APPLIED PROBLEMS OF MATHEMATICS AND MECHANICS

ALGULIEV R.M., SHIKHALIEV R.H.

NEURAL-NETWORK MODELING OF FIREWALL FUNCTIONING PROCESS FOR DETECTION OF THREATS

Abstract

The big part of modern methods on detection of threats is based on expert systems, which allow to identify known attacks. However, these methods are less successful at definition of attacks distinguished from expected patterns. Artificial neural network the large opportunities for identification of unknown attacks give at presence of the limited and incomplete data. In given clause doing one of two-step procedure of identification and authentication, which used analytical opportunities of neural networks.

Introduction

An issue of modern computer systems protection has been one of the major concerns aroused sharply over the recent years. Just one single attack on computer network can result in loss of information, either unauthorized use of network resources or massive change of big amounts of data. This makes users to set a question of efficiency of information protection systems on network. Timely and accurate detection of attacks on computers or computer systems will always remain major purpose for system administrators and researchers in the field of information security. The creations of individual hackers, wide range of hardware and operating systems in use, and constantly changing nature of threats for systems targeted for attacks are adding problems to the process of effective identification of attacks. Growing use of distributed computer networks and unprotected networks like Internet considerably increased the need for detection of attacks [1]. In this article we present an approach to the process of attack detection, which uses analytical capabilities of neural-networks using educating algorithm with return distribution.

Systems of attacks detection

There are a big number of methods of reaction to attacks on networks, but all of them require accuracy and timely identification of attack. The monitoring of unusual activity of the user is one of the ways of detection of unauthorized actions. There are two well-known categories of attacks, the attacks detection technologies try to detect, anomalies and misuse [2]. The misuse includes known attacks, which use known weak points of the systems. The anomalies mean any unusual activity, which can indicate the attack. If the observable actions of user do not correspond to expected mode of operation, then it can be said that the anomaly exist. The detection of misuse is a process, during which the attacks on networks are identified through comparison of the current activity with actions expected on the part of malefactor [3].

The majority of the modern approaches to the process of attacks detection use some form of analysis based on rules. The analysis based on rules rests on a set of certain rules determined beforehand, and introduced either by the network administrator or created automatically by the system or both these options are used together. The use of expert systems represents the most widespread approach in rule-based attack detection [4]. However these methods are less efficient in identification of attacks other than

expected patterns, and they are very difficult to build. The detection of misuse can be effective enough for those attacks, which have been programmed into detection system. However it is impossible to prevent all kinds of attacks, which may take place, and attempts to implement this are very hard to materialize. The detection of anomalies of any type is extremely important. The only problem in detection of anomalies is, probably, the big number of false alarms of danger. Unusual, but authorized use sometimes can also be classified as abnormal. Artificial neural networks represent potential for identification and classification of network activity on the basis of limited, incomplete and nonlinear sources of the data.

About artificial neural network

Artificial neural network consists of a set of elementary units, which are interconnected with each other and transform a set of the input data into a set of the desirable output data. The result of transformation is determined by characteristics of units and weights reflecting interrelations between them. By modification of interconnections between units on a network, it is possible to adapt for desirable output results [5,6]. Unlike expert systems, which can provide the user with the certain answer, irrespective of whether characteristics being considered correspond to characteristics incorporated into rules database, the neural networks can analyze the information and provide an opportunity for estimates of whether the data correspond to characteristics, this network is taught to recognize. While the degree of conformity of neural networks representation can reach 100 %, the authenticity of a choice completely depends on system's qualities in the analysis of patterns of the tasks submitted, i.e. on learning. Originally, neural networks are taught correct identification, through presenting to it patterns selected preliminary from subject domain. The reactions of neural networks are analyzed and system is adjusted in a way that allows reaching satisfactory results. In addition to the initial period of learning, neural networks also gains and accumulates experience with time, as it analyses the data from subject domain.

Neural networks based attacks detection systems

Relatively small amount of research on application of neural networks for attacks detection has been carried out to date. Artificial neural networks carry potential for solution of a big number of problems actually tried to be resolved through other modern approaches to attack detection. Artificial neural networks have been proposed as alternative to components of the statistical analysis of anomalies detection systems [7]. The statistical analysis includes statistical comparison of the current events with the predetermined set of reference criteria. This method is most frequently used for detection of deviations from typical mode of operation and identifies events similar to those signaling about attack [8]. Neural networks have been especially proposed to identify typical characteristics of system's users and to statistically identify deviations from users' established mode of operation. Artificial neural networks are also proposed for use in detection of computer viruses [5].

