UDC 004.8.032.2
DOI https://doi.org/10.15589/znp2024.4(497).21

NEURAL NETWORK MODELING OF SCHEMES FOR RECOGNIZING THE FACT AND TYPE OF UNAUTHORIZED INTRUSION INTO A USER'S COMPUTER NETWORK

НЕЙРОМЕРЕЖЕВЕ МОДЕЛЮВАННЯ СХЕМ РОЗПІЗНАВАННЯ ФАКТУ ТА ТИПУ НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЯ В КОРИСТУВАЦЬКУ КОМП'ЮТЕРНУ МЕРЕЖУ

Serhii P. Aloshyn
aleshsp@ukr.net
ORCID: 0009-0002-4239-4194

С. П. Альошин,
канд. техн. наук, доцент

National University "Yuri Kondratyuk Poltava Polytechnic", Poltava
Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава

Abstract. The recognition of the unauthorized intrusion into a user's computer network produces certain difficulties associated with a high degree of uncertainty. This is due to the similarity of infection symptoms with typical software failures of computer networks. In order to ensure high productivity and efficiency of detection of the type of intrusion into the user's computer network, the technology of synthesis of neural network models with forced training on a retrospective sample of real-world examples from practice is proposed. At the synthesis of an ensemble of recognition models, a neural network approach to the analysis of the state of the computer network is selected, based on the practical implementation of the Kolmogorov-Arnold theorem regarding the representation of a function of several arguments by the sum of compositions of functions of one variable. The modification of the synaptic set of the neural network is implemented through the application of the conjugate gradients method of the error backpropagation algorithm. The experimental results have demonstrated stable convergence of the learning process to minimal errors on the training and test sets of initial data. The practical significance of the research results lies in the creation of software tools for operational decision support in determining the fact of intrusion into the network and assessing the type of malware in order to take measures to minimize the probable damage. The developed technology, methodology, algorithms and software tools allow for supplement the capabilities of existing network protection programs to detect the fact and type of possible malware intrusions and are implemented as an independent application in the main code of a standard technical data analysis package. This approach ensures reliability of detection and efficiency of decision-making on protection of the user's network. The validity of the result is achieved by the training the model on a representative sample of retrospective precedents from the existing database.
Key words: Computer Network; Intrusion; Neural Network; Conjugate Gradients Method; Error Backpropagation Algorithm.

Анотація. Розпізнавання факту несанкціонованого проникнення в призначену для користувача комп'ютерну мережу становить певні труднощі, пов'язані з високим ступенем невизначеності, спричиненим схожістю симптомів зараження з типовими програмними збоями комп'ютерних мереж. Для забезпечення високої продуктивності та оперативності розпізнавання типу вторгнення в користувацьку комп'ютерну мережу запропоновано технологію синтезу нейромережевих моделей із примусовим навчанням на ретроспективній вибірці реальних прикладів із практики. Під час синтезу ансамблю моделей розпізнавання обрано нейромережевий підхід аналізу стану комп'ютерної мережі, що ґрунтується на практичній реалізації теореми Колмогорова-Арнольда щодо представлення функції кількох аргументів через суму композицій функцій однієї змінної. Модифікацію синаптичної множини нейромережі реалізовано методом спряжених градієнтів алгоритму зворотного поширення помилки. Експериментальні результати показали стійку збіжність процесу навчання до мінімальних помилок на навчальній і тестовій множинах вихідних даних. Практичне значення результатів дослідження полягає у створенні програмного інструментарію для оперативної підтримки ухвалення рішень з фіксації факту вторгнення в мережу та оцінювання типу шкідливої програми для вжиття заходів щодо мінімізації ймовірного збитку. Розроблена технологія, методичний, алгоритмічний і програмний інструментарій дають змогу доповнити можливості наявних програм захисту мереж щодо розпізнавання факту й типу можливих вторгнень

шкідливих програм і реалізується як самостійний додаток в основному коді стандартного пакета технічного аналізу даних. При цьому забезпечується надійність розпізнавання й оперативність ухвалення рішення щодо захисту користувацької мережі. Достовірність результату досягається навчанням моделі на репрезентативній вибірці ретроспективних прецедентів з наявної бази даних.
Ключові слова: комп'ютерна мережа; вторгнення; нейронна мережа; метод спряжених градієнтів; алгоритм зворотного поширення помилки.

