Marek Bogusław ALEKSANDER [1], Volodymyr KARPINSKYI, Yuriy KHLAPONIN, Oleksandr YUDIN
[1] STATE HIGHER VOCATIONAL SCHOOL IN NOWY SACZ, INSTITUTE OF ENGINEERING
1 Zamenhofa St., 33-300 Nowy Sacz Pl

Organization of security control of wireless telecommunication network based on fuzzy networks

Abstract

The problem solution of security control of wireless computer network nodes, which is based on the use of the apparatus of fuzzy sets is presented in this article. The approach used in the paper aims to an automation that will improve the efficiency of control of the nodes and operations of a network administrator. The approach allows forming a system of security control of the wireless computer network based on neuro-fuzzy (hybrid) network, which is characterized by high adaptability, ease use, the ability to identify better the sequence of the analysis of vulnerabilities in the wireless computer network nodes. The feature of the proposed approach takes the dynamic nature of the wireless computer network into account.

Keywords: linguistic variable, neuro-fuzzy network, neural network, wireless network.

1. Introduction

The basic element of fuzzy inference procedures is a base of fuzzy rules owing to which knowledge of experts about specificity of functioning of a given object (a system) is provided in a form of linguistic utterances: if <inputs>, so <outputs>. A possibility of such interpretation of expert information is an undoubted advantage of the fuzzy logic [1]. However, in the fuzzy logic instrument there are no mechanisms of training. For this reason the fuzzy inference results depend strongly on a type of the membership function by which formalization of fuzzy terms (values) is made. Furthermore, the initial set of the fuzzy rules formulated by the experts can turn out to be incomplete and contradictory.

Ability to learn is the main feature of the neural networks. It is accomplished by specially designed algorithms, for example an algorithm of regressive propagation of an error. There is no need for a priori information about a structure of the required functional relationship to train a neural network. The only need is a training set in a form of pairs <input - output>. However, this is due to the fact that the trained neural network - a weighed oriented graph – does not yield the content interpretation [2]. The neural network – a graph (a spline function) is a result of training. An advantage of the models built on the network base constitutes a possibility of obtaining new information about a problem area in a form of a prognosis. A disadvantage of the neural networks is a presentation of knowledge about the problem area in a special form which differs significantly from possible interpretation of the content of the existing mutual relationships and links.

The neural networks and fuzzy logic are different mathematical constructions, and joining them provides a possibility of obtaining completely new quality. The neuro-fuzzy networks or hybrid networks in concept of the programmers creating them combine advantages of the neural networks and fuzzy inference systems in themselves. The neural network obtained in such a way has two basic properties. First, it enables to develop and present system models in a form of fuzzy rules which are characterized by visualization and simplicity of content interpretation. Second, the methods of the neural networks, which make training realization in the real time scale possible, are used to form the fuzzy rules [3].

2. Formulating of the problem

In paper [4] the solution of the task of organization of security control of computer wireless network nodes on basis of fuzzy logic is considered. This approach is based on automation of security control, providing an increase in its effectiveness, and owing to it an improvement of operational efficiency of a administrator computer network. However, performed experiments indicated that the base of the fuzzy rules obtained earlier should be adapted more precisely. In the introductory part of the paper it is pointed out that this task can be solved by use of the neuro-fuzzy networks.

3. Main part

The fuzzy base of knowledge about the system of the security control of the computer wireless network nodes based on the fuzzy logic includes 25 rules obtained owing to combination of terms of two linguistic input variables: T1 - "node autonomy" i T2 - "connection quality". Each linguistic variable is described by five linguistic terms (linguistic values): $T1$ = {«very low», «low», «average», «high», «very high»}; $T2$ = {«very weak», «weak», «average», «good», «very good»}. The linguistic output variable "node importance" is described by a set of terms $T3$ = {«very low», «low», «average», «high», «very high»}.

Additional work performed with participation of experts showed that it was better to assign the linguistic input variables in the same quantitative scales which characterize node autonomy or connection quality in the range of 1..100%. Moreover, the performed experiments indicated that changes in certain rules in the knowledge base should be made. For example, the nodes placed in so called "the risk zone" which is characterized by high probability of turning off equipment due to a low level of battery charging are important for a system in terms of providing the maximum control for the wireless network nodes. For such nodes the value of the second input variable - connection quality – should be considered: the higher connection quality, the quicker analysis of the wireless node security can be made, because a rate of information exchange will be higher in this case. The fuzzy base of knowledge mentioned including the factors given above is presented in Table 1.

