8th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS
Suceava, Romania, May 25 – 27, 2006

ADAPTIVE NETWORKS SAFETY CONTROL ON FUZZY LOGIC

Vadim MUKHIN[1], Elena PAVLENKO[2]
National Technical University of Ukraine "Kiev Polytechnic Institute"
Pr. Pobedy.37, 03056, Kiev, Ukraine
[1]mukhin@comsys.ntu-kpi.kiev.ua

Abstract. *In this paper we suggest a new approach to design of the adaptive network safety control mechanisms. This approach is based on the fuzzy logic theory and allows to formalize both quantitative and qualitative parameters of the network safety system. Also it is suggested an algorithm for design of the model for the adaptive network safety control mechanism with safety functional requirements formalization on the fuzzy logic.*
Keywords: *network, adaptive safety control, security level, fuzzy logic.*

Introduction

The modern computer networks are rather complex systems with the next main components: the hardware units, the communication links, the network software and the special supporting software tools. The development of the network technologies is cause that the reliability and the safety of network resources become more and more important, especially for the networks where are processing, accumulating, transferring and storing the data that must be secured. Nowadays, there is a set of new arising problems for the network safety assurance, that should be solved immediately.

The network security mechanisms require the additional hardware/software resources and, consequently, they take additional time for the information processing in network. [1] Thus, the increasing of the network security level causes the volume increasing of service data, transmitted and processed in the networks, so the network performance on the user's information processing will decrease. On the other hand, generally there is no necessity to provide the network safety on the maximum level constantly. In those periods of time, when the network processes the less important data, it is quite possible to lower the network security level, that will result in decreasing of the service information volume and will increase the network performance on the user's data processing. Thus, the optimal way is to use the special mechanism for the network safety control, which will be adaptively determine the required network security level for the certain period, and will increase the efficiency of the network functioning. So, the safety control in the modern computer networks requires an adjustable security mechanism that runs in a real-time mode. Such mechanism is adaptive control of the network safety, that is based on the adaptive changing of the network security level.

The modern mechanisms for the adaptive network safety control

The realization of the adaptive network safety control concept is based on the adaptive control means that contain the following components: tools for the security level analysis; tools for the attacks detection; tools for the adaptation; control tools.

The tools for the security level analysis realize an evaluation of the required security level according to the importance of the data that are processing in this period.

The tools for the attacks detection perform the revealing of the suspicious actions in the computer networks.

The adaptation tools determine the required networks security level for the certain period depending on the processing information importance.

The control tools coordinate the functioning of all components of the adaptive safety control system for the computer network.

Thus, the adaptive control system is complex control mechanism that ensures the required security level depending on the processing information importance in the real-time mode.

The approaches to the adaptive network safety control mechanisms design

At the present time, there are two main approaches to design of the adaptive network safety control: [2]
1. mechanisms that based on patterns model;
2. mechanisms that based on the identifier.

We suggest to realize the adaptive safety control mechanism on the patterns model approach, and as patterns model there are the safety profiles, i.e. parameters of the network safety configuration.
The adaptive network safety control system forms the safety profiles records on the experimental data about the network security tools. [3, 4]
The structure of the adaptive network safety control system with the safety profiles records is shown on fig. 1.