TASK STATEMENT

The technology used to create modern viruses, Trojan programs, and computer "worms" allows for the concealment of malicious code within a system. Therefore, the application of modern antivirus software of the Internet Security class within a computer network is not always prompt or effective in neutralizing the vulnerabilities of the operating system or database. In such circumstances, it is very important to promptly recognize both the fact of unauthorized intrusion and the type of malicious software code in order to select the optimal countermeasure and preserve the functionality of the user's network.

The situation is complicated by the fact that the known characteristic features or symptoms of infection can be caused both by a number of factors, including the impact of malware and other software or hardware problems. In such cases, the recognition method based on the application of intelligent technologies, specifically on artificial neural networks in the environment of modern technical data analysis packages is believed to be a timely, useful, and effective solution.

The indicators of unauthorized intrusion are well-known today [1]. The most commonly observed examples can be enumerated as follows:

– The computer behaves strangely, unusually;

– Unexpected messages or images appear on the screen;

– Unexpected sounds are heard, which are played in a random order;

– Programs start unexpectedly without the user's explicit command;

– A network screen reports that an application is trying to connect to the Internet, even though the user has not started the program;

– Subscribers receive e-mail messages that that were not sent by the operator;

– The computer frequently freezes or programs suddenly run slower;

– The operator receives multiple system error messages;

– The operating system fails to load when the computer is powered on.

– Files or folders are absent or changed;

– The hard disk access light is on even though no programs have been initiated by the operator, etc.

Modern software platforms (MATLAB, Statistica, etc.) provide the functionality to design a neural network environment and apply an ensemble of known neural network architectures of different complexity and forced learning rules using listed features [2].

ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

The prospective directions of traffic analysis and intrusion detection based on neural networks are analyzed in [1]. The researches of this issue mainly focus on the application of different neural network architectures [2, 3].

One of the popular techniques is the use of deep learning for network anomaly detection [4–6]. Paper [7] investigates convolutional neural networks (CNN) for analysis of network data and detection of anomalous patterns to effectively recognize intrusions, determines benefits and disadvantages of using CNN. Al-Jarrah O. and Arafat A. proposed Intrusion detection system based on neural network classification of attack behavior [8].

The considerable attention is paid to the formalization of the subject area, mathematical model of the network. Paper [9] examines mathematical model and structure of a neural network for detection of intrusion.

A lot of studies also focus on the problems of data collection and data preparation for neural network analysis, collection and detection of features of the intrusion [10, 11].

Therefore, current research in the field of neural networks for intrusion recognition is actively developing and covers a wide range of techniques and approaches, which contributes to the development of secure computer systems.

SEPARATION OF PREVIOUSLY UNRESOLVED PARTS OF THE OVERALL PROBLEM

The unresolved part of the overall problem is the formalization of features of intrusion into the user's computer network, formal mapping of the space of features and the state space of the network according to the given conditions (efficiency, reliability, accuracy), and the use of modern software platforms for the construction of an ensemble of neural network models in order to determine the fact of intrusion into the network and its type.

PURPOSE OF THE STUDY

The purpose of the research is to increase the productivity of technical tools for identifying and categorizing network intrusions, in order to automate the process of analysis, reduce the number of incorrect decisions, shorten the reaction time in decision making, and minimize possible losses.

The developed technology is represented as an ensemble of neural network models for intrusion recognition, integrated into the main code of the existing technical analysis package as software applications.

METHODS, OBJECT, SUBJECT AND METHODS OF RESEARCH

Methods. Observation, measurement, analysis and synthesis, neural networking.

Object of the study is neural network models for intrusion recognition.

Subject of the study is development of the the neural network models for intrusion recognition, integrated into the main code of the existing technical analysis package as software applications.