One of the advantages of neural networks usage in detection of misuse is the flexibility, which these networks provide. Neural networks are capable of analyzing data received from a network, even if these data are incomplete or distorted, and providing opportunity to carry out the analysis of these data in a nonlinear mode. Moreover, capability of processing data from a big number of sources in a nonlinear mode is especially important, as some attacks, coordinated by a number of hackers, can be carried

out against a network. As the protection system of computing resources requires timely and quick identification of attacks, the speed of processing in neural networks can be sufficient for reacting to attacks in real time mode before network suffers irrecoverable damage, which is another one advantage of this approach. It is typical that the output data of neural networks are expressed in the form of probability, neural networks gives an opportunity of forecasting of the further misuse. The neural network based system of misuse detection identifies probability indicating that some event, or series of events signal that an attack is being carried out against the system. As neural networks gains "experience", it improves its ability to determine which of these events has attributes of attack. Then this information can be used for generation of a series of events, which should have been activated, if attempt of attack really took place. Tracing down consecutive location of these events, the system is capable of improving the analysis of events and implement protective measures before the attack is successful. However, the most important advantage of neural networks in misuse detection is their ability to "study" characteristics of deliberate attacks and identify elements, which are not similar to those observed on a network before. Neural networks can be "taught" to recognize known suspicious events with high degree of accuracy. The probability of attack against the system can be assessed and potential threat outlined, irrespective of whether this probability exceeds the threshold established.

The reason for which neural networks have not been applied earlier in tasks of misuse detection was connected to requirements for neural networks teaching, as the ability of artificial neural networks to identify attacks completely depends on teaching system accuracy, i.e. on a teaching method used and number of teaching samples. The degree of training requires a big volume of data to make sure that results are statistically meaningful. The neural networks teaching with aim of misuse detection may probably require carrying out of thousand individual attacks, but it is difficult to obtain such volume of information.

Neural solution for users identification

It's known, that when passing two-stage authenticity identification procedure, first, the authorized users enter their user names and, if the user names coincide with names available in users' authenticity identification database (first stage), then the users are offered to enter their passwords for firewall screens. If the passwords are entered correctly, then users are given an access to protected corporate network resources [9].

Let's assume, that malefactor after having obtained the user name in some way, for example, through social engineering (by gathering data about users' and their close relatives), through various selection strategies (dictionaries, exhaustive search etc.), and application of powerful adjusted software for generation of huge quantity of combinations of symbols has identified correct password [9]. Even in this case, the neural network solution we propose will not allow the malefactor to access protected network resources.

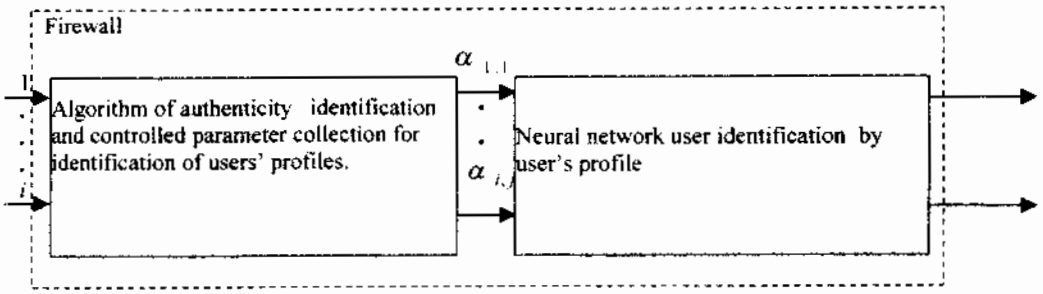
Consider the block diagram of user identification model implemented in firewall (fig.1). It is supposed that the user leaves "imprints" (user profile) when logging in system (authenticity identification) and neural networks are used for examining these imprints with aim of authorized users' identification. If the mode of user's behavior does not match the imprints, this user is not allowed to access protected network resources and system administrator is alerted about attack.