Tab. 1. Rules of the fuzzy base of knowledge

No.	**Very low**	**Low**	**Average**	**High**	**Very high**
Very weak	**low**	**low**	**very low**	**very low**	**very low**
Weak	**average**	**average**	**low**	**low**	**very low**
Average	**high**	**high**	**average**	**low**	**very low**
Good	**very high**	**high**	**high**	**average**	**low**
Very good	**very high**	**very high**	**high**	**average**	**low**

Modelling the neuro-fuzzy networks was made in the Matlab mathematical packaging environment. The neuro-fuzzy (hybrid) network of the Matlab package is an adaptive system of neuro-fuzzy inference (Adaptive-Network-Based Fuzzy Inference System, ANFIS). The hybrid constitutes a multilayer neural network without feedback in which ordinary (non-fuzzy) signals, weights and activation functions are used. The fundamental idea, underlying the model of the hybrid networks is use the existing data set to establish parameters of the membership function which fits best to the particular system of fuzzy inference. For finding the parameters of the membership function the known procedures of training of the neural networks are used.

On the one hand, the ANFIS hybrid network is a neural network with one output and a few inputs being fuzzy linguistic variables. The terms of input linguistic variables are described by the standard membership functions, whereas the terms of the output variable are presented by linear or constant membership function. On the other hand, the ANFIS hybrid network is a fuzzy inference system of the Sugeno type [1].

Training the neural network to communicate what is required from it, so the following facts should be considered while selecting data for training the neural network [5]:

- while solving real tasks by the neural network it is often difficult to determine a relationship of the output indicator with data held, therefore the greatest amount of data should be collected;
- presence of correlations between data does not allow performing their classification, therefore a simple rejection algorithm according to a degree of importance cannot be used;
- in order to lower a share of the „very big size” factor a certain number of variables is frequently removed; however, there is a risk of removing ones which transfer important information.

Since there is no experimental data needed to train the neural networks, a task appeared to develop an approach enabling to obtain such a set of data. A set of the data for training and testing the neural networks was generated by a program on basis of a developed simplified mathematical model, based on the following assumptions pertaining to the values of wireless node importance depending on a value of its autonomy and quality of connections. (Fig. 1).

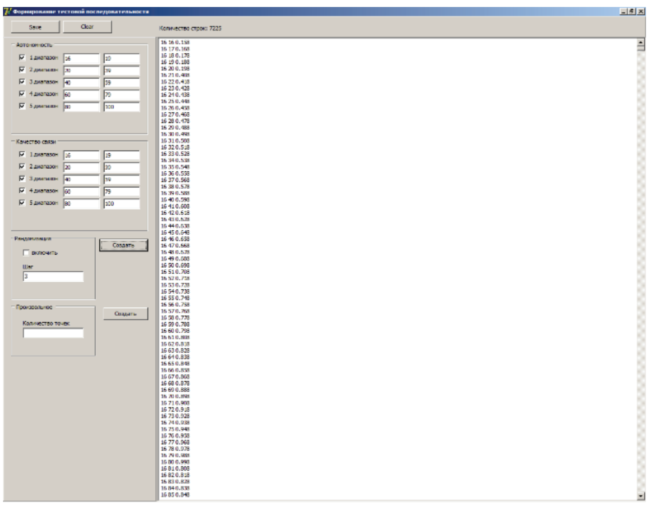


Fig. 1. The program for creating sets of data for training and testing the neuro-fuzzy network

Node importance can take values in the range from 0 to 1. Since the „node importance” linguistic variable is presented by five terms, it can safely be made that numerical values of importance for each term are in the range from 0 to 0.2. Thus, the input variables change in the range from 1 to 100.

Therefore, for two input variables we obtain 10000 possible combinations. Each linguistic variable is also presented by five terms. Thus, within the scale limits for one term the numerical values change in a range from 1 to 20. For two variables we obtain 400 values. As it has been mentioned above, importance within one term can take values from 0 to 0.2. In such a way we obtain the matrix of 20×20, which values differ about 0.0005 horizontally, and about 0.01 vertically. Then, a set of data for training the neuro-fuzzy network can be made and for it the numerical values of importance will be calculated according to the formula:

$$V=0.01\cdot(QC-1)+AV\cdot 5\mathrm{E}-4, \qquad (1)$$

where: V - importance, QC – connection quality, AV – node autonomy.