THE MAIN MATERIAL

The search for analytical relations of intrusion signs with the type and nature of penetration into the network is expedient to present a formal mapping of the space of signs to the space of network states with specified conditions (efficiency, reliability, accuracy):

$$F: X \to Y_{opt},\ X \subset \Re^m,\ Y_{opt} \subset \Re, \qquad (1)$$

where X is vector of user network state features;

Y_{opt} is output value of the network status class number (intrusion type).

The formalization of the problem of recognizing classes of network states in the space of fixed features is expressed as follows:

$$s \in S, S \qquad (2)$$

where P(*S*, *X*) is decisive rule for recognizing classes S in the feature space X;

$s \in S, S$ is set of recognizable classes (states) of the computer network;

$x \in X, X$ is set of input signs of network intrusions;

δ is model adequacy;

δ_0 is acceptable model training error.

The set of input factors $X^n = \{x_1, x_2, ..., x_n\} \subset X$ with the class alphabet provides the realization of the rule of pattern recognition [12]:

$$\omega_g \in \Omega_k, \ \text{ if } L(\omega, \{\omega_g\}) = \sup_i L(\omega, \{\omega_i\}) \qquad (3)$$
$$L(\omega, \{\omega_g\}) \to \omega_g \in \Omega_k,$$

where $\overline{X} = (x_1, ..., x_n) \in X$ is set of input factors;

$L(\omega, \{\omega_g\})$ is a rule for assigning of an object ω_g to the appropriate class.

The main task of analysis is to evaluate the fact, internal structure, character and type of intrusion into the network, so it is reasonable to formalize the problem of detection in the space of fixed features to the level of analytical solving rule.

Let there be a list of factors for several types of intrusions W, where $W = (\omega_g),\ g \in \overline{I} = \{1, 2, ..., I_m\}$ and their belonging to some classes $\Omega_p, \Omega_g = \{1, 2, ..., J_i\}$ is fixed. When objects come to the analysis, the task of assigning them to one or another class is solved with some errors and time consumption. If the constraints have not been taken into account, the whole set of features can be used regardless of their information capabilities. Otherwise, recognition algorithms should include time $(t < T_0)$ and material $(s < S_0)$ constraints, where T_0 and S_0, respectively, allowable time and material resources for the implementation of software and tools in the task of recognizing the fact and type of intrusion into the network.

Given the acceptable risks, the problem formulation in the form of (2) can be expressed as (4), where the productivity of the solution depends on specific acceptable risks (damages) in the decision making:

$$\begin{aligned} &SupK_E(S, P, X, T_k) \\ &\Re u(\Delta T) \le A_0 \\ &\Re u(\delta) \le B_0 \end{aligned} \qquad (4)$$

where $s \in S, S$ is a set of current states of the user network;

$p \in P, P$ is set of forecasts of the dynamics of the network states;

$x \in X, X$ is set of input factors;

$T_k, k \in \{0, 1, 2, ...\}$ is decision-making moments;

K_E is decision efficiency criterion;

$\Delta T, \delta$ is decision time interval and current degree of model adequacy, respectively;

$\Re u(\Delta T)$ is expected damage from delayed decision making;

$\Re u(\delta)$ is expected damage from the model inadequacy;

A_0 is acceptable damage from the decision made at the boundary of the time interval;

B_0 is acceptable damage from errors on the test set of precedents.

The type of decisive rule to be adopted depends on the trade-off between efficiency and risk, taking into account the characteristics of the considered subject area.

Approximation of the state function of the computer network in the intrusion feature space

The productive use of the neural network approach to analyze the state of a computer network is based on the Kolmogorov-Arnold theorem on the representation of a function of several arguments by the sum of compositions of the functions of one variable and its adaptation to the Hecht-Nielsen neural network format:

$$y(x) = \alpha \sum_{i=1}^{H} v_i \left(w_{i1} x_1 + w_{i2} x_2 + ... + w_{in} x_n + u_i \right), \qquad (5)$$

where *H* is dimension of training sample;

are neural network parameters;

n is number of neurons;

$w_{i1}, w_{i2}, ..., w_{in}$ are weight coefficients of neurons.