Assume, that all user names are numbered by whole numbers i (i=1,2,3...) and users are given j (j= 1,2,3...) sessions to pass through two-step authenticity identification procedure during time T_0. $T_{i,j}$ is the real time of stay of user i in a session j.

$\alpha_{i,j}$ is a controlled parameter for i user's profile identification in a session j determined by the relation:

$$\alpha_{i,j} = \frac{T_{i,j}}{T_0}.$$

As seen from this relation, $\alpha_{i,j}$ is determined in an interval [0,1], i.e. $\alpha_{i,j} \in [0,1]$.



Output 1 - "authorized user";
Output 2 - "unauthorized user".

Fig.1. Block diagram of user identification model in firewall

So, our task consists of finding distribution pattern for $\alpha_{i,j}$ for every i authorized user in an interval [0,1], i.e. identification of model of authorized activity of authorized user in passing two-stage authenticity identification procedure. For this purpose it is necessary to collect $\alpha_{i,j}$ for authorized users during some time T (few hours or few days) and through calculation of mathematical expectations and dispersions to get sample of teaching patterns for teaching neural network. It is extremely important, when calculating, to exclude bad samples or abnormal dropouts from teaching sample. Based on sample obtained, teaching of neural network on authorized users' identification is conducted on the basis of $\alpha_{i,j}$ distribution on interval [0,1].

For users' profile identification, we propose an algorithm for realization in firewall, which describes authenticity identification and users' profile controlled parameter collection procedure during time T (fig. 2). T_0 is the confidential time allocated to each user to enter the system and regulated by firewall. User's behavior during passing two-stage authenticity identification procedure during time T_0 is considered by this algorithm and the reading of user's profile controlled parameter $\alpha_{i,j}$ is carried out.

Taking into account said above, assume that user's identification model implemented in firewall uses neural network, when functioning, to identify the user by distribution $\alpha_{i,j}$ on interval [0,1]. If neural network identifies the difference between new and authorized users' profiles, then the output 2 (fig.1) or otherwise output1 are activated (fig.1). So the malefactor passing through two-stage authenticity identification procedure will be denied an access to protected resources of CN.

Conclusion

The detection of attacks is a difficult problem because of huge amount of vulnerability present in computer systems, constantly changing nature of threats and growing use of distributed network systems and unprotected networks, such as Internet. Neural networks

