FUZZY MODELLING OF A NETWORK DENIAL OF SERVICE (DOS) ATTACK PHENOMENON.

IHEKWEABA. OGECHI[1], IHEKWEABA.CHUKWUGOZIEM[2], INYIAMA H.C[3]

ABSTRACT - **This paper presents the fuzzy modeling of a network Denial of Service (DoS) attack characteristics. Conventional methods for achieving same purpose were showcased. Also, the need for a fuzzy logic approach as well as an improved mechanism for generating the fuzzy inference rules were outlined. Further, the paper discusses the basic concept of fuzzy logic, fuzzy systems and reasons for their adoption in modern control operations. DoS attack detection, using some basic traffic characteristics: bitrates, entropy and Hurst experiment as it's inputs, was x-rayed. Here, an attack trace file collected at the edge router of the Computer Science Department, University of California Los Angeles was used to develop the fuzzy inference model.**

The data set was partitioned into a training dataset and a testing dataset. The fuzzy concept learning system (FCLS) algorithm was used for constructing the fuzzy decision tree, using the trace files. Inference rules were then generated from the constructed decision tree. The simulation and evaluation of the fuzzy model was performed with the testing dataset.

KEY WORD: **Fuzzy concept learning system (FCLS), Hurst parameter (H), Entropy (E), Fuzzy system (FS), Certainty factors (CF), Fuzzy attribute (FA), Membership function (MF).**

1.0. INTRODUCTION

Due to the simplicity of the concept and the availability of the relevant attack tools, launching a DoS attack is relatively easy. However, defending a network resource against the attack is disproportionally difficult. In the most general sense, a complete DoS defense system should be able to detect the existence of the attack in real-time as well as trigger a classification and a corresponding response mechanism.

Classification refers to distinguishing between normal traffic (sent by legitimate users) and attack traffic (sent by nodes controlled by the attacker) Response mechanisms usually involve either dropping the traffic that was identified as attack, at the classification phase or taking some other planned action. Classification and response are usually resource-demanding procedures, that should not be running continuously, but only when an attack is suspected. For this reason, a comprehensive DoS defense system must include a mechanism that monitors the traffic, signaling the development of an attack when necessary. The system developed in this work, has the inherent property of low false alarm and high correct detection rate, all in real time. This is because, the earlier a DoS attack is detected, the easier it is to block it, otherwise it snowballs.

Several anomaly detection methods have been proposed against DoS attacks in the literature [14][15][16]. In these methods, the network traffic activity was captured and then a profile representing its stochastic behavior created. This profile was mainly based on metrics such as the network traffic rate, the number of packets or bytes for each protocol, the rate of connections, the number of different IP addresses, etc. Any activity that deviates from the assumed profile is treated as a possible attack.

However, there is a serious problem with these statistical anomaly detection methods. This is borne by the fact that it is hard to decide an appropriate metric on the global scale, because of the linear superposition of this microbased detection of a typical large network. In 1993 LeLand *et al* [17] discovered that the network traffic is self-similar; a basic characteristic that is vital in DoS detection. The research done by Li [18] first mathematically proved that there is a statistically significant change in the average Hurst parameter of the DoS flood attack. Allen *et al* [19] and W. Scalier *et al* [20] proposed a method using Hurst parameter to identify an attack. In practice, an attack causes a decrease in the traffic's self-similarity. Here, the normal range of the Hurst parameter is considered to be (0.5- 0.99), and during an beyond the range, when there is no attack. The problem with this selection method is that it can only detect the presence of an attack after the attack had occurred.

Fuzzy rule-based models have been widely used on control and pattern classification problems [19] [20] [21] [22] [23] [24]. The interest in using fuzzy rule based classification systems arises from the fact that such systems simultaneously accommodate both accuracy and comprehensibility of the classification results [25] [26]. Fuzzy logic has the capability to deal with the vague and imprecise boundaries between normal traffic and attack traffic [22].

The basic idea for designing a fuzzy rule-based classification system is to automatically generate fuzzy rules from numeric data (i.e, a number of pre-labeled training examples) or heuristics. Hence, rule-based construction for a classification problem has always been a challenging exercise. In this paper, a fuzzy concept learning system (FCLS) approach is used to build a fuzzy model for detecting and classifying traffic as either attack or normal. The network trace file of normal and attack traffic is used to build the fuzzy decision tree from which the fuzzy inference rules of DoS defense system, is generated.

2.0 FUZZY LOGIC AND FUZZY SYSTEMS

Fuzzy logic is a superset of conventional (Boolean) logic that has been extended to handle the concept of partial truth-truth values between “completely true” and completely false”[27]. As it’s name suggests, it is the logic underlying modes of reasoning which are approximate rather than exact. The importance of Fuzzy logic derives from the fact that most modes of human reasoning and especially common sense reasoning are approximate in nature. Fuzzy logic is a problem-solving control system methodology, capable of generating conclusions based upon vague, ambiguous, imprecise, noisy or missing input information. This approach follows naturally how a professional is able to solve a problem.

Fuzzy logic incorporates a simple rule based IF, THEN statements rather than attempting to model the system.

Fuzzy logic is empirically based; it relies on the operators’ experience rather than the technical details of the system being controlled. Expressions such as voltage is low, are common instead of voltage is 2V.

Fuzzy logic is currently preferred in control systems because it is robust and does not insist on noise- free inputs and can implement non linear systems without any known mathematical models. The output control is usually a smooth control function even when a wide range of input variations exist [10].

It is easier to modify the system for the purpose of either altering or improving it’s performance, by changing the rule structure, rule base, membership function defuzzyfication process.

The cost of fuzzy system implementation is low. Since the system can easily be simulated before implementation.

Multiple inputs and outputs can be achieved with Fuzzy logic controlled systems[13]. The number of the signals being a major determinant of the complexity of the rule base.