It can be stated that there is such a set of numbers H, n, α, v_i, u_i, at which the function is approximated by the series over the whole area of its definition and can be realized by a three-layer neural network with any predetermined error. This fundamental position is the basis of all subsequent procedures, because if it is possible to establish a deterministic analytical connection of the whole set of signs of network intrusion with the type (class) of this intrusion, then

all subsequent options are derived from this system-forming procedure.

The main task of the analysis is to evaluate the fact, internal structure of the character and type of intrusion into the network, therefore it is reasonable to formalize the task of recognition in the space of fixed signs consistently to the level of analytical decisive rule.

Instrumentally, this problem is solved in the paradigm of the gradient methods of error backpropagation. The adequacy of neural network models is determined by the productivity, errors on training, control and test sets when training on a representative sample of examples, allows us to assert the validity of decisions made based on the results of modeling.

In this case, the presence or absence of intrusion signs is recorded in nominal or digital terms and fed to the input of the synthesized neural network, designed in the package of the selected neuroemulator.

The modification of the synaptic set of the neural network is based on the enumeration of all possible combinations of synapse weights using the error backpropagation algorithm [13]:

$$w_{qh}^{(n)}(t) = w_q(t-1) + \Delta w_h^{(n)}(t), \qquad (6)$$

$$w_q(t-1) = w_q(t) + \alpha \cdot \frac{\partial E(k)}{\partial w_q(t)};$$

where w is an array of synaptic coefficients;

q is a number of neuron output in n-th layer;

h is a number of neuron input in n-th layer;

n is a network layer number.

The network will continue to learn until the condition is met:

$$\frac{1}{m}\sum_{j=1}^{n}\sum_{i=1}^{m}(y_j - d_j)^2 \Rightarrow \min(\ddot{a} \le \ddot{a}_0), \qquad (7)$$

where y_j is a current network state;

d_j is a learning result (response) of the network at the j-th output, at i-th example of training sample;

$j = 1,n$ is a network output number;

m,n is an example number;

m,n is dimension of the example array and the number of output elements of the network.

Thus, as a result of synthesis of the ensemble of models with forced learning on a representative sample of examples from the retrospective set of the database, the key analytical expressions describing the process of synthesis of models for recognition of the fact and type of unauthorized intrusion into the user's computer network are presented.

The experimental studies demonstrated a stable convergence of the learning process towards a minimum error rate (Fig. 1). In this case, the performance and accuracy levels that are acceptable for practice were experimentally achieved.

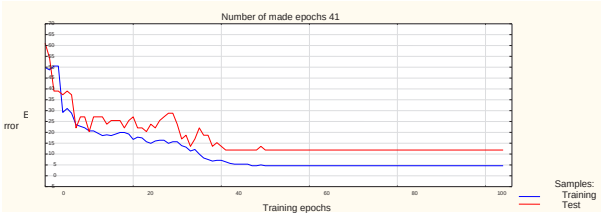

Fig. 1. Dynamics of the iterative process of weight coefficients modification with different initial training conditions

The task is solved on the platform of a standard technical data analysis package and does not require additional material and financial costs.

DISCUSSION OF THE RESULTS OBTAINED

The issue of detection of the type of unauthorized intrusion into a user's computer network has been formulated and solved through the application of intelligent technologies based on artificial neural networks, which have been developed within the environment of technical data analysis packages. This approach ensures reliability of detection and efficiency of decision-making on protection of the user's network. The validity of the result is achieved by the training the model on a representative sample of retrospective precedents from the existing database.

CONCLUSIONS

In order to automate the determination of the fact and type of unauthorized intrusion into the user's computer network, it is necessary to find the functional dependence of its state on the detected features. This task is solved by applying the technology of forced training of neural networks and implemented by circuit models of different architecture and complexity as a problem of class recognition.

