nowadays organizations are much more dependent on network based system to store the information. Intrusion detection system is increasingly a key part of systems defence which helps in detecting abnormal activities on the network to keep data secure [20]. This Fuzzy rule base IDS will detect the unwanted traffic on the network. It monitors network traffic in order to check suspicious activity. In case of detection of any malicious activity it alarms. The system will not actually detect the intrusion but will detect the activity on network that may or may not be an intrusion [20] [11]. System will store all known attacks signatures in database and compared activity on network to the stored data. If there will be any variation occurs in existing data then it is easy for us to detect either the activity is intrusion or not. If any intrusion activity recognized then alarm will perform some reasonable actions. This system has emerged as a significant field of research, because theoretically it is impossible to set up a system without any vulnerability. This rule based system can do its job in two ways: Passive & Reactive. In passive intrusion detection system sensor senses intrusion on the traffic and store information of intrusion in log files and signals the alert. But in reactive intrusion detection system when sensors sense any intrusion activity, it will automatically perform some actions or in simple words it will react when any intrusion occurs on the network. IDS can be tuned accurately. As tuning process is time consuming but it is effective for IDS. Measurement of accuracy of IDS depends on the way it detects attack i.e. by rule set. Signature based detects only known and simple type of attacks but anomaly based detection detects different type of attacks but in this case higher number of false positives occurs.

II. BACKGROUND STUDY

Due to increasing importance of Cyber Security rule based Intrusion Detection Systems has become an active research area. **Lough *et al.*, (2001**) observe the factors and changing behaviour of network when any intruder enters into network. Here intrusion is classified into signatures and uses only system logs to detect an intrusion. Some of them such as passive sniffing attacks that do not appear in the audit logs cannot be classify. The reason behind system vulnerability was the security design process which is based upon past assumptions [5]. **Toosi *et al.*, (2006)** observed that intrusion detection system is to classify activities of a system into two major categories such as normal activity and suspicious activity. The objective of this paper is detect intrusions in computer networks by expose ANFIS as a Neuro-Fuzzy classifier. Rules and member functions are determined with their initial locations by subtractive clustering. In this method fuzzy rules are generated without the aid of human expert and all these fuzzy rules are effective for detecting intrusion as well as novel attacks in a computer network. Multi-class classification and detection of intrusion type. By using methods of feature selection we will continue does study on reducing fuzzy input variables [12]. **Panda1 *et al.*, (2007)** proposed a network intrusion detection system based on Naïve Bayes algorithm. In this patterns of the network services over data sets were labelled by services. With the help of these patterns attacks were detected in the dataset by using the algorithm named the naïve Bayes Classifier [10]. **Tsai a *et al.*, (2009)** It is consider a large number of machine learning techniques for the review including single, hybrid and ensemble classifiers that are used in the intrusion detection domain. Developing the

intrusion detection systems using machine learning techniques still needs to be researched because there are some limitation in it such as baseline classifiers, the architecture of multiple classifiers and feature selection [4]. **Sharmila Devi, *et al.,* (2012)** the existing network intrusion detection system SNORT which is an intrusion detection system and its main drawback i.e. by increasing the network traffic performance of snort degrades. Then discuss about different research areas which were taking place to improve the performance of existing system with the help of genetic algorithm. In described techniques, Genetic Algorithm decreases the false positive rate. Proposed detection system uploads and update new rule to the system. Implementation of Genetic Algorithm is unique as it considers both temporal and spatial information during encoding the problem. New rules are generated at run time, so administrator has no need to keep track of all these rules [2]. **Bapuji1 *et al.,* (2012)** observed that the implementation of Soft Computing and Artificial Intelligence methods/techniques are used widely in Intrusion Detection System are gaining its ability to learn and evolve which makes them more accurate and efficient in facing the enormous number of unpredictable attacks. Soft Computing paradigm of evolutionary computation techniques for synthesizing intrusion detection programs on Mobile Ad hoc Networks. Since prevention techniques cannot be sufficient and new intrusions continuously emerges, IDS is an indispensable part of a security system. IDS detect possible violations of a security policy by monitoring system activities and response. If we detect an attack once it comes in to the network, a response can be initiated to prevent or minimize damage of the system. The two major techniques for machine learning were highlighted, with the use of Genetic Algorithm and Artificial Neural Network providing intrusion system with extra intelligence [3]. **Shanmugavadivu *et al.,* (2012)** identify that intrusion detection system which are increasingly a key part of system defence are used to identify abnormal activities in a computer system. By making use of the fuzzy rule learning strategy which are more effective for detecting intrusions, an effective set of fuzzy rules for inference approach were identified automatically in a computer network. First of all in these mining single length frequent items of normal data as well as attacks data is done to generate the definite rules. Then, fuzzy rules that are generated by mining were identified by fuzzifying the definite rules and these rules were given to fuzzy system, which classify the test data [11].