Due to its capacity to capture human expertise and to formalize approximate reasoning processes, it is a veritable tool for handling the challenges of congestion control in ATM networks. The basic steps employed in Fuzzy logic implementation, involves identifying and defining the control objective, determining the input and output relationships, developing the rule base using simple IF, THEN, AND, OR operations, and determining the Fuzzy logic membership functions[14]. Subsequently, the necessary routines are created if the system is intended to be implemented in software. Otherwise, the rules are coded directly into the system for hardware based implementation.

Crisp set theory can be generalized to the fuzzy set theory as follows. For any crisp set A, it is possible to define a characteristic function XA: x < 0,1 as in the following equation.

$$xA\,(x) \quad = \{i, \quad x\in \chi$$

$$\{0, \quad x\chi \;\ldots\ldots\ldots\ldots\ldots\ldots.6$$

When this idea is extended to fuzzy sets, the characteristic function is generalized to a membership function that assigns to every X ϵ A a value from the unit internal (0, 1) instead of the two-element set [0, 1]. Here “1” represent elements that are completely in the fuzzy set, ‘‘0” represents the elements that are completely not in f. Subsequently,values between “0” and “1” represent partial inclusion in F. The membership functions of a fuzzy set F are represented by $\mu_{f.}$ μ_f and F are related by the following equations [12]

$$\mu f : x \longrightarrow [0,1]\ldots\ldots\ldots\ldots\ldots\ldots\ldots(7)$$

$$F =\{(x_i\ \mu_f,\ (x)\}|Z\epsilon x \ \text{ and } 0 < \mu_f(x) < i\}$$

$$F=\{(_{xi},\mu_f(x))\}|X\epsilon X\text{and}0\leq\mu_f(x)\leq 1\}\ldots\ldots\ldots\ldots(8)$$

Although, the characteristic function xA(x) in classical set defines a crisp boundary, the membership function μ_f in fuzzy set gives the degree of membership for each element xЄ X.

Fuzzification makes the real input parameters of Bitrate, Entropy and Hurst Exponent as fuzzy sets. In this paper, the fuzzy sets of Bitrate(BRT), Entropy(ENT) and Hurst(HST) parameters are

BRT = {L, M, H}, ENT={L, M, H} and HST= {L, M, H}, where “L” stands for LOW, “M” starts for medium, and “H” for High.

The task of DoS detection was formulated as a pattern classification problem. Here, the observed traffic was classified as normal or attack traffic. In the DoS detection mechanism used in this paper, the incoming traffic was monitored in terms of various features for fuzzy logic decision making, using attack network traces generated at test machines at the border router of computer science department, University of California Los Angeles. The traces used in this paper can be found at the location [11].

Fuzzy linguistic rules can be derived from either expert knowledge or mathematical strategies [10]. However, this paper used the Fuzzy Concept Learning System algorithm (FCLS) to generate the fuzzy rules from a network attack traffic. The fuzzy rules generated using these techniques will be able to provide better classification rates in DoS attacks.

Fuzzy systems have several important characteristics that suit intrusion detection, these include,

- The ability to readily combine inputs from widely varying sources
- The ability to handle intrusion signals which naturally, cannot be crisply defined (e.g at what threshold should an alarm be set?).
- The fact that since the degree of alert that can occur with an intrusion is often fuzzy, the best solution thus must leverage on fuzzy systems.

3.0 NETWORK TRAFFIC PARAMETERS AND THE FUZZY MODEL

This paper considers important network traffic parameters necessary to build a functional fuzzy model for the proposed DoS attack defense system. These traffic features capture both the instant and the longer-term statistical behaviour of the traffic, while avoiding high computational time as well as attendant costs.

The parameters include the following; the Bitrates, also referred to as the Traffic Rate (TR) or Packet rate (PR). This is a measure of the number of packet flows per unit time. It is a very important index in this subject matter, since a very high rate of incoming traffic is by far the most conspicuous indicator of a flooding DoS attack [1].

Usually in traffic rate analysis, there is need to keep track of the packets in the TCP header as well as the total number of TCP packets (Payload) during a specific observation period [2].

The following definitions are important:

$$\text{Rtd}(K_i) = \frac{\text{Total number of a stage (K) in a TCP header}}{\text{Total number of TCP packets (inbound)}}$$

$$\text{Rtd}(K_o) = \frac{\text{Total number of a flag (K) in a TCP header}}{\text{Total number of TCP packets (outbound) (i.e flag rate)}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots..(1)$$

Here, td means the sampling period. In the equation 1, K stands for one of six flags: SIN, FIN, RST, ACK, PSH, and URG flags, denoted as S, F, R, A, P, U, for either inbound (i) or outbound (o) network traffic.

For example, $[R_1A_i]$ represents the ACK flag rate of inbound traffic, when the sampling period is one second.

A protocol rate is also defined by the ratio of the number of TCP, UDP, or ICMP packets to the total number of IP packets as follows:

$$\text{Rtd}(\{\text{TCP}|\text{UDP}|\text{ICMP}\}i) = \frac{\text{Total number of (TCP|UDP|ICMP) packets (Inbound)}}{\text{Total number of IP packet}} \quad \ldots\ldots\ldots\ldots..(2)$$

$$\text{Rtd}(\{\text{TCP}|\text{UDP}|\text{ICMP}\}o) = \frac{\text{Total number (TCP|UDP|ICMP) packets (outbound)}}{\text{Total number of IP packets}}$$

Similarly, for example, $R_2\,[UDP_0]$ stands for the UDP protocol rate of outbound network traffic, assuming the sampling period of two seconds. In terms of byte length:

$$\text{Rtd}\{\text{(TCP byte length)in}\} = \frac{\text{Total number of bytes per packets}}{\text{Total number of IP packets}}$$

Another parameter, the entropy relates to data with a probabilistic description. It is inherently associated with the randomness or uncertainty of information conveyed by the data.

Usually, the entropy contained in normal internet traffic and traffic under DoS attack differ significantly [3]. Entropy can also be used to describe the burstiness of network traffic data [4]. The entropy of the value of the incoming bitrate is computed according to [5] as:

$$E = - \sum f_i \text{ logfi } \log_2 f_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Where f_i is the probability density function obtained from the normalized histogram values for the bitrate. This is expected to yield a higher value when the probability distribution expands over a wider range of values, indicating an increase in uncertainty [6].