The practical significance of the research results lies in the creation of software tools for operational decision support in determining the fact of intrusion into the network and assessing the type of malware in order to take measures to minimize the probable damage.

The developed technology, methodology, algorithms and software tools allow for supplement the capabilities of existing network protection programs to detect the fact and type of possible malware intrusions and are implemented as an independent application in the main code of a standard technical data analysis package.

REFERENCES

[1] Ilyenko, A., Ilyenko, S., Kravchuk, I., & Herasymenko, M. (2022). Prospective directions of traffic analysis and intrusion detection based on neural networks. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology*. № 1(17), С. 46–56. https://doi.org/10.28925/2663-4023.2022.17.4656.

[2] Karpinski, M., Shmatko, A., Yevseiev, S. et al. (2021). Detection of Intrusion Attacks using Neural Networks. *In proceedings of International Scientific and Practical Conference "Information Security and Information Technologies"*, Kharkiv – Odessa. Kharkiv, September 13– 19, Kharkiv. Pp. 117–124.

[3] Reddy Kesavulu E. (2013). Neural Networks for Intrusion Detection and its Applications. *In Proceedings of the World Congress on Engineering*, 2013. Vol II, WCE 2013, July 3–5, London, U.K,

[4] Maithem Mohammed, Al-sultany G.A. (2021). Network intrusion detection system using deep neural networks. ICMAICT 2020. *Journal of Physics: Conference Series* 1804 012138. Pp. 313–316. doi:10.1088/1742-6596/1804/1/012138

[5] Kim Jin, Shin Nara, Jo Seung, Kim Sang (2017). Method of intrusion detection using deep neural network. *IEEE*, 2017. Pp. 313–316.

[6] Shpinareva, I.M., Yakushina, A.A., & Rudnichenko, N.D. (2021). Detection and classification of network attacks using the deep neural network cascade. *Herald of Advanced Information Technology*, 2021, Vol.4 No. 3. Pp. 244–254.

[7] Mohammadpour, L. et al. (2018). A Convolutional Neural Network for Network Intrusion Detection System. *Proceedings of the Asia-Pacific Advanced Network*, Auckland, 5-8 August 2018, 2018. Pp. 50–55.

[8] Al-Jarrah, O. (2015). Network Intrusion Detection System Using Neural Network Classification of Attack Behavior. *Journal of Advances in Information Technology*. Vol. 6, No. 1, February, 2015. – 8 pp.

[9] Zahoruiko, L., Martianova, T., Al-Hiari, M. et al. (2024). Mathematical model and structure of a neural network for detection of cyber attacks on information and communication systems. *IAPGOS* (*"Informatics, Control, Measurement in Economy and Environmental Protection"*) . Vol. 3, 2024. Pp. 49–55.

[10] Mieshkov, V.I., & Virolainen, V.O. (2015). Analiz suchasnykh system vyiavlennia ta zapobihannia vtorhnen v informatsiino-telekomunikatsiinykh systemakh [Analysis of modern systems for detecting and preventing intrusions in information and telecommunication systems]. *Problems of information security in information and communication systems*. Dnipropetrovsk, 2015. Pp. 1–4 [in Ukrainian].

[11] Haidur, H.I., Hakhov, S.O., & Bryhynets, A.A. (2023). Vyiavlennia merezhevykh anomalii z vykorystanniam alhorytmiv neironnykh merezh [Detection of network anomalies using neural network algorithms]. *Telecommunications and information technologies*. No 1(78), 2023. Pp. 61–73 [in Ukrainian].

[12] Haykin, S. (2009). Neural Networks and Learning Machines. Prentice Hall, 2009. 906 pp.

[13] Aloshyn, S.P. (2018). Neural network basis for decision support in the space of factors and states of high dimension. Poltava: Skytech, 2018. – 208 pp.

[14] Shun, J., & Malki, H.A. (2008). Network Intrusion Detection System Using Neural Networks. *2008 Fourth International Conference on Natural Computation*, Jinan, China, 2008. Pp. 242-246, doi: 10.1109/ICNC.2008.900.