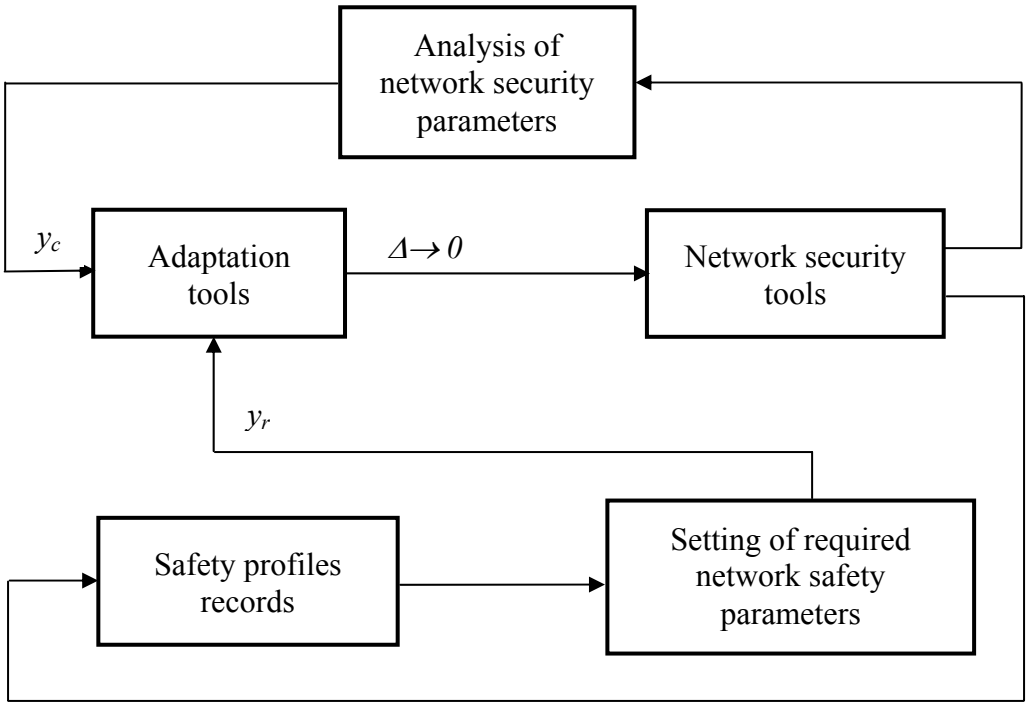

Figure 1. The adaptive network safety control system with the safety profiles records.

Let us consider the specifics of this system functioning. When the network safety parameters are constant, there is no error of regulation: $\Delta = y_c - y_r = 0$, and the adaptation mechanism is in a sleeping mode. If the network safety parameters are changed (as reaction to variation of the security level of the processing information), there is an error of regulation: $\Delta = y_c - y_r \neq 0$, the adaptation mechanism is launched and the parameters of network security system are changed to the required values. So the goal of the adaptation mechanism is to reduce the error of regulation to zero ($\Delta \rightarrow 0$).

The safety profiles records

As it was mentioned before, the safety profile is a set of the network security parameters, that determine the required network safety level. The profiles are generated on the criteria for the information security evaluation. [5,6] The functional criteria for the network security level

evaluation according to ISO 15408: "The common criteria for information technology security evaluation" are the next: FAU:security audit, FCO: communication, FCS:cryptographic support, FDP:user data protection, FIA:identification and authentication, FMT: security management, FPR:privacy, FPT:protection of the TSF, FRU:resource utilization, FTA:TOE access, FTP: trusted path/channels. [7]

Besides the functional criteria, the standard ISO 15408 also defines the criteria for the safety guarantee, that allow to evaluate a correctness of the safety services realization, such as: ACM:configuration management, ADO:delivery and operation, ADV: development, AGD: guidance documents, ALC: life cycle support, ATE: tests, AVA: vulnerability assessment.

Thus, the criteria for the network safety evaluation are the set of quantitative and qualitative requirements to the security mechanisms.

The adaptive network safety control mechanism can be effectively realized only on the complete information on the security system parameters. [8,9,10] Thus, the realization of the adaptive network safety control requires to take into consideration not only quantitative, but also qualitative criteria for the network safety.

According to the above mentioned requirements, we suggest to use the theory of fuzzy logic and fuzzy sets for the adaptive network safety control mechanisms realization.

The algorithm for the adaptive network safety control on the fuzzy logic

Nowadays, there are no any discrete algorithms that operate simultaneously with qualitative and quantitative parameters to receive the determined result. The functional (qualitative) criteria for the network security level evaluation can not be adequately formalized without the fuzzy logic approach. The fuzzy logic theory allows formalize the decisions support even in the non-uniform multi-dimensional environment. [11]

The description of the networks safety parameters using the fuzzy logic theory allows effectively to formalize and to analyze not only quantitative, but also the qualitative safety network parameters by representation them as $\forall x \in X \quad A = \{x, \mu_A(x)\}$, where $\{x, \mu_A(x)\}$ is pair of components (singleton), that consists from an element x and its proximity degree $\mu_A(x)$ to set X. [12,13]

We suggest to use the linguistic variables for the functional criteria formalization for the network security level evaluation. Generally, the linguistic variable can be characterized by a set of components: $<x, T, D>$ where x is the name of linguistic variable, T - its term-set or set of its possible values, D - the range of these values. [14]

The concept of the network control mechanism design on the fuzzy logic based on the synthesis of the experiments planning theory and the fuzzy sets theory.