- Finally, the Hurst parameter H measures the degree of self-similarity. It has been studied in detail in [7] that the self-similarly properties of normal and attack traffic are distinctively different. Since the Hurst parameter is an indicator of the self similarity of traffic, it is very important in DoS detection; Xiang et al [8]. The (R/S) analysis described in [9] is used to compute the actual value of the Hurst parameter for the incoming bitrate. If x is the bit rate of the incoming traffic, n is the observation time, and N is the total number of observation points. Thus, (R/S) is given by:

$$(R/S)N = \frac{\underset{n-1\leq n\leq N}{\mathrm{Max}} \sum_{n=1} (x - X) - \underset{n-1\leq n\leq N}{\mathrm{min}} \sum_{n=1} (X - X)}{\sqrt{\frac{£\,(x - x)2}{n - 1}}}$$

$$N \qquad \text{..............}(4)$$

The Hurst parameter and $(R/S)_N$ are related by

$(R/S)_N \quad = \quad CN^H,$

$H \quad = \quad \log N(\{R/S\}_N)$………………(5)

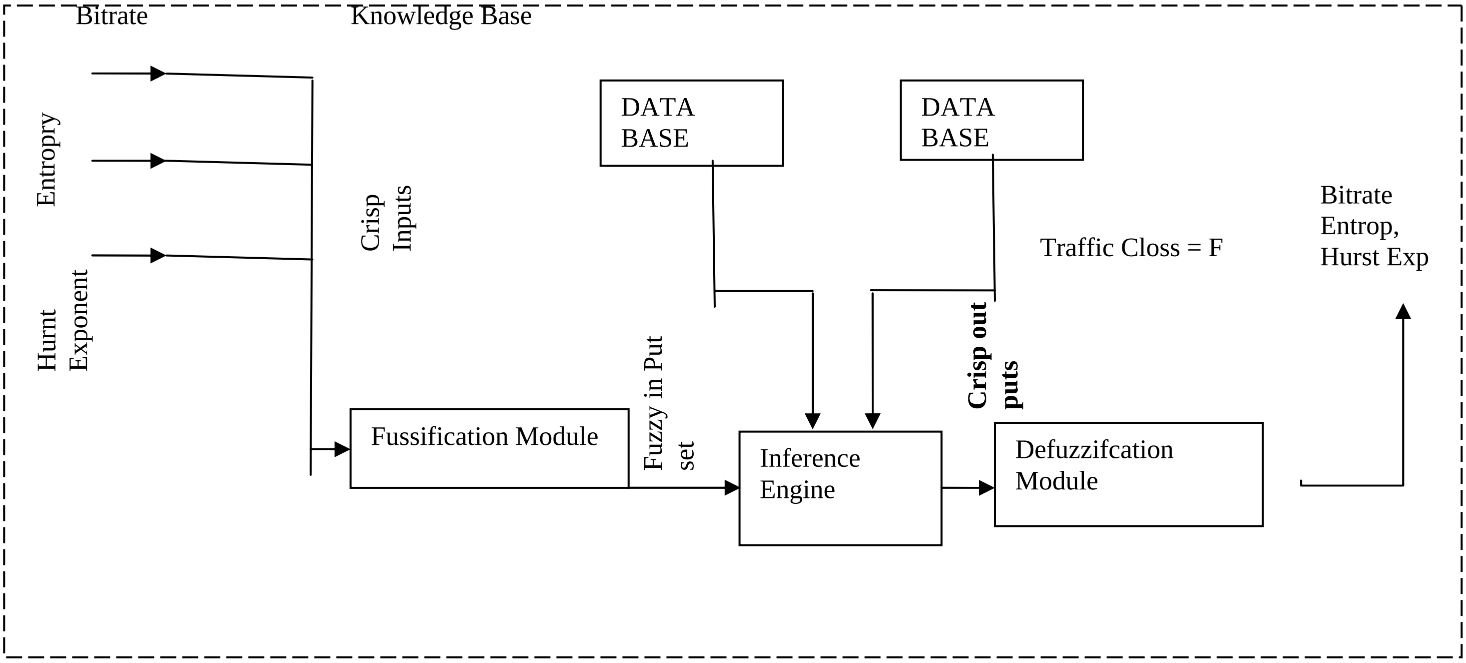


Fig 1.0: The general fuzzy logic block for the DoS attack detection system

4.0 GENERATING THE FUZZY RULES FOR THE SECURITY SYSTEM

There are two common sources of information for building fuzzy models; prior knowledge and data (process measurement). In this paper the fuzzy model is constructed from data.

The data used for generating the fuzzy rules are the university of California Computer Science Department packet traces available at [11].

In building the model, the relationship between these input parameters (Bitrate, Entropy, Hurst parameter) and an output parameter (Traffic class) can be mapped by fuzzy linguistic rules;

Traffic class = f (Bitrate, Entropy, Hurst parameter).

The structure of the proposed fuzzy DoS attack detection model is shown in figure 1.0 below.

The distribution was obtained by network research lab and modified for public use by the laboratory for advanced research. It contains packet traces collected on August 2001 at the border router of computer science department, university of California LOS Angeles. The attack traffic traces were generated by running the attack tool on test machines, attacking another test machine at ULCA computer science department.

The trace is of the format:

Packet-Time IP-from IP-to Port-from Port-to Length flag Seg-form Seg-to ACK WIN

The packet length was used to compute Bitrate, Entropy and the Hurst Exponent. For this work, the trace was partitioned into training data set and testing dataset.