[15] Young, T., Nammous, M. K., & Saeed, K. (2019). Advanced Computing and Systems for Security. *Natural language processing: speaker, language, and gender identification with LSTM*. Berlin, Germany: Springer; 2019. Pp. 143–156.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Ilyenko, A., Ilyenko, S., Kravchuk, I., Herasymenko, M. (2022). Prospective directions of traffic analysis and intrusion detection based on neural networks. *Кібербезпека: освіта, наука, техніка*. № 1(17), С. 46–56. https://doi.org/10.28925/2663-4023.2022.17.4656

[2] Karpinski, M., Shmatko, A., Yevseiev, S. et al. (2021). Detection of Intrusion Attacks Using Neural Networks. *Міжнар. наук.-практ. конф. «Інформаційна безпека та інформаційні технології»*, Харків – Одеса, 13-19 вер. 2021 р. : матер. конф. Харків : ХНЕУ ім. С. Кузнеця, С. 117–124.

[3] Reddy Kesavulu E. (2013). Neural Networks for Intrusion Detection and its Applications. *In Proceedings of the World Congress on Engineering*, 2013. Vol II, WCE 2013, July 3–5, London, U.K.

[4] Maithem Mohammed, Al-sultany G.A. (2021). Network intrusion detection system using deep neural networks. ICMAICT 2020. *Journal of Physics: Conference Series* 1804 (2021) 012138, 2021. Pp. 313–316. doi:10.1088/1742-6596/1804/1/012138

[5] Kim Jin, Shin Nara, Jo Seung, Kim Sang (2017). Method of intrusion detection using deep neural network. *IEEE*, 2017. Pp. 313–316.

[6] Shpinareva, I.M., Yakushina, A.A., Rudnichenko, N.D. (2021). Detection and classification of network attacks using the deep neural network cascade. *Herald of Advanced Information Technology*, Vol.4 No.3. Pp. 244–254.

[7] Mohammadpour, L. et al. (2018). A Convolutional Neural Network for Network Intrusion Detection System. *Proceedings of the Asia-Pacific Advanced Network*, Auckland, 5-8 August 2018, Pp. 50–55.

[8] Al-Jarrah, O. (2015). Network Intrusion Detection System Using Neural Network Classification of Attack Behavior. *Journal of Advances in Information Technology*. Vol. 6, No. 1, February, 2015. – 8 pp.

[9] Zahoruiko, L., Martianova, T., Al-Hiari, M. et al. (2024). Mathematical model and structure of a neural network for detection of cyber attacks on information and communication systems. *IAPGOS* (*"Informatics, Control, Measurement in Economy and Environmental Protection"*) . Vol. 3, Pp. 49–55.

[10] Мєшков, В.І., & Віролайнен, В.О. (2015). Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. *Проблеми безпеки інформації в інформаційно-комунікаційних системах*. Дніпропетровськ, 2015. С. 1–4.

[11] Гайдур, Г. І., Гахов, С.О., & Бригинець, А. А. (2023). Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. *Телекомунікаційні та інформаційні технології*. No 1(78), 2023. С. 61–73.

[12] Haykin, S. (2009). Neural Networks and Learning Machines. Prentice Hall, 2009. 906 pp.

[13] Aloshyn, S.P. (2018). Neural network basis for decision support in the space of factors and states of high dimension. Poltava: Skytech, 2018. 208 pp.

[14] Shun, J., Malki, H.A. (2008). Network Intrusion Detection System Using Neural Networks. *2008 Fourth International Conference on Natural Computation*, Jinan, China. Pp. 242–246, doi: 10.1109/ICNC.2008.900.

[15] Young, T., Nammous, M. K., Saeed, K. (2019). Advanced Computing and Systems for Security. *Natural language processing: speaker, language, and gender identification with LSTM*. Berlin, Germany: Springer; 2019. Pp. 143–156.

Дата надходження статті до редакції: 16.11.2024
Дата затвердження статті до друку: 24.11.2024