III. PROBLEM AND APPROACH

There are number of techniques used for preventing the network from attacks and enhance the performance of the network. But still few challenges are there which need some concern. The existing systems fails to recognize normal behaviour and suspicious activity accurately. Sometimes the system inferred the intruder as the normal activity and permits that activity to get into the network but on the other hand it blows the alarm as it interprets the normal user as the intruder. Thus, generate the false alarms. The key issue that found in intrusion detection system is to protect the immune agents from corruption by suspicious activities [2]. To enhance the performance of intrusion detection system that will distinguish between the normal and abnormal user behaviour while monitoring the network traffic. So the basic need of the rule based intrusion detection system is to enhance system performance by reducing false alarm rates and also check the severity of attacks. To develop a system that can recognize normal behaviour and abnormal behaviour more effective. To make a measurable progress in the field of intrusion detection system, this rule based system recognizes normal and abnormal behaviour and also the severity of attack. If any attack shows higher severity then it will become easier to make a decision.

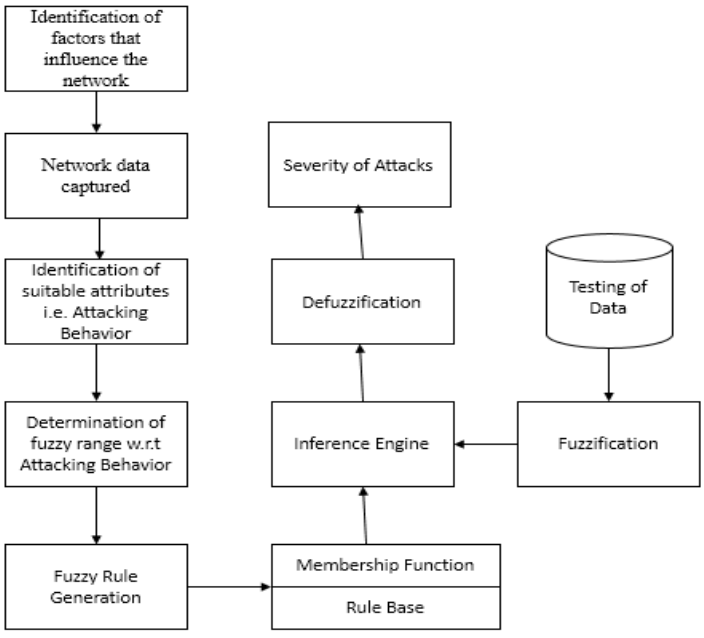

Fig 1: Architecture of rule based intrusion detection system

IV. FUZZY RULE BASE TO IDENTIFY SEVERITY OF ATTACKS

The process of Rule based intrusion detection system starts with the identification of those critical factors, which directly or indirectly influenced the network behaviour. After deciding those factors, set up the values for those parameters.

Providing values to some of these parameters sometimes may be a tedious task. Values for network factors are stored in the fact base (or working memory). Further, parameters are then fuzzified and creates a fuzzy knowledge base, which is basically a collection of fuzzy rules [6].

Fuzzification process will be started in which all the crisp values provided with the input variables will be transformed to the fuzzy values and for all the inputs respective rules will be generated. Then those fuzzy rules are process on the facts in the working memory in the fuzzy inference engine by applying any fuzzification method [13][16][17]. At the end the outcome of the fuzzy inference engine are defuzzified to provide the severity of attacks i.e. Low, Medium, High.