The traffic in the training dataset is further partitioned

Bitrate of the normal and attack trace:

The bitrate is computed from the trace data using the variant of equation (2) i.e

$$\text{Rtd}\ [[\text{TCP byte length}]_{in}] = \frac{\text{total number of byte length}}{\text{Total number of TCP packet}}$$

Entropy:

The entropy of the normal and attack traffic is computed using equation (3): i.e

$$E = -\sum f_i \ \text{logfi} \ \log_2 f_i$$

Hurst Exponent:

The Hurst parameter in the normal and attack traffic is computed using equations (4) and (5) i.e

$$(R/S)N = \frac{\underset{I\le n\le N}{\text{Max}}\sum_{n=1}^{N}(x-x) - \underset{1\le n\le N}{\min}\sum_{n=1}^{N}(x-x)}{\sqrt{\frac{\sum_{n=1}^{N}(x = x)^2}{N}}}$$

$$H = \text{Log}_N \ (R/S)_N)$$

Due to the large volume of data in the ULCA packet trace file [11], five samples of representative records were drawn at random. Each sample consists of 100 consecutive trace entities (records). The Bitrate, entropy, and Hurst parameter for each of the representative five samples are computed using the appropriate formula as presented above.

From the computations the following tabulation was obtained:

Bitrate	Entropy	Hurst Parameter	Traffic – Class
24.97	$7.3058e^{-134}$	0.7857	DOS Attack (A)
14.20	$9.5941e^{-043}$	0.8589	DOS Attack (A)
11.20	$2.1128e^{-026}$	0.6702	DOS Attack (A)
5.33	$5.8996e^{-006}$	0.5264	Normal (N)
3.81	0.0033	0.5318	Normal (N)

Table 2: Data set from analysis of Attack and Normal trade files (UCLA Computer Science Department Packet Traces).

The data set given on table 2 is used to generate the fuzzy decision tree, then from the fuzzy decision tree decision rules that form the knowledge base of the proposed fuzzy Dos defense model knowledge base, was thus generated.

The fuzzy concept learning system (FCLS) algorithmic is used for constructing the fuzzy decision tree from the data set of tables 2, and then fuzzy rules are generated from the construction fuzzy decision tree.

Referring to table 2, the traffic class (attack or normal) is determined by the values of the respective network attributes.

Definition 1 [12]

Let S be a set of attributes that determine attributes Z, S = {X, Y, ……….W}, and let tj(x) denote the value of the attribute x of the jth training instance (i.e., the jth tuple of a relation) in a dataset, then the fuzziness of the attribute x, denoted by FA (x), is defined by

$$FA(x) = \underline{\Sigma(I - N_{\underline{xi}}\,(t,(x)))}\ldots\ldots\ldots\ldots\ldots\ldots\ldots(9)$$

J=i

C

Where c is the number of training instances, Xi is any linguistic term of the attribute X, and μx_i (t_i (x)) indicates the degree of membership that the value of the attribute x of the jth training instances belongs to the linguistic term x_i.

Definition 2, [12]:

Every certainty factor node in the path of a fuzzy decision tree is associated with a certainty factor (CF) value. The certainty factor value CF is defined by

$$CF = \min\{Avg(F_1), Avg\,(F_2), Avg\,(F_3)\}\ \ldots\ldots.\ (10)$$

Where Avg(F_1), Avg (F_2), Avg (F_3) are the average values of the linguistics terms F_1, F_2 and F_3 respectively, and F_1, F_2 and F_3 are in a path

$D_1 \xrightarrow{F_1} D_2 \xrightarrow{F_2} D_3 \xrightarrow{F_3}$(CF) in the tree, and

$$A\,vg\,(Fi) = \frac{\sum_{j=1}\ \mu_{fi}\left((tj\,(Di)\right)}{S}\qquad\ldots\ldots..\ (11)$$

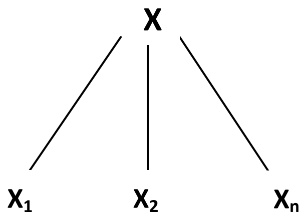
Where tj (Di) represents the value of the attribute D_i of the jth tuple of a relation, S is the number of training instances (i.e., the number of tuples in the relation) in which the value of the attribute D_i is the linguistic term F_i, μ_{fi} (tj (D_1)) indicates the degree of membership that the value of the attribute Di of the j^{th} tuple of a relation belongs to the linguistic term Di and $1 \leq i \leq 3$.

The FCLS Algorithm

Step 1: Fuzzify the relation into fuzzy.

Step 2: Select an attribute among the set S of antecedent attributes that has the smallest FA. Assume attributes X with the smallest FA; then position the set T of the training instances into subsets T_1, T_2…., and Tn according to the fuzzy domain {X_1, X_2……Xn} of the attribute X_i respectively. Compute the average value of Avg (X_i) of X_i based on equation 11, where $1 \leq i \leq n$.

Step 3: Let the attribute X be the decision node, and sprout the tree according to the Fuzzy domain of the attribute X shown as follows:



Where $X_{1,}$ X_2……. Xn are linguistic terms represented by fuzzy sets and the set

{X_i, X_2, …………..Xn) is the fuzzy domain of the attribute X.

Step 4: Let S = S – {X}, where – is the difference operator between sets.

Step 5:

Fuzzification of the trace data set of table 2:

From table 2, it can be seem that the attribute traffic class is determined by the attributes Bitrate, Entropy and Hurt Exponent. In this case

S = {Bitrate, Entropy, Hurst Parameter} and

Z = Traffic class, where the attributes.

Bitrate, Entropy and Hurst Parameter are called antecedent attributes and the attribute Traffic class is called a consequent attribute. From table 2, it can be seen that the values of the attribute Traffic class are Dos attacks and Normal, and the domains of the attribute Bitrate, Entropy and Hurst Parameter are from 3.81 to 24.47, from 7.3058e^{-134} to 0.0033 and from 0.5264 to 0.8589 respectively.

The membership function curves adopted for these parameters are shown below based on their efficacy for control applications [ ] as well as heuristics.