The functional criteria for the network security level evaluation (for example, knowledge and experience of the experts) are formalized as polynomial:

$$Y = \beta_0 + \sum_{i=1}^{n} \beta_i X_i + \sum_{u,j=1}^{n} \beta_{ju} X_j X_u, \qquad (1)$$

where Y – the depended linguistic variable, β_i – right fuzzy coefficient, X- the name of linguistic variable, $j \neq u$.

The productive rules for the network security level evaluation on the functional criteria are in the implicative form "If …, then …, else… ", and the set of productive rules forms an orthogonal 2^n-matrix, where n is factors dimension.

We suggest the algorithm for design of the prognostic model for the adaptive network safety control mechanism on the safety functional requirements formalization in the multi-dimensional space.

The suggested algorithm is realized in the following steps:

1. The factors determination for the network safety control mechanisms.
2. The opposite scale and the terms for each factors delimitation.
3. The generation of the matrix with the functional criteria for the network security level evaluation.

4. The generation of the linguistic variables for the formalization of the qualitative information on the network safety.
5. The forming of factors polynomial for the functional criteria formalization on the network safety:

$$Y = \beta_0 + \sum_{i=1}^{n} \beta_i X_i + \sum_{u,j=1}^{n} \beta_{ju} X_j X_u, \qquad (2)$$

where $j \neq u$.
6. The analysis of the errors in the network safety control mechanism functioning.
7. The evaluation of the weights of the polynomial coefficients for the functional safety parameters formalization.
8. The adequacy analysis of the formed polynomial to the adaptive network safety control system.
9. The adequacy analysis of the formed model for the network safety control mechanism.
10. The accuracy analysis of the formed model by the Fisher's criterion:

$$F_{crit} = S_r^2 / S_b^2 < F_{table} \qquad (3)$$

Thus, we suggest the approach to design of the network safety control mechanism model on the synthesis of the experiments planning theory and the fuzzy sets theory, and also on the formalization of the functional requirements to the network safety.
The decisions on the network safety control are generating using the prognostic model of the adaptive network safety control mechanisms and the results of the precise solutions of the fuzzy equations.
According to Zadeh's expansion principle the fuzzy number X is the solution of the fuzzy equation $F(X, A_1, \ldots, A_n) \subseteq B$, if $\forall t$:

$$F^{-1}(t) = \varnothing,$$

$$\mu_F(t) = \sup_{F(X,A_1,\ldots,A_n)=t} \min \left[\mu_X(x), \mu_A(a1), \ldots \mu_A(an)\right], \qquad (4)$$

where $F(X, A_1, \ldots, A_n)$ - the value of the fuzzy function from the fuzzy arguments, $A_1, \ldots, A_n$, B - known fuzzy arguments, X - unknown fuzzy arguments, $\mu_F(t)$ – the proximity degree of X to set of arguments B.

The value of fuzzy function $F(X_1, X_2, \ldots, X_n)$ from the fuzzy arguments $X_1, X_2, \ldots, X_n$ is the fuzzy set with proximity degree function $\mu_F(t)$:

$$\mu_F(t) = \begin{cases} \sup \min \left[\mu_X(x), \mu_A(a1), \ldots, \mu_A(an)\right] \\ F(X_1, \ldots, X_r) = t \\ F(t)^{-1} = \varnothing \end{cases}. \qquad (5)$$

The analysis of the network security mechanisms parameters

We have performed the parameters analysis of the network security mechanisms of two types: first type is security mechanisms with the fixed security level, second type is security mechanisms based on the adaptive safety control approach. The results of this analysis are shown on Fig.2. and Fig.3.
Fig.2 shows, that the network security level in the security mechanism of the first type remains constant for the all period, and for the safety guarantee of the processing data this level should be maximum high (100%). As a consequence, the amount of computational operations for the data security, which depends on the network security level, also is on the maximal values constantly. (Fig. 3)
The network security level in the security mechanisms of the second type (on the adaptive safety control approach) is changed depending on the required safety level for the data that are processing at the certain moment. So, it is rather frequently appears that the network security level is less than its the maximum possible value. In result, the amount of computational operations for the data security also is changed, and the average amount of the computational operations for data security is less than for the security mechanism of the first type (Fig. 3).
Thus, the performance of the user's data processing in computer networks with the information security systems based on the adaptive safety control mechanism is reduced less, than in the networks that use the usual information security mechanisms with the fixed security level. Therefore, the using of the suggested approach to the information security mechanism design is effective.