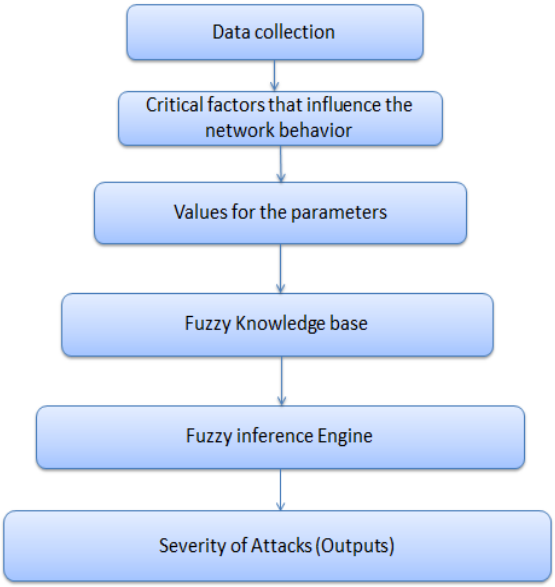

Figure 2: Rule based Fuzzy inference system for Intrusion Detection System

V. FUZZY RULE BASE INFERENCE ENGINE PROCESS FOR INTRUSION DETECTION SYSTEM

Step 1: Identification of critical factors

This is the initial and most important step of fuzzy inference process. It is fact that there are many factors on which behaviour of network affects when any intruder enters into network. Different factors plays different role and performance of proposed system increased or decreased according to the selection of those factors. Factors that affect network when any intruder enters into network are:

Existence: It is a fact that to detect the intrusion attempt there is something ever existed is sufficient. Entrance of intruder in network can be checked by static scanning of the file system existence. If we found any altered permissions and special files then there is possibility of entering of intruder. As we know when any intruder enters into network he/she must try to use files that place on the network or change permissions so that without knowing to original user he/she can access data. So the scanning of files will be done that place on network to check change in Existence.

Sequence: It is the fact that several things happened in strict sequence is sufficient to specify the intrusion. As we know there are several things on network that exists in a particular sequence. If we found any changes in sequence there may be a chance of any intrusion on the network. When data is transferred in the form of packets, these packets move in a sequence from source to destination. If we found any packet drop from sequence which indicates the intruder attempt on the network then all the packets resent to check. All packets have sequence number while sending from source to destination. When any packet drop, sequence is disturb. Sometimes more than one sequence number missing while sending data.

Partial order: Several events are defined in a partial order which means there is order of event occurrence on network. When the order of occurrence of event changes, it shows that there is going something wrong on network security. We divide the partial order in three fuzzy sets and range i.e. Low_changes, Minor_changes and Major_changes.

Duration: It is one of the important factor which helps in detecting intruder on network. This requires that something is existed or happened for not more than or less than a certain interval of time. This factor tell us that every event is occurs for some particular period of time and not more than or less than that time. If it found that some events take long time for occur then there is chance of attacks.

Interval: Things happened an exact (plus or minus clock accuracy) interval apart. This is specified by the conditions that an event occur no earlier and no later than *x* units of time after another event. Simply interval means every event occurs in particular interval of time. When one event stops next will be start. So when found any changes in this interval, there is chance of attack.

Step 2: Fuzzification

This phase involves the designing of the fuzzy expert system for the identification of attacking behaviour and severity of attacks. In this phase, input and output variables are defined. Here fuzzy sets are defined and the input is fuzzified with the help of defined membership function [7] [8].

Table 1 Fuzzy Linguistic Variables and their membership values

Factors	**Fuzzy Input Variables and their Memebership range**		**Fuzzy output Variables and their Memebership range**			
			Null	Low	Medium	High
Existence	No_changes	0-3				
	Low_changes	2.8-5.5				
	Severe_changes	5-10				
Sequence	Low	0-2.5				
	Medium	2.3-5.2				
	High	5-10				
Partial order	No_change	0-2.7				
	Minor_change	2.5-5.1	0-2.5	2.2-5.3	5-7.7	7-10
	Major_change	4.9-10				
Duration	Remain same	0-2.3				
	Less_than_prevoius	1.9-5.3				
	More_than_prevoius	5-10				
Interval	remain_same	0-2.7				
	Low_change	1.4-8.6				
	Severe_change	5.6-10				

In this table the fuzzy input variables have given the range and for these values there will be some respective output values that ranges are set for the output variables

Step 3: Fuzzy Rule Construction

The knowledge base of the fuzzy rule based system stores knowledge in the form of the rule and draw inference by using these rules. So for engineering the knowledge base, the formation of rules take place. The rule in the fuzzy system is in simple if-then statements [12].