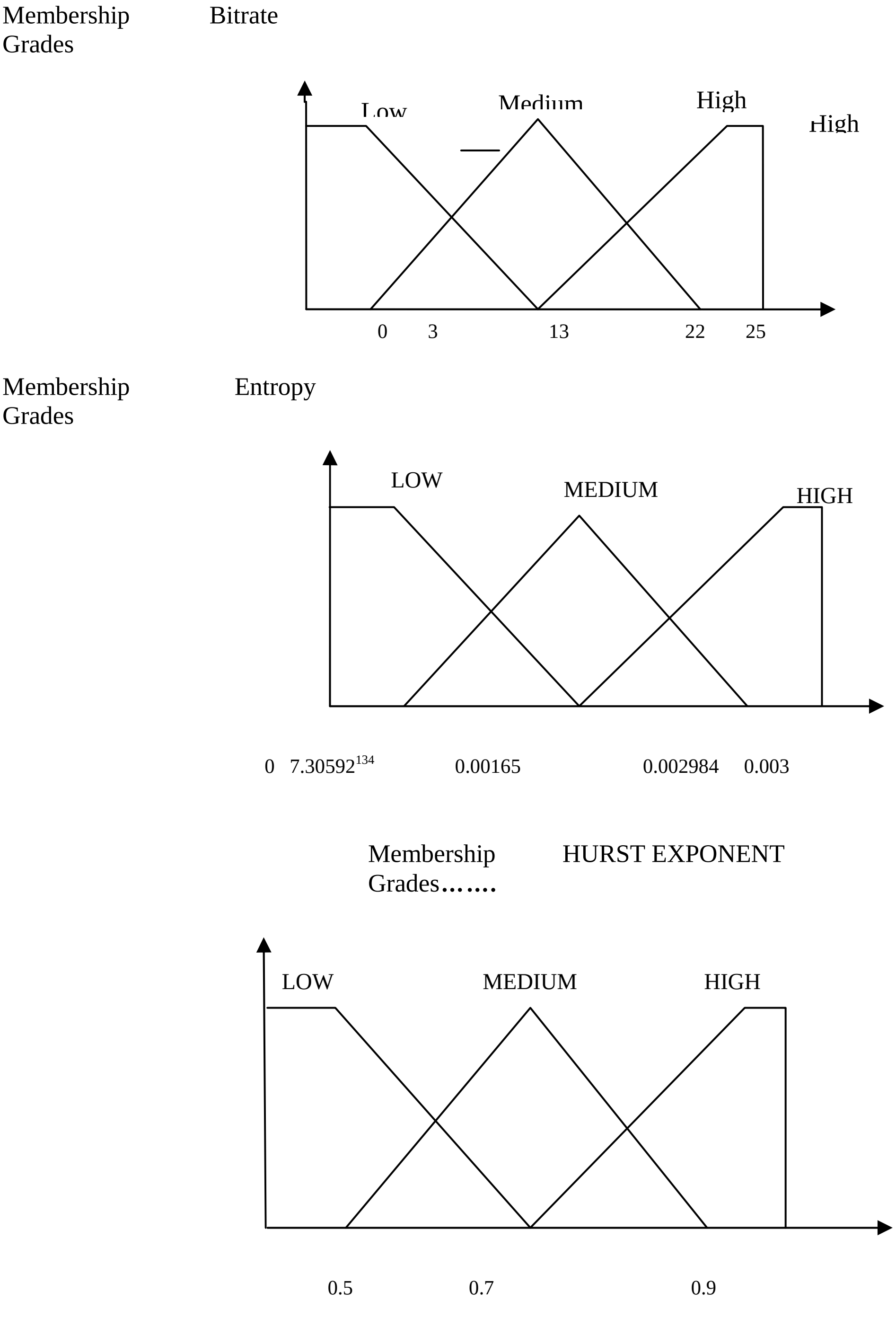


Fig. 3: Membership Function Curves

Step 1:

The result of the fuzzification of the relations in table 2 is the fuzzy relation shown in table 4

BRT	ENT	HST	TC	
{H/0.1}	{L/1.0}	{H/0.75}	{A/1.0}	Attribute TC being infuzzitiable is added as a single fuzzy set i.e its membership value.
{M/0.65}	{L/0.5}	{H/1.0}	{A/10}	
{M/0.75}	{L/0.85}	{M/0.65}	A/1.0}	
{L/0.65}	{M/0.75}	{M/0.85}	{N/1.0}	
{L/0.5}	{H/1.0}	{M/1.0}	{N/1.0}	

Table 4: Fuzzy relation

Where:
BRT = Birate; ENT = Entropy; HST = Hurst Parameter;
TC = Traffic Class; H = High; M = Medium; L = Low
Step 2:
Select an attribute among the set
S = {BRT, ENT, HST} of antecedent Attributes that has the smallest FA (fuzziness)
Based on equation (9), the fuzziness of each attribute in the set
S = {BRT, ENT, HST} is computed as follows:
FA (BRT) = [(1-0.1) + (1-0.65) + (1-0.75) +
(1- 0.65) + (1-0.5)] = 1.45
FA (ENT) = [(1-1) + (1-0.5) + (1-0.85) +
(1 - 0.75) + (1-1)] = 0.9
FA (HST) = [(1-0.75) + (1-1) + (1-0.65) +
(1- 0.85) + (1-1)] = 0.75

The attribute with the smallest FA (Fuzziness) is HST i.e Hurst parameter. Hurst exponent is used as the root to grow the tree. After applying the FCLS algorithm, the fuzzy decision tree is constructed as shown in figure 5.