The numerical values of importance obtained on basis of calculating according to formula (1) should be compared with the minimal values of importance for the first term of the output variable (Tab. 2).

Tab. 2. Rules of the fuzzy based on knowledge

No.	Range	Minimal numerical values of importance
1	0 – 0.2	0
2	0.21 – 0.4	0.2
3	0.41 – 0.6	0.4
4	0.61 – 0.8	0.6
5	0.81 - 1	0.8

Let us consider the following example: Let us assume that AV = 39, QC = 40. According to formula (1) we find V = 0.1955. According to the set values of the input variables it can be said that autonomy is "low", and connection quality - "weak". On basis of Tab. 1 we find the value of node importance - „average”. The minimal numerical value of importance in this case is 0.4. The final result of the numerical value of the node importance for the set values AV QC, V = 0.4 + 0.1995 = 0.5955.

An evaluation of quality of the developed mathematical model of fuzzy inference system according to formula 1 was made by the regression analysis. According to the analysis results quality of the developed model is relatively high: a value of the coefficient of determination exceeds 0.8 and is $R2$ = 0.87694. Thus, 87.6% of the calculated parameters of the model explains relationships and changes of the parameters which are trained among the factors in question.

Let us consider one more condition which has a significant influence on forming a test and training sequence. An analysis of information obtained from the experts showed that wireless equipment at charging a battery below 14% went almost entirely to the automatic operating mode.

Apart from it, if connection quality is estimated as lower than 15%, time needed to analyze the node safety lengthens strongly because of bad quality of connection. Taking the above factors into account a range of the input variable changes while forming the test and training sequence was corrected and set from 16 to 100.

For effective training the modern neural networks require training data sets of a big size, because quality of network training depends on a set size. For this reason, for purposes of the neuro-fuzzy network training a set of training data of a size of 5202 lines was created and it includes over 70% of all possible values. The text data set consisted of 2023 lines, that are comprised almost 30% of the values. The data sets were created by the following algorithm. An area of possible values of the output variables was divided into 400 squares of a side of 5 units. Therefore, each square includes 25 values. Among those 25 values, 18 units were selected at random to the training sequence, 7 – to the test sequence. The membership functions of the input variables of the fuzzy inference system were presented by the Gauss functions (Fig. 2).

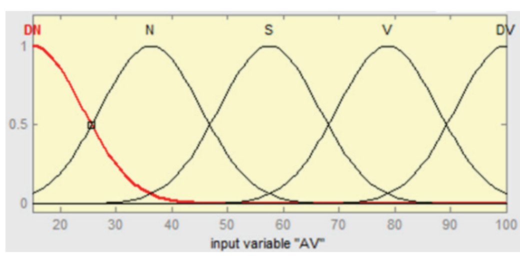


Fig. 2. The membership functions of the terms of the «node autonomy» linguistic variable

Neuro-fuzzy Network training was within 8000 cycles. A training error at such a number of the cycles for the given sequence was slightly less than 2% (Fig. 3). From the training error diagram it results that real training was completed after 6500 cycles – the error ceased to change.

The training set was rigorously sequential. It is possible that if the data were selected randomly, other values of the errors and training cycles would be obtained.