Step 4: Fuzzy Inference Rule generation

These if-then rule statements are used to formulate the conditional statements that is a part of fuzzy logic [6] [7].

IF: Condition-1 and Condition-2 and Condition-3 Condition-4

THEN: Take Action-4

In this system, 243 such type of fuzzy IF-THEN rules are generated. Some sample IF-THEN rules for Attacks from the rule base are given as below:

- *IF Existence is No_changes AND Sequence is Low AND Partial_order is No_change AND Duration is Remain_same AND Interval Remain_same THEN Attack is Null.*
- *IF Existence is Severe_changes AND Sequence is High AND Partial_order is Major_change AND Duration is More_Than_Previous AND Interval Severe_change THEN Attack is High.*
- *IF Existence is Low_changes AND Sequence is Medium AND Partial_order is Minor_change AND Duration is Less_than_previous AND Interval is Low_change THEN Attack is Medium.*
- *IF Existence is Low_changes AND Sequence is High AND Partial_order is Major_change AND Duration is Less_than_previous AND Interval Remain_same THEN Attack is Medium.*

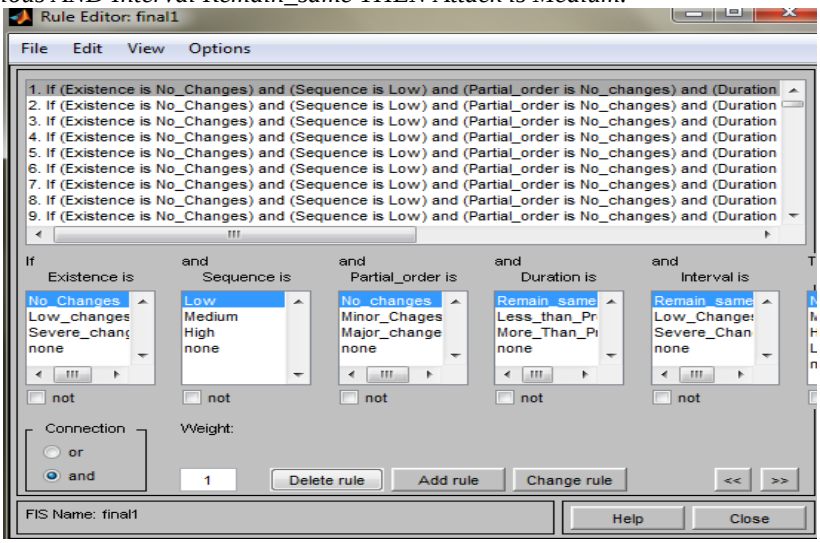

Fig 3: Rule Editor for the identification of attacking behavior

VI. EXPERIMENTAL RESULTS

In this paper, five critical network factors are analysed in our classifier for the identification of attacking behaviour and severity of attacks. At first the critical factors identified for attacking behaviour are considered as inputs for the fuzzy inference system and are represented in the form of fuzzy linguistic variables with their member elements. Then each variable is assigned with fuzzy membership using triangular membership functions.