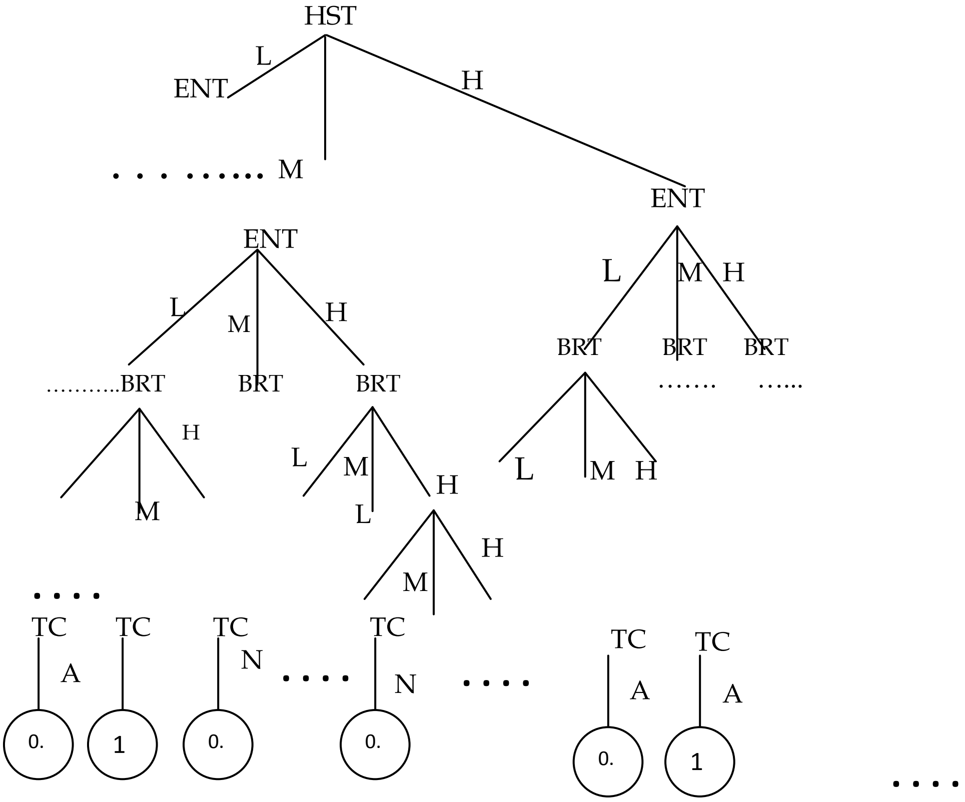


Figure 5: Fuzzy decision tree of table 4.

As shown in figure 5, the fuzzy decision tree constructed from the fuzzy selection table contains null paths. The method for completing fuzzy decision tree null path based on Sudkamp Hammell [ ] is used to complete the null path. It states that for every path in the fuzzy decision tree created by the FCLS algorithm, if there are some null paths, then a hypothetical certainty factor mode is created by each null path. In this case, the path from the root node to a hypothetical certainty factor node forms a virtual fuzzy rule. Applying the method [13], the null path in the fuzzy decision tree is completed. The fuzzy decision tree derived from figure 5 after applying the methods [13] is shown in figure 6.

In order to minimize the error of the degree of belief of the generated virtual rules, the values associated with each hypothetical certainty factor node in figure 6 is equal to 0.5.

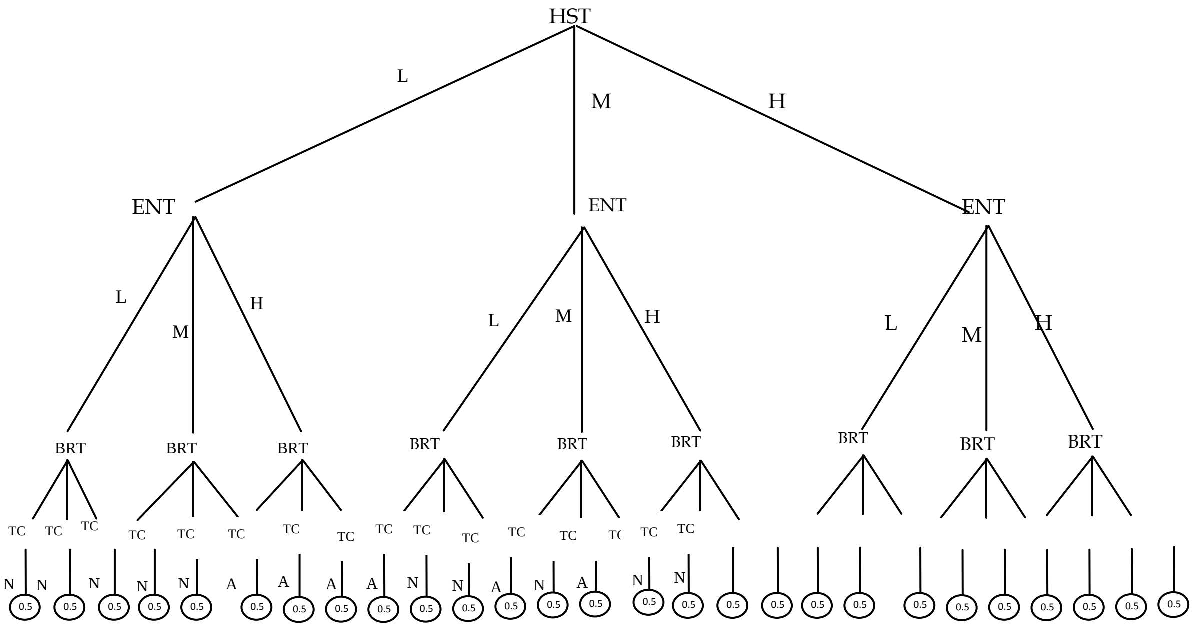


Fig 6 Completed fuzzy decision tree

Consequently, using the necessary schema, the following fuzzy rules are generated.