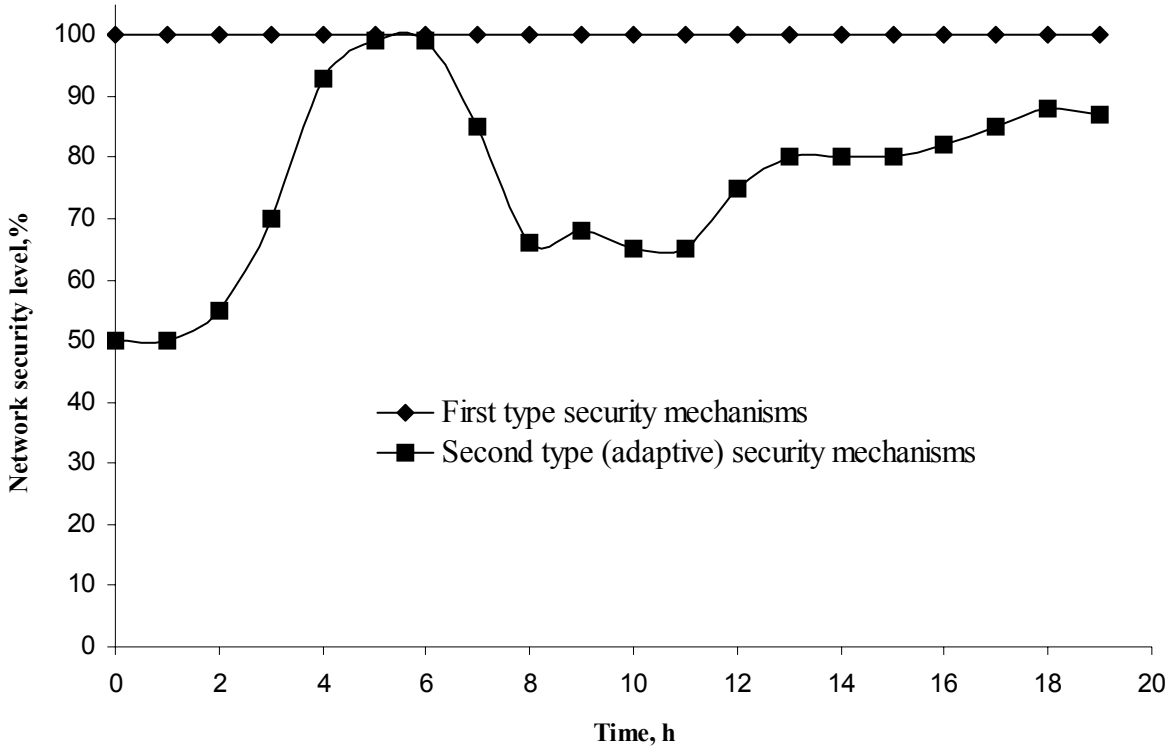

Figure 2. The network security level variation in the time for two types of the security mechanisms.