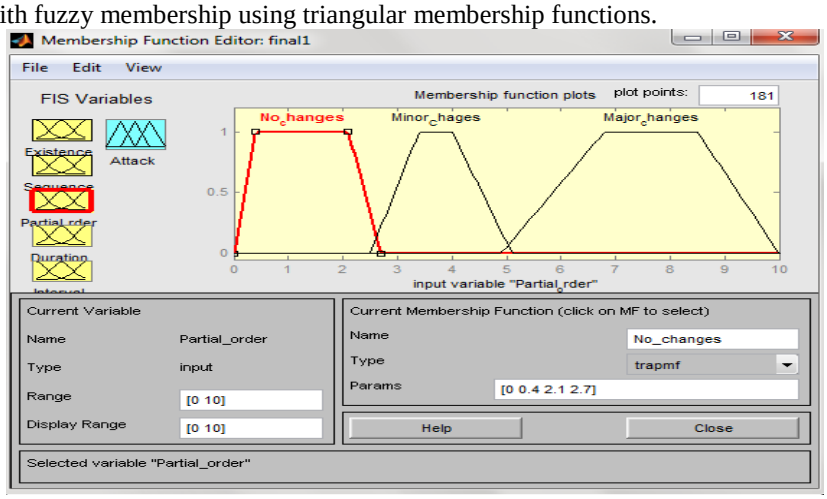

Fig. 4.Membership Function Editor for Partial order

The membership function for *partial_order* has three fuzzy sets *No_Change, Minor_change, Major_Chnage.* The membership function used in this system is the triangular membership function. It is also necessary to set the range for output membership function accordingly. Similarly for the other input variables membership function have been defined

Following is the figure that shows the membership functions of the output variables. The fuzzy set of attack and range is assigned. Attack has four fuzzy sets namely Null, Low, Medium and High. The range for null is in between 0 to 2.5, for low is in between 2.2 to 5.3, for medium is in between 5 to 7.7 and for high is in between 7 to 10.

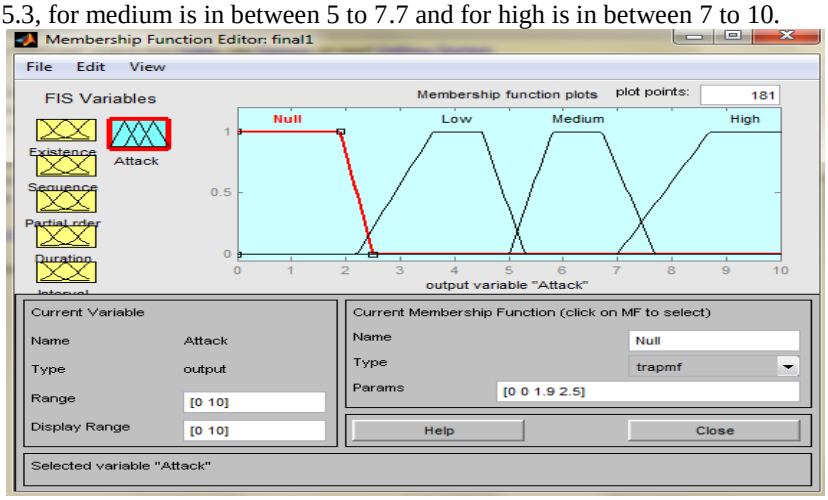

Fig. 5: Membership function editor for output severity of attacks

When the membership functions are selected, rule editor is used for generating rules. In Fuzzy Inference Systems, based on the template keystroke data provided by the different users, decisions are made and outputs are generated.

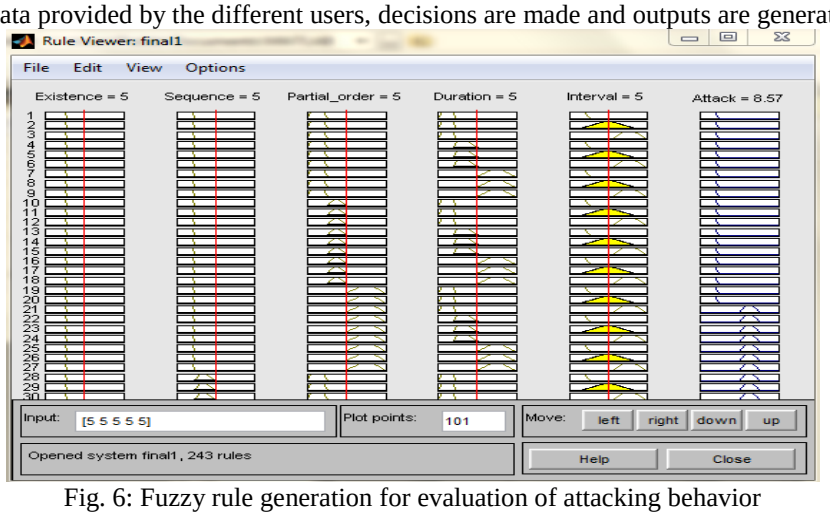

Fig. 6: Fuzzy rule generation for evaluation of attacking behavior

Using the Surface Viewer, a three-dimensional curve can be viewed that represents the mapping from two inputs and one output. By taking existence and sequence as input and attack as output Surface view