IF HST is LOW and ENT is LOW and BRT is LOW THEN
TC is Normal (CF = 0.5)

IF HST is LOW and ENT is LOW and BRT is MEDIUM THEN
TC is Normal (CF = 0.5)

IF HST is LOW and ENT is LOW and BRT is HIGH THEN
TC is Normal (CF = 20.5)

IF HST is LOW and ENT is MEDIUM and BRT is LOW THEN
TC is Normal (CF = 20.5)

IF HST is LOW and ENT is LOW and BRT is MEDIUM THEN
TC is Normal (CF = 0.5)

IF HST is LOW and ENT is MEDIUM and BRT is HIGH THEN
TC is Attack

IF HST is LOW and ENT is HIGH and BRT is LOW THEN
TC is Attack

IF HST is LOW and ENT is HIGH and BRT is LOW THEN
TC is Attack

IF HST is LOW and ENT is HIGH and BRT is MEDIUM THEN
TC is Attack

IF HST is LOW and ENT is HIGH and BRT is HIGH THEN
TC is Attack

IF HST is MEDIUM and ENT is LOW and BRT is LOW THEN TC is Normal (Cf = 0.5)

IF HST is MEDIUM and ENT is LOW and BRT is MEDIUM THEN TC is Normal (Cf = 0.83)

IF HST is MEDIUM and ENT is LOW and BRT is HIGH THEN TC is Attack (Cf = 1.0)

IF HST is MEDIUM and ENT is MEDIUM and BRT is MEDIUM THEN TC is Normal (Cf = 0.83)

IF HST is MEDIUM and ENT is MEDIUM AND BRT is MEDIUM THEN TC is Attack (Cf = 0.5)

IF HST is MEDIUM and ENT is MEDIUM and BRT is HIGH THEN TC is Normal (Cf = 0.5)

IF HST is MEDIUM and ENT is HIGH and BRT is LOW THEN TC is Normal (Cf = 0.75)

IF HST is MEDIUM and ENT is HIGH and BRT is MEDIUM THEN TC is Attack (Cf = 0.5)

IF HST is MEDIUM and ENT is HIGH and BRT is HIGH THEN TC is Attack (Cf = 20.5)

IF HST is HIGH and ENT is LOW and BRT is LOW THEN TC is Normal (Cf = 0.5)

IF HST is HIGH and ENT is LOW and BRT is MEDIUM THEN TC is Attack (Cf = 0.83)

IF HST is HIGH and ENT is LOW and BRT is HIGH THEN TC is Attack (Cf = 1.0)

IF HST is HIGH and ENT is MEDIUM and BRT is LOW THEN TC is Normal (Cf = 0.5)

IF HST is HIGH and ENT is MEDIUM and BRT is MEDIUM THEN TC is Attack (Cf = 0.5)

IF HST is HIGH and ENT is MEDIUM and BRT is HIGH THEN TC is Attack (Cf = 0.5)

IF HST is HIGH and ENT is MEDIUM and BRT is HIGH THEN TC is Attack (Cf = 0.5)

IF HST is HIGH and ENT is HIGH and BRT is LOW THEN TC is Attack (Cf = 0.5)

IF HST is HIGH and ENT is HIGH and BRT is MEDIUM THEN TC is Attack (Cf = 0.5)

IF HST is HIGH and ENT is HIGH and BRT is HIGH THEN TC is Attack (Cf = 0.5)

Predicted Class			
Positive Class		Negative Class	
Actual Class	Positive class	True positive (TP)	False Negative (FN)
	Negative class	False positive (FP)	True Negative (TN)

5.0 Simulation and Performance Analysis

The proposed fuzzy security model is simulated using MATLAB and the performance of the system is evaluated using precision, recall and F-measure. For the evaluation of the model the network traffic and testing, the training dataset contains normal facts as well as DOS attack traffic. The testing dataset is given to the proposed system, which classifies the input as a normal or attack using the Fuzzy inference rule generated in the last section. The obtained result is then used to compute overall accuracy of the Fuzzy system. The overall accuracy of the fuzzy model is computed based on the definitions, namely; precision, recall and F-measures which are normally used to estimate the rare class prediction. It is advantageous to accomplish a high recall devoid of loss of precision.

F – measure is a weighted harmonic mean which evaluates the trade off between them.

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F – Measure} = \frac{(\beta^2+1 \text{ Precision . Recall})}{B^2. \text{ Precision + Recall}}$$

where, β = 1

$$\text{Overall accuracy} = \frac{TP + TN}{TP + TN + FN + FP}$$

Where TP = True positive is defined as the proportion of positive cases that were classified correctly.

TN = True negative is refined as the proportion of negative cases that were classified correctly.

FN = False Negative. The false negative rate (FN) is the proportion of positive cases that were incorrectly classified as negative.

FP = False positive. The false positive rate (FP) is the proportion of negative cases that were incorrectly classified as positive.

These metrics are computed using the confusion matrix in table 7 and defined as follows

Table 7: Confusion Matrix X

The training dataset as given on table 2 was used to develop the fuzzy model. This dataset is an extract from the case study track file (II). The testing dataset extracted from the trace file is given to the fuzzy system. The evaluation metrics are computed for both result and testing dataset in the testing and the retained result for both attack and normal data are given in table 8 which is the overall classification performance of the constructed fuzzy system on the VLCA computer science department network traffic (Dos attack traffic and normal traffic). By analyzing the result, the overall performance of the proposed system achieves more than 80% accuracy for the DOS attacks.

Proposed Fussy System

	Metric	Training	Testing
Dos attack	Accuracy	0.9478	0.9498269
	Recall	0.90144	0.904154
	F – measure	0.9452 26236	0.94687236
	Precision	0.51948	0.051858
Normal	Recall	0.99416	0.9876385
	F-measure	0.90376539	0.906838129
	Accuracy	0.920852	0.903019

Table 8: The classification performance of the proposed fuzzy DoS sentence model.

CONCLUSION

This paper proposed a fuzzy model for deleting own counteracting denial of service attack within a negative based on network traffic characteristics (Bitrate, Hurt exponent, and Entropy). The fizzy inference approach was used to develop a model for classifying network traffic based on traffic technique. Fuzzy modeling (i.e fuzzy learning strategy) is an effective technique for handling complex and uncertain situation such as the attack scenarios within computer networks. The fuzzy concept learning algorithm was used for constructing the fuzzy decision tree using dataset from the University of California Los Angeles Computer Science department trade files available at [11]. Fuzzy rules were generated from the constructed fuzzy decision tree. Another dataset from the case study trade file was used for evaluating the performance of the proposed fuzzy model and paralysis of the MATLAB simulation result (using confusion matrix) showed that the proposed fuzzy technique is effective in detecting and contracting DOS attacks in computer networks.