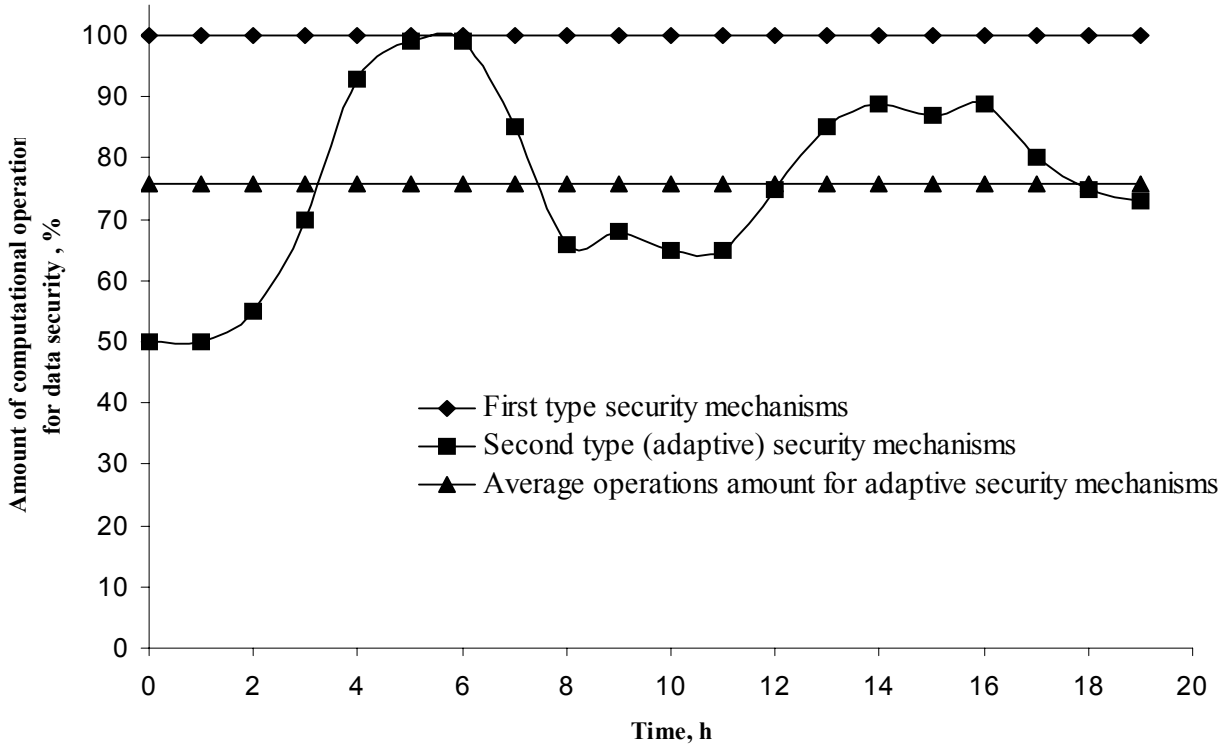

Figure 3. The variation in time of the computer operations amount for data security for two types of the security mechanisms

Conclusion

The realization of the network security mechanism on the adaptive safety control approach allows flexibly determine the network security level, required for the certain period. In result, the average losses of the network performance for the user's data processing, that are invoked by realization of the security mechanism, will be reduced. The efficiency of the network security system with the adaptive safety mechanism can be increased using the fuzzy logic. This approach allows, in particular, to formalize the functional criteria for the networks security level and to analyze the complete information on the network security parameters.

References

[1] Tolly K. (2002) *High-Speed Security*. The Tolly Group.

[2] Zhdanov A.A., Ryadovikov A.V. (2000) *Neuron Models in the Autonomous Adaptive Control Method*//Optical Memory and Neural Network, Vol. 9, No 2, - pp. 115-132.

[3] *Guide for Production of Protection Profiles and Security Targets*. (2000) ISO/JTC1/ SC27/N2449. DRAFT v0.9.

[4] *Controlled Access Protection Profile.* (1999) Version 1.d. U.S. Information Systems Security Organization. U.S. National Security Agency.

[5] Lee A. (2001) *Certificate Issuing and Management Components Family of Protection Profiles*. Version 1.0. U.S. National Security Agency, October 31.

[6] *Evaluation Methodology for the Common Criteria for Information Technology Security Evaluation*. (2002) version 1.1a, 19 April .

[7] Standard ISO 15408: *"The common criteria for information technology security evaluation"*. ISO Standards Bookshop.

[8] *Information technology — Security techniques — Protection Profile registration procedures*. (2001) ISO/IEC 15292:2001.

[9] Stoneburner G. (2001) *CSPP-OS - COTS Security Protection Profile - Operating Systems*. Draft Version 0.4. -- U.S. Department of Commerce, NIST, February 5.

[10] Sheridan M., Sohmer E., Varnum R. (2000) *A Goal VPN Protection Profile For Protecting Sensitive Information. Release 2.0.* // U.S. National Security Agency, 10 July.

[11]. Babuska, R. (1998) *Fuzzy Modeling for Control*. Boston: "Kluwer Academic Publishers" – 215 p.

[12] Rotshtein A., and Katefnikov D. (1998). *Identification of Non-Linear Objects by Fuzzy Knowledge Bases*.// Cybernetics and System Analysis, N 5 (34). – pp. 67 -78.

[13] Negnevitsky M. (2002) *Artificial intelligence: a guide to intelligent systems*. Addison-Wesley, NY. – 325 p.

[14] Nesteruk G. Ph., and Kupriyanov M. C. (2003) *Neural-fuzzy systems with fuzzy links* // Proc. of the VI-th Int. Conference SCM'2003. – St.-Petersburg, v.1. - pp. 341-344