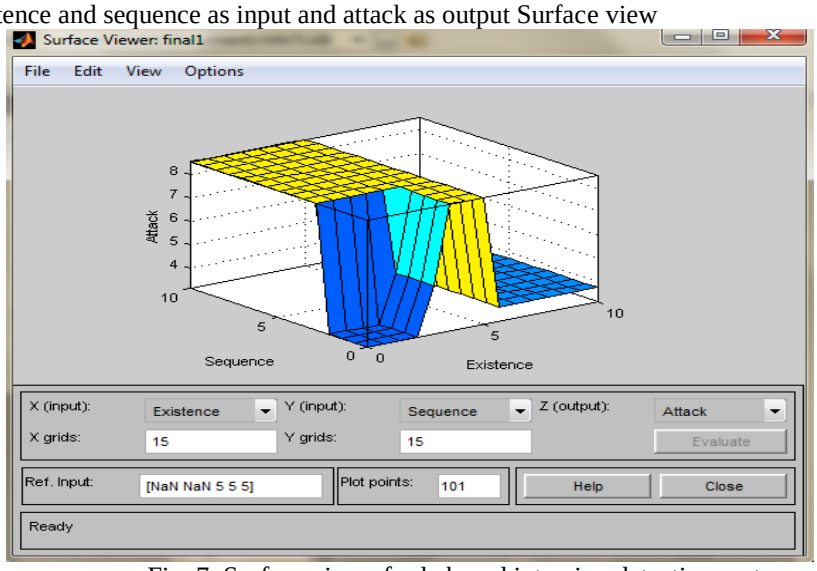

Fig. 7: Surface view of rule based intrusion detection system

The system is tested by using different defuzzification techniques. System is defuzzified on Centroid method, Bisector, SOM, LOM, MOM to test the robustness of the rules and knowledge engineering of tool.

Table 2 Defuzzified values of using different approaches

Existence	Sequence	Partial order	Duration	Interval	Defuzzified Values (Null.Low.Medium.High)									
					Centroid		Bisector		MOM		LOM		SOM	
					Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank
1.5	2.5	3	4	3.5	8.6436	1	8.6	1	8.75	2	10	1	7.5	2
7	3.5	2	6	6.5	3.8226	2	3.8	2	3.9	3	4.8	3	3	3
2	4	3.5	3	4	8.8369	1	8.9	1	9.2	1	10	1	8.4	1
6	6	4	7	5	3.8065	2	3.8	2	3.85	3	4.9	3	2.8	4
2	8	6	3.5	7	8.7556	1	8.8	1	9	1	10	1	8	1
3.5	5.5	8	7.5	9	3.7969	2	3.8	2	3.85	3	5	2	2.7	4
2.5	7	7.5	3	3.5	8.7834	1	8.8	1	9.1	1	10	1	8.2	1
9	3	5	6	4.5	3.7604	2	3.8	2	3.8	3	5.2	2	2.4	4
7.5	6.5	6	8	5.5	3.8285	2	3.8	2	3.95	3	4.8	3	3.1	3