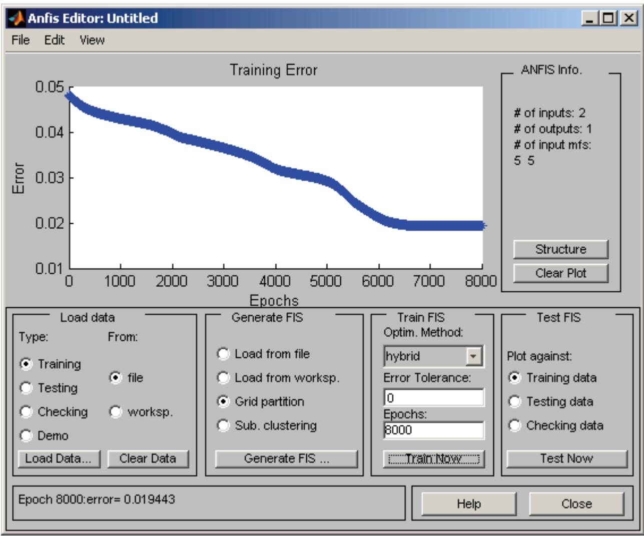


Fig. 3. The error on basis of the neuro-fuzzy network training

The diagrams of the membership functions for the „autonomy" and „connection quality" input variables after completing the neuro-fuzzy network training are presented in Figs 4 and 5, respectively. An external appearance of the membership function were changed greatly, especially for the "node autonomy" input variable.

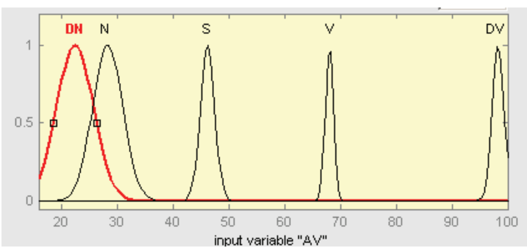


Fig. 4. The membership functions of the terms of the «node autonomy» linguistic variable after completing the neuro-fuzzy network training

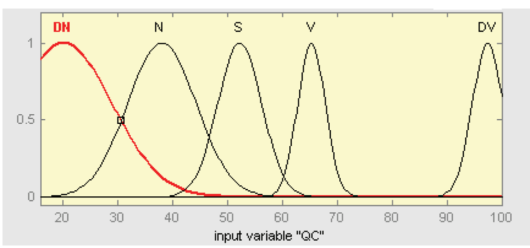


Fig. 5. The membership functions of the terms of the «connection quality» linguistic variable after completing the neuro-fuzzy network training

Verifying operating results of the neuro-fuzzy network after completing training by the test sequence are presented in Fig. 6. The verifying results give practically complete compliance of the test and computation data. The average error value is within 2%.

An error evaluation of the model which is characterized by an absolute value of scatter of a component resultant model is made according to formula [6]:

$$E=\sqrt{\frac{\sum_{i=1}^{n}(y_i-y_{pi})^2}{n-k}}\,, \tag{2}$$

where: n – a sample volume (a set), k – a number of factors.

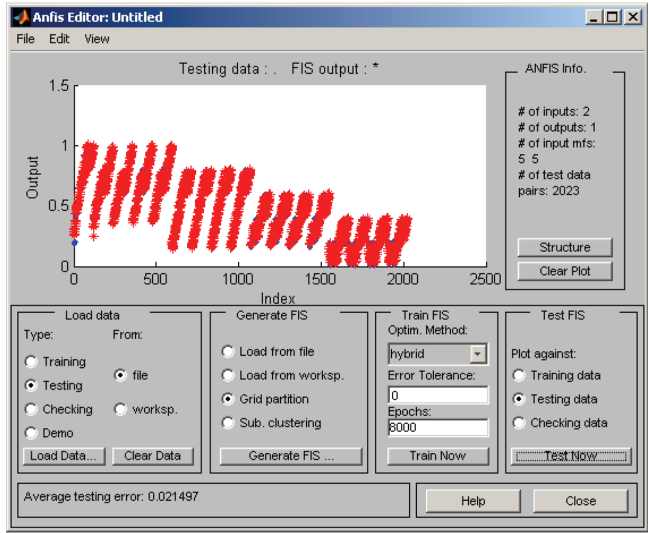


Fig. 6. Verifying operating of the neuro-fuzzy network trained by the test sequence

Values y_i and y_{pi} are obtained in the following way: y_i is a result of program operating for 7225 pairs of the input variables, y_{pi} - a result of operating of the trained neuro-fuzzy module for the same pairs of the input variables. As a result of the computations a relatively low error value is obtained:

$$E=0.022446.$$

The obtained error value can be expressed as a percentage by use of the following formula:

$$E\%=\frac{E}{y_C}\cdot 100(\%)\,. \tag{3}$$

After substituting appropriate numerical values into formula (3) The following error value expressed as a percentage is obtained:

$$E\%=\frac{0.022446}{0.461622}\cdot 100(\%)=4.86\%\,. \tag{4}$$

4. Conclusions

A further development of the method of organization of security control of wireless computer network was obtained by use of the neuro-fuzzy (hybrid) network as a basis for creating the fuzzy inference module. Additional works with participation of experts and hybrid network training made enabled to on the one hand to improve significantly the fuzzy knowledge base, and on the other hand - to improve appearance of the membership functions of the terms of the input linguistic variables. Lack of experimental data needed for the hybrid network to train, caused a mathematical model of the fuzzy inference system had to be developed and on its basis – to develop a special program. The regressive analysis made showed that quality of the developed model was relatively high: determination coefficient $R2$=0.87694. Verifying the hybrid network trained by the test sequence showed that the testing error was also small and was slightly above 2%. The error characterizing scatter of parameters of the component and resultant model turned out to be insignificant.

Owing to it, the approach in question allows creating a system of organization of security control of a wireless computer network on basis of the neuro-fuzzy (hybrid) network, which is characterized by adaptability, easiness of use and the ability to better identify the sequence of the analysis of vulnerabilities in the wireless computer network nodes.

5. References

[1] Ross T.J.: Fuzzy Logic with Engineering Applications, 3rd Edition, Fabulous Printers Pte Ltd, Singapore, 2010.

[2] Rashid T.: Make Your Own Neural Network, CreateSpace Independent Publishing Platform, 2016.

[3] Chesney W.: Fuzzy Logic , Neural Network & Genetic Algorithms Handbook : Theory , Programming & Applications, Auris Reference, London, 2012..

[4] Yudin O., Khlaponin Y.: Kontrol zachyszczennosti bezdrotowych kompiuternych merezh. Nauka i technika Powitrjanych Zbrojnych Sył Ukrainy, no 2(19), pp. 92-96, 2015, (in Ukrainian).

[5] Minh N.D.: THE Effects of Training Data in the Learning Process of Adaptive Neural Fuzzy Networks for Solving the Problem of Classification of Details: http://research-journal.org/technical/ vliyanie -obuchayushhix-vyborok-na-process-obucheniya-adaptivnyx-nejro-nechetkix-setej-dlya-resheniya-zadachi-klassifikacij-detalej, 10.09.2016.

[6] Draper N.R., Smith H.: Applied Regression Analysis, Third Edition, Wiley, 2014.

Received: 07.07.2016 Paper reviewed Accepted: 01.09.2016

Marek Bogusław ALEKSANDER, PhD, eng.

Education: AGH University of Science and Technology in 2000 & Military University of Technology in 2004 & National Aviation University of Kyiv in 2016. Research interests: cryptology, mathematic modeling, wireless network security, electronics. Current position & Functions: docent of Institute of Engineering of State Higher Vocational School in Nowy Sacz. Publications: author and co-author of over 70 publications.

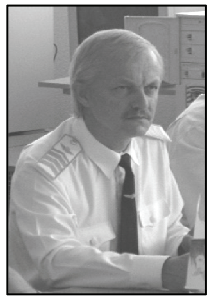
e-mail: aleksandermarek4@gmail.com

Volodymyr KARPINSKYI, PhD, eng.

Received the MSc degree in computer systems and networks in 2008, and the PhD degree in computer science from the Ternopil Technical University, Ukraine, and the West Pomeranian University of Technology Szczecin, Poland, in 2012 and 2013, respectively. He is a graduated project researcher at the TechnoCentre of Coventry University, UK. In the years 2009-2013 he has worked in the Evatronix, Bielsko-Biala, Poland. His research interests are in the area of computer systems and wireless networks.

e-mail: vkarpinskyi@gmail.com

Yuriy KHLAPONIN, PhD, eng.



Received the PhD in 1995 at the Kiev Military Institute of Management and Communications, and doctor of technical sciences in 2016 at the National Aviation University specialty telecommunication systems and networks. Research interests: information security, information security. Publications: over 70 scientific publications, including scientific articles, patents for inventions.

e-mail: yfcnz0408@ukr.net

Oleksandr YUDIN, PhD, eng.

Received the PhD in 1995 at the Kiev Military Institute of Management and Communications. Publications: over 40 scientific publications. He is working at the Poltava University of Economics and Trade. His research interests are in the area of computer systems and wireless networks., information security.

e-mail: izdo.judin@gmail.com