REFERENCES

[1] M.Kim, H.Na, K.Chae, H. Bang, and J.Na" "A combined Data Mining Approach for DDOS Attack Detection", Lecture Notes in Computer Scienc, Vol. 3090, Pp. 943-950, 2004.

[2] Cheolho Lee, Sanguk Noh, Kyunghee doi,Gshyun Jung "Characterizing DDOS attack with traffic rate analysis". IADIS International conference e-society 2003.

[3] Feinstein L., Schnackenbag D., Balupari R.and Kindod D., (2003) statistical Approaches to DDOS attack detection and response. Processings of the DARPA information Surrivability Conference and Exposition (DISCEX'03).

[4] Menashi Wang, Terra Madhyastta, Ngai Hang Chem, Spiros Papafimition, Christos Faloutsos "Data mining meets performance Evaluation" fast Algorithms for modeling Bursty Traffic" 18th International Conference on Data Engineering, 2002.

[5] Gelenbe E; Gellmam M. and Zoukas G. (2005) An autonomic approach to denial of service defense. In proceedings of the IEEE International Symposium on a world of wireless, mobile and multimedia Networks, Pp. 537 – 541.

[6] Gulay Oke and Georgios Zoukas "Distributed Defense against Denial of service attacks: A practical view". BCS International Academic Conference 2008 – Visions of Computer Science.

[7] Lim. (2006) Change Trend of Average Hurst Parameter of Traffic under DDOS flood attacks computers and security 25, Pp. 213 – 220.

[8] Xiang Y., Lin., Lei W.L. and Huang S.J. (2004) Detecting DDOS attack based on Network Self. Similarity. IEE Proceedings in Communication, 151, PP. 292 – 295.

[9] Cajuerio D.O. and Tabak B.M. (2004) The Hurst Exponent Over Time: Testing the Assertion that Emerging Markets Are Becoming more Efficient. Physical A, 336, PP. 521 – 537.

[10] Mamdani EH. Procky TJ, A Linguistics Self – Organizing Process Controller, Auromatica.

[11] VCLA CSD packet traces: http.//www.lasr.cs.vcla. Edu/ddos/tracks.

[12] Shyi-Ming Chen, Ming – Shiow Yeh “Generating Fuzzy rules from relectional database systems for estimating null values” cyberretics and systems: An International Journal, 28: 695 – 723, 1997.

[13] Shyi-Ming Chen, Ming – Shiow Yeh “Generating Fuzzy rules from relectional database systems for estimating null values”.

[14] C. Douligeris and A. Mitrokotsa. ‘DDOS attacks and defense mechanisms: Classification and state-of-the-art. Computer networks, 44 (5): 643 – 666 2004.

[15] Patcha and J.M. Park. “An overview of anomaly detection technologies: existing solutions and latest technologies trends.” Computer networks, (12): 3448 – 3470, 2007.

[16] P. Garcia – Teodoro, J. Diaz – Verde Jo and G. Kucia” Fernantez. “Anomaly based network intrusion detection: techniques, syst4ems and challenges.” Computers and security, 28 (1-2): 18-28, 2009.

[17] W.E. Leland, M.S. Taggu and W. Willinger. On the self – similar nature of Ethernet traffic (extended vasion) IEEE/Achi transactions on networking, 1994.

[18] M.Li. Change “trend of averaged Hurt parameter traffic under DDOS flood attacks” Computers of security, 25 (3): 213 – 220, 2006.

[19] M. Arima, E.H. Hera, J.S Katzberg, “A fuzzy logic and rough sets controller for HVAC systems”, proceedings of the IEEE WESCANEX, New York 1995.

[20] O. Cordon, F. Herrera, A Peregrin, “Applicability of the Fuzzy operators in the design of Fuzzy logic controller”, Fuzzy sets and systems, 1997.

[21] P.Y. Glorennes, ‘Application of fuzzy control for building energy management. In: Building Simulation”, International Building Performance simulation Association I, Sophia Antipolis, France, 1991.

[22] S.X. WU and W. Banzhat. “The use of computational intelligent in intrusion detection systems”. A review. Applied soft computing 10:1-35, 2010”.

[23] A Bardossy, L., Duckstein, “Fuzzy rule – based modeling with applications to geo-physical” biological and engineering systems”, CRC Press, 1995.

[24] J.C. Bezdek, S.K. Pal., “Fuzzy models for pattern Recognition, method that search for structures in Data” IEEE Press, Boca Ration 1992.

[25] Y. Jin, “Fuzzy modeling of High – Fimensional Systems: Complexity Reductions and Interpretability Improvement” IEEE Trans on Fuzzy Systems, 2000.

[26] Jui, Y., Von Section, W., and Sandhoft, B:: “on Generating FCZ Fuzzy Rules Systes from Dels using Evolution Strategies”, IEE Trans, on systems, man and Cybernetics – part B: Cybernetics 29 (1999).

[27] http://www.lpa.co.uk/fln.htm?gclid=CL60pZzG7J8CFdx05Qod8R-ydg

AUTHORS PROFILE

Engr. (Mrs) Ogechi Ihekweaba is a lecturer in the Department of Computer Engineering, Michael Okpara University Of Agriculture, Umudike, Abia State, Nigeria.

She is an ex student of Ido-Ani secondary School, Ondo State. Holds a Bachelor’s degree (B.Eng) in Computer Science & Engineering, a Master’s degree (M.Eng) in Computer Science & Engineering and she is at the verge of completing a Doctorate degree (PhD) in Computer Engineering.

Her area of specialization is Network Security and Computational Intelligence. She served as an Engineer with a Telecommunication outfit, CSAT COM Ltd. As a lecturer, she headed the Computer Science Department of OSISATECH. She is currently the SIWES and Seminar Coordinator for the Department of Computer Engineering, Michael Okpara University of Agriculture, Umudike.

She had several publications, and is a member of professional bodies which include: Nigeria Computer Society (NCS), Computer Professionals of Nigeria (CPN), Nigeria Society of Engineers (NSE). She is also a COREN registered Engineer.