VII. CONCLUSION AND FUTURE SCOPE

The fuzzy rule based system for Intrusion Detection System is able to identify the attacks and checks their severity. There are many factors that influence the network behaviour. But in this system we consider the critical five factors that are analysed for the identification of intruder or malicious activity. After analysis, these factors are passed through fuzzy inference system. Fuzzy inference system provides more accuracy and increase the performance of the intrusion detection system. Thus this system reduces the false alarm rate and increase performance of system. This fuzzy rule based system is scalable because it provides consistency in performance and reliability with regards to the increased traffic over the network. . Intrusion detection system will help in detecting problems that are not prevented by other security measures. This system will alert the appropriate staff by fire alarm when attacks are detected. Early anti-virus

software did not detect all known viruses and sometimes created false alarms on many normal user actions. We anticipate that over time the improvement in performance of IDS products will likely parallel that of anti-virus software. Intrusion detection system is useful for every field like bank where online banking is done, in the large organizations where companies useful log data is present, it also useful for scientist who shares their information through network for further research, social websites where more and more cybercrimes are occurred nowadays. Everywhere where information is access through network, intrusion detection system would be used. In future we continue our work in this direction in order to build an efficient intrusion detection model which when detect any intrusion automatically prevent it according to their severity of attacks.

REFERENCES

[1] Ahmad, I., Abdullah, A. B., Alghamdi, A. S., Hussain, M., & Nafjan, K. (2011). "Features Subset Selection for Network Intrusion Detection Mechanism Using Genetic Eigen Vectors". In *Proceedings of 2011 International Conference on Telecommunication Technology and Applications (ICTTA 2011)* (pp. 75-79)

[2] Devi, S., & Nagpal, R. (2012) "Intrusion Detection System Using Genetic Algorithm-A Review", *International Journal of Computing & Business Research, Hisar-125001, Haryana, India.*

[3] Bapuji, V., Kumar, R. N., Govardhan, A., & Sarma, S. S. V. N. (2012). "Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System". *Network and Complex Systems*, *2*(4), 24-31.

[4] Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). "Intrusion detection by machine learning: A review". *Expert Systems with Applications*, *36*(10), 11994-12000

[5] Lough, D. L. (2001). "A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation)".

[6] Ross T. J. (2005). "Fuzzy logic with engineering applications." John Wiley & Sons.

[7] Fasanghari M., Montazer G. A. (2010). "Design and implementation of fuzzy expert system for Tehran Stock Exchange portfolio recommendation, Expert Systems with Applications," 37, 6138-6147.

[8] Matthews C. (2003). "A formal specification for a fuzzy expert system, Information and Software Technology", 45, 419–429.

[9] Lippmann, R. P., & Cunningham, R. K. (2000). "Improving intrusion detection performance using keyword selection and neural networks". *Computer Networks*, *34*(4), 597-603.

[10] Panda, M., & Patra, M. R. (2007). "Network intrusion detection using naive bayes". *International journal of computer science and network security*,*7*(12), 258-263.

[11] Shanmugavadivu, R., & Nagarajan, N. (2011). "Network Intrusion Detection System Using Fuzzy Logic". *Indian Journal of Computer Science and Engineering (IJCSE)*, *2*(1), 101-111.

[12] Kahani, M. (2006, January). "A Neuro-Fuzzy Classifier for Intrusion Detection Systems". In *CSICC2006 conference*.

[13] Ashok, J., Raju, Y., & Munisankaraiah, S. (2010). "Intrusion detection through honeypots ". *International Journal of Engineering Science*.

[14] Revathi, M., & Ramesh, T. (2011). "Network intrusion detection system using reduced dimensionality". *Indian Journal of Computer Science and Engineering*, *2*(1), 61-67.

[15] Thomas, C., & Education, S. (2009). "Performance Enhancement of Intrusion Detection Systems using Advances in Sensor Fusion". *Supercomputer Education and Research Centre Indian Institute of Science, Doctoral Thesis, 304pp.*

[16] Tzeyoung, M. W. (2009). IATAC." Intrusion Detection Systems," 6th Edition, Information Assurance Tools Report.

[17] Carroll, L. "Properties of membership functions,fuzzification and defuzzification".

[18] Dhanalakshmi, Y., & Ramesh Babu, I. (2008). "Intrusion detection using data mining along fuzzy logic and genetic algorithms". *International Journal of Computer Science and Network Security*, *8*(2), 27-32.

[19] Garibaldi, J. M. (2005). "Fuzzy expert systems". In *Do Smart Adaptive Systems Exist?* (pp. 105-132). Springer Berlin Heidelberg.

[20] S. I. (2001)." Intrusion Detection Systems: Definition, Need and Challenges. *SANS institute Reading Room Site"*.