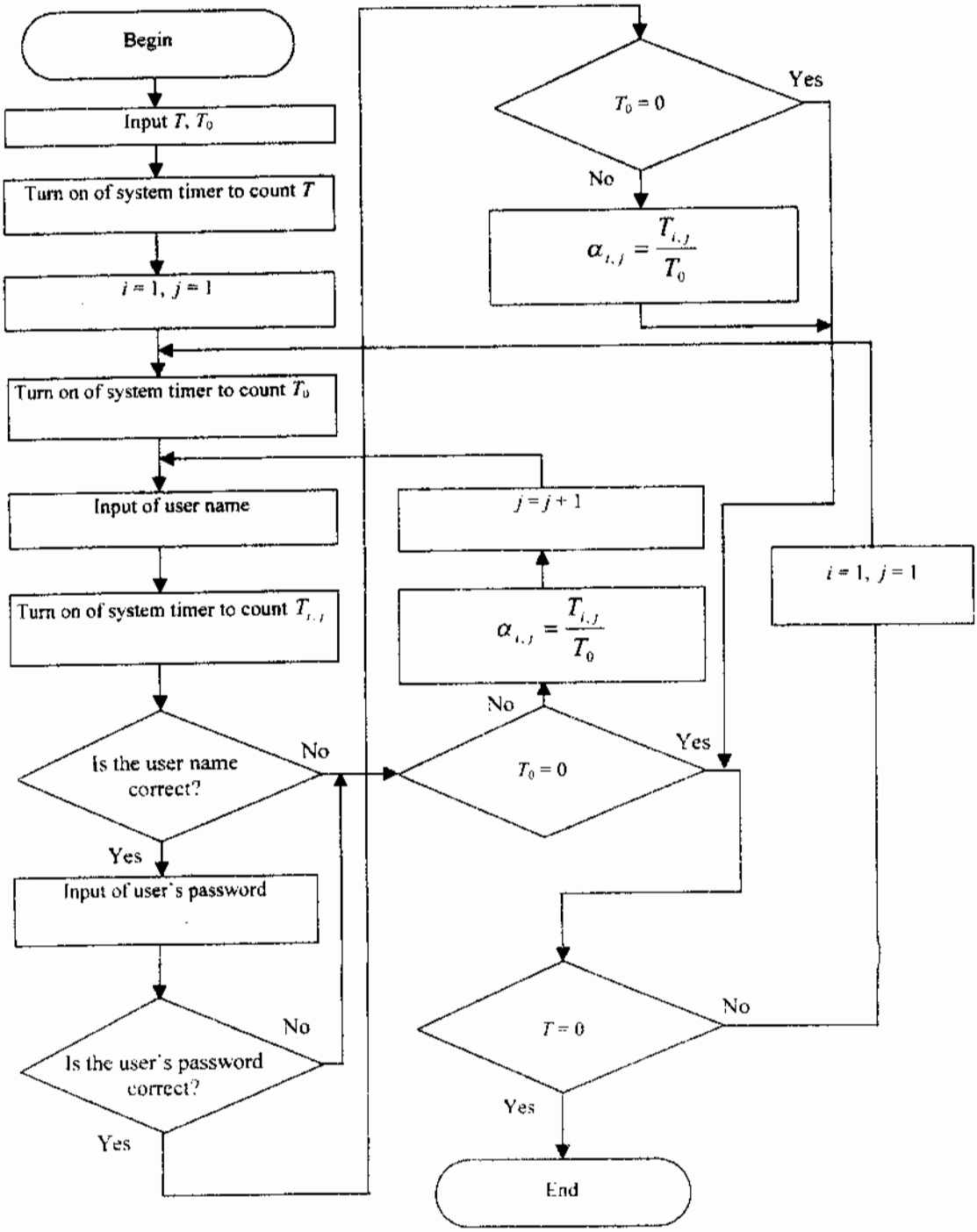


Fig. 2. Algorithm of authenticity identification and collecting of controlled parameter to identify user profile

have certain advantages in detection of known and unknown attacks, rather than classical expert systems. We believe that two-stage users authenticity identification model implemented in firewalls and based on use of neural networks that we proposed in this

Article can resolve the problem of attack detection for protected resources of CN. To reveal analytical characteristics of this model through testing, it is fit for purpose to construct imitating model.

References

[1]. Mukherjee, B., Heberlein, L.T., Levitt, K.N. (May/June, 1994). Network Intrusion Detection. IEEE Network. pp. 28-42.

[2]. Helman, P., Liepins, G., and Richards, W. (1992). *Foundations of Intrusion Detection. In Proceedings of the Fifth Computer Security Foundations Workshop,* pp. 114-120.

[3]. Kumar, S. and Spafford, E. (1994) *A Pattern Matching Model for Misuse Intrusion Detection.* In Proceedings of the 17th National Computer Security Conference, pp. 11-21.

[4]. Denning, D. E. (February, 1987). *An Intrusion-Detection Model.* IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp. 222-232.

[5]. Fox, K. L., Henning, R. R., Reed, J. H., and Simonian, R. (1990). *A neural network approach towards intrusion detection.* In Proceedings of the 13th National Computer Security Conference, pp. 125-134.

[6]. Hammerstrom, Dan. (June, 1993). *Neural Networks At Work.* IEEE Spectrum. pp. 26-53.

[7]. Debar, H., Becker, M., and Siboni, D. (1992). *A neural network component for an intrusion detection system.* In Proceedings of the 1992 IEEE Computer Society Symposium on Research in Computer Security and Privacy, pp. 240-250.

[8]. Helman, P. and Liepins, G., (1993). *Statistical foundations of audit trail analysis for the detection of computer misuse.* IEEE Trans. on Software Engineering, 19 (9), pp. 886-901.

[9]. Alguliev R.M.. *About one algorithm of detection of threat at access in corporate network.* Of News of AS of Azerbaijan. Ser physical - technical and mathematical sciences, 1998, № 6, pp. 213 - 216.

[10]. Gorban A.N. *Training of neural networks.* M.: JV Paragraph, 1990, 156 p.

Alguliev R.M., Shikhaliev R.H.
Information-Telecommunication Scientific Center of AS Azerbaijan.
9, F.Agayev str., 370141, Baku, Azerbaijan.

Received November 13, 2000; Revised January 19, 2001.
Translated by authors.